# Cisco Catalyst SD-WAN Remote Access Features

**Note** To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

# Cisco Catalyst SD-WAN Remote Access Feature History

*Table 1: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst SD-WAN Remote Access | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco vManage Release 20.7.1 | Remote access refers to enabling secure access to an organization's network from devices at remote locations.<br>Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) integrates remote access functionality into Cisco Catalyst SD-WAN. SD-WAN RA enables Cisco IOS XE Catalyst SD-WAN devices to function as remote access headends, managed through Cisco SD-WAN Manager. This eliminates the need for separate Cisco Catalyst SD-WAN and remote access infrastructure, and enables rapid scalability of remote access services.<br>Remote access users can use the same software- or hardware-based remote access clients as with solutions that do not integrate with Cisco Catalyst SD-WAN. For remote access users, benefits include extending Cisco Catalyst SD-WAN features to remote users. Remote access users can access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet. |
| Cisco Catalyst SD-WAN Remote Access Configuration Using Cisco SD-WAN Manager | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device, using Cisco SD-WAN Manager. Configure Remote Access using the System feature profile in a configuration group. |
| Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN mode Using Cisco SD-WAN Manager | Cisco IOS XE Catalyst SD-WAN Release 17.12.1a<br>Cisco Catalyst SD-WAN Manager Release 20.12.1 | This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device in SSL-VPN mode, using Cisco SD-WAN Manager. |
| Monitor Cisco Catalyst SD-WAN Remote Access Devices | Cisco IOS XE Catalyst SD-WAN Release 17.14.1a<br>Cisco Catalyst SD-WAN Manager Release 20.14.1 | This feature enhances the monitoring of remote access devices. Cisco SD-WAN Manager can provide the following information:<br>• Number of remote access (RA) headends in the network and the supported RA mode (IPsec/SSLVPN).<br>• Number of remote access sessions in the network and sessions per remote access headend, categorized into remote access client type. |

# SD-WAN Remote Access Feature Summary

*Table 2: SD-WAN RA Feature Summary*

| Feature | Description |
|---|---|
| Cisco Catalyst SD-WAN Remote Access connection type (also referred to as mode) | • IKEv2/IPsec<br>• SSL-VPN (TLS)<br>**Note** IKE2/IPsec is the recommended and the default mode when configured from Cisco SD-WAN Manager. |
| Supported remote access clients | Cisco Catalyst SD-WAN Remote Access enables Cisco IOS XE Catalyst SD-WAN devices to terminate connections from the following types of client:<br>IPsec mode:<br>• Software: Cisco AnyConnect (IKEv2/IPsec)<br>• Hardware: Cisco IOS-XE router functioning as a small office/home office (SOHO) remote access client<br>SSL mode:<br>• Software: Cisco AnyConnect (SSL mode)<br>**Note** Remote access clients must be pre-configured with the DNS names or public IP addresses of the primary and backup Cisco Catalyst SD-WAN Remote Access headends. |
| Supported platforms for the Cisco Catalyst SD-WAN Remote Access headend | IPsec mode:<br>• Cisco Catalyst 8300-1N1S-6T<br>• Cisco Catalyst 8300-1N1S-4T2X<br>• Cisco Catalyst 8300-2N2S-4T2X<br>• Cisco Catalyst 8300-2N2S-6T<br>• Cisco Catalyst 8500-12X<br>• Cisco Catalyst 8500-12X4QC<br>• Cisco Catalyst 8500L<br>• Cisco Catalyst 8000V Edge Software<br>SSL(TLS) mode:<br>• Cisco Catalyst 8000V Edge Software |

| Feature | Description |
|---|---|
| Supported certificate authority (CA) servers | Any simple certificate enrollment protocol (SCEP)-capable CA server.<br>The CA server provisions certificates on the Cisco IOS XE Catalyst SD-WAN devices that enable the remote access headend to authenticate itself to remote access clients when the headend is configured to use certificate-based authentication.<br>It is common for the CA server to be deployed at a data center site in the service VPN, together with the RADIUS server. |
| Authentication, authorization, and accounting (AAA) management | RADIUS/extensible authentication protocol (EAP) server for authentication of remote access clients and for per-user policy management.<br>It is common for the RADIUS server to be deployed at a data center site, together with the CA server. |
| Configuration method | Cisco SD-WAN Manager CLI template and using configuration groups. |
| Monitoring | • Monitoring Cisco Catalyst SD-WAN Remote Access devices through Cisco SD-WAN Manager.<br>• Monitoring also through **show** commands and syslogs on the remote access headend devices. |