Cisco AnyConnect Secure Mobility Solution

What's New in Cisco AnyConnect Secure Mobility Client Version 3.1

Q. What IPv6 VPN features are supported in Cisco AnyConnect® Secure Mobility Client Version 3.1? What Cisco® ASA Software version is required for these features?

A. The new IPv6 features include the ability to tunnel over an IPv6 public network and/or to an IPv6 security gateway. IPv6 traffic can be tunneled over the connection for Secure Sockets Layer (SSL), including Transport Layer Security and Datagram Transport Layer Security (TLS/DTLS) connections, but not for IPsec with Internet Key Exchange version 2 (IPsec/IKEv2) in this release. To take advantage of the updated IPv6 features, Cisco ASA Software Version 9.0 is required.

Q. What features in the new Cisco AnyConnect Client support IPv6 connectivity?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, the Network Access Manager supports IPv4 and IPv6 (dual stack). The following VPN features are supported in the new Cisco AnyConnect Secure Mobility Client when making an IPv6 connection:

- Load balancing
- Session roaming (the ASA resolves to a different IP address due to IPv4/IPv6 network address translation)
- HostScan: Posture assessment
- Prelogin check
- Open IPv6 ports
- Split tunneling (include/exclude)
- Always-On
- Trusted Network Detection
- IP protocol bypass
- IP protocol fallback: Fallback from IPv4 to IPv6 (or IPv6 to IPv4) during the initial connection when the primary Cisco Adaptive Security Appliance address is not reachable
- IPv6 Domain Name System (DNS)
- Network Address Translation IPv6 to IPv4 (NAT64)

Q. What operating systems are supported with IPv6?

A. Starting with Cisco AnyConnect Client Version 3.1, IPv6 VPN connectivity is supported on Windows Vista, Windows 7, and Mac OS X 10.6 and later. Also starting with AnyConnect Client Version 3.1, the AnyConnect™ Network Access Manager supports IPv6 on Windows Vista and Windows 7. Unfortunately, Windows XP does not have the capabilities necessary for Cisco AnyConnect Secure Mobility Client to support IPv6 on Windows XP devices.

Q. Is Cisco AnyConnect Secure Mobility Client Version 3.1 supported on mobile platforms at this time?

A. Cisco AnyConnect Mobile is on a separate release schedule from Cisco AnyConnect Secure Mobility Client for desktop operating systems. Cisco AnyConnect Mobile 3.0, for Apple iOS and Android, supports Next-Generation Encryption and IPsec IKEv2. It does not yet include enhanced IPv6 functionality.

Q. Does the Cisco AnyConnect Network Access Manager help differentiate corporate and noncorporate assets?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, the Network Access Manager can provide differentiated network access for corporate and noncorporate devices provided the corporate device has a machine credential (username/password or certificate that is locked to the device).

Q. Does the Cisco AnyConnect Network Access Manager support Next-Generation Encryption Suite B?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, the Network Access Manager supports the following Suite B capabilities: Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) certificates.

Q. Does the Cisco AnyConnect Network Access Manager support mobile broadband/3G connectivity?

A. Starting in Cisco AnyConnect Secure Mobility Client Version 3.1, the Cisco AnyConnect Network Access Manager supports mobile broadband/3G (wireless wide area network [WWAN]) connections on Windows 7, provided the mobile broadband adapter is using the Windows Mobile Broadband interface.

Q. Does the Cisco AnyConnect client permit end users to defer an update to the client software when making a VPN connection to the Cisco Adaptive Security Appliance?

A. Starting with Cisco ASA Software Version 9.0 and Cisco AnyConnect Secure Mobility Client Version 3.1, end users are permitted to upgrade their Cisco AnyConnect client version at a later point in time, subject to policy. Previous versions of Cisco AnyConnect client would update immediately after making a VPN connection to the Cisco ASA Adaptive Security Appliance.

Q. I am a Cisco AnyConnect Secure Mobility Client Version 2.5 customer. Will I encounter any usability changes in the client when I upgrade to Version 3.x?

A. Yes. The user interface has been updated to accommodate the additional capabilities in Cisco AnyConnect Secure Mobility Client Version 3.x. The Cisco AnyConnect client product documentation contains screenshots that illustrate the changes and highlight the usability enhancements in Version 3.x.

