Configuring SBC for RADIUS Authentication

In this section:

Related articles:

- Show Table OAM
- Show Status OAM
- Admin - CLI
- Radius Authentication - CLI
- Administration - Users and Application Management
- Users and Application Management - Radius Authentication
- OAM - Radius Authentication

Overview

The SBC Core is configurable using CLI and EMA interfaces, and the access to these interfaces are authenticated using the user credentials. User credentials can be verified using local or external authentication. For local authentication, the user credentials are validated against locally stored user database and for external authentication, the user credentials are sent to an remote RADIUS server and authenticated.

Since 3.1 release, SBC Core platforms have included the ability to configure one remote server per SBC for the purpose of authenticating users from this server using Remote Authentication Dial In User Service (RADIUS) protocol. The username and encrypted password are sent to the remote RADIUS server in an ACCESS_REQUEST packet. The user is allowed/denied access to the SBC based on the response from the RADIUS server.

SBC users are currently segregated into the following groups which define the privileges of each user. Access to data/commands is allowed/prevented based on the group of the user who is trying to acquire the access.

- Administrator
- Operator
- FieldService
- Guest
- SecurityAuditor
- Calea

Since the RADIUS protocol does not provide a means to assign users to a group, the implementation currently hard codes every RADIUS authenticated user to the Administrator group.

The SBC Core supports the following RADIUS authentication improvements:

- Obtain Correct Privileges via RADIUS Transaction – When a user is authenticated using RADIUS, the correct privilege is obtained via RADIUS transaction itself using a Vendor Specific Attribute (VSA).
- Configure Multiple RADIUS Servers – Up to three RADIUS servers are now configurable per SBC.

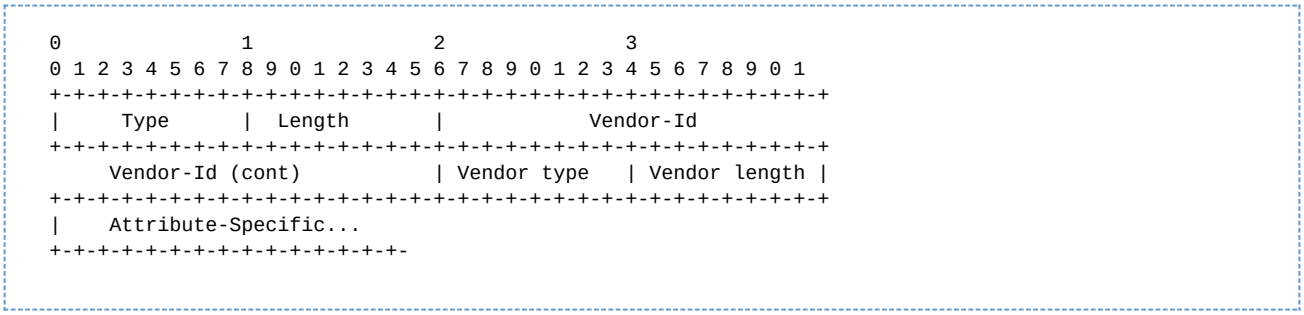
To configure RADIUS authentication for SBC Core, you must first enable external authentication and then configure the remote RADIUS server.

Obtain Correct Privileges via RADIUS Transaction

When a user is authenticated via RADIUS, the user is assigned to a group provided by the RADIUS server as part of the ACCESS_ACCEPT packet.

Note
If EMS is used for RADIUS authentication, the group information is passed in a VSA message as plain text after the vendor ID. The string start with "Sonus-Groups". No Vendor-specific formatting is used by EMS.

For SBC RADIUS authentication, RADIUS server is configured to return the group name using a VSA in ACCESS_ACCEPT packet. The VSA should be in the following format.



The Vendor-Id is a SMI Network Management Private Enterprise Code of the vendor Sonus as specified in RFC 2865.

- Vendor ID for Sonus is "2879".
- Vendor type can be "1" considering this is the first instance of using VSAs. Type "1" can be the identifier for a group name from server.
- Vendor length is the length of the group name itself. This is followed by a string consisting of a case-sensitive group name.

