Configure Device Authorization Control (DAC) Management through Smart Network Application (SNA)

Objective

The Smart Network Application (SNA) system displays an overview of the network topology including detailed monitoring information for devices and traffic. SNA enables viewing and modifying of configurations globally on all supported devices in the network.

SNA has a feature known as the Device Authorization Control (DAC) that allows you to configure a list of authorized client devices in the network. DAC activates 802.1X features on SNA devices in the network and an embedded Remote Authentication Dial-In User Service (RADIUS) or RADIUS Host Server can be configured on one of the SNA devices. DAC is done via Media Access Control (MAC) authentication.

This article provides instructions on how to configure the DAC Management through SNA.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx550X Series

Note: Devices from the Sx250 Series can provide SNA information when they are connected to the network, but SNA cannot be launched from these devices.

Software Version

- 2.2.5.68

DAC Workflow

You can configure DAC management through the following steps:

- Activate DAC
- Configure RADIUS Server and Clients
- DAC List Management

Activate DAC

To access and activate DAC, follow these steps:

Step 1. Click the Options menu on the upper-left corner of the SNA page to show available options.
Step 2. Choose **Edit DAC mode**.

DAC Edit Mode is now activated. You should see the blue frame below the topology map and the control panel on the bottom of the screen.

Step 3. (Optional) To exit DAC Edit Mode, click the **Exit** button.

**Configure RADIUS Server and Clients**

Step 1. In the Topology view, choose one of the SNA devices and click on its **Options** menu.

Step 2. Click **+ Set as DAC server**.

Step 3. If the device has more than a single IP address, choose one of those addresses as the one to be used by DAC. In this example, 192.168.1.127 | Static is chosen.
Note: The list of addresses indicates whether the IP interface is static or dynamic. You will be warned that choosing a dynamic IP might cause unstable connection.

Step 4. Click DONE.
Note: When editing an existing DAC server, the address currently used by its clients is pre-selected.

The DAC RADIUS server is highlighted in solid black in the Topology view.

Step 5. Choose one of the SNA devices and click on its Options menu.

Note: If no clients are selected, you will be unable to apply the settings.

If a switch is already a client of the DAC RADIUS server, its IP address is in the NAS table of the RADIUS server and the RADIUS server is configured in its RADIUS server table with usage type 802.1X or all in priority 0. This switch is pre-selected.

If a client is chosen, which already has a RADIUS server configured for 802.1X other than the previously selected server, you will be notified that the proceedings will interrupt the existing RADIUS server operation.

If a client is chosen, which has a RADIUS server configured for 802.1X in priority 0 other than the previously-selected server, an error message is displayed and DAC is not configured on this client.

Step 6. Click + Set as client.
Step 7. Check the check box or check boxes of the port or ports from the client switch to apply 802.1X authentications.

**Note:** In this example, GE1/1, GE1/2, GE1/3, and GE1/4 ports are checked.
Note: The SNA recommends a list of all edge ports or all the ports that are not known to be connected to other switches or clouds.

Step 8. (Optional) Click the **Select Recommended** button to check all recommended ports.

Step 9. Click **DONE**. The DAC RADIUS client is highlighted in dashed blue in the Topology view.
Step 10. Click **Apply** to save the changes.

Step 11. Enter a Keystring that will be used by the DAC RADIUS server with all its clients on the network.

Note: In this example, Cisco1234 is used.
Step 12. (Optional) Toggle the button to **Auto Generated** to use an auto-generated Keystring.

Step 13. Click **Continue** on the upper-right hand corner of the page.

Step 14. Review the changes then click **APPLY CHANGES**.

Step 15. (Optional) Uncheck the **Save to startup configuration** check box if you do not wish to save the settings in the configuration file.

Step 16. (Optional) If you are using a Read Only account, you may be prompted to enter your credentials to continue. Enter the password in the **Password** field then click **SUBMIT**.
Step 17. The Status column should contain green check boxes that confirm successful application of changes. Click **DONE**.

