



Specialized DHCP deployments and client customization

This chapter explores advanced client-side configurations and introduces specialized DHCP functionalities such as Single Sign-On (SSO) with On-Demand Application Provisioning (ODAP). It also provides a concluding overview of the comprehensive DHCP features covered throughout this guide.

- [Feature history for specialized DHCP deployments and client customization, on page 1](#)
- [Configurable DHCP clients, on page 2](#)
- [SSO - DHCP ODAP client-server, on page 3](#)

Feature history for specialized DHCP deployments and client customization

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature history for specialized DHCP deployments and client customization

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1ea	Specialized DHCP Deployments and Client Customization: The feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Specialized DHCP Deployments and Client Customization: Introduced the support for advanced client-side configurations and specialized DHCP functionalities such as Single Sign-On (SSO) with On-Demand Application Provisioning (ODAP).	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Configurable DHCP clients

Beyond simply obtaining an IP address, DHCP clients can be configured with specific parameters, behaviors, or identifiers to influence their interaction with DHCP servers and to meet particular network requirements. This section details how to customize a DHCP client's behavior.

DHCP Client ID

A DHCP client can be configured with a unique Client ID. This identifier is used by the DHCP server to track specific clients, regardless of their MAC address, which can change. For example, when a device's network adapter is replaced). Using a Client ID ensures that a client always receives the same IP address from the server, even if its hardware changes, or allows for specific policies to be applied based on the ID.

Configure DHCP client ID

Use this procedure to configure a specific client ID for a DHCPv4 client interface on your switch.

This is useful for devices that require a fixed IP address but are still managed by DHCP, or for tracking specific devices in a network.

Before you begin

Configure the interface as a DHCPv4 client using the **ip address dhcp** command.

Procedure

Step 1 Enter interface configuration mode for the desired interface.

Example:

```
Device# configure terminal
Device(config)# interface GigabitEthernet1/0/1
```

Step 2 Configure the DHCP client identifier.

Example:

```
Device(config-if)# ip dhcp client client-id GigabitEthernet1/0/1
```

The string keyword allows a user-defined ASCII string.

Example:

Example with a custom string:

```
Device(config-if)# ip dhcp client client-id string "MyOfficePC-001"
Device(config-if)# end
Device#
```

What to do next

Verify on the DHCP server that the client is recognized by its configured Client ID and receives the expected IP address.

Configure DHCP client to request specific options

Use this procedure to configure a DHCPv4 client interface to request specific DHCP options.

A DHCP client can explicitly request specific options from the DHCP server. While servers typically provide a standard set of options, a client might need additional, non-standard information to function correctly. This configuration allows the client to signal its requirements to the server.

This is useful when client applications or services require particular information such as, specific server addresses, custom parameters, and so on, that are delivered through DHCP options.

Before you begin

Configure the interface as a DHCPv4 client using the **ip address dhcp** command.

Procedure

Step 1 Enter interface configuration mode for the desired interface.

Example:

```
Device# configure terminal  
Device(config)# interface GigabitEthernet1/0/1
```

Step 2 Configure the DHCP client to request specific DHCP Options.

Example:

```
Device(config-if)# ip dhcp client request option 6  
Device(config-if)# ip dhcp client request option 15  
Device(config-if)# end  
Device#
```

Specify the numeric code of the desired DHCP option. You can specify multiple options.

This example shows DHCP client requesting Option 6—DNS servers and Option 15—Domain Name.

Step 3 Verify that the client received the requested DHCP Options.

SSO - DHCP ODAP client-server

Single Sign-On (SSO) with DHCP On-Demand Application Provisioning (ODAP) is a specialized solution that leverages DHCP to facilitate the initial setup and configuration of client devices for SSO-enabled applications. This typically involves Cisco Identity Services Engine (ISE) or similar platforms.

SSO - DHCP ODAP is a mechanism where a DHCP server, in conjunction with an identity management system like, Cisco ISE, provides network configuration and directs a newly connected client to an application

or portal for initial provisioning or authentication. This enables a 'zero-touch' experience for users, allowing them to quickly access required applications after connecting to the network.

How SSO - DHCP ODAP works

The SSO - DHCP ODAP process guides a user from initial network connection to authenticated application access, often without manual configuration.

Summary

The process involves these key components:

- DHCP server: provides initial IP address and network parameters
- Identity Management System: such as Cisco ISE, that authenticates users or devices, authorizes access, and provides provisioning instructions
- ODAP client: the end device such as, laptop, mobile device, and so on, that receives DHCP information and is directed to the provisioning portal
- ODAP application or portal: the web-based interface where users complete their SSO setup or application registration

Workflow

These stages describe how SSO - DHCP ODAP works:

1. Client connects and obtains IP: The client connects to the network and sends a DHCP Discover message. The DHCP server—potentially with a relay agent—assigns an IP address and provides specific DHCP options, including a URL for the ODAP portal.
2. Client redirection to ODAP portal: Upon receiving the DHCP options, the client's browser, or a built-in agent is automatically redirected to the specified ODAP portal URL.
3. User authentication and authorization: The user attempts to access the ODAP portal. The identity management system intercepts the request, authenticates the user—for example, using corporate credentials—and authorizes their access based on policies.
4. Application provisioning and SSO setup: After successful authentication, the ODAP portal guides the user through the necessary steps to provision applications, install certificates, or configure SSO for future access to corporate resources. This might involve downloading client software or configuring browser settings.
5. Network access and application use: Once provisioning is complete, the identity management system updates the client's network access policy, allowing full access to the corporate network and SSO-enabled applications.

Configure DHCP server for ODAP

Use this procedure to configure a DHCP server pool to provide the ODAP portal URL to clients. This is typically done using a custom DHCP option or a standard option like Option 43 if the ODAP client supports it.

Configuring SSO - DHCP ODAP involves setting up the DHCP server to provide specific options that direct clients to the ODAP portal, and configuring the identity management system to handle the provisioning process.

This is typically implemented in enterprise environments using Cisco ISE for user and device onboarding.

This step ensures that clients are directed to the correct provisioning portal upon connecting to the network.

Before you begin

- Configure a DHCPv4 or DHCPv6 pool.
- Deploy and configure Cisco ISE or similar identity management system with the ODAP portal URL and authentication policies.
- A DHCP pool must exist.

Procedure

Step 1 Enter DHCP pool configuration mode for the desired pool.

Example:

```
Device# configure terminal
Device(config)# ip dhcp pool ODAP_POOL
Device(dhcp-config)#
```

Step 2 Configure the ODAP portal URL.

The exact option and format may vary. Often, Option 43—Vendor-Specific Information—or a custom user-defined option is used. Consult your identity management system's documentation for the precise option and value.

Example:

Example using a generic string option:

```
Device(dhcp-config)# option 240 ascii "https://ise.example.com/portal/odap"
```

Example:

Example using Option 43, if supported by the client or ODAP system:

```
Device(dhcp-config)# option 43 hex
010468747470733A2F2F6973652E6578616D706C652E636F6D2F706F7274616 C2F6F646170
Device(dhcp-config)# exit
Device(config)# end
Device#
```

In this example of Option 43, 01 is the sub-option code for URL, 04 is the length of URL, followed by the hex representation of `https://ise.example.com/portal/odap`. The exact sub-option and format depend on the ODAP client implementation.

What to do next

Verify client redirection and successful provisioning through the ODAP portal.