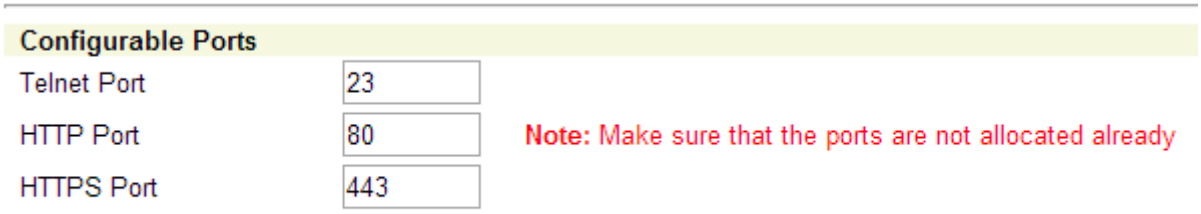
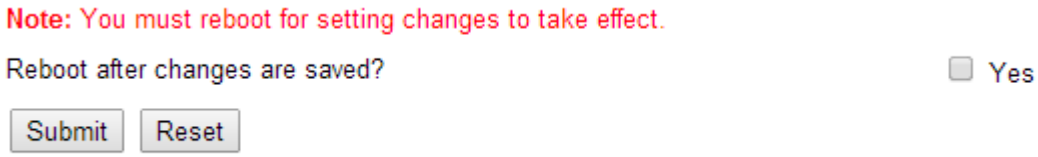
Securing your Access Gateway FAQ

The purpose of this document is show the many ways to securely manage your Access Gateway (AG).

Access Control – changing the default ports – These changes will be made in the Configuration/Access Control screen. Default ports for Telnet, HTTP and HTTPS management can be re-assigned.



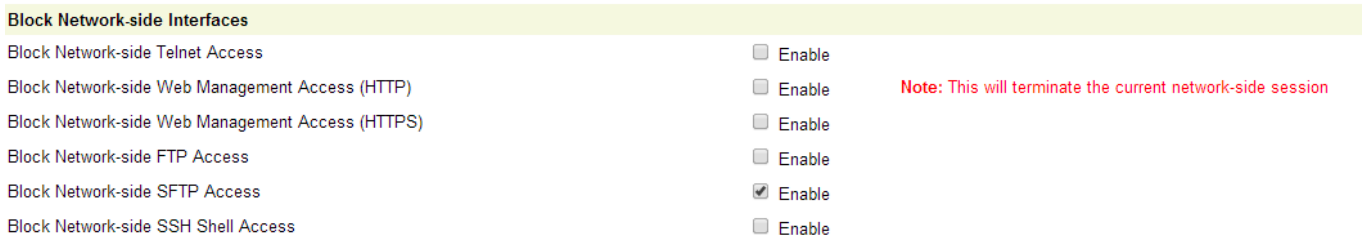
Once you have set the ports to the new settings, scroll to the bottom of the screen. Check Yes for the *Reboot after changes are saved?* option and Submit to have it take effect.



Note: If you will be making multiple changes on this screen, you can wait until all changes are made before rebooting the AG. The only change on this configuration page that requires a reboot is the Configurable Ports.

Access Control – Blocking management interfaces –Network (WAN) Side

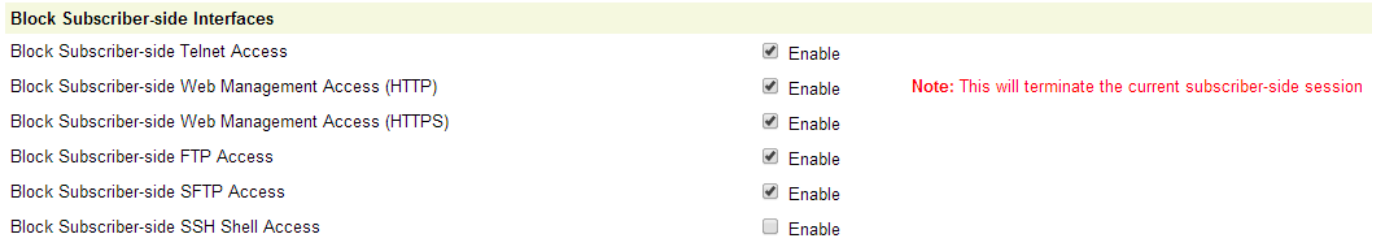
By default, all network side management interfaces are allowed, except for SFTP.



To block management of one or more of the management interfaces, you will need to Enable the access you wish to block, and then submit the changes at the bottom of the screen.

Access Control – Blocking management interfaces –Subscriber (LAN) Side

By default, all subscriber side management interfaces are blocked, except for SSH.



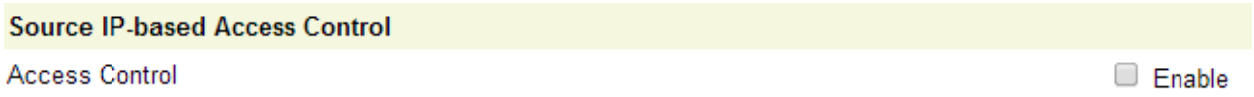
To allow management of one or more of the management interfaces, you will need to unblock the access by unchecking Enable for each access you wish to allow, and then submit the changes at the bottom of the screen.