After the DAC is configured, an alert is displayed whenever a new non-blacklisted device is rejected on the network through a DAC-enabled RADIUS server. You will be asked whether to add this device to the whitelist of authorized devices, or send it into a blacklist so that you are not alerted again.

When informing the user of the new device, SNA provides the MAC address of the device and the port which the device attempted to access the network.

If a rejection event is received from a device that is not a DAC RADIUS server, the message is ignored, and all further messages from this device for the next 20 minutes are ignored. After 20 minutes, SNA checks again if the device is a DAC RADIUS server. If a user is added to the whitelist, the device is added to the DAC group of all DAC servers. When this configuration is saved, you can choose whether to save this setting immediately to the startup configuration of the server. This option is selected by default.

Until a device is added to the whitelist, it is not allowed access to the network. You can view...
and change the white and black lists at any time, as long as a DAC RADIUS server is defined and reachable. To configure the DAC List Management, skip to DAC List Management.

When applying the DAC settings, you are presented with a report listing actions that will be applied to the participating devices. After you approve the changes, you can decide if the settings should additionally be copied to the startup configuration file of the configured devices. Finally, apply the configurations.

The report displays warnings if some steps of the DAC configuration process are missed, along with the status of the actions as handled by the devices.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The device identifiers (Host name or IP address)</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Possible actions for DAC server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enable RADIUS server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disable RADIUS server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update client list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Create RADIUS server group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Delete RADIUS server group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Possible actions for DAC client:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add RADIUS server connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update RADIUS server connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remove RADIUS server connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update 802.1x settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update interface authentication settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update interface host and session settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It is possible (and likely) for multiple actions to appear for each device. Each action can have its own status.</td>
<td></td>
</tr>
<tr>
<td>Warnings</td>
<td>Possible warnings for DAC server include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Selected IP interface is dynamic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Possible warnings for DAC clients include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device is already a client of a different RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No ports are selected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Warnings also contain links to the sections of the DAC where they can be addressed. Changes can be applied when warnings are present.</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>• Pending</td>
<td>When the status is a failure, the error message is shown for the action.</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Failure</td>
<td></td>
</tr>
</tbody>
</table>
**DAC List Management**

Once you have added client devices and selected which of their ports are to be authenticated, all unauthenticated devices detected on those ports are added to the list of Unauthenticated Devices.

DAC supports the following lists of devices:

- **White List** — Contains the list of all clients that can be authenticated.
- **Black List** — Contains the list of clients that must never be authenticated.

If you want devices and their ports to be authenticated, they must be added to the white lists. If you do not want them to be authenticated, no action is required as they will be added to the blacklist by default.

**Add Devices to Whitelist or Blacklist**

To add devices to the whitelist or blacklist, follow these steps:

Step 1. Click the **Options** menu on the upper-left corner of the SNA page to show available options.

Step 2. Choose **DAC List Management**.

Step 3. Click the **UNAUTHENTICATED DEVICES** tab. This page will display the list of all unauthenticated devices.
Note: Alternatively, you can click the DAC List Management System icon at the upper-right corner of the SNA page.

Step 4. (Optional) Check the check box next to the MAC address of the device or devices that you want to add to the whitelist and click **Add to Whitelist**.

Step 5. (Optional) Check the check box next to the MAC address of the device or devices that you want to add to the blacklist and click **Add to Blacklist**.
Step 6. (Optional) Check the check box next to the MAC address of the device or devices that you want to dismiss and click **Dismiss**.

**Note:** All packets entering on the ports on the device are authenticated on the RADIUS server.

You should now have added a device to the Whitelist or Blacklist.

**Manage Devices on Whitelist or Blacklist**

To manage the white or black lists, click the **WHITELIST** or **BLACKLIST** tab accordingly.
You can perform the following tasks in these pages:

- **Remove from list** — This action removes the chosen device or devices from the list.
- **Move to Blacklist or Move to Whitelist** — This action moves the chosen device or devices to the specified list.
- **Add a device** — This action adds a device to either the black or white list by entering its MAC address and clicking the **ADD+** button.
- **Search a device using MAC address** — Enter a MAC address and click the **Search** button.

You should now have managed the devices on the DAC list.