Using PowerOn Auto Provisioning

- Information About PowerOn Auto Provisioning, on page 1
- Guidelines and Limitations for POAP, on page 2
- Setting Up the Network Environment To Use POAP, on page 4
- Configuring a Switch Using POAP, on page 5
- Verifying the Device Configuration, on page 5
- Related Documents for POAP, on page 6

Information About PowerOn Auto Provisioning

PowerOn Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

When a Cisco Nexus Series switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode and checks for a USB device containing the configuration script file. If it finds one, it checks that device to see if it also contains the software image files and the switch configuration file.

If the switch does not find a USB device, or if the USB device does not contain the needed image files or switch configuration file, the switch also locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The switch then obtains the IP address of a TFTP server or the URL of an HTTP server from which it downloads the necessary configuration files.

Note The DHCP information is used only during the POAP process if any configuration files are unavailable on the USB device.

If the backup configuration file does not have the administrative username and the password, POAP causes a console lockout after completion. It is a mandatory step to add the username and the password in the configuration file.

Disabling POAP

POAP is enabled when there is no configuration in the system. It runs as a part of bootup. However, you can bypass POAP enablement during initial setup. If you want to disable POAP permanently (even when there is no configuration in the system), you can use the 'system no poap' command. This command ensures that POAP is not started during the next boot (even if there is no configuration). To enable POAP, use the 'system poap' command or the 'write erase poap' command. The 'write erase poap' command erases the POAP flag and enables POAP.

- Example: Disabling POAP

```
switch# system no poap
switch# sh boot
Current Boot Variables:
 sup-1
NXOS variable = bootflash:/nxos.9.2.1.125.bin
Boot POAP Disabled

POAP permanently disabled using 'system no poap'


Boot Variables on next reload:

sup-1
NXOS variable = bootflash:/nxos.9.2.1.125.bin
Boot POAP Disabled

POAP permanently disabled using 'system no poap'


switch# sh system poap
System-wide POAP is disabled  using exec command 'system no poap'
POAP will be bypassed on write-erase reload.
(Perpetual POAP cannot be enabled when system-wide POAP is disabled)
```

- Example: Enabling POAP

```
switch# system poap

switch# sh system poap

System-wide POAP is enabled
```

- Example: Erase POAP

```
switch# write erase poap
This command will erase the system wide POAP disable flag only if it is set.
Do you wish to proceed anyway? (y/n)  [n] y
System wide POAP disable flag erased.

switch# sh system poap
System-wide POAP is enabled
```

Guidelines and Limitations for POAP

- The Cisco Nexus switch software image must support POAP for this feature to function.
- POAP can be triggered even when the startup-config is present using the **boot poap enable** command.
- If a LACP Layer 3 port-channel is configured on an uplink device connected to the Cisco Nexus device that is being bootstrapped using POAP, the port-channel is not active because all the member links are in a suspended state. Therefore, the Cisco Nexus device that is being bootstrapped using POAP cannot

reach the DHCP server or any other infrastructure device needed for POAP. To work around this issue, configure a static L3 port-channel on the uplink device connected to the Cisco Nexus device that is being bootstrapped using POAP.

- If you use POAP to bootstrap a Cisco Nexus device that is a part of a vPC pair using static port-channels on the VPC links, the Cisco Nexus device activates all of its links upon POAP startup. The dually connected device at the end of the VPC links might start sending some or all of its traffic to the port-channel member links connected to the Cisco Nexus device, and the traffic would be lost.

  To work around this issue, you can configure LACP on the vPC links so that the links do not incorrectly start forwarding traffic to the Cisco Nexus device that is being bootstrapped using POAP.

- If you use POAP to bootstrap a Cisco Nexus device that is connected downstream to a Cisco Nexus Series 7000 device through a LACP port-channel, the Cisco Nexus 7000 Series device defaults to suspend its member port if it cannot bundle it as a part of a port-channel. To work around this issue, configure the Cisco Nexus 7000 Series device to not suspend its member ports using the no lacp suspend-individual command from interface configuration mode.

- Important POAP updates are logged in the syslog and are available from the serial console.

- Critical POAP errors are logged to the bootflash. The filename format is *date-time*_poap_*PID*_[init,1,2].log, where *date-time* is in the YYYYMMDD_hhmmss format and *PID* is the process ID.

- Script logs are saved in the bootflash directory. The filename format is *date-time*_poap_*PID*_script.log, where *date-time* is in the YYYYMMDD_hhmmss format and *PID* is the process ID.

- The Scheduler configuration cannot be replayed using POAP. The reason that the Scheduler configuration cannot be replayed is that it is associated with the user (for example "admin") that was logged in when the Scheduler configuration was created. Because the configuration replay using POAP is not associated with any specific user, the scheduler configuration cannot be replayed and fails.

  Instead of configuring the Scheduler, configure the Embedded Event Manager (EEM). An EEM configuration can be downloaded and replayed using POAP.

- You can bypass password and basic POAP configuration by using the **skip** option at the POAP prompt.