Source IP-based Access Control – this feature allows you to limit access to the management interfaces to the IP addresses added to the Access Control IP list. If an attempt is made from an IP address not in the list, the AG will drop the packet.

By default, the IP address of 172.30.30.173 is added. It is recommended that this IP address remains in case you accidentally lock yourself out by not adding your own IP address to the source list when configuring this feature. By keeping this address, you will be able to have someone onsite connect by setting their device to this IP address and disable Source IP access control so you can regain access.

You may create the list by adding individual IP addresses or a range by entering the starting and ending IP addresses.

When you have completed your list, you will need to enable Source IP-based Access Control, and submit the changes at the bottom of this screen. A reboot is not required.

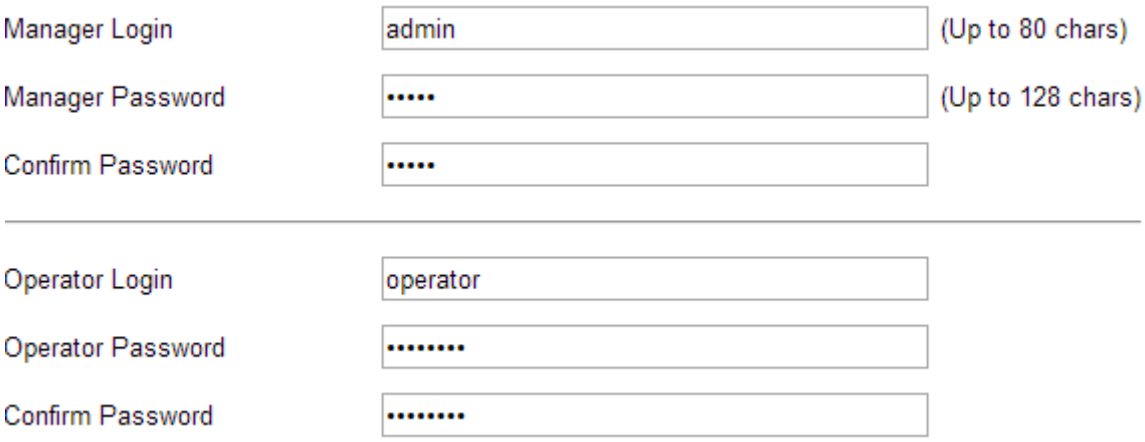


Changing the Manager and Operator user name and password.

Manager access allows you access to all configuration screens and allows you to make changes. The default user name and password is admin.

Operator access allows you access to almost all configuration screens, however you can only view the settings. There are no Submit or OK buttons so changes cannot be made. The default user name and password is operator.

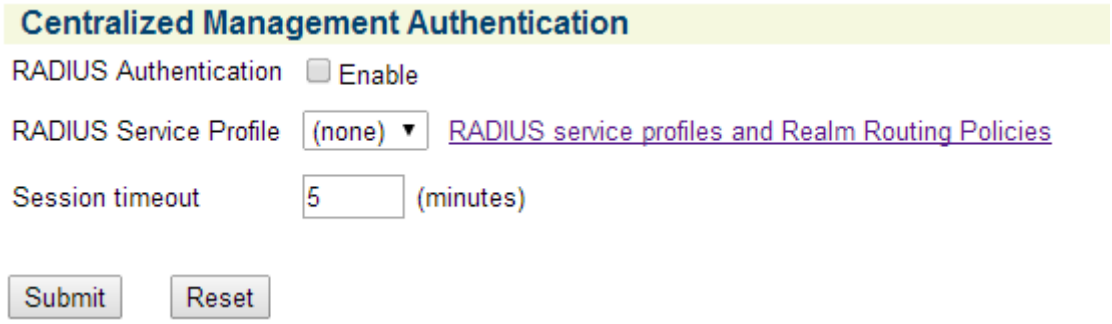
To change these settings, navigate to the System/Login screen.



Once here, you may change these settings. The user name for both the Manager and Operator logins is restricted to 80 characters and the password is restricted to 128 characters. Special characters are allowed. Once your changes are made, click on Submit at the bottom of this screen. You will need to log in again once the changes are made as the user name and password have been changed.

Administration Concurrency – When this feature is enabled, it allows only one manager and up to three operators to login concurrently. If you receive a 403 Forbidden message when trying to login through the web management interface as a manager, or a message in telnet stating that a manager is already logged in, then Administration Concurrency is enabled and there is already a manager connection made.

Centralized Management Authentication – With this feature, you extend the management login to authenticate against a Radius server, restricting the user to specific interfaces based on their user profile. With this feature you can allow/prevent access for users to the Web Management Interface, Telnet/CLI interface, FTP and the Remote Radius Login test page. Please refer to document, **How to use Centralized Management Authentication v2.pdf** for complete details on setting up this feature.



IPSEC – Using the IPSEC feature, you can have the AG create an IPSEC tunnel to an external network then create policies that would allow management of the AG through the secure tunnel. For more detail, please refer to the document, How to initiate an IPSEC tunnel from the NSE.