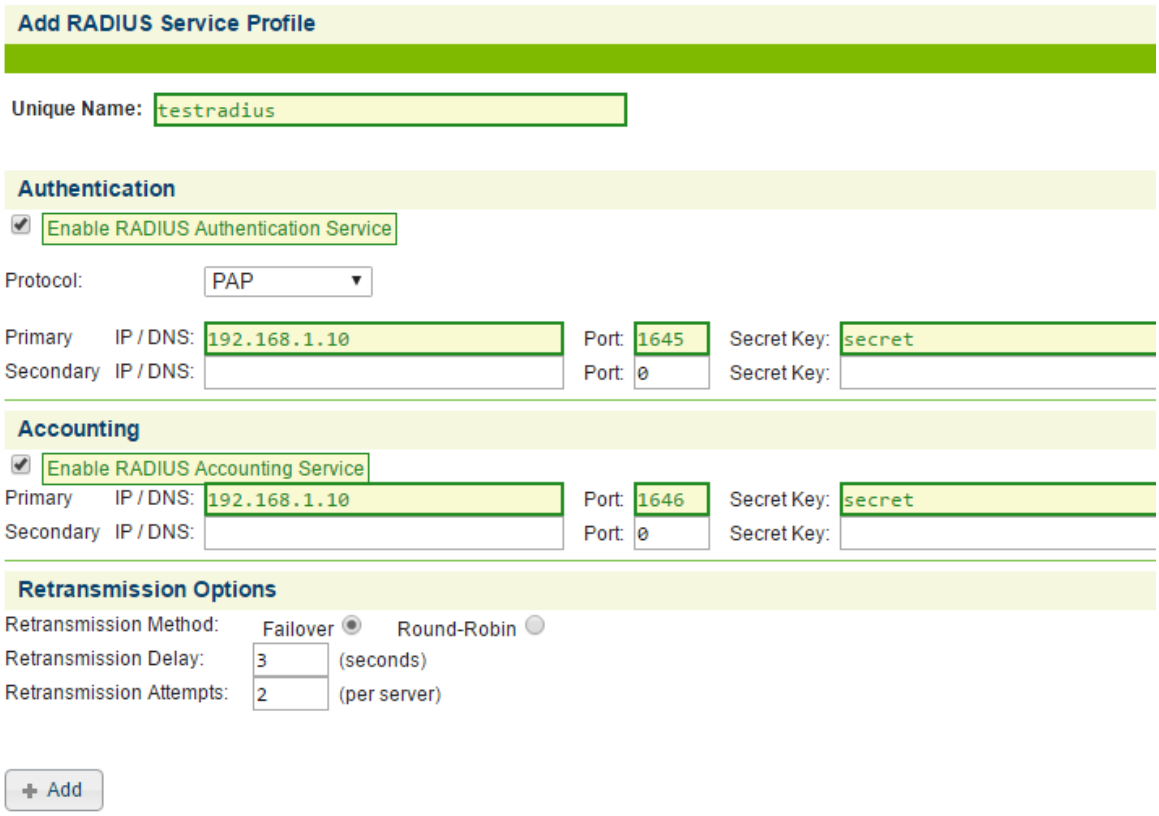
Purpose: How to configure the Centralized Management Authentication feature.

