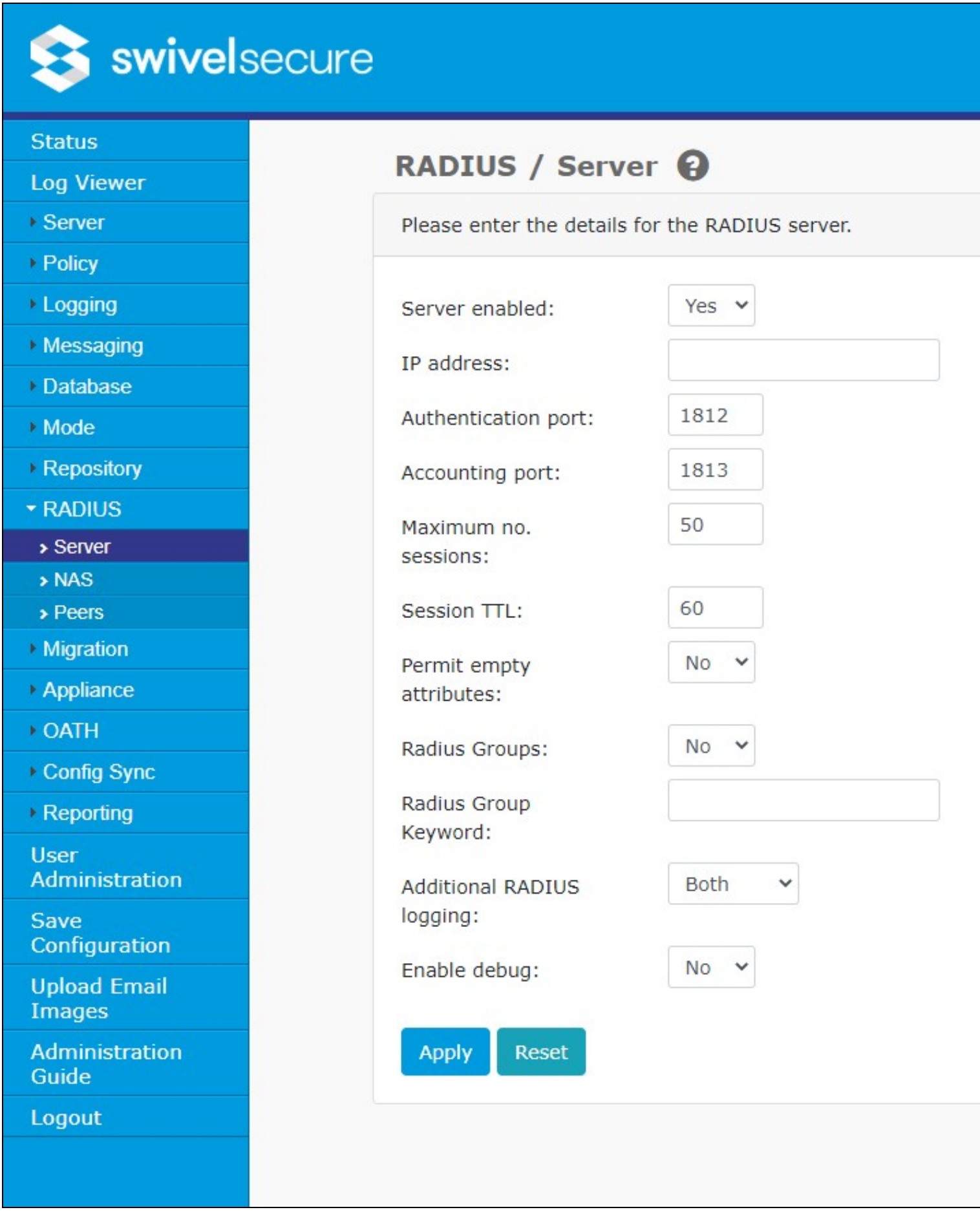
Swivel Core V4 RADIUS Menu

Contents

Server



- **Server enabled**: Enable/disable the RADIUS authentication interface.
- **IP address**: IP address of the network interface the RADIUS server will bind to. If no address is entered the RADIUS server will service requests on all interfaces. See below for details on using virtual IPs.