  When you use the **skip** option, no password will be configured for the **admin** user. The **copy running-config startup-config** command will be blocked until a valid password is set for the **admin** user.

- The certificates (for example SSL) or configuration that are needed to be applied to the switch should be present in the configuration file.

- The syntax of the poap_script.py file should be validated using any python validation tool before using the file for POAP. Otherwise, if the poap_script.py file is edited and has a syntax error, the POAP process will exit without giving an error.

- Beginning with NX-OS 7.0(3)I7(4), RFC 3004 (User Class Option for DHCP) is supported. This enables POAP to support user-class option 77 for DHCPv4 and user-class option 15 for DHCPv6. The text displayed for the user class option for both DHCPv4 and DHCPv6 is "Cisco-POAP".

  - With RFC 3004 (User Class Option for DHCP) support, POAP over IPv6 is supported on Nexus 3000 switches.

    - Beginning with NX-OS 9.2(2), POAP over IPv6 is supported on N3K-C36180YC-R and N3K-C3636C-R switches.

The POAP over IPv6 feature enables the POAP process to use IPv6 when IPv4 fails. The feature is designed to cycle between IPv4 and IPv6 protocols when a connection failure occurs.

- For secure POAP, ensure that DHCP snooping is enabled.
- To support POAP, set firewall rules to block unintended or malicious DHCP servers.
- To maintain system security and make POAP more secure, configure the following:
    - Enable DHCP snooping.
    - Set firewall rules to block unintended or malicious DHCP servers.
- POAP is supported on both MGMT ports and in-band ports.

Setting Up the Network Environment To Use POAP

SUMMARY STEPS

1. Modify the basic configuration script provided by Cisco or create your own script. For information, see the *Python Scripting and API Configuration Guide*.
2. Every time you make a change to the configuration script, ensure that you recalculate the MD5 checksum by running **# f=poap_nexus_script.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f** using a bash shell. For more information, see the *Python API Reference Guide*
3. (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device accessible to the switch.
4. Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. (This information is provided to the switch when it first boots.)
5. Deploy a TFTP or HTTP server to host the configuration script. In order to trigger the HTTP request to the server, prefix HTTP:// to the TFTP server name. HTTPS is not supported.
6. Add the URL portion into the TFTP script name to show correct path to the file name.
7. Deploy one or more servers to host the software images and configuration files.

DETAILED STEPS

Step 1 Modify the basic configuration script provided by Cisco or create your own script. For information, see the *Python Scripting and API Configuration Guide*.

Step 2 Every time you make a change to the configuration script, ensure that you recalculate the MD5 checksum by running # **f=poap_nexus_script.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f** using a bash shell. For more information, see the *Python API Reference Guide*

Step 3 (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device accessible to the switch.

Step 4 Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. (This information is provided to the switch when it first boots.)

You do not need to deploy a DHCP server if all software image and switch configuration files are on the USB device.

Step 5 Deploy a TFTP or HTTP server to host the configuration script. In order to trigger the HTTP request to the server, prefix HTTP:// to the TFTP server name. HTTPS is not supported.

Step 6 Add the URL portion into the TFTP script name to show correct path to the file name.

Step 7 Deploy one or more servers to host the software images and configuration files.

Configuring a Switch Using POAP

Before you begin

Make sure that the network environment is set up to use POAP. For more information, see the Setting Up the Network Environment To Use POAP, on page 4 section immediately preceeding this section.

SUMMARY STEPS

1. Install the switch in the network.
2. Power on the switch.
3. (Optional) If you want to exit POAP mode and enter the normal interactive setup script, enter **y** (yes).
4. (Optional) If you want to bypass password and basic POAP configuration, enter **skip**.

DETAILED STEPS

Step 1 Install the switch in the network.

Step 2 Power on the switch.

If no configuration file is found, the switch boots in POAP mode and displays a prompt that asks if you want to abort POAP and continue with a normal setup.

No entry is required to continue to boot in POAP mode.

Step 3 (Optional) If you want to exit POAP mode and enter the normal interactive setup script, enter **y** (yes).

The switch boots, and the POAP process begins.

Step 4 (Optional) If you want to bypass password and basic POAP configuration, enter **skip**.

POAP is aborted and password configuration is skipped.

What to do next

Verify the configuration.

Verifying the Device Configuration

To verify the configuration after bootstrapping the device using POAP, use one of the following commands:

Command	Purpose
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.
show time-stamp running-config last-changed	Displays the timestamp when the running configuration was last changed.

For detailed information about the fields in the output from these commands, see the Cisco Nexus command reference for your device.

Related Documents for POAP

Related Topic	Document Title
Configuration Script	*Cisco Nexus 3000 Series NX-OS Python API Reference Guide*
DHCP Options and BOOTP Vendor Extensions	RFC2132—http://tools.ietf.org/html/rfc2132
TFTP Server Address Option for DHCPv4	RFC5859—http://tools.ietf.org/html/rfc5859