Manage External Authentication

This chapter describes the tasks related to external authentication in Cisco NCS 2000 SVO.

- Manage External Authentication, on page 1
- Limitations for RADIUS or TACACS Authentication, on page 2
- RADIUS Authentication, on page 2
- TACACS Authentication, on page 7

Manage External Authentication

From 12.1 onwards, SVO supports RADIUS and TACACS modes of external authentication. Ensure that you enable and use either RADIUS or TACACS authentication method. You can add a maximum of up to ten servers for each of RADIUS or TACACS on SVO.

There should be at least one RADIUS or TACACS authentication server that is configured for authentication to be enabled. In order to delete the last RADIUS or TACACS server, you must disable the external authentication first, and then delete the RADIUS or TACACS server.

When your login to SVO with the external authentication enabled, SVO first tries with the configured list of servers. If external authentication servers are not reachable, then SVO uses local authentication provided the local authentication is enabled on SVO.

To manage SVO, the following users are created:

- Local users (local authentication)—Specifies users who are created to manage SVO instances.
- External users (external authentication)—Specifies users who are created on the external authentication servers.

For more information related to users, see External Authentication Users for SVO.

The following table lists some external authentication scenarios that describe some possible authentication errors, causes, and actions.

Table 1: External and Local Authentication Scenarios

External and Local Authentication Combination	Possible Authentication Scenario	Possible Cause	Action to be Taken
• External Authentication Enabled and Local Authentication Disabled	Server denies authentication	External username or password is incorrect	Enter the correct username and password to log in to the system
	Server not reachable	IP address, shared secret or port number is not configured correctly although username or password could be correct	You are locked out of the system. Ensure that you have configured correct IP address, shared secret, and port number
• External authentication enabled and Local authentication enabled	Server denies authentication (although location authentication is enabled)	External username or password is incorrect	Enter the correct username and password to log in to the system Local authentication only works when the RADIUS or TACACS external servers are not reacheable
	Server not reachable (Local authentication is enabled)	IP address, shared secret, port number is not configured correctly although username or password could be correct	Use local authentication credentials to log in to SVO

Limitations for RADIUS or TACACS Authentication

- In Release 12.1, an external user list is maintained with username and its respective group (admin, editor, or viewer). The user list is populated whenever a new username is successfully authenticated. This user list is limited to 500 users. The delete (-) button available under the **External Authentication** tab is activated when 450 users limit is reached. Whenever you click the delete (-) button, the external users are cleared. In the user list, if the user limit is reached (500 users), then the new external user (501^{th} external user) cannot login to SVO.

  If you are logged in as external user and cleared the list, ensure that you must relogin on all the logged-in sessions. If you do not relogin, the system might not respond properly and information might not appear properly.

- In Release 12.1 external authentication is applicable only on SVO web user interface. External authentication using logging into the Netconf console is not supported.

RADIUS Authentication

Use the following tasks to manage RADIUS authentication on SVO.

Note Only an admin or superuser can manage RADIUS authentication on SVO.

1. Create RADIUS Server Entry on SVO, on page 3
2. Enable RADIUS Authentication, on page 4
3. Modify RADIUS Server Parameters, on page 4
4. Disable the RADIUS Authentication, on page 5
5. Delete the RADIUS Server from SVO, on page 5

Create RADIUS Server Entry on SVO

Use this task to create RADIUS server entry on SVO. Only an admin or superuser can add RADIUS server.

Before you begin

Log into the SVO Web Interface

Ensure that you have added SVO instances with RADIUS IP addresses in the Cisco Secure ACS server.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, perform the following steps:

a) Click the + button.

The **Create RADIUS server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the RADIUS server.
- **IP Address**—IPv4 or IPv6 address of the RADIUS server.
- **Authentication Port**—1812 is default for RADIUS. The range is from 0 to 65535. RADIUS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the RADIUS server.
- **Confirm Shared Secret**—Confirm the above shared secret for the RADIUS server.

c) Click **Add**.

The RADIUS server is added to the RADIUS server list on SVO.

Enable RADIUS Authentication

Use this task to enable RADIUS authentication. Only an admin or superuser can enable RADIUS authentication. You can add upto ten RADIUS servers on SVO.

Before you begin

- Log into the SVO Web Interface
- Create RADIUS Server Entry on SVO, on page 3

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, perform the following steps:

a) Check the **Enable RADIUS Authentication** check box to enable RADIUS server on SVO.

b) Check the **Enable node as final authentication when RADIUS server is reacheable** check box to enable the RADIUS server as a final authentication option.

Note When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

c) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the RADIUS server before retrying to contact the server.

d) In the **Attempts** field, enter the number of attempts to contact the first RADIUS server in the authentication list. If there is no response after the allotted number of attempts, then SVO tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify RADIUS Server Parameters

Use this task to modify RADIUS authentication settings. Only an admin or superuser can modify RADIUS server settings.

Before you begin

Log into the SVO Web Interface and Create RADIUS Server Entry on SVO, on page 3

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to edit from the list of available RADIUS servers and perform the following tasks:

a) Click the edit icon.

The **Modify RADIUS server** dialog box appears.

b) Edit the following fields:

- **IP Address**
- **Authentication Port**
- **Shared Secret**
- **Confirm Shared Secret**

c) Click **Save**.

Disable the RADIUS Authentication

Use this task to disable RADIUS authentication.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the External Authentication tab.

The External Authentication window appears.

