



Zero-Touch Provisioning

- [Zero-Touch Provisioning Overview, on page 1](#)
- [DHCP Server Configuration for Zero-Touch Provisioning, on page 2](#)
- [DHCPv6 Support , on page 2](#)
- [Sample Zero-Touch Provisioning Configurations, on page 3](#)
- [Additional References for Zero-Touch Provisioning, on page 13](#)
- [Feature Information for Zero-Touch Provisioning, on page 14](#)

Zero-Touch Provisioning Overview

Zero-touch provisioning (ZTP) provides open bootstrap interfaces to automate network device provisioning in heterogeneous network environments.

When a device that supports ZTP starts up, and does not find the startup configuration (during initial installation), the device enters the zero-touch provisioning mode. The device searches for a DHCP server, bootstraps itself with its interface IP address, gateway, and Domain Name System (DNS) server IP address, and enables Guest Shell. The device then obtains the IP address or URL of an HTTP or a TFTP server, and downloads the Python script from an HTTP or a TFTP server to configure the device.

ZTP is supported through data ports on these platforms.

- IE-9300
- IE-3500/IE-3500H

Guest Shell provides the environment for the Python script to run. Guest Shell runs the downloaded Python script and applies an initial configuration to the device.



Note The Guest Shell used for the ZTP process does not require an SD card to be present.



Note If ZTP fails, the device falls back on AutoInstall to load the configuration file. For more information, see IIoT Autoinstall Configuration Guide.

DHCP Server Configuration for Zero-Touch Provisioning

In ZTP, a DHCP server must be running on the same network as the new device that is being provisioned.

When the new device is switched on, it retrieves the IP address information of the HTTP or TFTP server where the Python script resides, and the folder path of the Python script from the DHCP server. For more information on Python Scripts, see the *Python API* chapter.

The DHCP server responds to DHCP discovery events with the following options:

- Option 150: (Optional) Contains a list of IP addresses that point to the HTTP or TFTP server in the management network that hosts the Python scripts to be run.
- Option 67: Contains the Python script file path in the HTTP/TFTP server.

After receiving these DHCP options, the device connects to the HTTP or TFTP server, and downloads the Python script. At this point, because the device does not have a route to reach the HTTP or TFTP server, it uses the default route provided by the DHCP server.

DHCP Client Behavior

From Cisco IOS XE Amsterdam 17.2.1 release onwards, the device product identification (PID), Cisco Network Plug and Play (PnP), the serial number, and the MAC address is set in the DHCP client options.

These client options can be used as variables at the DHCP server. The DHCP client options can be used to identify the device and send a unique Python file through option 67 or boot filename.

Table 1: DHCP Client Options

Device Information	DHCPv4	DHCPv6
Product ID	124	16/toggles
Serial number	61/toggles	16/toggles
MAC address	61/toggles	1
Cisco Network PnP	60	15

DHCPv6 Support

In Cisco IOS XE Fuji 16.9.1, DHCP Version 6 support is added to the Zero-Touch Provisioning feature. DHCPv6 is enabled by default, and will work on any device that boots without a startup configuration.

DHCPv6 is supported by both TFTP and HTTP download of Python scripts. If this download fails, the device reverts to the initial or factory settings (without any configuration). For both DHCPv4 and DHCPv6 to work, the correct HTTP or TFTP file path must be available in the DHCP configuration.

There can be scenarios where the same interface can have both IPv4 and IPv6 addresses, or two different interfaces in a network—one can receive IPv4 traffic and the other, IPv6 traffic. We recommend that you use either the DHCPv4 or DHCPv6 option in your deployment.

The following is a sample DHCPv4:

```

host <hostname> {
    hardware ethernet xx:xx:xx:xx:xx:xx;
    option dhcp-client-identifier "xxxxxxxxxxxxxx";
    option host-name "<hostname>".
    option log-servers x.x.x.x;
    fixed-address x.x.x.x;
    if option vendor-class-identifier = "..." {
        option vendor-class-identifier "...";
        if exists user-class and option user-class = "iPXE" {
            filename "http://x.x.x.x/.../<image>";
        } else {
            filename "http://x.x.x.x/.../<script-name>";
        }
    }
}

```

The following is a sample ISC DHCPv6 server configuration:

```
option dhcp6.bootfile-url "http://[2001:DB8::21]/sample_day0_script.py";
```