Q. Have there been any user interface changes in Cisco AnyConnect Secure Mobility Client Version 3.1?

A. Yes, we have introduced some user interface changes. The Mac OS X user experience is now more consistent with the experience on Windows devices. In addition, we have updated the AnyConnect look-and-feel for Windows device users as well. In order to be more consistent with the behavior of other Windows applications, Cisco AnyConnect Secure Mobility Client Version 3.1 no longer operates as a tray flyout on Windows.

Q. Can I perform a posture assessment directly from the Cisco Adaptive Security Appliance part of a remote access connection?

A. Yes, you can do posture assessment using HostScan. It requires both the Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client. HostScan is also part of Cisco Secure Desktop. Both are licensed through the Cisco AnyConnect Premium license.

Q. What licenses are required for my employee's mobile devices and tablets to connect?

A. The Cisco Adaptive Security Appliance requires an AnyConnect Essentials or an AnyConnect Premium license enabling remote access, plus a Cisco AnyConnect Mobile license for connectivity.

Q. How many Essentials or Mobile licenses do I need per user?

A. Both the Essentials and Mobile licenses are per ASA and **not** per user. You need to buy a license tier for the maximum number of concurrent users that you need to support at any given time on each ASA.

Q. Where can I get a trial Cisco AnyConnect Mobile license?

A. A three-month trial Cisco AnyConnect Mobile license can be obtained here.

Q. When ordering licenses, what does L-mean in front of some of the licenses?

A. Licenses that begin with L- are electronically delivered (versus normal paper license ordering). eDelivery licenses are delivered significantly faster than paper licenses as they do not need to be manufactured and shipped to you.

Q. Where could I find more information about Cisco AnyConnect licensing?

A. Please refer to our licensing documentation here.

What Is New in Cisco AnyConnect Secure Mobility Solution?

Q. What is the Cisco AnyConnect Secure Mobility Solution?

A. The Cisco AnyConnect Secure Mobility Solution combines web security and remote access VPN for an exceptionally comprehensive and secure enterprise mobility solution. Most enterprise traffic is web-based, which dramatically increases the level of security threats. The Cisco AnyConnect Secure Mobility Solution uses the Cisco AnyConnect Secure Mobility Client and Cisco ASA 5500 Series Adaptive Security Appliance with either a premises-based Cisco Web Security Appliance or Cisco Cloud Web Security to provide acceptable use policy (AUP) controls, malware filtering, data security, and application visibility and control.

Q. What are the web security feature differences in the Cisco AnyConnect Secure Mobility Solution between Cisco AnyConnect Secure Mobility Client Version 2.5 or Cisco AnyConnect Secure Mobility Client Version 3.1 and later?

A. With Cisco AnyConnect Secure Mobility Client Version 3.0 and later, an organization has the choice and flexibility of using either the premises-based Cisco Web Security Appliance or the Cisco Cloud Web Security service for enhanced web security. Cisco AnyConnect Secure Mobility Client Version 2.5 works solely with the Cisco Web Security Appliance.

Q. Is there licensing for the Cisco AnyConnect Secure Mobility Client itself?

A. Yes, the Cisco AnyConnect Essentials license provides full VPN tunneling and telemetry features. The Cisco AnyConnect Premium license supports all Essentials license capabilities, plus advanced features such as clientless SSL VPN, Cisco Secure Desktop capabilities (including HostScan), and support for the Cisco AnyConnect Secure Mobility Solution. For more information, please see the licensing overview document here.

Q. How can I learn more about the Cisco AnyConnect Secure Mobility Solution?

A. More information is available here.

Cisco AnyConnect Secure Mobility Client

Q. What is the Cisco AnyConnect Secure Mobility Client?

A. The Cisco AnyConnect Secure Mobility Client is a multifunctional security client that supports security services, remote-access VPN, 802.1X, and web security. This modular client offers organizations the ability to select those features that are most applicable to their secure connectivity needs, providing maximum flexibility and benefit.

Q. I thought Cisco AnyConnect was just VPN. What changed?

A. Customers told Cisco they wanted to minimize the number of applications installed on the endpoint but wanted the flexibility to customize the installation so that only those functions that were being used would appear to the end user. As a result, the Cisco AnyConnect Secure Mobility Client became a multi-modular/multi-function client starting with Version 3.0.

