



Source Interface and VRF Support in LDAP

The Source Interface and VRF Support in LDAP feature allows you to configure a dedicated LDAP source interface IP address and virtual routing and forwarding (VRF) details on Cisco Integrated Services Routers (ISR) Generation 2. The source interface address (the address can be an IPv4 or IPv6 address) and VRF details are populated while creating a TCP connection between the Cisco ISR Generation 2 and the LDAP server. This module describes how to configure this feature.

- [Information About Source Interface and VRF Support in LDAP, on page 1](#)
- [How to Configure Source Interface and VRF Support in LDAP, on page 2](#)
- [Configuration Examples for Source Interface and VRF Support in LDAP, on page 4](#)
- [Feature History for Source Interface and VRF Support in LDAP, on page 4](#)

Information About Source Interface and VRF Support in LDAP

Source Interface and VRF Support in LDAP Overview

When Cisco Cloud Web Security and Cisco Integrated Services Routers (ISR) Generation 2 (G2) are deployed back-to-back, they require a Lightweight Directory Access Protocol (LDAP) request to traverse the VPN tunnel between Cloud Web Security and the Cisco ISR G2. In such cases, the source interface IP address (example, the IP address of the LAN interface) must be specified in the LDAP query. Prior to the introduction of the Source Interface and VRF Support in LDAP feature, the source interface address cannot be specified in the source IP field of the LDAP query; instead the tunnel interface IP address was used in the source IP field.

The Source Interface and VRF Support in LDAP feature helps you configure a dedicated LDAP source interface address on Cisco ISR G2. The source interface address is configured on the Cisco ISR G2, and the device uses this interface address to originate all LDAP packets it sends to the LDAP server. The source interface address is also used for polling the end-server to ensure the reachability of the end-server.

The source interface IP (either an IPv4 or IPv6 address) address and virtual routing and forwarding (VRF) details are populated in the LDAP query while creating a TCP connection between the Cisco ISR G2 (client) and the LDAP server.

The VRF instance is configured on the Cisco ISR G2 and VRF table ID details are set in the socket option before creating a TCP connection to allow multiple instances of a routing table to coexist on the same device at the same time. Because routing instances are independent of each other, the same or overlapping IP address can be used without conflict.

Cloud Web Security with LDAP Source Interfaces

The following illustration shows a Cloud Web Security deployment that uses an Authentication, Authorization, and Accounting (AAA) configuration that supports source interface address and virtual routing and forwarding (VRF) details, while establishing a TCP connection between Cisco Integrated Services Routers (ISR) Generation 2 (G2) and Cloud Web Security.

The following section describes the packet flow that happens in the deployment scenario shown in the illustration:

1. A AAA process posts a bind or search request to the Lightweight Directory Access Protocol (LDAP) process.
2. The LDAP process processes the AAA request.
3. A TCP connection is established <<between what >>before sending the request to the LDAP server.

While creating the TCP connection, the source IP address and the VRF table details are set in the LDAP socket context.

4.
 - If the `{ip | ipv6} ldap source-interface` command is configured under the `aaa group server ldap` command, the source IP address and VRF details are populated before the TCP connection is established.
 - If the `{ip | ipv6} ldap source-interface` command is configured in global configuration mode; globally for the box, the source IP address and VRF details are populated after the TCP connection is established.
 - If the `{ip | ipv6} ldap source-interface` command is not configured, the best local IP address and the default table ID details are populated in the TCP packet while establishing the connection.
 - If you have configured the source interface address both under the `aaa group server ldap` command and in global configuration mode, the configuration under the `aaa group server ldap` command has the highest priority.
5. The LDAP process uses the TCP connection to send or receive packets.
6. If the source interface address or VRF configurations are changed or removed, the LDAP process tears down all existing TCP connections and establishes a new TCP connection with a new source interface address or the best local IP address when sending an LDAP packet.

How to Configure Source Interface and VRF Support in LDAP

Configuring LDAP Source Interface and VRF

If you have configured the source interface address and virtual routing and forwarding (VRF) instance under the `aaa group server ldap` command and in global configuration mode, the configuration under the `aaa group server ldap` command has the highest priority.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device(config)# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	aaa group server ldap group-name Example: Device(config)# aaa group server ldap ldap-server-group	Groups different Lightweight Directory Access Protocol (LDAP) servers into distinct lists and methods and enters LDAP server-group configuration mode.
Step 5	{ip ipv6} ldap source-interface interface-type interface-number Example: Device(config-ldap-sg)# ip ldap source-interface gigabitethernet 0/0/0	Specifies the source interface IP address in the LDAP packets.
Step 6	{ip ipv6} vrf forwarding vrf-name Example: Device(config-ldap-sg)# ip vrf forwarding cws-vrf	Configures a virtual routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) LDAP server group.
Step 7	server name Example: Device(config-ldap-sg)# server ldap-server	Specifies the LDAP server.
Step 8	exit Example: Device(config-ldap-sg)# exit	Exits LDAP server-group configuration mode and returns to global configuration mode.
Step 9	{ip ipv6} ldap source-interface interface-type interface-number [vrf vrf-name] Example: Device(config)# ip ldap source-interface gigabitethernet 0/1/0 vrf cws-vrf-1	Specifies the source interface IP address in the LDAP packets.

	Command or Action	Purpose
Step 10	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for Source Interface and VRF Support in LDAP

Example: Configuring LDAP Source Interface and VRF

```

Device(config)# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server ldap ldap-server-group
Device(config-ldap-sg)# ip ldap source-interface gigabitethernet 0/0/0
Device(config-ldap-sg)# ip vrf forwarding cws-vrf
Device(config-ldap-sg)# server ldap-server
Device(config-ldap-sg)# exit
Device(config)# ip ldap source-interface gigabitethernet 0/1/0 vrf cws-vrf-1
Device(config)# end

```

Feature History for Source Interface and VRF Support in LDAP

This table provides release and related information for features explained in this module.

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

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	Source Interface and VRF Support in LDAP	The source interface, which can be an IPv4 or IPv6 interface, and virtual routing and forwarding (VRF) details are populated while creating a TCP connection between a Cisco device and the LDAP server. Support for this feature was introduced on all the models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.8.1a	Source Interface and VRF Support in LDAP	Support for this feature was introduced on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.