Sample Zero-Touch Provisioning Configurations

Sample DHCP Server Configuration on an In-Band Port Using TFTP Copy

The following is a sample DHCP server configuration using TFTP copy when the DHCP server is connected through the in-band port on a device:

```

Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 150 ip 203.0.113.254
Device(config-dhcp)# option 67 ascii /sample_python_dir/python_script.py
Device(config-dhcp)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# no ip dhcp client request tftp-server-address
Device(config-if)# end

```

Sample DHCP Server Configuration on an In-Band Port Using HTTP Copy

The following is a sample DHCP server configuration using HTTP copy when the DHCP server is connected through the in-band port on a device:

```

Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii http://192.0.2.1:8000/sample_python_2.py

```

```
Device(config-dhcp)# end
```

Sample DHCP Server Configuration on a Linux Ubuntu Device

The following sample DHCP server configuration shows that the server is either connected to the management port or the in-band port in a device, and that a Python script is copied from a TFTP server.

```
root@ubuntu-server:/etc/dhcp# more dhcpd.conf
subnet 10.1.1.0 netmask 255.255.255.0 {
  range 10.1.1.2 10.1.1.255;
  host 3850 {
    fixed-address 10.1.1.246 ;
    hardware ethernet CC:D8:C1:85:6F:00;
    option bootfile-name !<opt 67> "/python_dir/python_script.py";
    option tftp-server-name !<opt 150> "203.0.113.254";
  }
}
```

The following sample DHCP configuration shows that a Python script is copied from an HTTP server to the device:

```
Day0_with_mgmt_port_http
-----
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.2 192.168.1.255;
  host C2-3850 {
    fixed-address 192.168.1.246 ;
    hardware ethernet CC:D8:C1:85:6F:00;
    option bootfile-name "http://192.168.1.46/sample_python_2.py";
  }
}
```

After the DHCP server starts running, you must start the management network-connected device. The rest of the configuration is automatic.

Sample DHCPv6 Server Configuration on a Management Port Using TFTP Copy

The following is a sample configuration using TFTP copy when the DHCPv6 server is connected through the management port on a device:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool ztp
Device(config-dhcpv6)# address prefix 2001:DB8::1/64
Device(config-dhcpv6)# domain-name cisco.com
Device(config-dhcpv6)# bootfile-url tftp://[2001:db8::46]/sample_day0_script.py
Device(config-dhcpv6)# exit
Device(config)# interface vlan 20
Device(config-if)# ipv6 dhcp server ztp
Device(config-if)# end
```

Sample Python Provisioning Script

The following is a sample Python script that can be used from either an HTTP server or a TFTP server:

```
print "\n\n *** Sample ZTP Day0 Python Script *** \n\n"

# Importing cli module
import cli

print "\n\n *** Executing show platform *** \n\n"
cli_command = "show platform"
cli.executecli(cli_command)

print "\n\n *** Executing show version *** \n\n"
cli_command = "show version"
cli.executecli(cli_command)

print "\n\n *** Configuring a Loopback Interface *** \n\n"
cli.configurecli(["interface loop 100", "ip address 10.10.10.10 255.255.255.255", "end"])

print "\n\n *** Executing show ip interface brief *** \n\n"
cli_command = "sh ip int brief"
cli.executecli(cli_command)

print "\n\n *** ZTP Day0 Python Script Execution Complete *** \n\n"
```

Boot Log for Cisco IE9300 Series Switches

This section displays sample Zero-Touch Provisioning boot logs.



Note The logs shown here are for illustrative purposes; your actual console output may differ.

The following example shows how to configure the device for Day Zero provisioning:

```
Initializing Hardware...
Aikido Bus encryption enabled

System Bootstrap, Version v26_1_1r [FC1], RELEASE SOFTWARE (P)
Compiled Wed 04/22/2026 15:48:53 by rel

Current ROMMON image : Primary
IE-9310-16P8S4X platform with 4194304 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0

<<</o/p truncated >>>
```

Please read the following carefully before proceeding. By downloading, installing, and/or using any Cisco software product, application, feature, license, or license key (collectively, the "Software"), you accept and agree to the following terms. If you do not agree, do not proceed and do not use this Software.

This Software and its use are governed by Cisco's General Terms and any relevant supplemental terms found at <https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html>. If you have a negotiated agreement with Cisco that includes this Software, the terms of that agreement apply as well. In the event of a conflict, the order of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to the Software is valid only for the duration of the specified term, or in the case of a subscription-based license, only so long as all required subscription payments are current and fully paid-up. While Cisco may provide you licensing-related alerts, it is your sole responsibility to monitor your usage. Using Cisco Software without a valid license is not permitted and may result in fees charged to your account. Cisco reserves the right to terminate access to, or restrict the functionality of, any Cisco Software, or any features thereof, that are being used without a valid license.