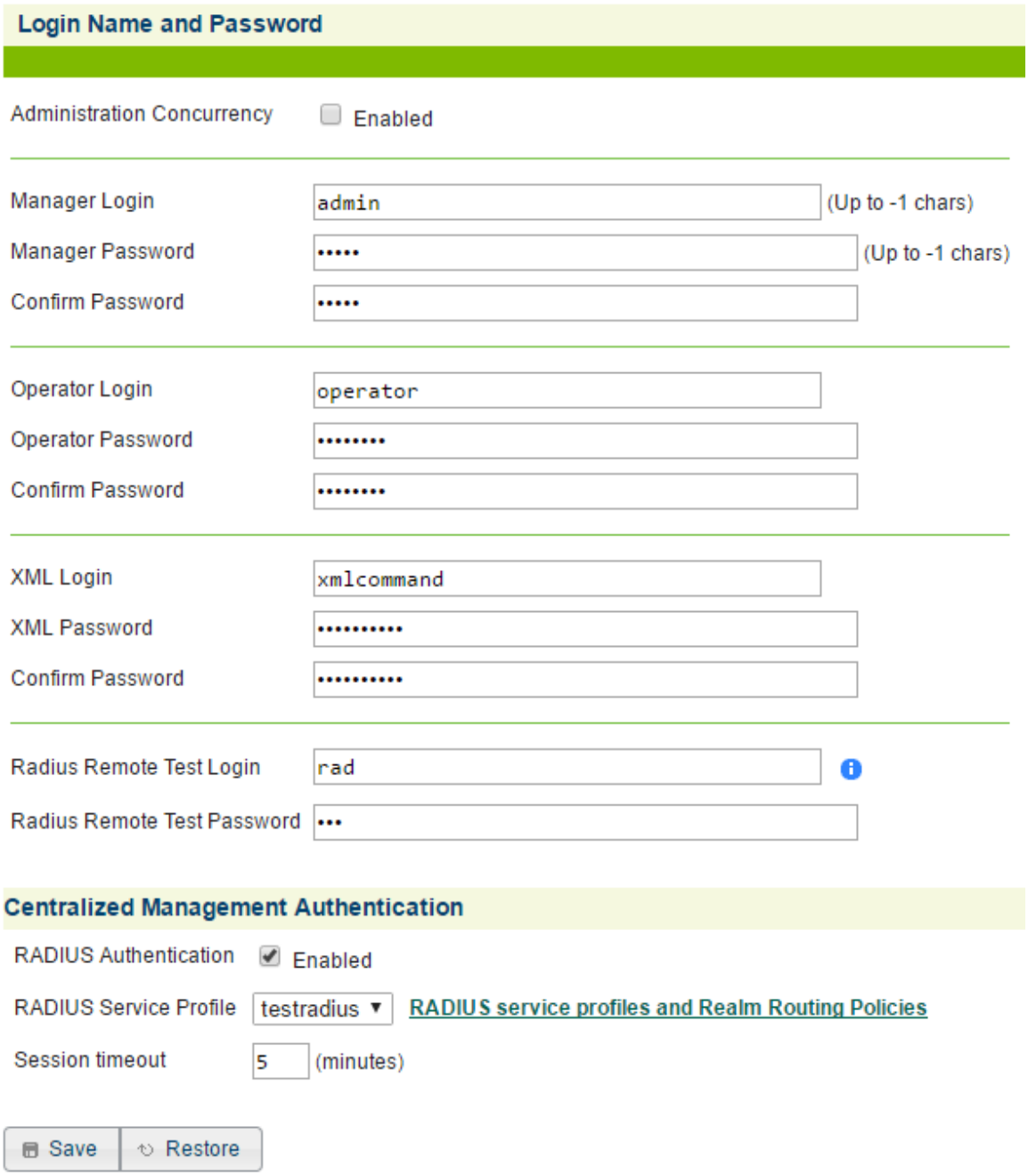
Beginning with version 7.1.008 administrators can extend the management login to authenticate against a Radius server, restricting the user to specific interfaces based on their user profile. With this feature you can allow/prevent access for users to the Web Management Interface, Telnet/CLI interface, FTP and the Remote Radius Login test page.

Step 1. Create a Radius profile.

Go to the Configuration/Realm Based Routing menu and select Add from the Radius Service Profiles section.



Step 2 – Enable Centralized Management Authentication.
Go to the System/Login screen, select the Radius profile and enable Radius Authentication.



Step 3 – Create the dictionary entry and user profile.

In the dictionary file on the radius server, you will need to add the Vendor Specific Attribute (VSA) for this feature. The Nomadix Vendor number is 3309 and this will need to be defined in the attribute as well.

Nomadix-Centralized- Management Attribute 18 string

In the User Profile, you will add this VSA to the user with the appropriate string value to set its access.

The following are examples of the settings you will most likely use the most. If you need other settings, contact Nomadix Technical Support (support@nomadix.com) for the correct string.

Admin/Manager access	v1,ALL:rwx grants read/write access to all management interfaces. This is the same as the manager login of the NSE.
Operator access	vx,ALL:r grants read-only access to all management interfaces. This is the same as the operator login of the NSE.
No FTP access	v1,FTPS: grants management access for WMI and Telnet/CLI and blocks ftp access to the NSE.