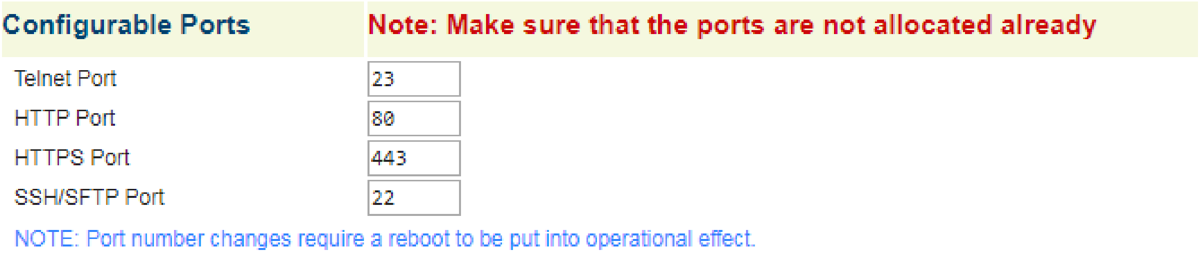
NOMADIX

Securing your Nomadix Gateway FAQ

The purpose of this document is to highlight the many ways to securely manage your Nomadix Gateway (NSE).

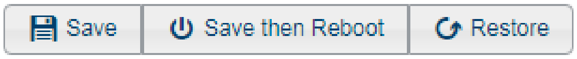
Access Control – changing the default ports – These changes will be made in the Configuration -> Access Control screen. By default, the NSE will use the default ports for Telnet, HTTP, HTTPS and SSH/SFTP. To secure the management of the NSE you should change off the default ports.



Configurable Ports	Note: Make sure that the ports are not allocated already
Telnet Port	23
HTTP Port	80
HTTPS Port	443
SSH/SFTP Port	22

NOTE: Port number changes require a reboot to be put into operational effect.

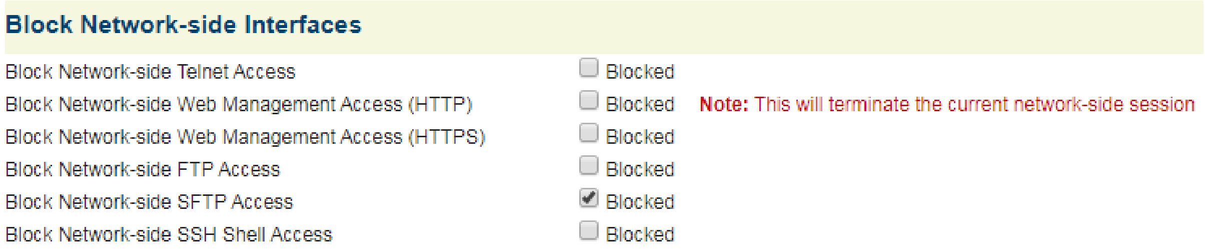
Once you have set the ports to the new settings, scroll to the bottom of the screen. Click on the Save then Reboot button to reboot the NSE and to have the changes take effect.



Note: If you will be making multiple changes on this screen, you can wait until all changes are made before rebooting the NSE. 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.



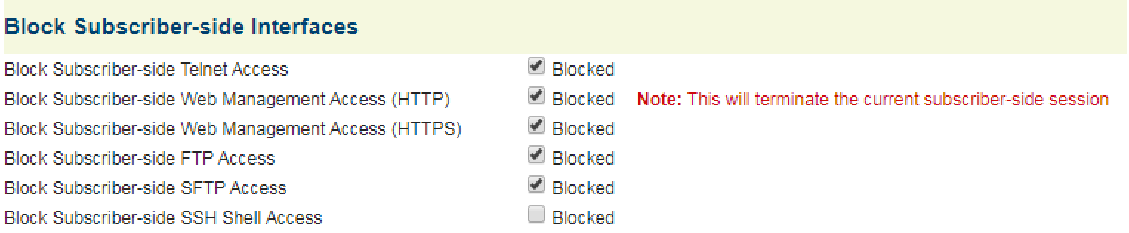
Block Network-side Interfaces

Block Network-side Telnet Access	☐ Blocked	
Block Network-side Web Management Access (HTTP)	☐ Blocked	**Note:** This will terminate the current network-side session
Block Network-side Web Management Access (HTTPS)	☐ Blocked	
Block Network-side FTP Access	☐ Blocked	
Block Network-side SFTP Access	☑ Blocked	
Block Network-side SSH Shell Access	☐ Blocked	

To block management of one or more of the management interfaces, you will need to check the box next to 'Blocked' for the interface you wish to deny access to and then save 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.