Step 3 In the RADIUS Configuration area, perform the following steps:

a) Uncheck the **Enable RADIUS Authentication** check box to disable RADIUS authentication on SVO.

b) Uncheck the **Enable node as final authentication when RADIUS server is reacheable** check box to disable the RADIUS server as a final authentication option.

Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the RADIUS Server from SVO

Use this task to delete the RADIUS server entry from SVO.

Before you begin

Disable the RADIUS Authentication, on page 5

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to delete and click the **-** button.

A confirmation message appears.

Step 4 Click **Yes**.

Dual Factor Authentication

SVO external authentication is enhanced to support challenge-response based authentication using RSA Secure login with the Cisco Secure ACS server. The dual factor authentication provides secure way of authentication using passcode and token system. RSA provisioning is performed on the RADIUS server and the user-level access privileges are configured and maintained on the RADIUS server.

Note RSA configuration is not supported on the TACACS server.

Challenge Response RSA Authentication

In the SVO login page, enter username and passcode or token passcode, and click **Login**.

Based on scenarios (whether the user logged in for the first time or has been locked out), and if a **Challenge/Response** dialog box appears, then you must enter the new soft token PIN in the **Response** field and then click **Ok**.

If username is configured for RSA authentication, then RADIUS passes on user information to the RSA server.

RSA server validates the User ID and associated token. RADIUS passes info to SVO and user can log in through SVO with token and the username.

RSA Authentication Scenarios

RSA Authentication Using the New PIN Mode

To log in to SVO using new PIN mode, follow the procedure:

1. For a user with the dual factor authentication configured on the Cisco Secure ACS server, enter username and token code (code that is generated by the RSA token code generator) (without a PIN as the PIN is not generated).
2. Once you click the **Login** button, the **Challenge/Response** dialog box appears. In the **Challenge/Response** dialog box, enter the PIN based on the policy that is configured on the RSA server.

3. Once the PIN is sent, then there is an additional confirmation dialog box appears. Renter the same PIN and you can log into SVO.

RSA Authentication Using the New Token Mode

Next Token mode is applied when the authentication process requires an additional verification of the token code. In this mode, you are notified to enter the next token code. For example, you must wait for the number that is displayed on the passcode or token code generator to change, and then enter the new number (without the PIN).

To log in to SVO using the new token mode, follow the procedure:

1. Enter the user ID.
2. Enter the passcode (enter your PIN, Press Next arrow button, and the passcode appears on the token generator).
3. Wait until your token code changes. When prompted, enter the new token code.

RSA Authentication Using the Normal Login Mode

To log in to SVO using the normal login mode, follow the procedure:

1. PIN is generated. Enter the username and the PIN in the passcode generator.
2. Copy the passcode code and paste the passcode code in the password field of SVO, and click **Login**.

TACACS Authentication

Use the following tasks to manage TACACS authentication.

Note Only an admin or superuser can manage TACACS authentication on SVO.

1. Create TACACS Server Entry on SVO, on page 7
2. Enable TACACS Authentication, on page 8
3. Modify TACACS Server Parameters, on page 9
4. Disable the TACACS Authentication, on page 10
5. Delete the TACACS Server from SVO, on page 10

Create TACACS Server Entry on SVO

Use this task to create TACACS server entry on SVO. Only an admin or superuser can add TACACS server. You can add upto ten TACACS server.

Before you begin

Log into the SVO Web Interface

Ensure that you have added SVO instances with TACACS IP addresses in the Cisco Secure ACS server.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS** Configuration area, perform the following steps:

a) Click the **+** button.

The **Create TACACS server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the TACACS server.
- **IP Address**—IP address of the TACACS server.
- **Authentication Port**—49 is default for TACACS. TACACS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the TACACS server.
- **Confirm Shared Secret**—Confirm the above shared secret for the TACACS server.

c) Click **Add**.

The TACACS server is added to the TACACS server list on SVO.

Enable TACACS Authentication

Use this task to enable TACACS authentication.

Before you begin

- Log into the SVO Web Interface
- Create TACACS Server Entry on SVO, on page 7

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, perform the following steps:

a) Check the **Enable TACACS Authentication** check box to enable TACACS server on SVO.

b) Check the **Enable node as final authentication when TACACS server is reacheable** check box to enable the TACACS server as a final authentication option.

Note When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

c) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the TACACS server before retrying to contact the server.

d) In the **Attempts** field, enter the number of attempts to contact the first TACACS server in the authentication list. If there is no response after the allotted number of attempts, then SVO tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify TACACS Server Parameters

Use this task to modify TACACS authentication settings. Only an admin or superuser can modify TACACS server settings.

Before you begin

Log into the SVO Web Interface and Create TACACS Server Entry on SVO, on page 7

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External** Authentication tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, select the TACACS server to edit from the list of available TACACS servers and perform the following tasks:

a) Click the edit icon.

The **Modify TACACS server** dialog box appears.

b) Edit the following fields:

- **IP Address**
- **Authentication Port**
- **Shared Secret**
- **Confirm Shared Secret**

c) Click **Save**.

Disable the TACACS Authentication

Use this task to disable TACACS authentication.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, perform the following steps:

a) Uncheck the **Enable TACACS Authentication** check box to disable TACACS authentication on SVO.

b) Uncheck the **Enable node as final authentication when TACACS server is reacheable** check box to disable the TACACS server as a final authentication option.

Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the TACACS Server from SVO

Use this task to delete the TACACS server entry from SVO.

Before you begin

Disable the TACACS Authentication, on page 10

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, select the TACACS server to delete and click the **-** .

A confirmation message appears.

Step 4 Click **Yes**.