Action Status Results

The following table defines the messages you will see in the Status column.

Status	Definition
Running	There are no pending commands for this module and it is communicating with the network server.
Link Lost	Manager/One has lost contact with this module for more than one minute.
Command Started	Manager/One is attempting to execute the command.
Command Sent Successfully	The command was received by the module.
Command Received	The module acknowledged that the command was received.
Command Executed Successfully	The command was executed on the module.
Command Not Sent	Manager/One failed to send the command to the module.
Command Sent	Manager/One sent the command but the module did not respond.
Command Failed	The module received the command but failed to execute the command.

Commands

Clicking on **Commands** in Manager/One's toolbar generates a pull-down menu containing all the commands that are available within the Manage function.

Load Firmware on Network

This command allows you to load a new firmware image to each of the modules contained in all network nodes within your Access/One Network. However, before you can load a new image, your FTP server parameters must be established correctly to let Manager/One know where to locate the new image (BIN) file.

To establish the correct FTP parameters and load new firmware at the network level, go to "Updating the Firmware" on page 35.

Reboot Network

This command reboots each module in all of the nodes within your Access/One Network. Rebooting is required when network-level configuration changes are made or a new firmware image is loaded.

To monitor the progress of the reboot operation, the network server generates the request in stages. When each module reports receiving the reboot command and successfully reboots, the network server performs a final self-reboot. You can monitor reboot progress reports with the View Action Status command.

Whenever you initiate the Reboot Network command, the system warns you that this action will affect multiple devices on the network and asks you to confirm the request. If you want to proceed, click on the **OK** button to initiate the reboot process, otherwise click on the **Cancel** button to abort the command.

See also, "Important Note About Rebooting" on page 4.

Update Node Names

This command must be executed at the node level. Go to "Update Node Names" on page 128.

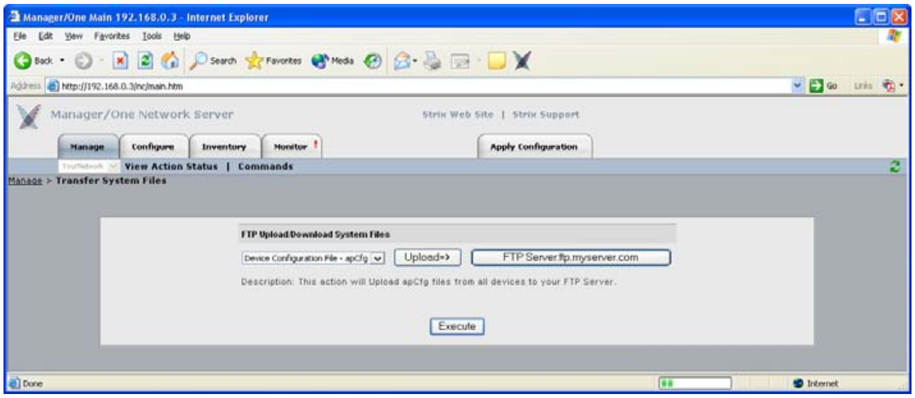
Update Network Membership

This command must be executed at the subnet level. Go to "Update Network Membership" on page 69.

Transfer System Files

This command allows you to transfer network (cloud) or device (module) configuration files between the network and your assigned FTP server. This is a useful tool if you want to backup or restore configuration files. However, before executing this command your FTP server parameters must be set up correctly using the Firmware Updates command.

When you choose the Transfer System Files command, Manager/One presents you with options to upload configuration files from their source on the network (either cloud or device) to your FTP server, or download configuration files from your FTP server to their source.



Manager/One Main 192.168.0.3 - Internet Explorer

Address http://192.168.0.3/nc/main.htm

Manager/One Network Server

Manage > Transfer System Files

FTP Upload Download System Files

Device Configuration File - apCfg

Description: This action will Upload apCfg files from all devices to your FTP Server.

Figure 52. Transferring System Files

Select either Device Configuration File or Cloud Configuration File from the pull-down list then click on the Download/Upload button to define the action you want to initiate.

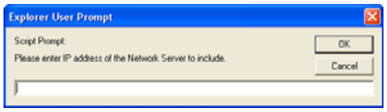
If you need to reset your FTP parameters, click on the **FTP Server:** button, otherwise click on the **Execute** button. When asked to confirm the action, click on the **OK** button to begin transferring files, or click on the **Cancel** button to abort the command.

Remote Network Server

This command allows to you include or exclude remote network servers.

Include

Choose this command to include a remote network server within your Access/One Network—a static network server must be specified in Network Topology before executing this command. When prompted, enter the IP address of the server you want to include then click on the **OK** button.


Explorer User Prompt

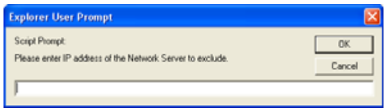
Script Prompt:

Please enter IP address of the Network Server to include.

Figure 53. Including Remote Servers

Exclude

Choose this command to exclude a remote network server from your Access/One Network—you can only exclude a server that is already included in your network. When prompted, enter the IP address of the server you want to exclude then click on the **OK** button.


Explorer User Prompt

Script Prompt:

Please enter IP address of the Network Server to exclude.

Figure 54. Excluding Remote Servers

The Configure Function

This function provides you with the tools you need to configure your Access/One Network at the network level and includes the following commands:

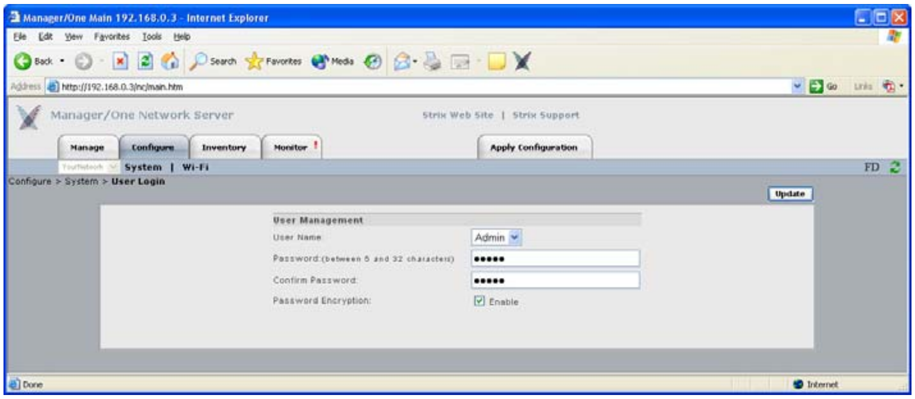
- System
    - User Login
    - Network Management
        - General
        - SNMP
        - Trusted IP Addresses
    - TCP/IP Settings
    - Network Topology
    - Priority/One - Class of Service
    - Radius Accounting
    - Syslog
    - Date and Time
    - Operating Environment
    - Firmware Updates
- Wi-Fi
    - Radio Parameters
    - Client Connect
    - Network Connect
    - Rogue Scan

System

This area of Manager/One contains the primary configuration commands for your Access/One Network in the system environment. Any commands executed here are automatically propagated across the network, so make sure the changes you initiate are changes that you want to apply to the entire network, otherwise go to “Managing Subnets and Nodes” on page 125 or “Managing Modules” on page 131.

User Login

This command displays the User Management window, allowing you to change the login password for users and enable/disable password encryption.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage Configure Inventory Monitor
Apply Configuration
System | Wi-Fi
FD
Configure > System > User Login
Update
Done Internet

User Management

User Name: Admin

Password:(between 5 and 32 characters) •••••

Confirm Password: •••••

Password Encryption: ☑ Enable

Figure 55. Managing User Logins

The following options are available with this command:

- **User Name**
  Choose a user name from the pull-down list. A valid user name is required to access the Web server interface within the network server module.

- **Password**
  Enter a meaningful password (between 5 and 32 characters) that you are likely to remember. The password is case-sensitive.

- **Confirm Password**
  Confirm your password here otherwise the system will reject it.

The default for the user name and the password is Admin (with a capitalized A) for both. We strongly recommend that you change the default password immediately after your initial login.

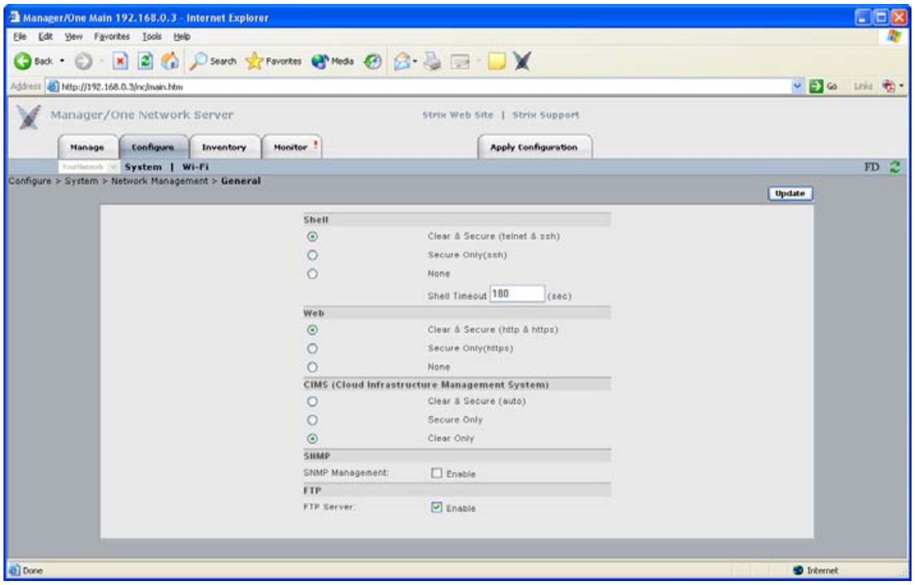
- **Password Encryption**
  Check this box if you want Access/One Network to encrypt your password for additional security.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Network Management

General

This command allows you to define the level of security for the various management interface options used to manage your Access/One Network, and provides options for enabling or disabling SNMP Management and FTP server functionality.



Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Done
Internet

Configure > System > Network Management > **General**

Shell
● Clear & Secure (telnet & ssh)
○ Secure Only(ssh)
○ None
Shell Timeout 180 (sec)

Web
● Clear & Secure (http & https)
○ Secure Only(https)
○ None

CIMS (Cloud Infrastructure Management System)
○ Clear & Secure (auto)
○ Secure Only
● Clear Only

SNMP
SNMP Management: □ Enable

FTP
FTP Server: ☑ Enable

Figure 56. General Management Interface Security

The following options are available with this command:

- **Shell**

  Choose **Clear & Secure** to allow network management via an unsecured Telnet connection and a Secure SHell (SSH) connection, or choose **Secure Only** to restrict management to an SSH connection only. Alternatively, you can choose **None** to prevent access from either option.

If you are allowing access via Telnet or SSH, enter a value—in seconds—in the Shell Timeout field to define how long the connection will remain open during idle periods. Setting the shell timeout value to 0 (zero) will disable the timer and keep the session open, even when idle.

- **Web**
  Choose **Clear & Secure** to allow network management from your Web browser via HTTP (clear) and HTTPS (secure), or choose **Secure Only** to restrict management via a secure HTTPS connection only. Alternatively, you can choose **None** to prevent all Web management access.

- **CIMS (Cloud Infrastructure Management System)**
  Choose **Clear & Secure** to allow network management via CIMS, where security levels are controlled automatically. Alternatively, you can define the security level manually by choosing **Secure Only** or **Clear Only**.

- **SNMP Management**
  Check this box to enable network management via an SNMP (Simple Network Management Protocol) management console. Your Access/One Network supports the 802.11 MIB (Management Information Base), as well as Strix proprietary MIBs. Any MIB I or MIB II compliant SNMP management console (such as CiscoWorks or HP OpenView) can be used to manage your network remotely.

- **FTP Server**
  Check this box to enable FTP server functionality (this box must be checked if you want to update your firmware or transfer system configuration files).