Q. Is the Cisco AnyConnect Secure Mobility Client available as an upgrade for existing Cisco customers?

A. Cisco recommends that existing customers upgrade to the latest version to take advantage of the new features and bug fixes. Customers with an existing Cisco SMARTnet® Service contract can upgrade free of charge. Customers running the Cisco VPN Client are encouraged to upgrade to Cisco AnyConnect Secure Mobility Client to take advantage of the latest VPN features. The low-cost AnyConnect Essentials licensing option provides an attractive migration opportunity for existing Cisco VPN Client customers.

Q. What if my organization wants to take advantage of only one or two modules in the Cisco AnyConnect Secure Mobility Client?

A. Cisco designed the Cisco AnyConnect Secure Mobility Client with customization in mind. New features are modular. Customers can install just the modules applicable to their deployment needs and install new modules as their needs evolve.

Q. What modules are available for the Cisco AnyConnect Secure Mobility Client?

A. The primary modules include VPN (which is part of the Cisco AnyConnect core), the Network Access Manager (providing 802.1X connectivity), posture assessment (Cisco AnyConnect HostScan), the Cisco Web Security module, and telemetry. The modules available depend on the operating system having the capability to support such functionality. Each module listed in this Q&A details the operating systems supported.

Q. What is the Cisco Telemetry module?

A. The Cisco Telemetry module is used in conjunction with the Cisco Web Security Appliance. This optional module provides confidential feedback from endpoints to the web filtering infrastructure, using information about the origin of malicious content. This enhances web security protection levels by working to strengthen the filtering algorithm and improves the accuracy of the URL reputation database by analyzing and correlating endpoint data.

Q. I am in a hurry and about to get on an airplane. I want to download my email just before boarding. Can I avoid software updates and just download my mail?

A. Yes, starting with ASA 9.0 and Cisco AnyConnect Secure Mobility Client 3.1, end users are permitted to defer an upgrade to their Cisco AnyConnect Secure Mobility Client to a later point in time subject to policy.

Q. Can an end user defer Cisco AnyConnect Secure Mobility Client updates indefinitely?

A. Yes, the end user can defer an update each time that person makes a VPN connection provided Cisco AnyConnect Secure Mobility Client on that machine is not below a minimum required version set by the Cisco Adaptive Security Appliance administrator.

Q. What happens if a machine is earlier than the required minimum version of Cisco AnyConnect Secure Mobility Client? Can the user defer?

A. If a machine connects to a Cisco Adaptive Security Appliance and the version of Cisco AnyConnect Secure Mobility Client is earlier than the minimum required version, the end user cannot defer the update.

Q. Which operating systems support deferred update?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, deferred update is supported on Windows, OS X, and Linux.

Q. Can deferred updates be supported prior to Cisco Adaptive Security Appliance Software Version 9.0 (ASA 9.0)?

A. Deferred update is supported through custom policy attributes which were introduced with Cisco ASA 9.0. In the future, other features that use custom policy attributes will not require an update to the Cisco Adaptive Security Appliance, but Cisco ASA 9.0 is required to implement deferred updates and custom policy attributes.

Cisco AnyConnect VPN

Q. I see that the Cisco AnyConnect Secure Mobility Client supports IPsec. Will Cisco AnyConnect Secure Mobility Client work with Cisco VPN 3000 Series concentrators?

A. No. Cisco VPN 3000 Series concentrators support IPsec/IKEv1. Cisco AnyConnect Secure Mobility Client Version 3.0 and greater supports IPsec/IKEv2 connectivity but not IPsec/IKEv1.

Q. Does the Cisco AnyConnect Secure Mobility Client work with Cisco PIX® Security Appliances?

A. No. The Cisco PIX Security Appliances do not support the Cisco AnyConnect Secure Mobility Client.

Q. Why does the Cisco AnyConnect Secure Mobility Client support IKEv2 and not IKEv1?

A. IKEv2 offers greater security and mobility capabilities when compared to the older IKEv1. Unlike IKEv1, IKEv2 is capable of supporting AnyConnect features such as HostScan and secure mobility. However, HostScan and client policy and software updates will be performed over a SSL connection.