- **Authentication port**: Port for RADIUS authentication traffic.
- **Accounting port**: Port for RADIUS accounting traffic.
- **Maximum no. sessions**: Maximum number of concurrent RADIUS requests to be serviced at any one time.
- **Session TTL**: the time to live (TTL) in seconds for a single RADIUS session. Mainly relevant for two-stage authentication.
- **Permit empty attributes**: Enable/disable the servicing of RADIUS requests containing empty attributes. The RADIUS standard states that empty attributes should not be used, and by default these non-conforming requests will be dropped. Enabling this option will allow the RADIUS server to operate with clients who do not adhere to the standard and send empty attributes.
- **Radius Groups**: ; Allows group membership information to be passed back with the RADIUS response, using Vendor specific attributes defined at the NAS level
- **Radius Group Keyword**: This restricts the group membership information to only pass back the group names that include this keyword.
- **Additional RADIUS logging**: Enable/disable additional information, this will add the RADIUS entries for successful and failed RADIUS authentication attempts
- **Enable debug**: Enable/disable debugging of RADIUS authentication. Only use this option if you are attempting to resolve a problem as it will generate large log files.

NAS

swivelsecure

- Status
- Log Viewer
- Server
- Policy
- Logging
- Messaging
- Database
- Mode
- Repository
- RADIUS
  - Server
  - NAS
  - Peers
- Migration
- Appliance
- OATH
- Config Sync
- Reporting
- User Administration
- Save Configuration
- Upload Email Images
- Administration Guide
- Logout

RADIUS / NAS

Please enter the details for any RADIUS network access servers. A NAS
of the Sentry server via the RADIUS interface.

NAS:

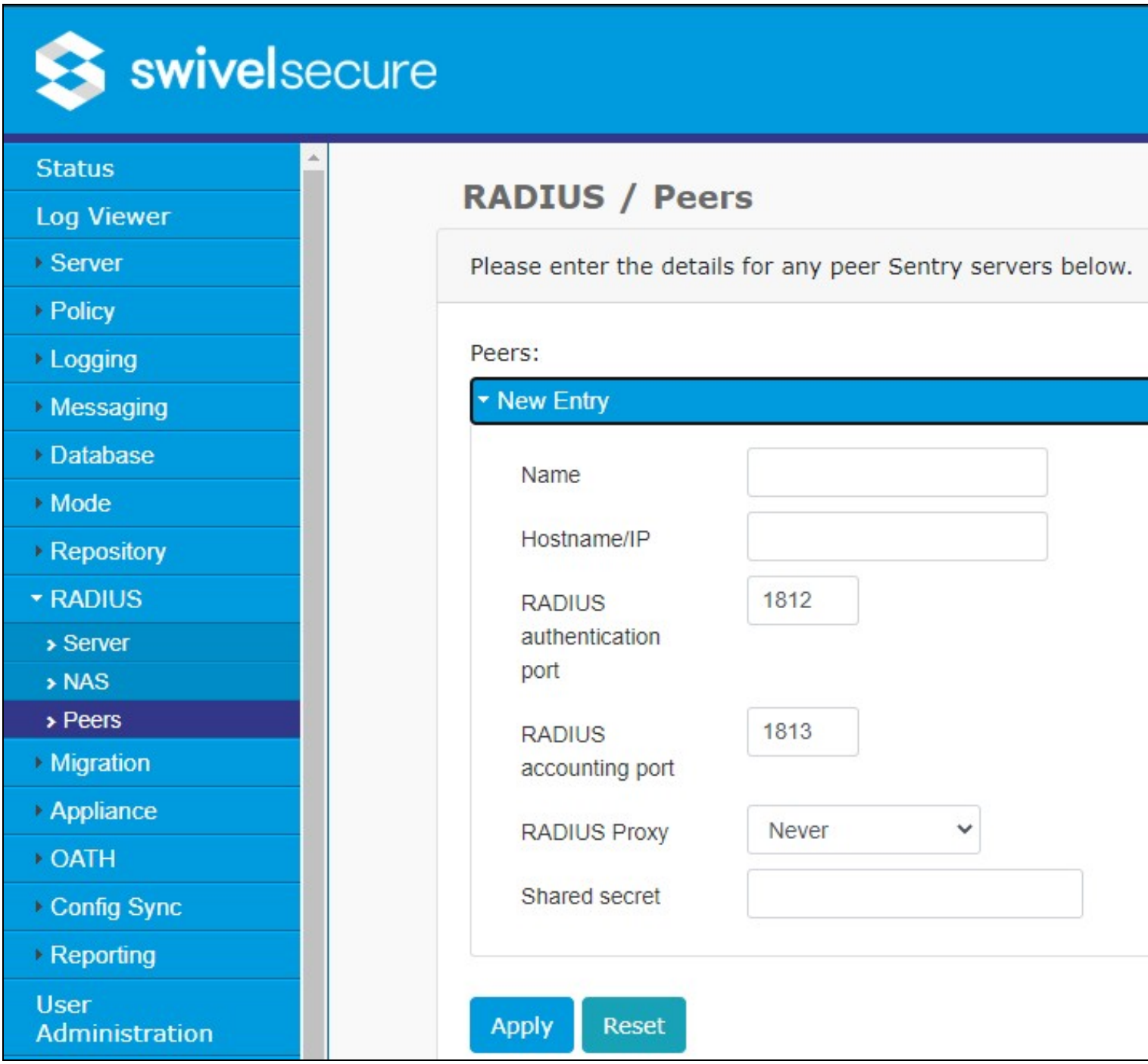
NetscalerSoc12

Name:	NetscalerSoc12
NAS Identifier:	
Hostname/IP:	NSoc12
Secret:	••••••••••••••••••••
Group:	---ANY---
EAP protocol:	None
Authentication Mode:	All
Vendor (Groups):	None
Change PIN warning:	No
Two Stage Auth:	No
Allow blank password at Stage One:	No
Send Security String after Stage One:	Yes
Even if User has Valid String:	Yes
Check password with repository:	No
Push Enabled:	No
Authenticate	No

For each configured NAS:

- **Name**: Friendly name to uniquely identify the NAS from others in the list.
- **Identifier**: Prior to version 4.1.0.6062, **Name** was called **Identifier**. The label was changed to avoid confusion with **NAS Identifier**.
- **NAS Identifier**: (from 4.1.0.6062) The NAS identifier as sent by the NAS. This can be blank, in which case it is ignored when evaluating Dynamic NAS entries.
- **Hostname/IP**: Host name or IP address of the NAS.
- **Secret**: Secret shared between the Swivel server and the NAS.
- **Group**: If a group is specified (eg an Active Directory group) only members of that group will be able to authenticate via this NAS. If --ANY-- is specified any Swivel user can authenticate via their NAS.
- **EAP protocol**: Allows RADIUS EAP protocol to be specified. Unfortunately, this does not currently work, and should always be set to "None".
- **Authentication Mode**: Defines what authentication modes are allowed via this NAS: All, Dual Channel or Single Channel. For example if an agent is dual channel only, a user cannot authenticate using a TURing image.
- **Vendor (Groups)**: Indicates what RADIUS parameters should be used to pass back group information. Select from the drop down list of Vendors
- **Change PIN Warning**: If this option is set when a user authenticates via RADIUS and their PIN is due to expire, rather than send a RADIUS-Accept packet Swivel will send a RADIUS-Challenge packet. This can be detected by Juniper (and other VPNs)to redirect the user to a change-PIN page
- **Two Stage Auth**: If this is set to Yes then Swivel expects the password to be pass in a RADIUS authentication request and if the password is correct, Swivel returns a RADIUS challenge prompting for the one-time code.
- **Allow blank password at State One**: Normally the first stage of the authentication is the password and normally this cannot be blank. However under certain circumstances a blank password in the first stage may be valid. This setting allows this.
- **Send Security String after Stage One**: If this is set to Yes (the default), then for two-stage authentication, a (dual channel) security string will be sent automatically after a correct password. Set this to No to use Single channel two-stage, or if security strings are sent in advance.
- **Even if User has Valid String**: The first stage of a two-stage authentication can be used as a trigger for sending a user a message with a one-time code or security string in it for authentication. Setting send security string after stage one will enable the sending id such a message to the user if they submit a valid password at stage one. If the user already has a valid security string that they can use then by setting ?Even if user has valid string? to no, the user will not be sent a new string if one is not required. This can be used with the Multiple Authentications per message setting to allow a user to reuse a message until it times out.
- **Check Password with Repository**: If Yes, then the Swivel server checks the password sent (one- or two-stage) against the user's repository (e.g. Active Directory).
- **One Touch Enabled**: If Yes, then the authentication method used will be One Touch instead of PAP. For more information about the OneTouch configuration on RADIUS please see How To Configure OneTouch On RADIUS
- **Authenticate non-user with just password**: for two-stage authentication, if this is set to Yes, then users with no Swivel account can check their password against the repository named in the Repository -> Servers section. No further authentication is required for such users.
- **Username attribute for repository**: If Check Password with repository is enabled, this defines which attribute is passed to the repository as the username. If blank, the account username and fully-qualified domain name (for LDAP) are both tried.
- **Allow alternative usernames**: If Yes, allows the username to be specified using an attribute other than the default username.
- **Alternative username attributes**: If "Allow alternative usernames" is enabled, specifies which user attributes are checked to match the user.
- **OTC timeout (mins)**: If > 0, the time (in minutes) before a user on the internal network needs to reauthenticate to Swivel. See the next option for what constitutes an internal user. External users must always reauthenticate to Swivel.
- **Internal IP ranges**: The IP ranges which constitute the internal network, when the OTC timeout option is active. These can be specified in CIDR notation, and multiple networks can be specified, separated by commas. For this feature to work, the RADIUS NAS must be capable of sending the calling station ID to the Swivel server as part of the RADIUS request. Otherwise, the NAS IP will be used.
- **Send username in challenge**: If enabled, the challenge sent by Swivel after a successful password in a two-stage authentication will consist of the username followed by a colon, then the usual challenge. This allows for customisation of NAS challenge pages where the username is not included in the page.

Peers



Peers are used to proxy authentication to other RADIUS servers. They are useful when moving from another authentication platform to Swivel: you can use them to pass the authentication request to the old RADIUS server if the account is not yet set up on Swivel.

The settings for each peer are as follows:

- **Name**: the name for the peer.
- **Hostname/IP**: the IP address or host of the peer.
- **RADIUS authentication port**: the port on the peer server to use to proxy authentication.
- **RADIUS accounting port**: the port on the peer server to use to proxy accounting.
- **RADIUS Proxy**: the conditions under which to proxy authentication
- **Shared secret**: the RADIUS shared secret

Using Virtual IPs

If you do not specify an IP address for the server, it will listen on all available IP addresses. This can cause problems when using a virtual IP (VIP) address. Although the server will receive requests on the VIP, it will respond on the physical IP. In most cases, this will cause the request to fail, because the NAS will not recognise the response, coming from a different IP. The fix for this is to specify the VIP as the server IP address. The down side to this is that if the appliance does not have the VIP, RADIUS will fail to start, so if the VIP switches from primary to standby, the standby will not be ready to accept RADIUS requests.

In versions 4.1.0.6062 onwards, this situation is handled: if you specify an IP address that is not currently available, RADIUS will not start. However, the appliance will regularly monitor the IP addresses, and if the IP address becomes available, it will automatically start the RADIUS server. Therefore, when using virtual IP addresses, the recommendation from this version forward is to specify the VIP on both appliances as the RADIUS server IP.

Dynamic NAS

From version 4.1.0.6062 onwards, Sentry has the ability to handle NAS entries dynamically. There are two aspects to this:

1. You can have two different NAS entries, with different settings, for the same NAS IP address, provided the NAS identifier is different. If one entry has a NAS ID, then all entries for that IP address must have one: there is no option for a "default" NAS ID if no other matches.
2. You can specify an IP address range, using CIDR notation, so that multiple IPs can use the same settings.