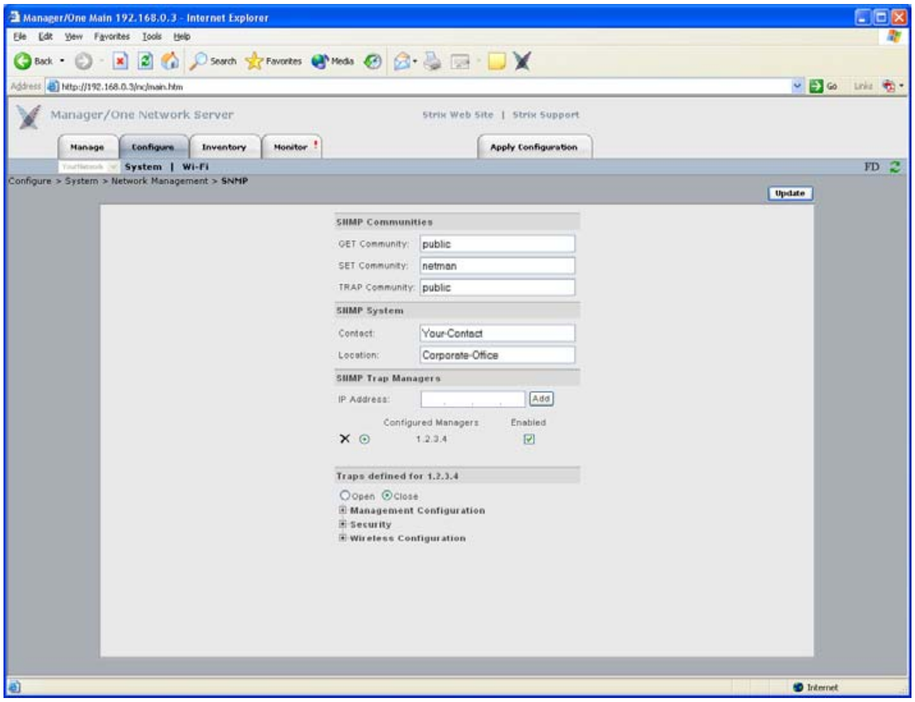
After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

SNMP

This command allows you to define the SNMP Communities, the SNMP System, and any specific SNMP Trap Managers. With SNMP enabled and the settings on this page defined, your Access/One Network will support most common SNMP management consoles.

The system also supports Syslog (System Logging) via an SNMP manager (in parallel with basic Syslog services) where Syslog text information is encoded in an SNMP trap message and presented to the operator.

SNMP (Simple Network Management Protocol is a standard protocol that regulates network management over the Internet. SNMP uses TCP/IP to communicate with a management platform, and offers a standard set of commands that make multi-vendor operability possible. SNMP uses a standard set of definitions, known as a MIB (Management Information Base), which can be supplemented with Enterprise-specific extensions. Strix provides its own proprietary MIBs. For more information about Strix MIBs, contact Strix technical support.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage Configure Inventory Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Internet

Configure > System > Network Management > SNMP

SNMP Communities

GET Community: public

SET Community: netman

TRAP Community: public

SNMP System

Contact: Your-Contact

Location: Corporate-Office

SNMP Trap Managers

IP Address: Add

	Configured Managers	Enabled
✕ ⊙	1.2.3.4	☑

Traps defined for 1.2.3.4

○ Open ● Close

⊞ Management Configuration

⊞ Security

⊞ Wireless Configuration

Figure 57. Configuring Access/One Network for SNMP

The following options are available with this command:

- **SNMP Communities**

  Enter your GET Community (read), SET Community (write) and TRAP Community in the corresponding fields. The defaults for these fields are:

  - GET Community: **public**
  - SET Community: **netman**
  - TRAP Community: **public**

- **SNMP System**

  Enter the Contact and Location information for the person managing your Access/One Network.

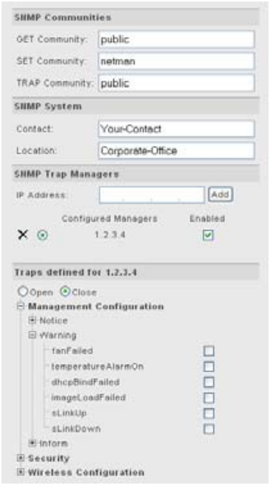
- **SNMP Trap Managers**

  Enter a valid IP address for any SNMP Trap Manager you intend to use. The SNMP Trap Manager you choose must be enabled, so ensure that the appropriate box is checked. If you have multiple SNMP Trap Managers assigned, you can delete a manager by clicking on the **X** icon associated with each manager.

- **Traps**

  Choose **Open** to expand the primary elements of the SNMP Trap Manager tree. From here you can make management selections by checking (or unchecking) the appropriate check boxes. When finished making your selections, choose **Close** to collapse the tree.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.



SNMP Communities

GET Community: public

SET Community: netman

TRAP Community: public

SNMP System

Contact: Your-Contact

Location: Corporate-Office

SNMP Trap Managers

IP Address: [. . .] [Add]

	Configured Managers	Enabled
✕ ⦿	1.2.3.4	☑

Traps defined for 1.2.3.4

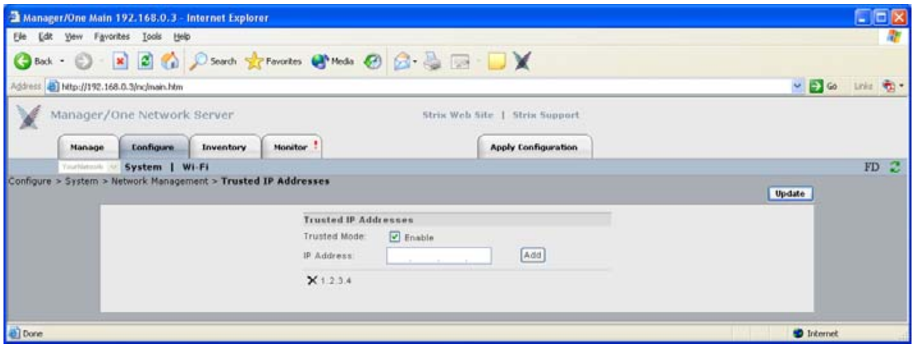
○ Open ⦿ Close

```
⊟ Management Configuration
   ⊞ Notice
   ⊟ Warning
       fanFailed               □
       temperatureAlarmOn      □
       dhcpBindFailed          □
       imageLoadFailed         □
       sLinkUp                 □
       sLinkDown               □
   ⊞ Inform
⊞ Security
⊞ Wireless Configuration
```

Figure 58. Managing Traps

Trusted IP Addresses

This command allows you to enable or disable the Trusted Mode and assign specific trusted IP addresses. When this mode is enabled, only addresses assigned here will be trusted by the network for management at any network module.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Add
Done
Internet

Configure > System > Network Management > **Trusted IP Addresses**

Trusted IP Addresses

Trusted Mode: ☑ Enable

IP Address:

✕ 1.2.3.4

Figure 59. Assigning Trusted IP Addresses

The following options are available with this command:

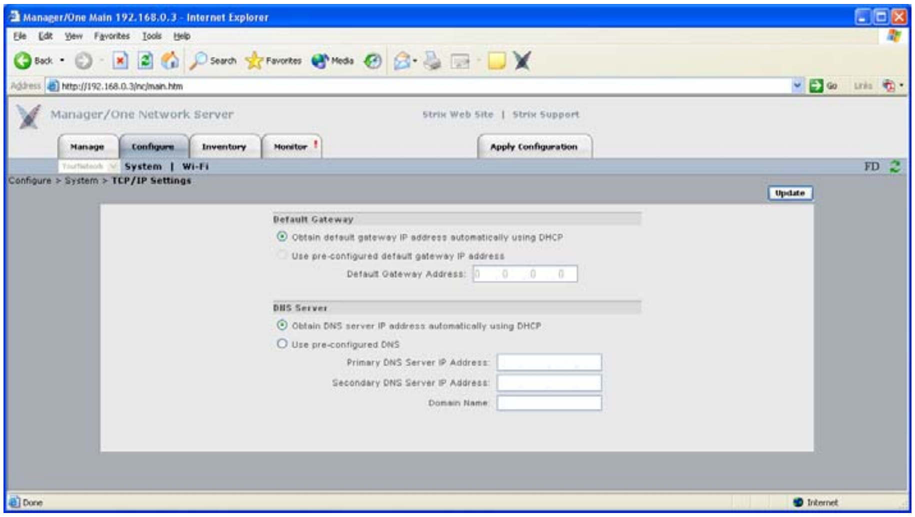
- **Trusted Mode**
  You can only enable this option if you have added at least one trusted IP address. Once a trusted IP has been added, check this box to enable the trusted mode (or uncheck the box if you want to disable this feature).

- **IP Address**
  You must add at least one IP address if you want to enable the trusted mode feature. To add an address, simply enter a valid IP address in this field then click on the **Add** button (the new address is listed below this field). You can add as many trusted IP addresses as you want. To delete an address, click on the **x** icon alongside the address, then confirm your request at the pop-up dialog. However, if you have only one trusted IP address listed, you cannot delete the address if the trusted mode is enabled—you must disable the trusted mode before attempting to delete a sole trusted IP address.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

TCP/IP Settings

This command allows you to specify whether Access/One will obtain the Default Gateway and DNS IP addresses automatically, or use pre-configured static IP addresses.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Done
Internet

Configure > System > TCP/IP Settings

Default Gateway

● Obtain default gateway IP address automatically using DHCP

○ Use pre-configured default gateway IP address

Default Gateway Address: 0 . 0 . 0 . 0

DNS Server

● Obtain DNS server IP address automatically using DHCP

○ Use pre-configured DNS

Primary DNS Server IP Address:

Secondary DNS Server IP Address:

Domain Name:

Figure 60. TCP/IP Settings

The following options are available with this command:

- **Default Gateway**

  The system is set up to use DHCP (Dynamic Host Configuration Protocol) to obtain the default gateway IP address automatically (default).

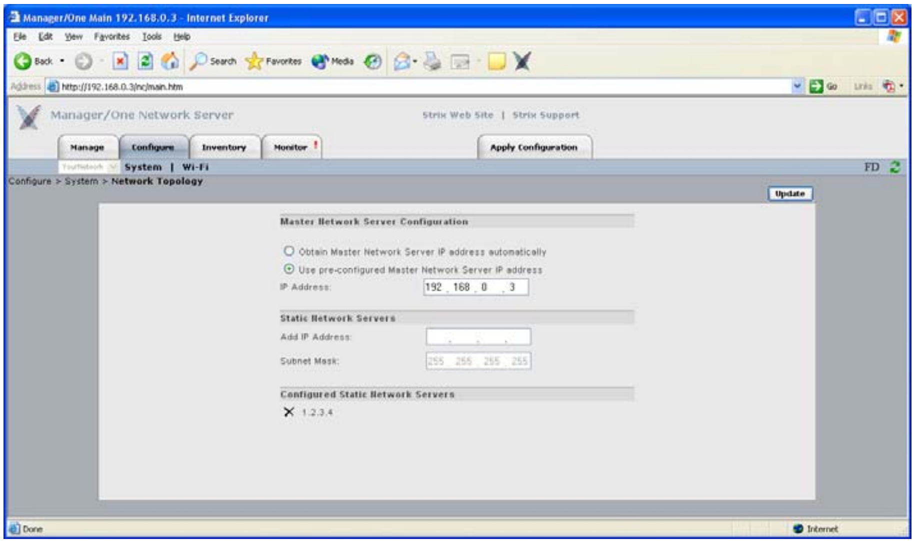
When using wireless uplinks between nodes, Access/One Network's self-tuning feature requires that a default gateway and/or DNS is specified to determine delays to the host Ethernet. When DHCP is used across the network (default), specifying both of these will satisfy this requirement.

- **DNS Server**
  Choose whether you want the system to use DHCP to obtain the DNS IP address automatically (default), or use a pre-configured static IP address. If you choose the latter option, enter IP addresses for the primary and secondary (if any) DNS server. DNS is used by your Access/One Network modules to lookup the names of various servers (for example, the RADIUS and FTP servers). You must specify a Domain Name when static IP addresses are used. This has the effect of appending the Domain Name to non-fully qualified address requests (for example, the FTP server host name configured as FTP123 will become FTP123.yourdomain.com).