Q. Can the Cisco AnyConnect Secure Mobility Client Version 3.0 establish a VPN connection to Cisco ASA Software releases prior to 8.4?

A. The Cisco AnyConnect Secure Mobility Client Version 3.0 is backward-compatible with Cisco ASA Software Release 8.0.x with all preexisting AnyConnect Secure Socket Layer (SSL) features. However, the new Cisco AnyConnect Secure Mobility Client Version 3.0 features, such as IKEv2, will require ASA 8.4 or later and the associated Cisco Adaptive Security Device Manager (ASDM) version. Always review the Cisco AnyConnect client release notes to determine the correct version of ASA software to fully utilize the new capabilities of that release.

Q. If I have a profile from Cisco AnyConnect Secure Mobility Client Version 2.5 or earlier, do I have to rebuild the profile to use the latest version of Cisco AnyConnect client?

A. You will only need to rebuild the profile if you plan to use the new features in the later versions of Cisco AnyConnect clients.

Q. Will the standalone Cisco Diagnostics and Reporting Tool (DART) provide the diagnostics and reporting capabilities for all the new Cisco AnyConnect Secure Mobility Client features?

A. Yes. All integrated diagnostics and reporting capabilities will be captured by the Cisco DART tool.

Q. Is there any thought to offering a pandemic or emergency capability with Cisco AnyConnect Secure Mobility Client that can help with something as simple as people being forced to stay home due to a snowstorm?

A. Yes, the Cisco Adaptive Security Appliance supports a flexible licensing concept where the number of connections can burst to the maximum capabilities of the ASA. It is called Flex licensing and is a consumable license offering 56 days of burst licensing.

Q. Is the Cisco AnyConnect VPN FIPS compliant?

A. Certain Cisco AnyConnect Secure Mobility Client versions are FIPS compliant. Once our third-party test lab has completed their testing, the compliance document will be made available to anyone who purchases the Client VPN FIPS kit for their Cisco ASA appliance.

Q. Where can I find the Cisco AnyConnect Secure Mobility Solution privacy policy?

A. http://www.cisco.com/web/siteassets/legal/privacy.html.

Q. What is the Customer Experience Feedback module?

A. The Customer Experience Feedback module provides anonymous product usage information to Cisco. It is used to better understand specific feature usage by end users and provide performance and defect information back to Cisco. While on by default beginning in Cisco AnyConnect Secure Mobility Client Version 3.1, an administrator may disable the feature as part of their deployment. The feature cannot be enabled or disabled directly in the Cisco AnyConnect Secure Mobility Client user interface.

Cisco AnyConnect VPN: Next-Generation Encryption

Q. What is Next-Generation Encryption?

A. Next-Generation Encryption consists of United States National Security Agency (NSA) Suite B algorithms with IPsec/IKEv2 VPN, Encapsulating Security Payload (ESP) v3 with IKEv2, 4096-bit RSA key operations, and Diffie-Hellman group 24.

Q. What is included in NSA Suite B?

A. In 2005, the NSA specified a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength. These algorithms are: AES-GCM for encryption; SHA-2 for hashing; Elliptic Curve Diffie-Hellman (ECDH) for key exchange; and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures.

Q. Is Next-Generation Encryption included in Cisco AnyConnect Secure Mobility client or is it licensed separately?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, ESPv3 with IKEv2, 4096-bit RSA key operations, and Diffie-Hellman group 24 are included in both Essentials and Premium licenses on the ASA. NSA Suite B algorithms for remote access require an AnyConnect Premium license on the ASA.

Q. Is Next-Generation Encryption supported for both SSL and IPsec?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, NSA Suite B algorithms, ESPv3, and Diffie- Hellman group 24 are supported only on IPsec/IKE v2.

Q. Can the Next-Generation Encryption capabilities in Cisco AnyConnect Secure Mobility Client be used with our existing ASA?

A. Next-Generation Encryption is supported starting with ASA 9.0. Next-Generation Encryption is fully supported on the Cisco ASA 5500-X Series (5515, 5525, 5545, and 5555), Cisco ASA 5580 Series, Cisco ASA 5585-X, and Cisco ASA Services Module. The Suite B implementation on the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, and ASA 5550 Series is limited to ECDH Groups 19 and 20 and ECDSA-256 and -384. 4096-bit RSA keys, AES-GCM/GMAC, and ESP/HMAC-SHA-2 are not supported on the ASA5505, ASA5510, ASA5520, ASA5540, and ASA5550 due to hardware limitations.