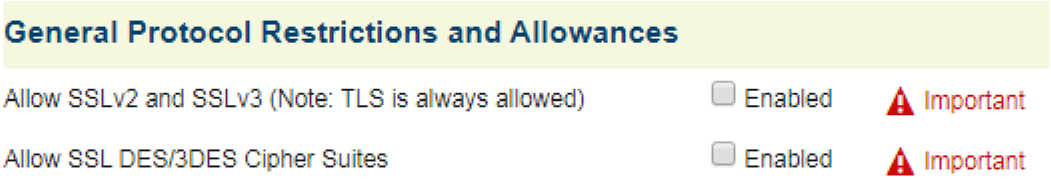


Block Subscriber-side Interfaces

Block Subscriber-side Telnet Access	☑ Blocked	
Block Subscriber-side Web Management Access (HTTP)	☑ Blocked	**Note:** This will terminate the current subscriber-side session
Block Subscriber-side Web Management Access (HTTPS)	☑ Blocked	
Block Subscriber-side FTP Access	☑ Blocked	
Block Subscriber-side SFTP Access	☑ Blocked	
Block Subscriber-side SSH Shell Access	☐ Blocked	

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

General Protocol Restrictions and Allowances – this feature was developed in response to the Poodle and Sweet32 attacks. You can select to allow the protocols and disregard the warnings.



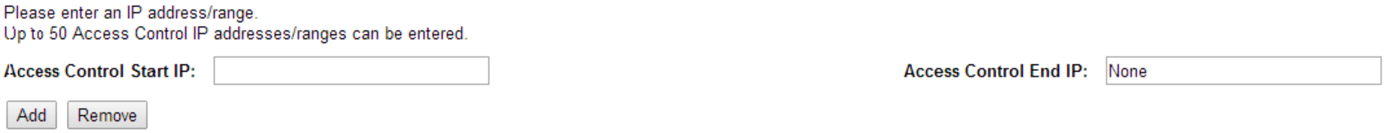
General Protocol Restrictions and Allowances

Allow SSLv2 and SSLv3 (Note: TLS is always allowed)	□ Enabled	⚠ Important
Allow SSL DES/3DES Cipher Suites	□ Enabled	⚠ Important

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 NSE 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.

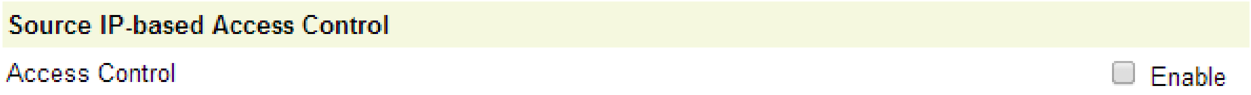
You may create the list by adding individual IP addresses or entering a range, by entering the starting and ending IP addresses.



Please enter an IP address/range.
Up to 50 Access Control IP addresses/ranges can be entered.

Access Control Start IP: ____ Access Control End IP: None

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.



Source IP-based Access Control

Access Control □ Enable

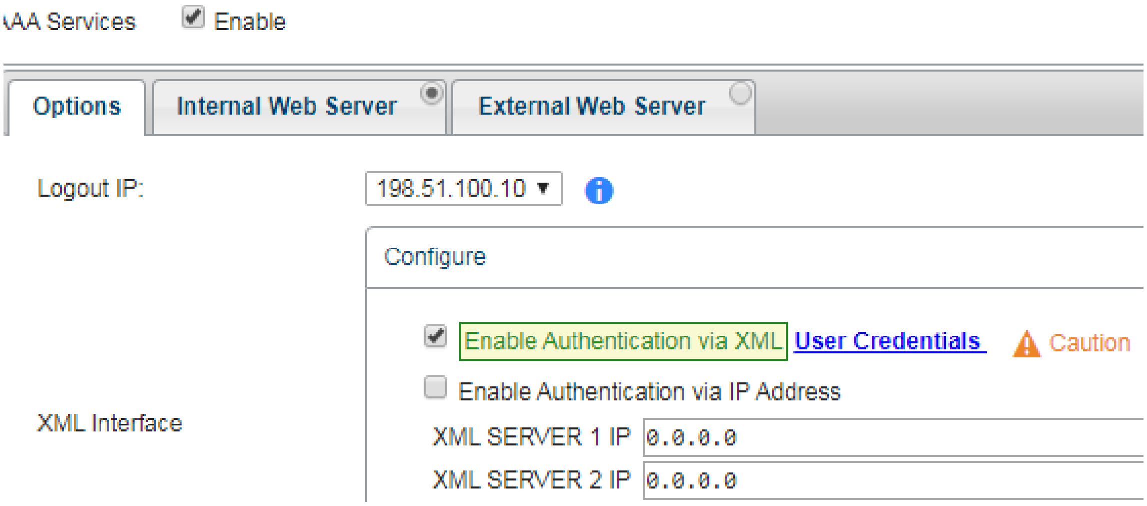
Changing the Manager and Operator username and password.

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

Staff access provides manager access to only the Subscriber Administration section, allowing staff to manage guest experience without providing access to other configurations of the NSE. The default username and password is staff

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

XML authentication has now been added to the Nomadix Gateway. It is used with the AAA setting to allow User Credentials. This allows XML credential authentication instead of needing to add specific IP addresses for each server. The default username and password is xmlcommand.