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Network Topology

This command allows you to define whether your Access/One Network will obtain its Master Network Server IP address automatically or use a pre-configured static IP address. It also provides you with the option of defining any static network servers.


Manager/One Main 192.168.0.3 - Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://192.168.0.3/nc/main.htm
Go
Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
YourNetwork
System | Wi-Fi
FD
Configure > System > Network Topology
Update
Done
Internet

Master Network Server Configuration

○ Obtain Master Network Server IP address automatically
● Use pre-configured Master Network Server IP address
IP Address: 192 . 168 . 0 . 3

Static Network Servers

Add IP Address: . . .
Subnet Mask: 255 . 255 . 255 . 255

Configured Static Network Servers

✕ 1.2.3.4

Figure 61. Network Topology

The following options are available with this command:

- **Master Network Server Configuration**
  Establishing a master/slave relationship between network servers facilitates efficient Wide Area Network management by reducing the amount of traffic between two subnets on the same network, as well as providing a single network server responsible for all Strix devices within its subnet. This feature enables a Master Network Server to be statically or dynamically assigned for every subnet (even within the same network), which Manager/One users are redirected to if they try to log into a non-Master Network Server.

  The Master Network Server supports SNTP (Simple Network Time Protocol) and is responsible for sending out the correct clock for the subnet as part of the CIMS protocol. In this way, only the Master Network Server need derive the clock from an independent stratum 1 or 2 clock source. If the Master Network Server fails, your Access/One Network quickly detects the failure, at which point the network server with the next lowest IP address assumes the role of master. In this case, when the failed Master Network Server comes back online, it immediately re-establishes its role as master.

  Choose whether you want the system to obtain the Master Network Server IP address automatically (default), or use a pre-configured static IP address. If you choose the latter option, enter a valid IP address in the appropriate field.

- **Static Network Servers**
  Static network servers are added to bond subnets together, allowing you to configure and manage multiple subnets. You do this by starting with one subnet and adding the Master Network Server IP addresses of other subnets to tie them together.

  Enter the IP address of a network server module on another subnet (the default subnet mask is 255.255.255.255), then click on the **Update** button. to add the server to a list. If you enter multiple static network servers, you must click on the Update button after each entry for your changes to take effect.

  To delete a static network server's IP address, simply click on the **x** icon alongside the address.

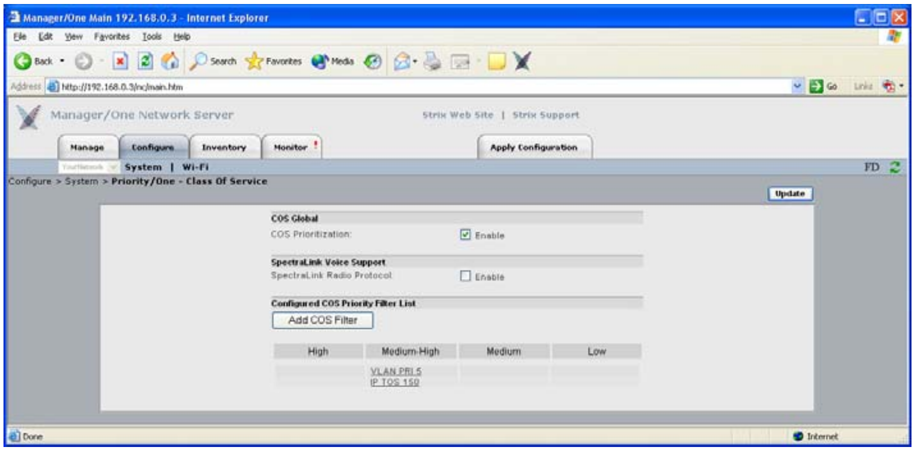
After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Priority/One - Class of Service

This command allows you enable and define Class of Service (CoS) filters to prioritize traffic throughout your Access/One Network. Supported filters include:

- VLAN
- IP TOS (Type of Service)
- IP Protocol

CoS filters establish separate queues for different priority streams based on the filters you define here. Data streams are then serviced according to their priority. In addition, this command allows you to enable or disable the SpectraLink® Voice Support feature.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Add COS Filter
Done
Internet

Configure > System > **Priority/One - Class Of Service**

COS Global

COS Prioritization: ☑ Enable

SpectraLink Voice Support

SpectraLink Radio Protocol ☐ Enable

Configured COS Priority Filter List

High	Medium-High	Medium	Low
	VLAN PRI 5 IP TOS 150		

Figure 62. Priority/One

The following options are available with this command:

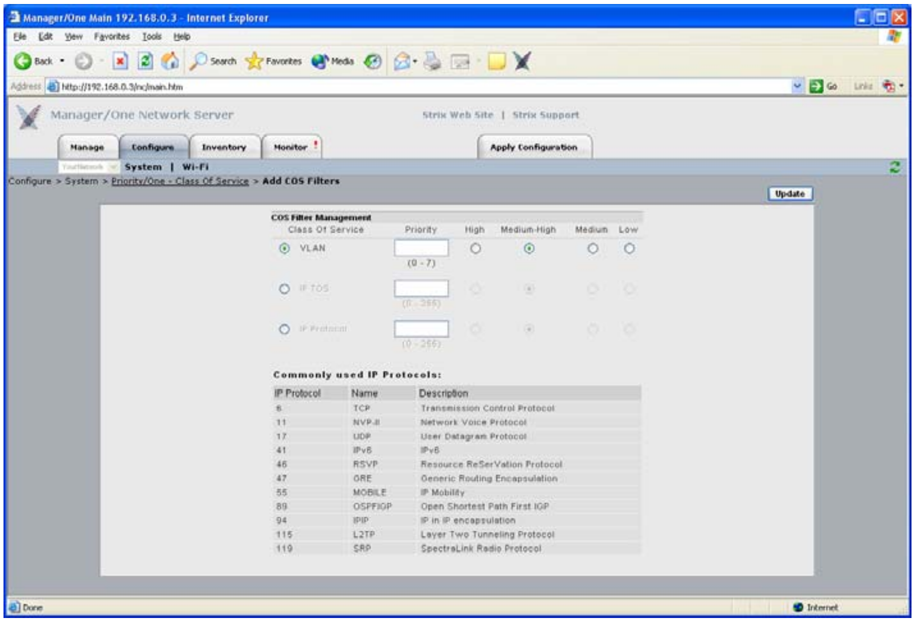
- **COS Global**
  Check the COS Prioritization box to enable COS filtering across the network, or uncheck the box to disable the COS filtering functionality.

- **Spectralink Voice Support**

  Check the SpectraLink Radio Protocol box to enable the SpectraLink Voice Support feature across the network. This feature gives a controlled preference to voice packets over data packets, ensuring that all voice packets are transmitted efficiently. Access/One Network prioritizes SpectraLink voice traffic over user data traffic.

- **Configured COS Priority Filter List**

  If you want to add a specific COS filter, click on the **Add COS Filter** button to display the COS Filter Management window. From here, you can add Class of Service filters and establish priorities for each class.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
Update
Done
Internet

Configure > System > Priority/One - Class Of Service > Add COS Filters

COS Filter Management

Class Of Service	Priority	High	Medium-High	Medium	Low
● VLAN	(0 - 7)	○	●	○	○
○ IP TOS	(0 - 255)	○	●	○	○
○ IP Protocol	(0 - 255)	○	●	○	○

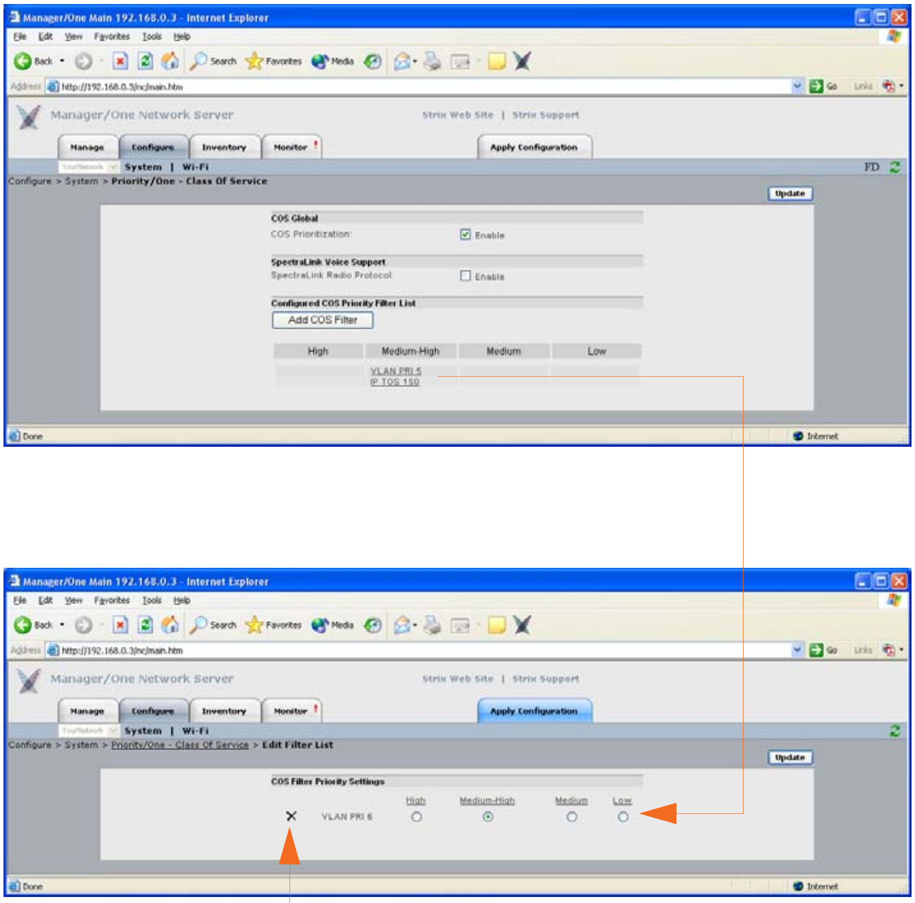
Commonly used IP Protocols:

IP Protocol	Name	Description
6	TCP	Transmission Control Protocol
11	NVP-II	Network Voice Protocol
17	UDP	User Datagram Protocol
41	IPv6	IPv6
46	RSVP	Resource ReSerVation Protocol
47	GRE	Generic Routing Encapsulation
55	MOBILE	IP Mobility
89	OSPFIGP	Open Shortest Path First IGP
94	IPIP	IP in IP encapsulation
115	L2TP	Layer Two Tunneling Protocol
119	SRP	SpectraLink Radio Protocol

Figure 63. Adding COS Filters

For each COS filter you add, you must click on the **Update** button to apply the change—you can only add one filter at a time. Each time you add a COS filter, Manager/One returns you to the main Priority/One page where you will see the new filter appended to a list. The list appears immediately under the Add COS Filter button.