If the RADIUS server does not provide a group or provides a group name which is not present in the SBC in the ACCESS_ACCEPT response, the user is denied access, and a log is written to the SECURITY event log stipulating that the SBC received an invalid group name from the RADIUS server.

Configure Multiple RADIUS Servers

The SBC supports configuring up to three RADIUS servers per SBC with the addition of `radiusServer` and `retryCriteria` parameters to `radiusAuthentication` configuration object.

When more than one RADIUS server is configured and RADIUS authentication is attempted, the server configured with the least priority value is tried first. If fallback is configured, the inverse priority order is followed to pick the next server for authentication. SBC allows a configurable number of retries and time-outs before retry.

Once the SBC sends an ACCESS_REQUEST, it waits until a configured amount of time (`retryTimer`) before resending the ACCESS_REQUEST. After a configurable number of failed attempts (`retryCount`), the RADIUS server is marked as unavailable, or out of service (OOS) for a configured amount of time (`oosDuration`), and the SBC moves to the next configured RADIUS server based on the configured priority. Once all RADIUS servers are attempted and deemed unreachable (or no responses are received), the SBC falls back to Local Authentication (if Local Authentication is enabled).

Note
An administrator can manually return an OOS RADIUS server back into service by setting `radiusServer state` flag first to `disabled`, and then back to `enabled` setting.

SBC includes statistics to check the status of a RADIUS server, as well as the time when an unavailable server automatically becomes available again. See "radiusAuthentication" statistic details at Show Table OAM or Show Status OAM pages.

Note
- IPv6 configuration for RADIUS server is not supported at this time.
- Access-Challenge support is not included in this release.
- SBC only supports Password Authentication Protocol (PAP) authentication via RADIUS at this time.
- RADIUS authentication not supported for REST interface.

Enable Remote Authentication

To enable remote authentication:

1. Login to SBC CLI.

2. Change to the Configuration mode:

```
> configure private
```

3. Execute the following command:

```
% set system admin <system name> localAuthenticationEnabled false
externalAuthenticationEnabled true
```

Info
For CLI configuration details, refer to Admin - CLI. To enable the external authentication using EMA, refer to Administration - Users and Application Management.

Configure RADIUS Server

To configure the remote RADIUS Server:

1. Logon to SBC CLI.

2. Change to the Configuration mode:

```
> configure private
```

3. Execute the following command:

```
% set oam radiusAuthentication
 radiusServer <server name>
  mgmtInterfaceGroup <string>
  priority <#>
  radiusNasIp <x.x.x.x>
  radiusServerIp <x.x.x.x>
  radiusServerPort <#>
  radiusSharedSecret <8-128>
  state <disabled | enabled>
 retryCriteria
  oosDuration <# minutes>
  retryCount <#>
  retryTimer <# milliseconds>
```

Info
For CLI configuration details, refer to Radius Authentication - CLI. To configure RADIUS server using EMA, refer to Users and Application Management - Radius Authentication and OAM - Radius Authentication.

Info
Each SBC user is provided a private home directory for SFTP and files used by the CLI (refer to "Unique Home Directories" section on the page Managing SBC Core Users and Accounts). When using Radius authentication, users are only known to the Radius server and therefore do not have private home directories on the SBC. To create these home directories, you must also create Radius users on the SBC (refer to Local Authentication - CLI).

Rules to Configure Radius Shared Secret Key

The supports all alphabetical, numeric, and special characters for setting the `radiusSharedSecret` key.

The following characters in the key must be escaped while setting a `radiusSharedSecret` for configuring a RADIUS server:

- # (hash) anywhere in the key
- \ (backslash) anywhere in the key
- “ (double quotes) at the beginning or end of the key

For example,

- Un-escaped key: ThisIsARadiusKeyWithDoubleQuote”andBackSlash\Hash#andAdoubleQuoteAtTheEnd”
- Escaped string: ThisIsARadiusKeyWithDoubleQuote”andBackSlash\\Hash\#andAdoubleQuoteAtTheEnd\”