Cisco AnyConnect Mobile

Q. What mobile platforms are supported with Cisco AnyConnect Secure Mobility Solution?

A. The key mobile platforms supported are Apple iOS and Android. Specific details on supported platforms and OS versions can be found in the Cisco AnyConnect Mobile and iOS data sheets.

Q. What version of Cisco AnyConnect Mobile for Android should I download and use?

A. Cisco recommends that you download Cisco AnyConnect Mobile for the Android smartphone manufacturer that you have, if available. If the device is rooted, the rooted version would be the next best option. Otherwise, the Android VPN Framework (Android AVF) version is an option on all Android 4.0 (Ice Cream Sandwich) or higher platforms.

Q. How can Cisco AnyConnect Mobile be deployed or installed on an Android device?

A. Cisco AnyConnect Mobile for Android can be installed onto devices by accessing the appropriate application store or marketplace on the device.

Q. Why aren’t all Android device manufacturers supported?

A. Cisco AnyConnect Mobile requires tight integration with the operating system (OS), which is locked down by the OS and/or device manufacturer. The secure capabilities of AnyConnect Mobile require special privileges on the device to operate and therefore require Cisco to work individually with each OS and/or device manufacturer to provide Cisco AnyConnect Mobile on various platforms for our customers. Special permissions are not required to support Android as of Ice Cream Sandwich assuming that the operating system support has been implemented correctly.

Q. What mobile platforms are supported by Cisco AnyConnect Mobile?

A. Cisco AnyConnect Mobile is primarily a VPN client at this time.

Q. How does the Cisco AnyConnect Secure Mobility Client differ on mobile platforms versus the Windows PC version?

A. Cisco AnyConnect Secure Mobility Client for mobile devices is presently focused on providing secure VPN connectivity, whereas Cisco AnyConnect Secure Mobility Client on Windows provides greater secure mobility capabilities. Cisco AnyConnect Secure Mobility Client for mobile devices is compatible with the Apple iOS Connect On-Demand feature, which enables a VPN connection to be established without user interaction, when a digital certificate is issued.

Q. How do I know if the VPN connection is up and working?

A. Depending up the mobile platform being used, you will either see the Cisco AnyConnect icon or a generic “VPN” text icon at the top of the screen. Secondly, you can open the Cisco AnyConnect Secure Mobility Client and view if it is on and passing traffic.

Q. Can I have users connecting to the same Cisco security gateway from different mobile devices and PCs?

A. Yes. Cisco’s security gateways like the Cisco ASA Adaptive Security Appliance are designed to accommodate this type of use.

Q. Can Cisco AnyConnect Mobile establish a VPN connection to releases prior Cisco ASA Software 9.0?

A. Existing AnyConnect SSL features are backward compatible with Cisco ASA Software Release 8.0.x. However, new Cisco AnyConnect Secure Mobility Client features may require a future Cisco ASA Software release and associated Cisco Adaptive Security Device Manager (ASDM) version.

Q. What licenses are required for Cisco Adaptive Security Appliances to work with the Cisco AnyConnect Secure Mobility Client?

A. Either a Cisco AnyConnect Essentials or Premium license is required on the Cisco ASA. There are no licenses directly on an endpoint device (PC, tablet, or smartphone). All customers with active Cisco SMARTnet® support contracts on their ASA security gateways may download the latest Cisco ASA or Cisco AnyConnect Secure Mobility Client software version from Cisco.com at no charge. Additional information on these options can be found in the Cisco AnyConnect Secure Mobility Solutions License Overview Brochure.

Q. What licenses are required to enable mobile device connectivity to my Adaptive Security Appliance (ASA)?

A. The Cisco ASA requires a Cisco AnyConnect Mobile license (L-ASA-AC-M-55XX=), as well as either a Cisco AnyConnect Essentials (L-ASA-AC-E-55XX=) or Cisco AnyConnect Premium Clientless SSL VPN Edition (L-ASA-SSL-YYYY=) license, where XX is the last two digits of your ASA model number and YYYY is the number of simultaneous users. Please contact your Cisco account team to acquire licenses for testing.