To edit or delete an assigned filter that appears in the list, click on the filter to generate the COS Filter Priority Settings window. From here you can edit or delete filters. To delete a filter, click on the **x** icon next to the filter in this window.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Done
Internet

Configure > System > **Priority/One - Class Of Service**

COS Global

COS Prioritization: ☑ Enable

SpectraLink Voice Support

SpectraLink Radio Protocol ☐ Enable

Configured COS Priority Filter List

Add COS Filter

High	Medium-High	Medium	Low
	VLAN PRI 5 IP TOS 150		

Configure > System > Priority/One - Class Of Service > **Edit Filter List**

COS Filter Priority Settings

		High	Medium-High	Medium	Low
✕	VLAN PRI 6	○	●	○	○

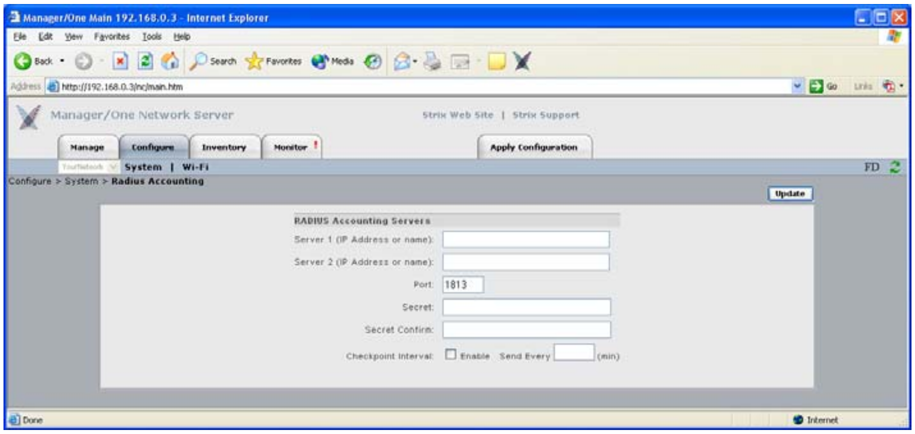
Click here to delete

Figure 64. Editing or Deleting COS Filters

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Radius Accounting

Through a wireless interface, your Access/One Network supports RFC 2866 standard RADIUS (Remote Authentication Dial-In User Service) accounting, allowing customers with existing RAS Radius-parsing scripts/tools to leverage their investment as well as customize their tools to extract all available statistical information. This command allows you to configure up to two RADIUS accounting servers, set up an authorization port, and establish a secret key.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Configure > System > Radius Accounting
Update
Done
Internet

RADIUS Accounting Servers

Server 1 (IP Address or name):

Server 2 (IP Address or name):

Port: 1813

Secret:

Secret Confirm:

Checkpoint Interval: □ Enable Send Every (min)

Figure 65. Setting Up RADIUS Accounting Servers

The following options are available with this command:

- **Server 1 (IP Address or Name)**
  Enter a valid IP address or name for Server 1.

- **Server 2 (IP Address or Name)**
  If you require a second (backup) server, enter a valid IP address or name for Server 2. Server 2 is only used if Server 1 becomes unavailable.

- **Port**
  Enter the authorization port for the primary RADIUS server (Server 1) in this field. This is the port the system uses when authorizing users.

- **Secret**
  Enter a secret key in this field for the primary RADIUS server. During the authentication process, the server and client exchange secret keys. The secret keys must match for communication between the server and the client to continue. The secret key is a valuable and necessary security measure.

- **Secret Confirm**
  Confirm your secret key in this field.

- **Checkpoint Interval**
  Check this box to enable a checkpoint interval, or uncheck this box to disable this feature.

- **Send Every**
  Once an interval time (in minutes) is established in this field, the reporting module will send interim reports for each wireless device associated to it at this interval period.

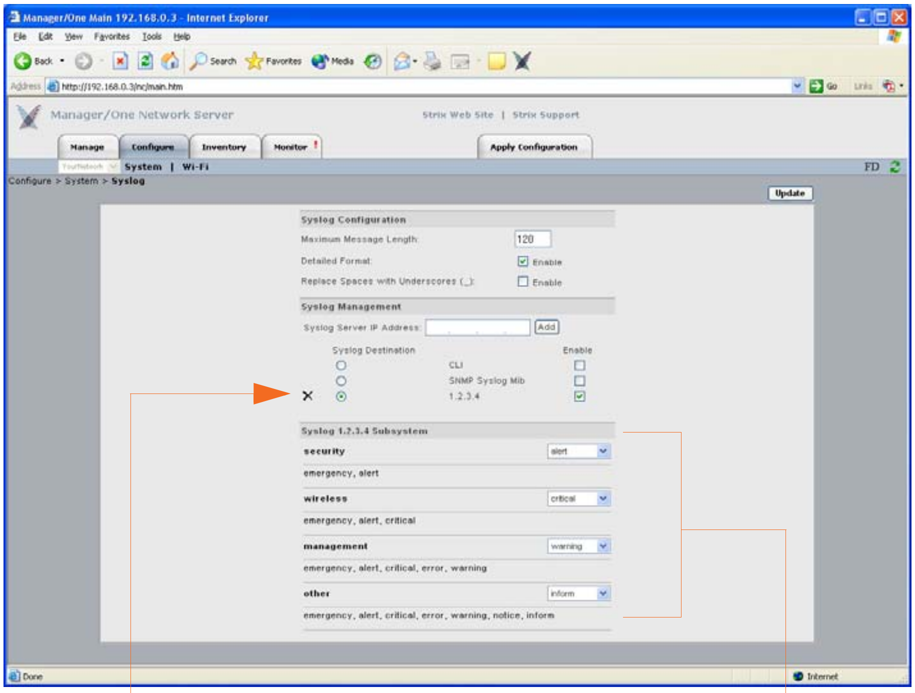
After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Syslog

Access/One Network offers comprehensive Syslog (system logging) functionality, including the ability to monitor Syslog events. Logged events can be sent to multiple Syslog servers, though using more than one server can impact the system's performance. This command allows you to:

- Define your Syslog configuration parameters.
- Assign the Syslog (system logging) server IP address.
- Define the event logging destination (Command Line Interface, SNMP Syslog MIB, or a defined Syslog server IP address).
- Establish the reporting level for each Access/One Network function (security, wireless, management, and other).

To access the Syslog window, choose **Syslog** from the System pull-down menu in the Configure function.



Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Add
Done
Internet

Configure > System > **Syslog**

Syslog Configuration

Maximum Message Length: 120

Detailed Format: ☑ Enable

Replace Spaces with Underscores (_): ☐ Enable

Syslog Management

Syslog Server IP Address: [. . .] Add

Syslog Destination		Enable
○	CLI	☐
○	SNMP Syslog Mib	☐
✕ ●	1.2.3.4	☑

Syslog 1.2.3.4 Subsystem

security: alert

emergency, alert

wireless: critical

emergency, alert, critical

management: warning

emergency, alert, critical, error, warning

other: inform

emergency, alert, critical, error, warning, notice, inform

Server IP Address added here

Reporting Levels

Figure 66. Configuring Access/One Network for Syslog

The following options are available with this command:

- **Syslog Configuration**

  This category allows you to define the Maximum Message Length, where the character length of Syslog messages will be restricted to the number you define here. In addition, you can enable/disable the Detailed Format feature which determines the level of detail reported in each message, and also enable a feature that forces the system to Replace Spaces with Underscores in messages.

- **Syslog Management**
  Enter a valid IP address for the Syslog server, then click on the **Add** button to add this server to the list of available Syslog destinations. You can add additional servers, but assigning multiple servers may degrade the system's performance. Once you've assigned the server(s), choose the destination for your event logging (CLI, SNMP Syslog MIB, and/or the Syslog server you assigned). The destination(s) you choose must be enabled, so ensure that the appropriate box is checked. If you have multiple IP addresses assigned, you can delete an IP address by clicking on the **x** icon next to the IP address.

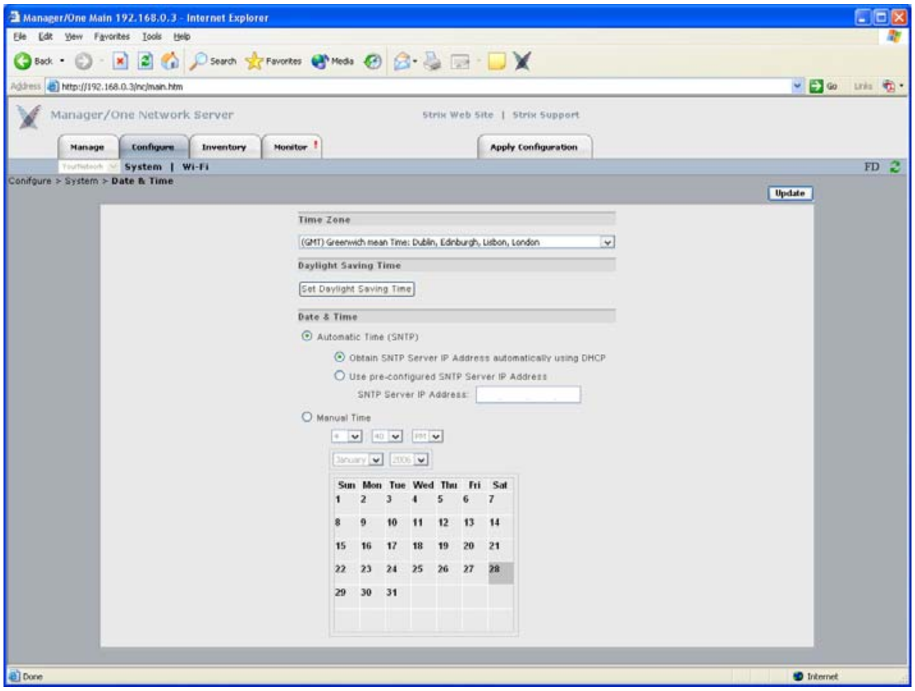
- **Syslog CLI Subsystem**
  Select the reporting level for each function (security, wireless, management, and other) from the corresponding pull-down list. Your available choices are:
  - none
  - emergency
  - alert
  - critical
  - error
  - warning
  - notice
  - inform
  - all

  If you select **all** from the pull-down list, this will include the debug level. The debug level will significantly increase (almost double) the number of Syslog messages that are returned and significantly degrade performance. The debug level should not be used for routine Syslog monitoring. For more information about Syslog messages, see "Syslog Messages" on page 171.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Date and Time

This command allows you to set the time zone, define daylight saving parameters, and choose between automatic time and manual time.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor !
Apply Configuration
System | Wi-Fi
FD
Update
Set Daylight Saving Time
Done
Internet

Configure > System > **Date & Time**

Time Zone

(GMT) Greenwich mean Time: Dublin, Edinburgh, Lisbon, London

Daylight Saving Time

Date & Time

● Automatic Time (SNTP)

● Obtain SNTP Server IP Address automatically using DHCP

○ Use pre-configured SNTP Server IP Address

SNTP Server IP Address:

○ Manual Time

4 40 PM

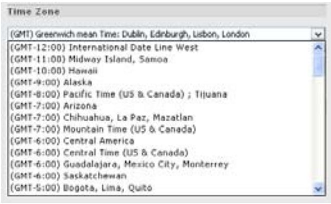
January 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Figure 67. Establishing the Correct Date and Time for Your Environment

The following options are available with this command:

- **Time Zone**
  Select the time zone from the pull-down list that applies to the geographic location where your Access/One Network is operating. The default time zone is Greenwich Mean Time (GMT).



Time Zone

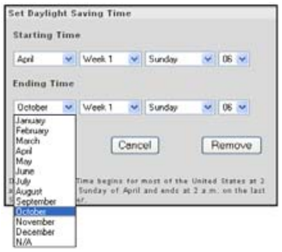
(GMT) Greenwich mean Time: Dublin, Edinburgh, Lisbon, London

(GMT-12:00) International Date Line West
(GMT-11:00) Midway Island, Samoa
(GMT-10:00) Hawaii
(GMT-9:00) Alaska
(GMT-8:00) Pacific Time (US & Canada) ; Tijuana
(GMT-7:00) Arizona
(GMT-7:00) Chihuahua, La Paz, Mazatlan
(GMT-7:00) Mountain Time (US & Canada)
(GMT-6:00) Central America
(GMT-6:00) Central Time (US & Canada)
(GMT-6:00) Guadalajara, Mexico City, Monterrey
(GMT-6:00) Saskatchewan
(GMT-5:00) Bogota, Lima, Quito

Figure 68. Time Zones

Daylight Saving Time

This option allows you to configure the Daylight Saving Time for your chosen time zone. Click on the **Set Daylight Saving Time** button to reveal the configuration window.



Set Daylight Saving Time

Starting Time

April | Week 1 | Sunday | 06

Ending Time

October | Week 1 | Sunday | 06

Time begins for most of the United States at 2 … Sunday of April and ends at 2 a.m. on the last …

Figure 69. Configuring Daylight Saving Time

Choose the month, week, day and year from the available pull-down menus for both the Starting Time and Ending Time to establish your daylight saving time. To apply your selections, click on the **Update** button in the Set Daylight Saving Time window (not the Update button on the main page). To remove all daylight saving time settings, simply click on the **Remove** button. You can also close this window without making changes (or even after making changes) by clicking on the **Cancel** button.