```
% Failed to initialize nvram
% Failed to initialize backup nvram
```

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco IE-9310-16P8S4X (ARM64) processor with 536215K/3071K bytes of memory.
Processor board ID FDO2825J0JB
2048K bytes of non-volatile configuration memory.
4012312K bytes of physical memory.
523264K bytes of Crash Files at crashinfo:.
2650112K bytes of Flash at flash:.
```

```
Base Ethernet MAC Address      : 70:da:48:e3:d1:80
Motherboard Assembly Number    : 73-103494-02
Motherboard Serial Number      : FDO28220ESW
Model Revision Number          : 13
Motherboard Revision Number    : 09
Model Number                   : IE-9310-16P8S4X
System Serial Number           : FDO2825J0JB
IO FPGA version                : 0xc0e
Data Path FPGA version         : 0x801
```

```
Autoinstall: No start-up config. Triggering swap drive
Config and Image is not found in any media
Autoinstall: swap drive fail, continue autoinstall
```

```
No startup-config, starting autoinstall/pnp/ztp...
```

```
Autoinstall will terminate if any input is detected on console
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv4 on Vlan1
```

```
Autoinstall trying DHCPv6 on Vlan1
```

```
Acquired IPv4 address 29.29.29.30 on Interface Vlan1
Received following DHCPv4 options:
```

```
domain-name      : cisco.com
bootfile         : http://29.29.29.1/ztp_cli.py
dns-server-ip    : 10.10.10.10
si-addr          : 29.29.29.1
```

OK to enter CLI now...

pnnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnnp-discovery

Attempting bootfile http://29.29.29.1/ztp_cli.py

CCO server (devicehelper-ng.cisco.com.) can't be resolved (1/5) by (pid=445, pname=PnP Agent Discovery, time=07:04:59 UTC Thu Jun 18 2026)

CCO server (devicehelper-ng.cisco.com.) can't be resolved (2/5) by (pid=445, pname=PnP Agent Discovery, time=07:05:15 UTC Thu Jun 18 2026)

CCO server (devicehelper-ng.cisco.com.) can't be resolved (3/5) by (pid=445, pname=PnP Agent Discovery, time=07:05:31 UTC Thu Jun 18 2026)

Loading http://29.29.29.1/ztp_cli.py

CCO server (devicehelper-ng.cisco.com.) can't be resolved (4/5) by (pid=445, pname=PnP Agent Discovery, time=07:05:47 UTC Thu Jun 18 2026)

Loading http://29.29.29.1/ztp_cli.py The process for the command is not responding or is otherwise unavailable

day0guestshell activated successfully

Current state is: ACTIVATED

day0guestshell started successfully

Current state is: RUNNING

Guestshell enabled successfully

CCO server (devicehelper-ng.cisco.com.) can't be resolved (5/5) by (pid=445, pname=PnP Agent Discovery, time=07:07:37 UTC Thu Jun 18 2026)

Welcome to ZTP!

Python version is

3.9.25 (main, Mar 9 2026, 00:00:00)
[GCC 11.5.0 20240719 (Red Hat 11.5.0-14)]

Hello!Changing the hostname

Line 1 SUCCESS: hostname 9300ZTP

NAME: "Switch 1", DESCR: "IE-9310-16P8S4X"

PID: IE-9310-16P8S4X , VID: V00 , SN: FDO2825J0JB

NAME: "Switch 1 - Power Supply B", DESCR: "Switch 1 - Power Supply B"

PID: PWR-RGD-AC-DC-H , VID: V01 , SN: DTH281901ZH

<Output truncated>

.
. .
.

Building configuration...

Current configuration : 84 bytes

```

!
interface Vlan1
 ip dhcp client client-id ascii FDO2825J0JB
 ip address dhcp
end

app-hosting appid day0guestshell
app-vnic AppGigabitEthernet port 1 trunk
vlan 4094 guest-interface 0
 guest-ipaddress 192.168.2.2 netmask 255.255.255.0
app-default-gateway 192.168.2.1 guest-interface 0
name-server0 10.10.10.10

Smart Licensing Status
=====
Smart Licensing is ENABLED
License Conversion:
  Automatic Conversion Enabled: True
  Last Data Push: <none>
  Last File Export: <none>
Export Authorization Key:
  Features Authorized:
    <none>
Utility:
  Status: DISABLED
Smart Licensing Using Policy:
  Status: ENABLED
  Reporting Mode: STANDARD
Account Information:
  Smart Account: <none>
  Virtual Account: <none>
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured
  VRF: <empty>
Miscellaneous:
  Custom Id: <empty>
Policy:
  Policy in use: CISCO default
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
Usage Reporting:

```

```
Last ACK received: <none>
Next ACK deadline: <none>
Reporting push interval: 0
Next ACK push check: <none>
Next report push: Jun 18 07:04:58 2026 UTC
Last report push: <none>
Last report file write: <none>
Trust Code Installed: <none>
License Usage
=====
No licenses in use
Product Information
=====
UDI: PID:IE-9310-16P8S4X,SN:FDO2825J0JB
Agent Version
=====
Smart Agent for Licensing: 8.0.6/51707fd08
License Authorizations
=====
Last Data Push: <none>
Last File Export: <none>
Overall status:
  Active: PID:IE-9310-16P8S4X,SN:FDO2825J0JB
  Status: NOT INSTALLED
Purchased Licenses:
  No Purchase Information Available
Usage Report Summary:
=====
Total: 0,  Purged: 0
Total Acknowledged Received: 0,  Waiting for Ack: 0
Available to Report: 2  Collecting Data: 0
Device Enforcement State:
NOT APPLICABLE
Product Analytics Report Summary:
=====
Product Analytics: AVAILABLE
Not Available Reason: <empty>
Total current Product Analytics reports: 0

Building configuration...
Current configuration : 9916 bytes
!
! Last configuration change at 07:07:52 UTC Thu Jun 18 2026
!
version 26.1
service timestamps debug datetime msec year
service timestamps log datetime msec year
!
hostname 9300ZTP -> host name changed as result of ZTP (python) script
!
!
logging console emergencies
no aaa new-model
rep ztp
rep autodisc
!
!
!
!

ZTP complete!
```

```
Guestshell destroyed successfully
Script execution success!
```

ZTP has completed the script execution and user is returned to the console prompt!

```
*Jun 18 2026 07:09:34.295: yang-infra: Default hostkey created (NETCONF_SSH_RSA_KEY)
*Jun 18 2026 07:09:34.775: yang-infra: Netconf SSH RSA key generated
```

Boot Log for Cisco IE3500 Series Switches

This section displays sample Zero-Touch Provisioning boot logs.



Note The logs shown here are for illustrative purposes; your actual console output may differ.

The following example shows how to configure the device for Day Zero provisioning:

```
Initializing Hardware...
Configuring SUP-FPGA bitstream [version 85]:
.....

System Bootstrap, Version v26_1_1r [FC1], RELEASE SOFTWARE (P)
Compiled Mon 03/16/2026 15:45:23 by rel

Current ROMMON image : Primary
IE-3500H-8T platform with 4194304 (8388608) Kbytes of main memory

boot: failed to load bs:
loading bootloader image failed: read failed
Validate Chip guard ... Success.
Preparing to autoboot. [Press Ctrl-C to interrupt] 0
boot: attempting to boot from [flash:ie35xx-universalk9.26.01.01.SPA.bin]
boot: reading file ie35xx-universalk9.26.01.01.SPA.bin
=====
Verifying image flash:ie35xx-universalk9.26.01.01.SPA.bin
WARNING: DEV-Keys are installed in box
SecureBoot: REL KEY signed image verified successfully!
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software [IOSXE], Cisco L3 Switch Software (IE35xx_IOSXE), Version 26.01.1, RELEASE

SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2026 by Cisco Systems, Inc.
Compiled Tue 07-Apr-26 18:20 by mcpre

This software version supports only Smart Licensing as the software licensing mechanism.

% Failed to initialize nvram
% Failed to initialize backup nvram

FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco IE-3500H-8T (ARM64) processor with 539974K/3071K bytes of memory.
Processor board ID FCW2846Y0PG
2048K bytes of non-volatile configuration memory.
4011280K bytes of physical memory.
524288K bytes of Crash Files at crashinfo:.
5242880K bytes of Flash at flash:.

Base Ethernet MAC Address	: 28:b5:91:96:7f:80
Motherboard Assembly Number	: 73-103455-03
Motherboard Serial Number	: FOC2842056S
Model Revision Number	: 12
Motherboard Revision Number	: 06
Model Number	: IE-3500H-8T
System Serial Number	: FCW2846Y0PG
SUP FPGA version	: 0x55

Autoinstall: No start-up config. Triggering swap drive
Config and Image is not found in any media
Autoinstall: swap drive fail, continue autoinstall

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

INSECURE DYNAMIC WARNING - Module: RCMD, Command: ip rcmd domain-lookup, Reason: No encryption is configured, Remediation: This is a legacy feature, please consider disabling it, Submode: configure, Parent CLI: Not Applicable

INSECURE DYNAMIC WARNING - Module: NTP, Command: ntp allow mode control, Reason: NTP allow mode control renders device susceptible to DDoS attacks, Remediation: If control mode needs to be enabled, configure a higher rate-limit delay and monitor the flow, Submode: configure, Parent CLI: Not Applicable

INSECURE DYNAMIC WARNING - Module: TELNET, Command: ip telnet comports enable, Reason: IP traffic is not encrypted, Remediation: Migrate to secure SSH-based remote access, Submode: configure, Parent CLI: Not Applicable

INSECURE DYNAMIC WARNING - Module: IP, Command: ip forward-protocol udp tftp, Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Remediation: This is a legacy feature, please consider disabling it, Submode: configure, Parent CLI: Not Applicable

Autoinstall trying DHCPv4 on Vlan1

Autoinstall trying DHCPv6 on Vlan1

INSECURE DYNAMIC WARNING - Module: SSH, Command: crypto key generate rsa modulus 2048 label TP-self-signed-3535075152, Reason: An SSH hostkey has been provisioned on the device with insufficient key length, Remediation: Please provision an SSH RSA hostkey with minimum modulus size of 3072 bits for enhanced security, Submode: exec, Parent CLI: Not Applicable