AA Services ☑ Enable

Logout IP: 198.51.100.10 ▼

XML Interface

☑ Enable Authentication via XML

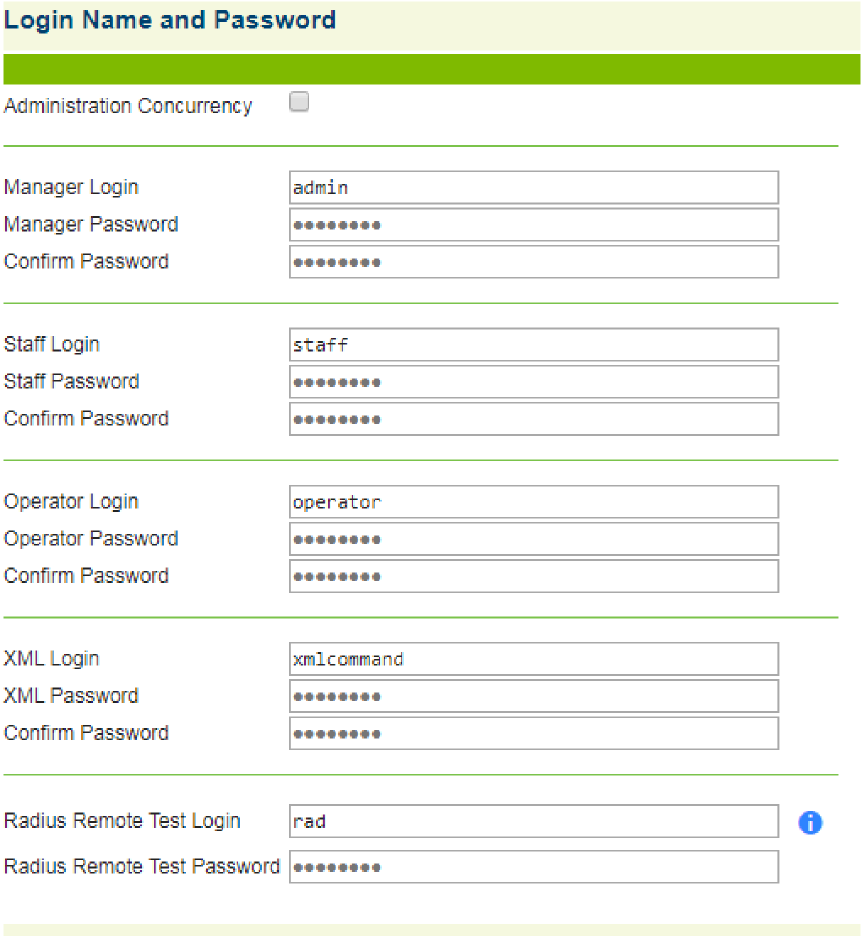
□ Enable Authentication via IP Address

XML SERVER 1 IP 0.0.0.0

XML SERVER 2 IP 0.0.0.0

Radius Test provides a method to test connection between the configured Radius server and NSE. Because it is a different login all current management interfaces must be closed, and the session timed out. Easiest method is to use another browser or machine. Default username and password is rad.

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



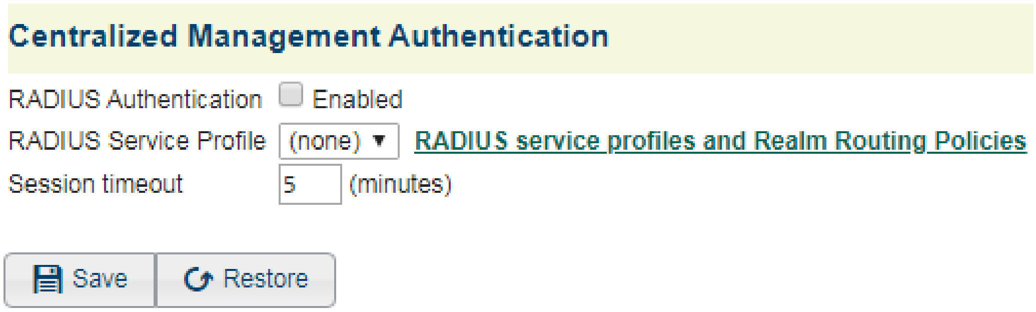
Login Name and Password

Administration Concurrency	☐	
Manager Login	admin	
Manager Password	●●●●●●●●	
Confirm Password	●●●●●●●●	
Staff Login	staff	
Staff Password	●●●●●●●●	
Confirm Password	●●●●●●●●	
Operator Login	operator	
Operator Password	●●●●●●●●	
Confirm Password	●●●●●●●●	
XML Login	xmlcommand	
XML Password	●●●●●●●●	
Confirm Password	●●●●●●●●	
Radius Remote Test Login	rad	ⓘ
Radius Remote Test Password	●●●●●●●●	

Once here, you may change these settings. The username for 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 Save at the bottom of this screen. If you make changes to the Manager login you will need to log in again once the changes are made as the username and password have been changed.

Administrative Concurrency when enabled allows only one management and up to three operator connections simultaneously.

Centralized Management Authentication – With this feature, you extend the management login to authenticate against a Radius server, restricting the user to specific access levels or 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.



Centralized Management Authentication

RADIUS Authentication ☐ Enabled

RADIUS Service Profile (none) ▼ RADIUS service profiles and Realm Routing Policies

Session timeout 5 (minutes)

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