Date and Time

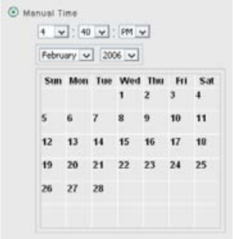
This option allows you to choose between Automatic Time and Manual time settings:

- **Automatic Time (SNTP)**
  SNTP (Simple Network Time Protocol) is an adaptation of the Network Time Protocol (NTP), used to synchronize computer clocks within the Internet. SNTP can operate in both unicast modes (point-to-point) and broadcast modes (point-to-multipoint). It can also operate in IP multicast mode where this service is available. If you selected Automatic Time (SNTP), you must choose whether you want the system to use DHCP to obtain the SNTP Server IP address automatically, or use a pre-configured static IP address. If you select the latter option, you must enter a valid IP address in the SNTP Server IP Address field.

With the Automatic Time (SNTP) option selected, the master network server transmits time/date synchronization packets periodically to Strix devices using the Strix Time Distribution (STD) protocol. Stack controllers use STD to adjust their own time and date. Time and date information is distributed in Greenwich Mean Time (GMT), allowing each device to adjust for its own time zone. This allows Access/One Network to span large geographic areas while maintaining time coherence.

If SNTP is configured at the network level, the master network server will proxy the SNTP time requests on behalf of your entire Access/One Network. The master network server effectively queries the SNTP server periodically and adjusts its own time/date accordingly. STD time/date information is then sent to all Strix devices on the network. If the master network server fails (for any reason), all Strix devices will then query the SNTP server individually.

- **Manual Time**
  Choose this option if you want to set the date and time manually. To do this, simply make your selections from the pull-down menus provided for hour, minute, AM/PM, month and year, then click on the day of the month on the calendar provided.



● Manual Time

4 : 40 : PM

February 2006

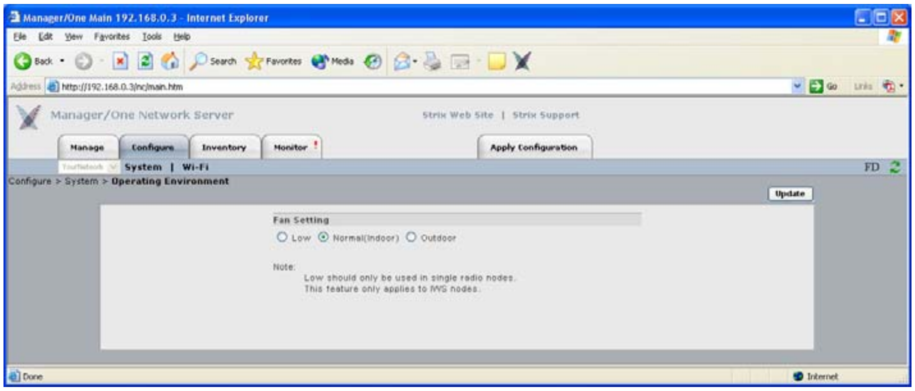
Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28				

Figure 70. Setting Manual Time

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Operating Environment

This command is applicable to the IWS only. It displays the Fan Setting window and allows you to choose between a Low, Normal (Indoor) and Outdoor speed setting for the node's cooling fan. Choose Normal if the affected node is to be installed in an environment with a regulated temperature, otherwise choose High if the operating environment is uncontrolled and prone to fluctuating temperatures and/or humidity. Generally, the Normal setting is used for indoor applications while the High setting is used for outdoor applications. Only use the Low setting for nodes with single radio configurations.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Done
Internet

Configure > System > **Operating Environment**

Fan Setting

○ Low ● Normal(Indoor) ○ Outdoor

Note:
Low should only be used in single radio nodes.
This feature only applies to IWS nodes.

Figure 71. Setting the Cooling Fan Speed

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Firmware Updates

This command allows you to set FTP parameters at the network level so that your Access/One Network knows where to find the new firmware (BIN) files. Procedural information for updating your Access/One Network's firmware has already been covered in "Updating Firmware Across the Network" on page 37.

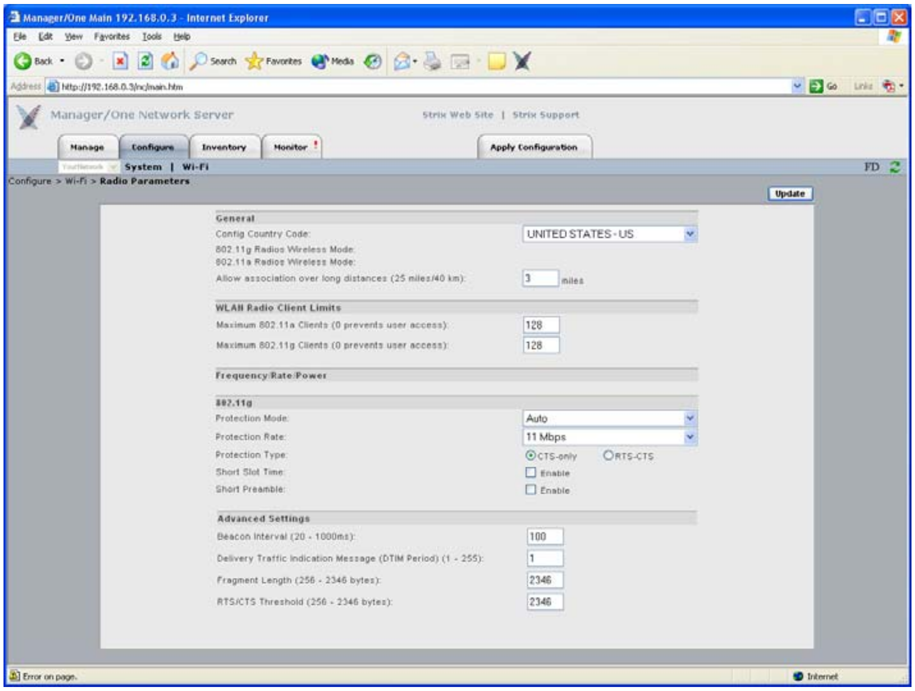
If you are uncertain about your FTP server's configuration parameters, consult with your network administrator.

Wi-Fi

This area of Manager/One contains the primary configuration commands for your Access/One Network in the Wi-Fi environment. Any commands executed here are applied to all wireless modules, so make sure the changes you initiate are changes that you want to apply to the entire network, otherwise go to "Managing Subnets and Nodes" on page 125 or "Managing Modules" on page 131.

Radio Parameters

This command allows you to define your Access/One Network's general radio parameters. The following graphic shows an example of the factory defaulted version of this page.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Error on page.
Internet

Address: http://192.168.0.3/nc/main.htm

Configure > Wi-Fi > Radio Parameters

General

Config Country Code: UNITED STATES - US

802.11g Radios Wireless Mode:

802.11a Radios Wireless Mode:

Allow association over long distances (25 miles/40 km): 3 miles

WLAN Radio Client Limits

Maximum 802.11a Clients (0 prevents user access): 128

Maximum 802.11g Clients (0 prevents user access): 128

Frequency/Rate/Power

802.11g

Protection Mode: Auto

Protection Rate: 11 Mbps

Protection Type: ● CTS-only ○ RTS-CTS

Short Slot Time: □ Enable

Short Preamble: □ Enable

Advanced Settings

Beacon Interval (20 - 1000ms): 100

Delivery Traffic Indication Message (DTIM Period) (1 - 255): 1

Fragment Length (256 - 2346 bytes): 2346

RTS/CTS Threshold (256 - 2346 bytes): 2346

Figure 72. Setting Up Radio Parameters

The following options are available with this command:

- **802.11g Radio Wireless Mode**
  This option allows you to select the 802.11g wireless mode from the options available in the corresponding pull-down list, including:
  - **802.11g**: This is the default standard 802.11g wireless mode.
  - **802.11g Only (No 802.11b)**: This mode restricts the radio to the 802.11g wireless mode only and does not allow 802.11b compatibility.
  - **802.11g Super**: This mode provides support for the Atheros Super G FastFrames throughput enhancement technology, with data rates up to 108Mbps and compatible with the 802.11g (54 Mbps) wireless technology. This translates to nearly double the throughput, but there are some limitations, including:
    - Only one operating channel is supported.
    - All user devices must also be capable of running 802.11g Super G and be configured for it. Super G is not an industry standard and so not all 802.11g user devices support this feature.
  - **802.11b Only (No 802.11g)**: This mode restricts the radio to the 802.11b wireless mode only and does not allow 802.11g compatibility.
- **802.11a Radio Wireless Mode**
  This option allows you to select the 802.11a wireless mode from the options available in the corresponding pull-down list, including:
  - **802.11a**: This is the default standard 802.11a wireless mode.
  - **802.11a Turbo**: This configures all 802.11a wireless modules in your Access/One Network to operate in Turbo mode, allowing them to operate with data rates at speeds up to 108 Mbps. This translates to nearly double the throughput, but all user devices must be capable of running the 802.11a Turbo mode and be configured for it. Turbo mode is not an industry standard and so not all 802.11a user devices support this feature.

- **Allow Association Over Long Distances**
  This option allows you to set a distance (up to 25 miles) for wireless associations over long distances (the default is 3 miles). Be aware that changing the distance here will affect all wireless modules. We recommend setting this value at the module level. For example, if you have a single 10 mile link and many shorter links setting this value to 10 miles will affect all links and slow down the network.

- **Maximum 802.11a Clients**
  This option allows you to restrict the number of 802.11a clients that can associate with each 802.11a access point. The default is 128. Setting this field to 0 (zero) prevents all 802.11a client access.

- **Maximum 802.11g Clients**
  This option allows you to restrict the number of 802.11g clients that can associate with each 802.11g access point. The default is 128. Setting this field to 0 (zero) prevents all 802.11g client access.

- **Transmit Power**
  This option allows you to select the level of transmit power from the choices available in the pull-down list (either Full, Half, Quarter, One Eighth, or Minimum). You can decrease the transmit power to decrease the range of the wireless modules in your Access/One Network. The default value for this parameter is **Full** (maximum power).

  Depending on the selected antenna(s) for your application—especially relevant to the OWS—it may be necessary to configure the transmit power. It is the installer's responsibility to ensure that the transmit power is set correctly for the chosen antenna(s). Operation in a manner other than is represented in this document is a violation of FCC rules.

  For a complete listing of the maximum power settings allowed for antennas, go to “Power Settings for Antennas” on page 165.

- **802.11a Channel Selector**
  These options extend the range of 802.11a wireless capability by allowing you to select 802.11a wireless channels. Check the corresponding box to enable an 802.11a channel of your choice.

- **802.11g Channel Selector**
  These options extend the range of 802.11g wireless capability by allowing you to select 802.11g wireless channels. Check the corresponding box to enable an 802.11g channel of your choice.

- **802.11g** (only)
  These options allow you to set up how your 802.11g wireless modules perform on the network (not applicable to 802.11a radios). Options that are specific to 802.11g radios include:

  - **Protection Mode**
    This is a mechanism to let 802.11g devices know when they should use modulation techniques to communicate with another 802.11b device, especially in wireless networks where there is a mixed environment that has 802.11g and 802.11b clients (and the clients are hidden from each other. The protection mode options are:

    - **None**
      This assumes there are no wireless stations using 802.11b (11 Mbps) technology. If operating in a mixed 802.11b/g network with minimal 802.11b traffic, choose this option to ensure the best performance for your 802.11g stations.

    - **Always**
      Protects 802.11b traffic from colliding with 802.11g traffic. This mode is not recommended, especially if only a few wireless stations are operating with 802.11b. Only use this mode in environments with heavy 802.11b traffic or where there is interference.

  - **Auto**
    This is the default mode and will enable protection for 802.11g stations if your Access/One Network finds an 802.11b client. In this mode, if the 802.11b client leaves the network the protection mode will revert to None automatically.

- **Protection Rate**
  Sets the data rate at which the RTS-CTS (Request-to-Send and Clear-to-Send) packets are sent (either 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps). The 11 Mbps data rate is the default.