Cisco AnyConnect Web Security

Q. Does the Cisco AnyConnect for Cloud Web Security module work with the Cisco Web Security Appliance?

A. No. The web security module is only required for interaction with the Cisco Cloud Web Security. With Cisco AnyConnect's Always-On capability, the endpoint is connected to the corporate network, and the Cisco Web Security Appliance provides web security in a transparent fashion.

Q. What is Cisco Cloud Web Security?

A. Cisco Cloud Web Security is the largest global provider of web security in a "Software as a Service" model for the purpose of keeping malware off corporate networks and controlling and securing employee web usage. With the addition of Cisco Cloud Web Security to the Cisco AnyConnect Secure Mobility Solution, organizations now have a choice to deploy a premises-based Cisco Web Security Appliance or cloud-based Cloud Web Security services to provide comprehensive protection for roaming employees.

Q. Is Cisco AnyConnect Secure Mobility Client an alternative to the Cisco ScanSafe AnyWhere+ client?

A. Cisco AnyConnect Secure Mobility Client Version 3.0 and beyond provides equivalent functionality to the ScanSafe AnyWhere+ 1.2 client. ScanSafe customers may deploy Cisco AnyConnect as an alternative to AnyWhere+ for extending the perimeter to roaming workers for the purpose of enabling consistent policy and security regardless of location (home, hotspots, client sites, etc.).

Q. Is an additional Cisco AnyConnect license needed to enable Cisco Cloud Web Security functionality?

A. No additional Cisco AnyConnect licenses are needed for Cisco Cloud Web Security connectivity. Licensing for the Cisco Cloud Web Security capabilities will be handled by existing Cisco Cloud Web Security licensing requirements.

Q. Does the 'Secure Trusted Network Detection' feature in the Cisco AnyConnect Web Security module override the beacon server functionality?

A. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, only the Secure Trusted Network Detection function is supported. There is no longer any need to install a beacon server.

Q. What is the default Connection Failure policy for the Cisco AnyConnect Web Security Module?

A. The default policy is Fail-open. The Cisco AnyConnect Web Security Module will bypass the Cisco Cloud Web Security towers and allow end-user to browse the Internet if the Cisco Cloud Web Security towers are unreachable. Cisco AnyConnect Secure Mobility Client Version 3.1 introduces a Fail-close option to prevent any internet access in case of failure to reach the Cloud Web Security towers.

Cisco AnyConnect Network Access Manager

Q. Does Cisco Any Connect Secure Mobility Client support IEEE 802.1X?

A. 802.1X over Ethernet (802.3) and Wi-Fi (802.11) is available as a separate module in Cisco AnyConnect Network Access Manager. This separately loadable module must be installed on the endpoint for Cisco AnyConnect Secure Mobility Client to perform 802.1X authentication.

Q. Does Cisco AnyConnect support wireless connectivity?

A. Yes. The Cisco AnyConnect Network Access Manager associated with Cisco AnyConnect Secure Mobility Client Version 3.0 and later supports wireless connectivity using an 802.11 wireless network interface card.

Q. Does Cisco AnyConnect support Wi-Fi Protected Access 2 (WPA2)?

A. Yes. The Cisco AnyConnect Network Access Manager in Cisco AnyConnect Secure Mobility Client Version 3.0 and later supports WPA2, provided WPA2 is supported by the wireless network interface card.

Q. I understand the Cisco AnyConnect Network Access Manager can be used to put different users on different VLANs on my wired network. Can I encrypt that data?

A. Yes. The Cisco AnyConnect Network Access Manager supports 802.1AE, also known as MACsec, which encrypts traffic over the wired LAN.

Q. What hardware is required for MACsec?

A. There are no hardware requirements for MACsec on the local machine. If the network interface card does not support MACsec, the encryption is done on the main processor on the local computer. A MACsec-capable switch is required on the network side.

Q. How do the 802.1X features in the Cisco AnyConnect Network Access Manager compare to the features in the Cisco Secure Services Client (SSC)?

