



Network Controller 3500

Quick Start Guide

Firmware Version 1.00.82

1. Configuring the Controller

1.1. Connect to the Controller:

The default LAN IP Address of the Controller is:

IP: **192.168.1.1**

Set your managing computer to:

IP **192.168.1.100**

Netmask **255.255.255.0**

Or **DHCP**

Connect the LAN cable, and open a web browser to address 192.168.1.1. Default

Username / Password for the administrator is

Username: **"root"**

Password: **"root"**

We recommend changing the default password after the first login.

1.2. Configure WAN settings:

Depending on your broadband ISP, set the Controller to DHCP, PPPoE or Static Address.

1.2.1. WAN DHCP

If your WAN connection is TCP/IP, and you expect the Controller to receive a dynamic address from a DHCP server, use this setting. This is most common with Cable Modem service, or if you are connecting the Controller to an existing routed network or T1 router. Simply select

Express Setup – DHCP Client

1.2.2. WAN PPPoE

If your WAN connection is DSL, or another kind of PPP-based network, use this setting. You will need a Name and Password from your ISP to connect. Select

Express Setup – PPPoE

Provide The User and Password in the text fields.

When connecting or reconnecting PPPoE it is recommended to reset or reboot the DSL Modem first and then reboot the Controller 3500.

1.2.3. Static WAN IP Address

If you have Static IP settings provided by your ISP, or you are adding the Controller to an existing network, select

Express Setup – Static IP

Provide the IP, Netmask, and DNS Server values provided by your ISP.

1.3. Configure LAN settings:

You can assign the LAN IP settings of the Controller by selecting:

Networks – WAN / LAN – Device IP

In most installations the Controller will provide DHCP services and IP addresses to Wired and Wireless subscribers. If you change the default IP Address be sure the DHCP settings match. Otherwise DHCP clients will receive addresses that cannot connect to the Controller. To configure DHCP Select

Networks – Server – DHCP Server

Default LAN IP: **192.168.1.1**
Default LAN Netmask: **255.255.255.0**
Default DHCP: **DHCP Server**
Default Start IP Address: **192.168.1.10**
Default IP Pool Size: **100**
Default Duration: **1440 minutes**

It is a good practice to reserve static addresses for Access Points or other hardware on the network, so that you can always find them. By default, addresses 192.168.1.2 to 192.168.1.9 will not be distributed by DHCP, and can be assigned as static addresses.

1.4. Configure Authentication

You have five authentication options in the Controller: Local, RADIUS, Hampton Inn HSIA, Terms of Service, or No Authentication. You can select No Authentication to create an open system.

Please note that all subscribers will need to establish a session on the Controller by opening their web browser before they can ping, send email, or establish other connections to the Internet. If using No Authentication they will not be interrupted or asked to login in any way when using their web browser.

The default authentication of the Controller: **Local Authentication**

Default Local User Account:

Username: **guest**
Password: **guest**

1.4.1. Configure Local Authentication

To manage user accounts directly from the Controller without an external authentication server, select:

Security – Authentication – Local Authentication

Click on **Add/Modify User** to see the current user database and make any changes.

1.4.2. Configure RADIUS Authentication

If you have a RADIUS Server set up to manage accounts on the network, or you are using a service provider to handling billing and authentication, select

Security – Authentication – RADIUS Server

Please consult your service provider or RADIUS documentation to determine the correct IP, port, and Shared Secret settings for your RADIUS Server. In addition you may need to register the Controller's IP Address and NAS ID (found under Networks – System) with the RADIUS Server in order for RADIUS to accept requests from the Controller.

1.4.3. Configure Hampton HSIA Authentication

To use the Hampton Inn HSIA Central Authentication Server (CAS), select

Security – Authentication – Hampton HSIA Authentication.

This will open a dropdown with Hampton specific configuration. The default values are for testing only, please contact Hampton Inn for valid configuration settings for the property you are installing.

- | | |
|-------------------------------|--|
| Central Authentication | Enter the correct URL for the Hampton portal page. These values must be provided by Hampton or the venue owner. |
| Property Code | Enter the Property Code provided by Hampton Inn. |
| Property Zip | Enter the Property Zip Code. |
| Gateway IP | Normally the Public IP of the Controller will be provided to the CAS automatically. If the Controller is behind a NAT firewall, you can use this field to override this and provide the IP Address of the Firewall here. Configure your Firewall to forward port 1111 to the Controller to enable Hampton HSIA Authentication through NAT. |

1.4.4. Configure Terms of Service

Many venue owners wish to provide open access, but want to limit it to users who have explicitly agreed to a legal terms of service to protect the venue. The terms of service feature will only allow access to users who specifically “click through” a legal agreement which you or the venues owner specifies.

To enable Terms of Service select:

Security – Authentication – Terms of Service

Subscribers will be presented with a form that you can customize by uploading a HTML file with the terms of service text. The file must contain the correct HTML POST form provided in the sample Terms_of_Service.htm file.