- **Protection Type**
  This option is only relevant when the Protection Mode is on. The options here are **CTS-only** or **RTS-CTS**. With CTS-only, the client is not required to send an RTS (Request-to-Send) to the AP. As long as the client receives a CTS (Clear-to-Send) frame from the AP then the client is free to send data. With the RTS-CTS option enabled, the client is required to send an RTS to the AP and wait for a CTS from the AP before it can send data (this option creates additional overhead and can cause performance degradation). The default is CTS-only.

- **Short Slot Time**
  802.11g defines the long slot time as 20 microseconds and a short slot time as 9 microseconds. 802.11b only supports the long slot time of 20 microseconds. In an environment with 802.11g devices only, this option (Short Slot Time) must be enabled for better performance—giving precedence to 802.11g traffic. Only disable this option in mixed (802.11b and 802.11g) environments. The default is enabled.

- **Short Slot Preamble**
  Short slot preamble improves network efficiency by reducing the preamble from 128 bits to 56 bits. 802.11g is required to support both short and long preambles (802.11b support for a short preamble is optional). If this option is enabled, any 802.11b clients associated with the network must support a short preamble. The default for this option is enabled.

- **Advanced Settings**

  These advanced settings are preconfigured with the optimum settings for your Access/One Network. Changing any of these settings may negatively affect the network's performance. For best results, leave these settings at their default values.

  - **Beacon Interval**

    The beacon is a uniframe system packet broadcast by the AP to keep the network synchronized. Enter a value in this field between 20 and 1000 (milliseconds) that specifies the beacon interval. The default value is 100.

  - **Delivery Traffic Indication Message (DTIM Period)**

    Enter a value between 1 and 255 that specifies the Delivery Traffic Indication Message (DTIM). Increasing this interval allows the station to sleep for longer periods of time resulting in power savings (in exchange for some degradation in performance). The default value is 1.

  - **Fragment Length**

    Enter a value between 256 and 2346. This setting determines the size of the wireless frame. Wireless frames are reassembled by your Access/One Network wireless modules before being forwarded to the Ethernet port, but only if the frame is smaller than the Ethernet MTU (1536 bytes). The default value is 2346.

  - **RTS/CTS Threshold**

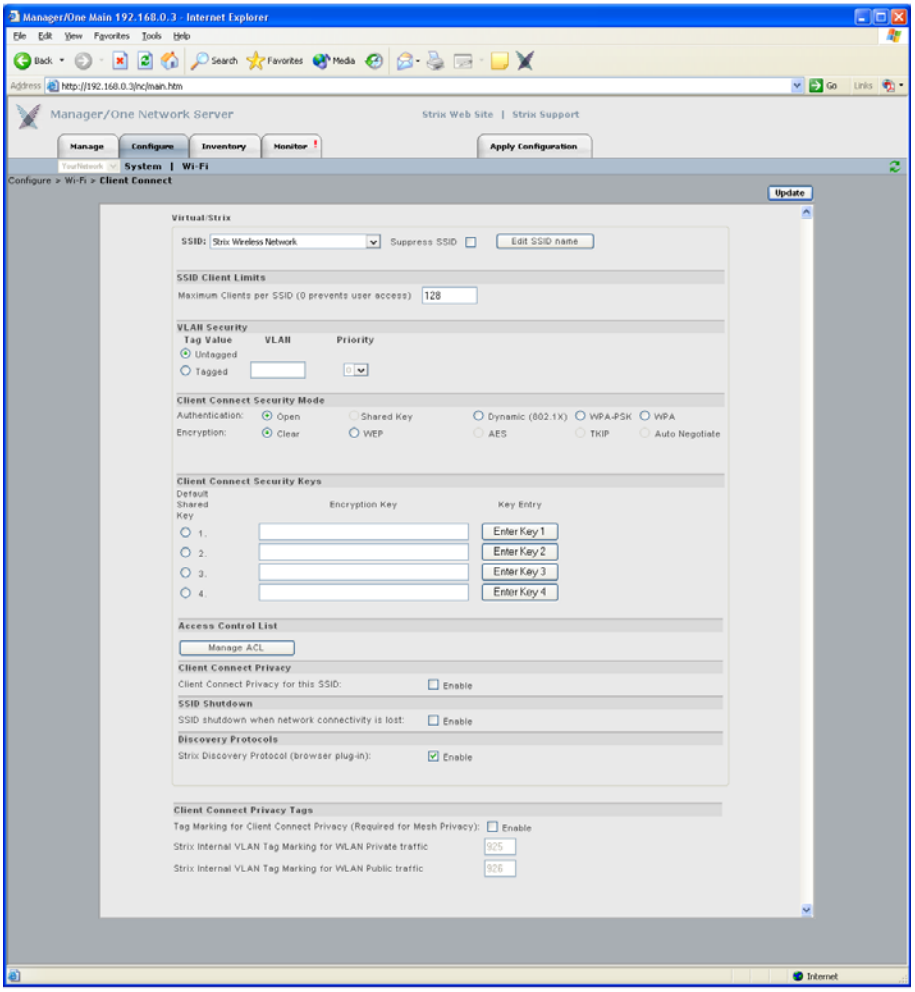
    This is a value that determines at what frame length the RTS-CTS function is triggered. By default, the threshold is set at its highest value. A lower value means that the RTS-CTS function is triggered for smaller frame lengths. A lower threshold value may be necessary in environments with excessive signal noise or hidden nodes, but may result in some performance degradation. Enter a value between 256 and 2346 to specify the RTS/CTS threshold. The default value is 2346.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Client Connect

Client Connect (Virtual/Strix) is the system topology that enables your Access/One Network to support and provide access to client devices using most wireless technologies, including 802.11a or 802.11g. With Client Connect you can customize each network node to support the wireless technologies you need in the locations you need them. Any mix of these technologies can be supported within a single node or across the entire Access/One Network.

This command allows you to define your Client Connect parameters. The following graphic shows the Client Connect window set to its default values.



Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
YourNetwork
System | Wi-Fi
Update
Edit SSID name
Enter Key 1
Enter Key 2
Enter Key 3
Enter Key 4
Manage ACL
Internet

Configure > Wi-Fi > Client Connect

Virtual/Strix

SSID: Strix Wireless Network　Suppress SSID □

SSID Client Limits

Maximum Clients per SSID (0 prevents user access) 128

VLAN Security

Tag Value	VLAN	Priority
● Untagged		
○ Tagged		0

Client Connect Security Mode

Authentication: ● Open　○ Shared Key　○ Dynamic (802.1X)　○ WPA-PSK　○ WPA

Encryption: ● Clear　○ WEP　○ AES　○ TKIP　○ Auto Negotiate

Client Connect Security Keys

Default Shared Key	Encryption Key	Key Entry
○ 1.		Enter Key 1
○ 2.		Enter Key 2
○ 3.		Enter Key 3
○ 4.		Enter Key 4

Access Control List

Client Connect Privacy

Client Connect Privacy for this SSID: □ Enable

SSID Shutdown

SSID shutdown when network connectivity is lost: □ Enable

Discovery Protocols

Strix Discovery Protocol (browser plug-in): ☑ Enable

Client Connect Privacy Tags

Tag Marking for Client Connect Privacy (Required for Mesh Privacy): □ Enable

Strix Internal VLAN Tag Marking for WLAN Private traffic 925

Strix Internal VLAN Tag Marking for WLAN Public traffic 926

Figure 73. Client Connect (Virtual/Strix)

The following options are available with this command:

- **SSID**

  An SSID (Service Set Identifier) is a unique name shared among all devices in a wireless network. Choose the network (SSID) or choose Add /Remove SSIDs from the pull-down list. If you add an SSID, the new SSID can be up to 32 alphanumeric characters and the characters are case-sensitive. In addition to adding and/or deleting SSIDs, this option allows you to edit an existing SSID name.

  - **Choosing an Existing SSID**

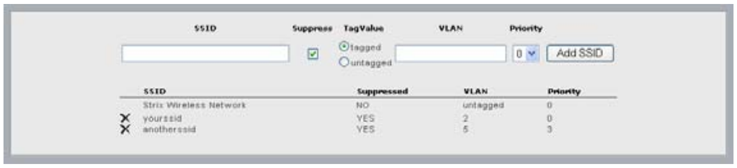
    To choose an existing SSID, simply select it from the pull-down list.

  - **Editing the Name of an Existing SSID**

    To edit the name of an existing SSID, choose an SSID from the pull-down list then click on the **Edit SSID Name** button. The SSID name is now editable and you can change it by over-typing on the existing name. If you do this, you must click on the **Update** button to apply your change.

  - **Creating a New SSID**

    To create a new SSID, choose Add/Remove SSIDs from the pull-down list to reveal the Add/Remove SSID window.



	SSID	Suppressed	VLAN	Priority
	Strix Wireless Network	NO	untagged	0
✕	yourssid	YES	2	0
✕	anotherssid	YES	5	3

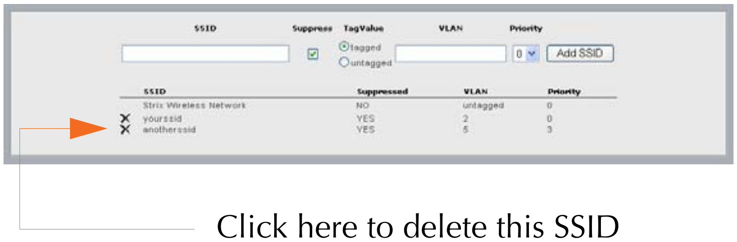
Figure 74. Adding an SSID

Enter a name for the new SSID in the SSID field. Check the **Suppress SSID** box if you want to prevent the broadcast of this SSID in beacons from all wireless modules in your Access/One Network (recommended).

Choose whether the new SSID should be tagged or untagged. However, there can be only one untagged SSID in the SSID table (the default SSID is always untagged). From this window you also have the option of assigning VLAN Security to the new SSID. When you have completed all data input for the creation of your new SSID, click on the **Add SSID** button. The new SSID is added to the list and will appear in the pull-down list in the main Client Connect window.

- **Deleting an SSID**

  To delete an existing SSID, simply click on the x icon next to the SSID you want to delete.



SSID	Suppress	TagValue	VLAN	Priority	
	☑	● tagged ○ untagged		0	Add SSID

	SSID	Suppressed	VLAN	Priority
	Strix Wireless Network	NO	untagged	0
✕	yourssid	YES	2	0
✕	anotherssid	YES	5	3

Click here to delete this SSID

Figure 75. Deleting an SSID

SSID Client Limits

Enter a value (up to 128) in the Maximum Clients per SSID field. The default is 128. If you enter a value of 0 (zero) you will effectively prevent all user access, with the exception of any Strix Network Connect devices.

VLAN Security

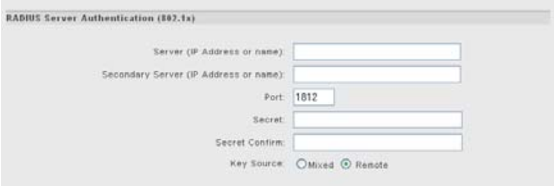
You can now associate a tagged or untagged VLAN with the selected SSID. If you define a tagged VLAN, you must assign a priority to it. The acceptable range for priorities is between 0 and 7, and the priority is chosen from the pull-down list. The lower the priority level you assign, the higher the priority will be given by a VLAN-aware Ethernet switch. Access/One Network does not support these priority levels as a queuing mechanism and ignores them while the frame is in transit through the network. The VLAN mechanism applies strictly to wireless stations. All devices on your Access/One Network generate only untagged traffic.