A. The Cisco AnyConnect Network Access Manager module is a replacement for the Cisco SSC's 802.1X functionality.

Q. What features in the Cisco SSC are not being carried over to the Cisco AnyConnect Network Access Manager?

A. In Cisco AnyConnect Secure Mobility Client Version 3.0 and later, the interaction between the Cisco SSC and the traditional Cisco VPN Client has been discontinued.

Q. Can I use the Cisco AnyConnect Network Access Manager with the traditional Cisco VPN Client?

A. Yes. You can use the Cisco VPN Client with the Cisco AnyConnect Network Access Module, but they are separate applications with separate user interfaces. There is no interaction between the Cisco AnyConnect Network Access Manager and the Cisco VPN Client.

Q. Can I use the Cisco AnyConnect Network Access Manager without the VPN function?

A. Yes. All of the components in the Cisco AnyConnect Secure Mobility client can be used independently. If you are not using the Cisco AnyConnect VPN functionality, you can install the Cisco AnyConnect Secure Mobility Client so that functionality is not enabled.

Q. I see there is a GINA module that is part of the Cisco AnyConnect Secure Mobility Client. When do I need to use that module?

A. The GINA module is used with the VPN portion of the Cisco AnyConnect Secure Mobility Client. It is used for pre-login authentication. The Cisco AnyConnect Network Access Manager does not require the separate GINA module for pre-logon authentication.

Q. I am currently running the Cisco Secure Services Client today. Do I need to uninstall it prior to installing the Cisco AnyConnect Network Access Manager?

A. No. The installation of the Cisco AnyConnect Network Access Manager will recognize that the Secure Services Client version 5.x is installed and will uninstall it as part of the Cisco AnyConnect Network Access Manager installation.

Q. Can I upgrade directly from the Cisco Secure Services Client Version 4.x?

A. Upgrading directly from the Cisco Secure Services Client Version 4.x is not supported. You will need to uninstall Version 4.x before installing the Cisco AnyConnect Network Access Manager.

Q. Will user configurations from the Cisco Secure Services Client be retained when I upgrade to the Cisco AnyConnect Network Access Manager?

A. Yes. The user's personal configuration information will be retained as part of the upgrade. If you choose to define more restrictive policies as part of the transition to the Cisco AnyConnect Network Access Manager, profiles the user created in the Cisco Secure Services Client that now violate the update in the Cisco AnyConnect Network Access Manager policy will not be supported.

Q. I have created an organization-specific XML for the Cisco Secure Services Client. Will I need to create a new one for the Cisco AnyConnect Network Access Manager?

A. No. As part of the installation of the Cisco AnyConnect Network Access Manager, Cisco AnyConnect Secure Mobility Client will import organization-specific configurations from the Cisco Secure Services Client Version 5.x. However, new features in the Cisco AnyConnect Network Access Manager will require an updated configuration file.

Q. The Cisco Secure Services Client has a management utility for complex configuration editing. What is the equivalent function in the Cisco AnyConnect client?

A. Cisco AnyConnect client offers a profile editor that can run either as a standalone utility or as part of the Cisco Adaptive Security Device Manager (ASDM) on Cisco ASA 5500 Series Adaptive Security Appliances.

Q. The Cisco Secure Services Client allowed me to limit the wireless encryptions and Extensible Authentication Protocol (EAP) methods the end user could select. Does the Cisco AnyConnect Network Access Manager support this functionality?

A. Yes, with improvements. The authentication policy in the Cisco Secure Services Client management utility could be applied to both deployed and user-created profiles. The authentication policy in the Cisco AnyConnect Network Access Manager is applicable only to user-created profiles, which means it can be tuned to only those capabilities that an end user should be able to access.

Q. Can I prevent users from adding any profiles to the Cisco AnyConnect Network Access Manager?

A. Yes. User profile configuration can be prevented through the authentication policy in the Cisco AnyConnect Network Access Manager profile editor.

Q. Can I prevent users from disabling the Cisco AnyConnect Network Access Manager?

A. Yes. You can use the Cisco AnyConnect Network Access Manager profile editor to prevent users from disabling the Network Access Manager. However, users who have administrative privileges on the local machine can stop the Cisco AnyConnect Network Access Manager service and uninstall the Network Access Manager.