If you wish to provide a terms of service login from a portal page, you must configure **Security – Local Authentication** and then use the HTML code under **System Tools – Maintenance – Terms of Service – View External HTML Code**. Configure your portal gage to redirect subscribers to under **Customization – Login Page – External Portal**.

1.4.5. Configure No Authentication

If you want any subscribers to get access to the network without any authentication mechanism, you can select

Security – Authentication – No Authentication

Subscribers will still be subject to other policies in the Controller such as black list, advertising, and redirection.

1.5. Configure Login Options

If you have enabled Local or RADIUS Authentication, the Controller will provide a default Internal Login Page to Subscribers for them to enter their username and password. The formatting of this page is standardized. If you want to make limited changes to the internal page, in terms of color and text, you can also select

Customization – Login Page – Custom

If you do not wish subscribers to be redirect at all, you can select

Customization – Login Page – No Redirect

In this case you will need to provide subscribers with the URL of your login page in some other way for them to get access.

The default login page: **Internal**

NOTE: Terms of Service and Hampton Inn HSIA Authentication have a different login process, so these redirect settings are ignored.

1.5.1. Configure Login Page Redirection (Captive Portal)

Many venues prefer to direct subscribers to an external website where they can see terms of service, manage their account, or login to the Controller. To create a custom login page, select

Customization – Login Page – External Portal

Provide the URL of the page you wish unauthenticated users to be directed to in the text box. You will also need to add this URL to the URL Pass through table, so that unauthenticated users can access it. Once the session is redirected, all further page control will be on the website. When you want users to login to the controller, you must embed the HTML code provided in the [code](#) link on your web page. When the user selects 'submit' on the redirected login page, their login information will be sent to the Controller, which will check their username/password against the local user database or external RADIUS Server.

As an additional option, you can set a HTML tag to direct the subscriber to a URL after they successfully authenticate. This HTML code goes on the redirected login page.

```
<input type="hidden" name="redirecturl" value="about:blank">
```

You supply the URL to send the subscriber to after they are authenticated under **value=**

If you wish to redirect subscribers in a “no authentication” configuration, provide a URL under **Customization – Login – Default Post-Authentication Redirect – Specify URL**.

1.6. Upgrading the Firmware

The firmware image in the Controller can be easily updated by selecting

System Tools – Maintenance – Firmware Upgrade

Use the browse button to select the firmware image on your managing computer that you wish to load. Clicking Upgrade will start the upgrade process. Once started the upgrade cannot be stopped, and the Controller must reboot. Logic in the Controller will insure that an invalid firmware image is not loaded. However, if the file is not transferred correctly you may need to try again after the Controller reboots. Look for the firmware version under System Status – System to verify the firmware version.

The firmware upgrade process can take up to five minutes.

Preventing Upgrade Problems:

These steps can be used if you are having trouble upgrading, or just want to make certain that there are no browser or network issue that interfere with the process.

1. Export your current settings and user database under **System Tools - Maintenance**
2. Disconnect WAN port.
3. Clear browser cache in Internet Explorer (so you don't get any old pages out of the cache) under **tools - internet options - delete files – delete all offline content - OK**

4. Upgrade NC3500 .bin file through LAN port.
5. After reboot, if the **System Status** page shows the correct Firmware Image version, you are done. You can import your original settings if you reset the factory defaults.
6. If the status page does not show the correct firmware version, or the NC3500 .bin image does not load, try resetting the Controller to Factory Default, unplug and replug the power, and repeat steps 4-6.

Note: If you get “Bad File”, “Digest”, or “Signature Errors” more than once, try downloading the upgrade from the ValuePoint FTP site and using the MD5 digest utility to insure that the files have not been corrupted in transit.

ValuePoint FTP:

70.133.189.66
User: customer
Password: vp2002

Note: It may be necessary to restore factory defaults after the firmware upgrade. If you have any problems please press the ‘default’ button for a few seconds after the Controller boots and the System and WLAN lights are on.

Note: If you have any HTTP GUI display problems please clear your Internet file cache in Internet Explorer by selecting Tools – Internet Options – Delete Files – Delete All Files.

2. Controller 3500 Default Settings

Web configuration login (**case sensitive**): username: **root** - password: **root**
Default LAN IP: **192.168.1.1**
Default WAN IP: **Static**
Default Authentication: **Local**
Default Login: **Standard**
Default Local Database Entry: username: **guest** password: **guest**
Default WEP: **disable**

Note: You can reset default settings by holding the hardware reset button for approximately 10 seconds when the Controller is running (the system light is flashing or solid, not off), or selecting “Reset Factory Defaults” in the Management GUI.

3. Optimizing Controller Performance

The Controller 3500 is designed to satisfy multiple network configurations and business models. If you are deploying the Controller in a high stress public environment where you will be using authentication, login redirect, Auto-IP, Auto-Proxy and other sophisticated features you can maximize the performance of the Controller by simplifying the WAN connection and providing a **Static IP Address**. This can be done with a Static IP Address from your ISP or by adding an inexpensive Gateway/Router to the Network to handle PPPoE or WAN side DHCP. **Auto-IP** and **Auto-Proxy** also consume significant resources, so disable these if subscribers do not need them.