Client Connect Security Mode

This option allows you to establish the authentication and encryption security modes for Client Connects. These include:

- **Authentication**
  - **Open**: Used for local authentication.
  - **Shared Key**: This option is not currently supported.
  - **Dynamic Key (802.1X)**: With this option, the RADIUS server gives a key to each user for unicast traffic. Multicast traffic uses the default key.
  - **WPA-PSK**: With this option, the WPA (Wi-Fi Protected Access) standard uses a Pre-Shared Key (PSK) mode that does not require the RADIUS infrastructure.
  - **WPA**: This option provides WPA, a subset of the 802.11i standard that boosts the original static WEP security by mandating 802.1x remote authentication.
- **Encryption**
  - **Clear**: Available for Open or Dynamic authentication. Messages will be sent unencrypted between user devices and your Access/One Network nodes.
  - **WEP**: Wired Equivalency Privacy (WEP) is a security protocol for WLAN. It encrypts data using an RC4 stream cipher of 64, 128 or 152 bits.
  - **AES**: Advanced Encryption Standard (AES) encrypts data using a symmetric 152 bit data block, and is generally considered the most secure option available.
  - **TKIP**: The Temporal Key Integrity Protocol (TKIP) is part of the IEEE 802.11i encryption standard for wireless LANs, providing per-packet key mixing, a message integrity check and a re-keying mechanism.
  - **Auto Negotiate**: With this option, the encryption mode will be negotiated in real time between the participating devices, allowing the simultaneous use of AES and TKIP.

Select the desired Authentication and Encryption modes from the available options. If you choose Dynamic (802.1x) or WPA authentication, you must configure the RADIUS server(s) on this page (these fields only appear when Dynamic or WPA is selected as the authentication type). See also, "Radius Accounting" on page 84.



RADIUS Server Authentication (802.1x)

Server (IP Address or name):

Secondary Server (IP Address or name):

Port: 1812

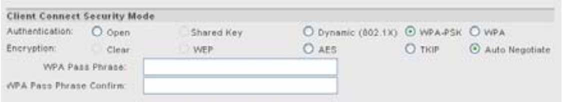
Secret:

Secret Confirm:

Key Source: ○ Mixed ● Remote

Figure 76. Configuring RADIUS Servers

If you choose WPA-PSK authentication, you must provide a WPA Pass Phrase and confirm the pass phrase (these fields only appear when WPA-PSK is selected as the authentication type.



Client Connect Security Mode

Authentication: ○ Open ○ Shared Key ○ Dynamic (802.1X) ● WPA-PSK ○ WPA

Encryption: ○ Clear ○ WEP ○ AES ○ TKIP ● Auto Negotiate

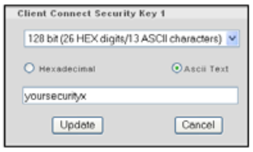
WPA Pass Phrase:

WPA Pass Phrase Confirm:

Figure 77. WPA Pass Phrase

Client Connect Security Keys

This option allows you to define up to 4 security encryption keys for your Client Connects. To define a security key, click on the **Enter Key 1** (through 4) button to reveal the security key window, then select either hexadecimal or ASCII format. Once you have selected the preferred format, choose 64 bit, 128 bit, or 152 bit encryption from the pull-down list and enter your security key. After entering the key, click on the **Update** button to add the new key to the list, or click on the **Cancel** button to abort the process.



Client Connect Security Key 1

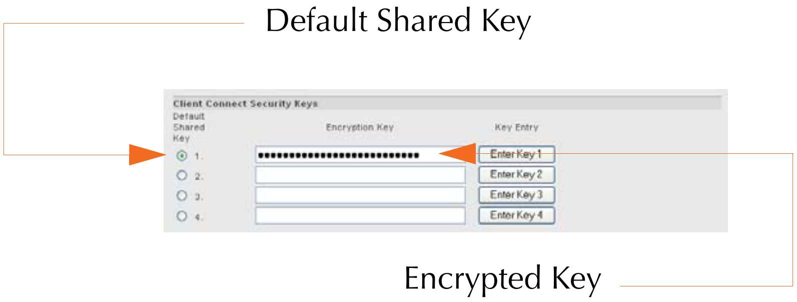
128 bit (26 HEX digits/13 ASCII characters)

○ Hexadecimal ● Ascii Text

yoursecurityx

Figure 78. Assigning Client Connect Security Keys

When you add a new Client Connect security key, the system encrypts the key and the encrypted key appears in the list. You can add up to 4 Client Connect security keys. After adding security keys, select one of the keys to act as the default shared key.



Default Shared Key

Client Connect Security Keys

Default Shared Key	Encryption Key	Key Entry
● 1.	•••••••••••••••••••••••••••	Enter Key 1
○ 2.		Enter Key 2
○ 3.		Enter Key 3
○ 4.		Enter Key 4

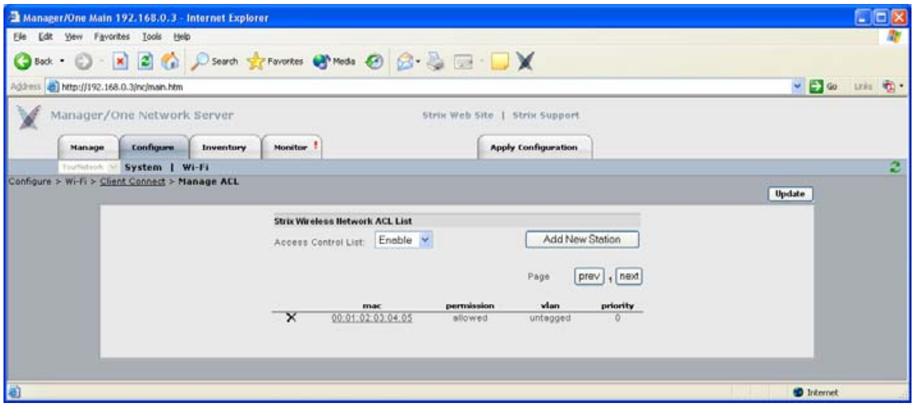
Encrypted Key

Figure 79. Encrypted Security Key

To delete a Client Connect security key, click on the **Enter Key 1** (through 4) button that applies to the key you want to delete. When the pop-up window appears, choose **None** from the pull-down list. The selected security key is removed from the list automatically.

Access Control List

This option allows you to configure an Access Control List (ACL) to determine which user devices (stations) are allowed to connect to your Access/One Network. To do this, simply click on the Manage ACL button to reveal the Manage ACL window.



Manager/One Main 192.168.0.3 - Internet Explorer

Address http://192.168.0.3/nc/main.htm

Manager/One Network Server

Configure > Wi-Fi > Client Connect > Manage ACL

Strix Wireless Network ACL List

Access Control List: Enable

	mac	permission	vlan	priority
✕	00:01:02:03:04:05	allowed	untagged	0

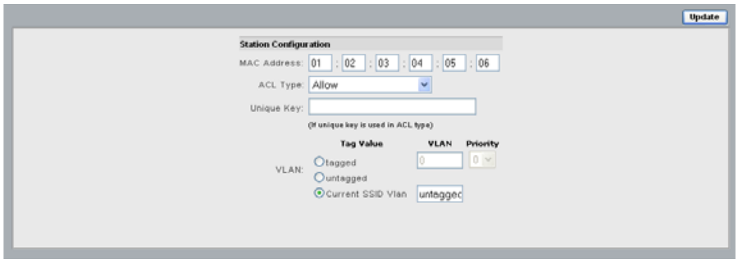
Figure 80. Configuring an Access Control List

Choose the preferred access level from the pull-down list. Your options include:

- **Disable**: All stations/clients can request association with an SSID in your Access/One Network. This means that the ACL will not be checked when a new station attempts to authenticate.
- **Enable**: All stations/clients are assigned a permission status based on their MAC address. If the MAC address of the station attempting to gain access is set to **Deny**, it will not be allowed to associate with the network. If the MAC address is set to **Allow**, or not configured in the ACL, the station will be allowed network access.
- **Strict**: Only stations assigned with **Allow** permissions in the ACL are granted access to the network, regardless of encryption settings. In addition, if the entry is configured for an encryption key, the station is also required to match that key before gaining access. If no ACL entry exists for a MAC address, it will not be allowed to associate with the network. The ACL accepts multiple levels of authentication concurrently so that stations with or without encryption (or shared key authentication) can be admitted.

Changing the ACL mode for wireless stations requires a reboot. A reboot is also required when adding or deleting ACL entries at the network level (though not at the module level).

To add a new station, click on the **Add New Station** button to reveal the Add New Station window.



Station Configuration

MAC Address: 01 : 02 : 03 : 04 : 05 : 06

ACL Type: Allow

Unique Key:

(If unique key is used in ACL type)

	Tag Value	VLAN	Priority
VLAN:	○ tagged	0	0
	○ untagged		
	● Current SSID Vlan	untaggec	

Figure 81. Adding a New Station

Enter the MAC address of the new station/client, then choose the ACL type from the pull-down list. These options include:

- Allow
- Deny
- Default Shared Key
- 64 bit (enter 10 digits)
- 128 bit (enter 26 digits)
- 152 bit (enter 32 digits)

If you choose any of the encryption types, enter the key in the **Unique Key** field. Alternatively, you can choose the Default Shared Key and the system will use the key you assigned as the default in Client Connect Security Keys. This key will be used for all unicast messages

If you want to assign a VLAN, go to VLAN Security to understand what you need to do with these fields. If CoS is disabled, your Access/One Network does not support VLAN priority levels as a queuing mechanism and ignores them while the frame is in transit through the network. The VLAN mechanism applies strictly to wireless stations. All Access/One Network devices generate only untagged traffic.

When you have completed your Access Control List (ACL) configuration, click on the **Update** button to apply your changes and return to the Manage ACL window. You must now click on the **Update** button in this window, then click on the **Apply Configuration** tab to apply all of your ACL changes across the network. You can now return to the main Client Connect window.

- **Client Connect Privacy**
  When enabled, this option offers Client Connect privacy by preventing Wi-Fi users from communicating with each other on the same module. Data from each Wi-Fi device is sent only to the Ethernet or backhaul ports, requiring a router or other access device for authentication before allowing the devices to exchange data. This is important in hotel applications where wireless users communicate with each other via Guestek or Wayport servers. The default is disabled.

- **SSID Shutdown**
  When enabled, this option shuts down all SSID functionality when network connectivity is lost. With this feature enabled, if connectivity to the gateway is lost, the access point will disassociate all attached wireless clients—the client will know there is a problem and will need to find another access point to re-establish connectivity with the network. The default is disabled.

- **Discovery Protocols**
  This option enables the Strix Discovery Protocol (browser plug-in). The default is enabled. If this option is disabled, the left pane in Manager/One will not be available and the auto-discovery feature will not function.

- **Client Connect Privacy Tags**
  This option is used if you want to prevent users from seeing each other on different modules. For total hotspot privacy, we recommend leaving the privacy WLAN tags at their default values.

  If you want to enable VLAN tag marking for Client Connect privacy (required for mesh privacy), check this box. If enabled, you must assign the tags (the defaults are 925 and 926).

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Network Connect

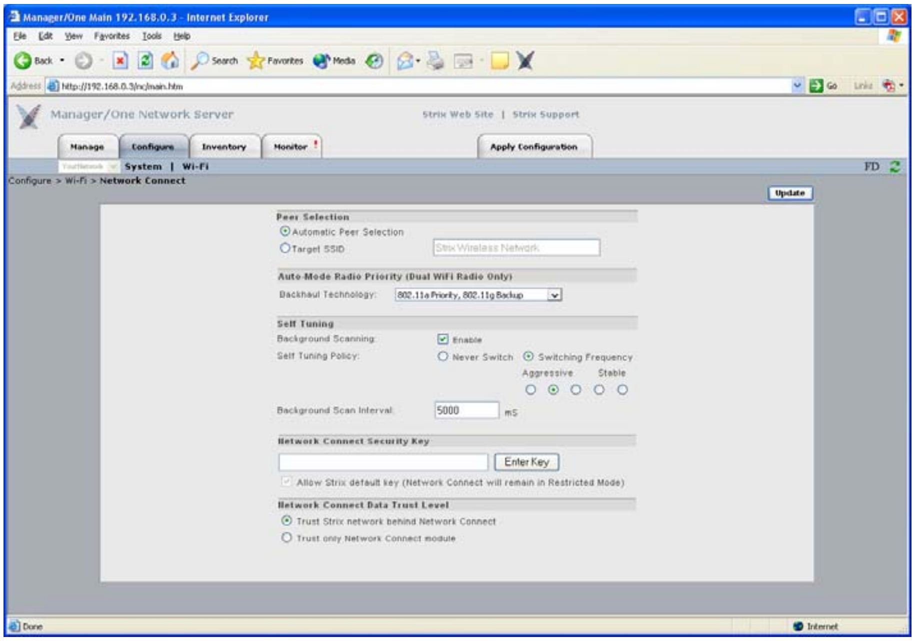
Network Connect is the infrastructure used by your Access/One Network for a wireless connection to an existing wired network (small or large). Each node within the network can utilize a wired Ethernet or wireless module (802.11a or 802.11g) for node inter-connectivity or connection to a wired legacy network.