Q. Does the Cisco AnyConnect Network Access Manager support certificates?

A. Yes. The Cisco AnyConnect Network Access Manager supports certificates, smartcards, key fobs, usernames/passwords, and tokens as network authentication credentials. Starting with Cisco AnyConnect Secure Mobility Client Version 3.1, the Cisco AnyConnect Network Access Manager supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates.

Q. Can the Cisco AnyConnect Network Access Manager take advantage of a user's Windows authentication and use those credentials instead of asking the user in a separate dialogue?

A. Yes. The Cisco AnyConnect Network Access Manager can use the credentials that the user enters into Windows, including smartcards and username/password combinations. A security advance starting with Windows Vista limits the use of username/password credentials to Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2).

Q. Does the Cisco AnyConnect Network Access Manager support multiple wired profiles?

A. Yes, the Cisco AnyConnect Network Access Manager supports multiple wired profiles unlike the native Windows connection manager.

Q. Does the Cisco AnyConnect Network Access Manager support different EAP methods for user and machine authentication?

A. Yes, the Cisco AnyConnect Network Access Manager does not require either the EAP types or the credential types to match between machine and user authentication.

Q. I heard that Cisco AnyConnect Network Access Manager offers something unique with regard to Remote Desktop Protocol (RDP) sessions. What is that all about?

A. The Cisco AnyConnect Network Access Manager accepts credentials from a remote RDP connection to authenticate the remote user to the network. This is useful with virtual machine farms where users access the virtual machine using an RDP connection.

Q. Does the Cisco AnyConnect Network Access Manager support whitelisting and blacklisting?

A. No, the Cisco AnyConnect Network Access Manager does not support either whitelisting or blacklisting. Instead, the Cisco AnyConnect Network Access Manager supports Enterprise Connection Enforcement. When Enterprise Connection Enforcement is engaged and the corporate Service Set Identifier (SSID) is in range, the end user will be able to connect only to the enterprise network.

Q. Does the Cisco AnyConnect Network Access Manager offer FIPS 140-2 support?

A. The Cisco AnyConnect Network Access Manager offers Federal Information Processing Standards 140-2 (FIPS 140-2) support on Windows XP with the use of special FIPS wireless network interface card (NIC) drivers.

Q. What EAP methods does the Cisco AnyConnect Network Access Manager support?

A. The following EAP methods are supported: 1) Extensible Authentication Protocol Transport Layer Security (EAP-TLS); 2) EAP-MD5; 3) EAP-MSCHAPv2; 4) EAP Generic Token Card (EAP-GTC); 5) Cisco Lightweight Extensible Authentication Protocol (LEAP) (Wi-Fi only); 6) EAP Protected EAP (EAP-PEAP) with either EAP-MSCHAPv2, EAP-TLS, or EAP-GTC inside the tunnel; 7) EAP Flexible Authentication via Secure Tunneling (EAP-FAST) with either EAP-GTC, EAP-TLS, or EAP-MSCHAPv2 inside the tunnel; and 8) EAP-Tunneled TLS (TTLS) with either EAP-MD5, EAP-MSCHAPv2, PAP, CHAP, MSCHAP, or MSCHAPv2 inside the tunnel.

Q. What operating systems does the Cisco AnyConnect Network Access Manager support?

A. The Cisco AnyConnect Network Access Manager supports Windows XP (32-bit), Windows Vista (32-bit and 64-bit), Windows 7 (32-bit and 64-bit), and Windows Server 2003 (32-bit).

Additional Information

Q. Where can I find more information on the Cisco AnyConnect Secure Mobility Client?

A. See the Cisco AnyConnect Secure Mobility Client site at: http://www.cisco.com/go/anyconnect.

Q. Where can I find more information on the Cisco AnyConnect Secure Mobility Solution?

A. See the Cisco AnyConnect Secure Mobility Solution site at: http://www.cisco.com/go/asm.

Q. Where can I find more information on the Cisco Adaptive Security Appliance?

A. See the Cisco Adaptive Security Appliance site at: http://www.cisco.com/go/asa.

Q. Where should I direct questions regarding mobile licenses?

A. Please send email to the ac-mobile-license-request AT cisco.com.

Q. Where can I direct feedback and questions about Cisco AnyConnect on mobile devices?

A. Please send email to the ac-mobile-feedback AT cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C67-712937-00 09/12