```

Acquired IPv4 address 29.29.29.19 on Interface Vlan1
Received following DHCPv4 options:
    domain-name      : cisco.com
    bootfile         : http://29.29.29.1/ztp_cli.py
    dns-server-ip    : 10.10.10.10
    si-addr          : 29.29.29.1

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

Attempting bootfile http://29.29.29.1/ztp_cli.py

Loading http://29.29.29.1/ztp_cli.py
Loading http://29.29.29.1/ztp_cli.py
CCO server (devicehelper.cisco.com.) can't be resolved (1/5) by (pid=444, pname=PnP Agent
Discovery, time=19:23:10 UTC Fri Jun 12 2026)

CCO server (devicehelper.cisco.com.) can't be resolved (2/5) by (pid=444, pname=PnP Agent
Discovery, time=19:23:26 UTC Fri Jun 12 2026)

CCO server (devicehelper.cisco.com.) can't be resolved (3/5) by (pid=444, pname=PnP Agent
Discovery, time=19:23:42 UTC Fri Jun 12 2026)

CCO server (devicehelper.cisco.com.) can't be resolved (4/5) by (pid=444, pname=PnP Agent
Discovery, time=19:23:58 UTC Fri Jun 12 2026)

CCO server (devicehelper.cisco.com.) can't be resolved (5/5) by (pid=444, pname=PnP Agent
Discovery, time=19:24:14 UTC Fri Jun 12 2026)
day0guestshell activated successfully
Current state is: ACTIVATED
day0guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully

Welcome to ZTP!

Python version is

3.6.8 (default, Dec 22 2020, 19:05:50)
[GCC 8.4.1 20200928 (Red Hat 8.4.1-1)]

Hello!Changing the hostname

Line 1 SUCCESS:  hostname 3500ZTP

Building configuration...
Current configuration : 8512 bytes
!
! Last configuration change at 19:24:34 UTC Fri Jun 12 2026
!
version 26.1
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname 3500ZTP  -> Hostname changed due to ZTP script
!
!
```

```
logging console emergencies
no aaa new-model
rep ztp
rep autodisc
!
!
!
!
login on-success log
ipv6 nd cache expire 14400
vtp domain cisco
vtp mode off
!
!
!
!

ZTP complete!

Guestshell destroyed successfully
Script execution success!

Press RETURN to get started!
```

Additional References for Zero-Touch Provisioning

Standards and RFCs

Standard/RFC	Title
RFC 5652	Cryptographic Message Syntax (CMS)
RFC 8040	RESTCONF Protocol
RFC 8366	A Voucher Artifact for Bootstrapping Protocols
RFC 8572	Secure Zero Touch Provisioning (SZTP)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	https://www.cisco.com/c/en/us/support/index.html

Feature Information for Zero-Touch Provisioning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Zero-Touch Provisioning

Feature Name	Release	Feature Information
Zero-Touch Provisioning	Cisco IOS XE 17.18.1	To address network provisioning challenges, Cisco introduces a zero-touch provisioning model. This feature was implemented on the following platforms: • Cisco IE-9300 Series Switches • Cisco IE-3500/IE-3500H Series Switches