Unlike traditional wired Ethernet LAN/WAN connections used by access points and WLAN switches, Access/One Network's wireless Network Connect option provides an advanced level of security between the network node and the LAN/WAN. By default, the wireless Network Connect link utilizes AES encryption with a secret key and cannot be compromised.

When nodes in your Access/One Network are configured for wireless Network Connect, the system provides several distinct advantages over a typical wireless network that uses wired connections. These advantages include:

- Secure networking
- Self tuning, rapid self-healing, and rogue device detection
- Scalability
- Simple installation
- Lowest cost of deployment

This command allows you to define your Network Connect parameters. The following graphic shows the Network Connect window set to its default values.


Manager/One Main 192.168.0.3 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.3/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Enter Key
Done
Internet

Configure > Wi-Fi > Network Connect

Peer Selection

● Automatic Peer Selection
○ Target SSID: Strix Wireless Network

Auto-Mode Radio Priority (Dual WiFi Radio Only)

Backhaul Technology: 802.11a Priority, 802.11g Backup

Self Tuning

Background Scanning: ☑ Enable
Self Tuning Policy: ○ Never Switch ● Switching Frequency
Aggressive ○ ● ○ ○ ○ Stable
Background Scan Interval: 5000 mS

Network Connect Security Key

☑ Allow Strix default key (Network Connect will remain in Restricted Mode)

Network Connect Data Trust Level

● Trust Strix network behind Network Connect
○ Trust only Network Connect module

Figure 82. Network Connect

The following options are available with this command:

- **Peer Selection**
  This option allows you to define peer selection criteria. These include either Automatic Peer Selection (where your Access/One Network chooses peers automatically, or selection by Target SSID (you must enter a valid SSID).

- **Auto-Mode Radio Priority (Dual Wi-Fi Radio Only)**
  This option allows you to establish a priority for which radio on the dual band wireless module will operate as a Network Connect in the **Auto** mode. The available choices are:

  - 802.11a Only
  - 802.11a Priority, 802.11g Backup
  - 802.11g Priority, 802.11a Backup
  - 802.11g Only

- **Self-Tuning**
  This feature allows you to enable or disable Background Scanning and configure the Self-Tuning Policy. When a Network Connect module first connects to the network, it performs an initial scan of all available Wi-Fi channels and generates a list of potential alternate Client Connects that are reachable. Following the initial scan, the Network Connect continually scans in the background to maintain the list and enable the system to make the following intelligent decisions:

  - When to drop the current path and select a better path, then connect to the appropriate node (self-tuning).
  - When to select the best path (or detect the loss of a path) and select the next best path, then connect to the appropriate node (self-healing).
  - Which APs are rogue devices.

  To fully optimize your network's ability to self-tune, self-heal and detect rogue devices, we recommend that the Background Scanning feature is always enabled (default).

Disabling Background Scanning will prevent Network Connects from reporting rogue AP devices.

- **Self-Tuning Policy**

  You can instruct the system to Never Switch during its self-tuning process, or establish a Switching Frequency (with 5 possible frequency states between stable and aggressive). When background scanning is completed, the self-tuning system determines the best potential client, based on RTD/RSSI scores and threshold values obtained during the scanning process. Threshold values become more critical when two Client Connects are very close with their scores. Normally, this can cause bouncing between the two Client Connects, but Access/One Network eliminates the bouncing effect by allowing you to move the threshold switching frequency from aggressive to stable.

- **Background Scan Interval**

  Enter a value in this field (in milliseconds) to define the interval between background scans. The default is 5000 milliseconds.

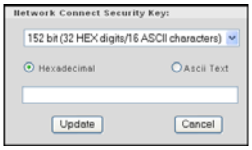
- **Network Connect Security Key**

  To protect wireless stations associated with each node, your Access/One Network provides WEP and AES ciphers for encryption and 802.1x remote authentication. The inter-node Network Connect wireless uplink is protected with an AES static key to prevent eavesdropping. The factory configured default key is hidden from view to retain secrecy for a basic network, but this key can be changed and each network can have its own unique key.

  The Network Connect solution for Access/One Network prevents unauthorized wireless connections from being established to the network by blocking user traffic in the following two scenarios:

  - If the Network Connect is configured for the default network name (AccessOne), Manager/One forces the administrator to approve/admit the node to the network before user traffic is bridged to the network.
  - If the two nodes that are wirelessly connected (via the uplink) have different Network Connect security keys configured. However, if the **Allow Strix default key** option is enabled then a Network Connect using the default security key can still connect with a network using a non-default security key.

To assign a security key, click on the **Enter Key** button. In the pop-up window, select the key entry method (hexadecimal or ASCII text), then enter the key that will serve as the default key to encrypt packets to be transmitted on a wireless uplink between nodes. The key length is fixed at 152 bits. After entering the key, click on the **Update** button to assign the key and return to the Network Connect window.



Network Connect Security Key:

152 bit (32 HEX digits/16 ASCII characters)

● Hexadecimal ○ Ascii Text

Figure 83. Network Connect Security Key

Enable the **Allow Strix default key** option if you want to allow Network Connects with a default key to connect with a network using a non-default security key. In this case, the network using a non-default security key can still be managed remotely. The default is enabled.

- **Network Connect Data Trust Level**

  This feature determines whether the Client Connect will allow traffic from a Network Connect only (for management purposes), or from devices beyond the Network Connect module—like a Client Connect on top of it, or Ethernet devices attached to it. This applies only when a Network Connect uses the default (non-provisioned) key when associating with a Client Connect.

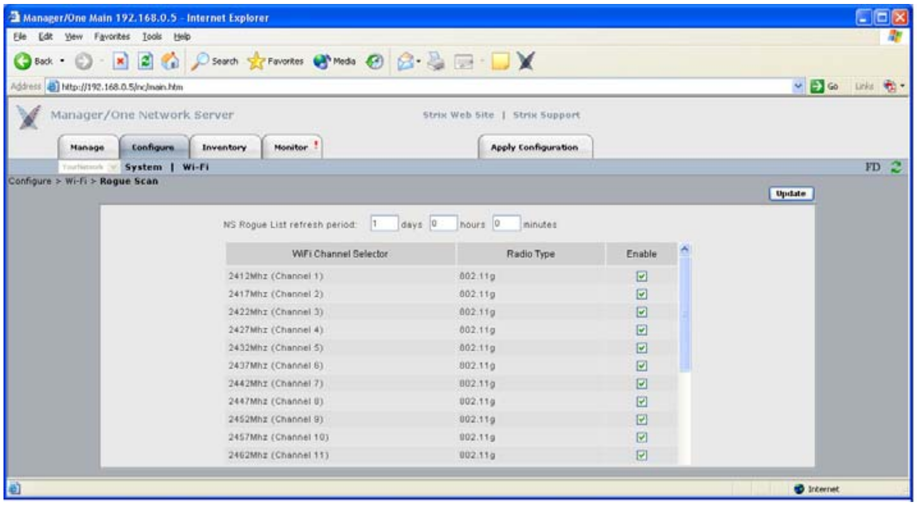
  Choose the preferred trust level policy for the Network Connect from the following options:

  - **Trust Strix Network behind Network Connect**: Trust the Strix network behind the Network Connect.
  - **Trust only Network Connect module**: Trust only the Network Connect module.

After inputting data (or making selections), click on the **Update** button to update this page, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.

Rogue Scan

This option allows you to define which channels are scanned for rogue devices by the defined country code. From the configuration window, you can enable or disable channels.


Manager/One Main 192.168.0.5 - Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.5/nc/main.htm
Go Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
System | Wi-Fi
FD
Update
Internet

Configure > Wi-Fi > Rogue Scan

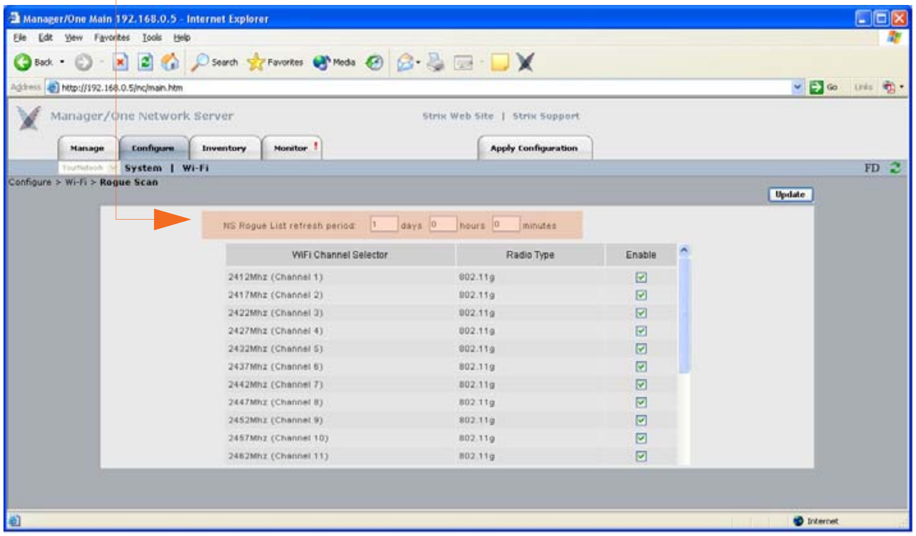
NS Rogue List refresh period: 1 days 0 hours 0 minutes

WiFi Channel Selector	Radio Type	Enable
2412Mhz (Channel 1)	802.11g	☑
2417Mhz (Channel 2)	802.11g	☑
2422Mhz (Channel 3)	802.11g	☑
2427Mhz (Channel 4)	802.11g	☑
2432Mhz (Channel 5)	802.11g	☑
2437Mhz (Channel 6)	802.11g	☑
2442Mhz (Channel 7)	802.11g	☑
2447Mhz (Channel 8)	802.11g	☑
2452Mhz (Channel 9)	802.11g	☑
2457Mhz (Channel 10)	802.11g	☑
2462Mhz (Channel 11)	802.11g	☑

Figure 84. Rogue AP Scanning

In addition to defining channels, the Rogue Scan configuration window allows you to define a refresh period—the elapsed time after which the network server refreshes the rogue device list. The default is 1 day. Making this refresh period too frequent will adversely impact the performance of the network.

Define the Refresh Period


Manager/One Main 192.168.0.5 - Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.0.5/nc/main.htm
Go
Links
Manager/One Network Server
Strix Web Site | Strix Support
Manage
Configure
Inventory
Monitor
Apply Configuration
YourNetwork
System | Wi-Fi
FD
Configure > Wi-Fi > Rogue Scan
Update
Internet

NS Rogue List refresh period: 1 days 0 hours 0 minutes

WiFi Channel Selector	Radio Type	Enable
2412Mhz (Channel 1)	802.11g	☑
2417Mhz (Channel 2)	802.11g	☑
2422Mhz (Channel 3)	802.11g	☑
2427Mhz (Channel 4)	802.11g	☑
2432Mhz (Channel 5)	802.11g	☑
2437Mhz (Channel 6)	802.11g	☑
2442Mhz (Channel 7)	802.11g	☑
2447Mhz (Channel 8)	802.11g	☑
2452Mhz (Channel 9)	802.11g	☑
2457Mhz (Channel 10)	802.11g	☑
2462Mhz (Channel 11)	802.11g	☑

Figure 85. Defining the Refresh Period for the Rogue List

If you make any changes to your channel selections in this window you must click on the **Update** button for your changes to take effect, then click on the **Apply Configuration** tab to propagate your changes across the network. If necessary, you can click on the factory default (**FD**) button in the toolbar to reset all data on this page to its factory default state.