# Cisco AnyConnect Secure Mobility Client Data Sheet

## Product Overview

The Cisco AnyConnect® Secure Mobility Client consistently raises the bar in remote access technology by making the experience more seamless and secure than ever. The AnyConnect Secure Mobility Client provides a secure connectivity experience across a broad set of PC and mobile devices. As mobile workers roam to different locations, an always-on intelligent VPN enables the AnyConnect Secure Mobility Client to automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method, such as Datagram Transport Layer Security (DTLS) protocol for latency-sensitive traffic - for example, voice over IP (VoIP) traffic, or TCP-based application access.

Cisco AnyConnect Secure Mobility Solution has built-in web security and malware threat defense, giving you a choice to use either the premises-based Cisco® Web Security Appliance or cloud-based Cisco Cloud Web Security for reliable and secure employee access to corporate resources. Secure mobility combines web security, malware threat defense, and remote access for a comprehensive and secure enterprise mobility solution. Consistent, context-aware security policies ensure a protected and productive work environment.

Robust posture assessment capabilities protect the integrity of the corporate network by restricting VPN access based on an endpoint's security posture. Prior to establishing connectivity, a system may be validated for compliance with various antivirus, personal firewall, or antispyware products, and may undergo additional system checks with a premium license. An advanced endpoint assessment option is available to automate the process of remediating out-of- compliance endpoint security applications.

In addition to industry-leading VPN capabilities, the Cisco AnyConnect Secure Mobility Client enables IEEE 802.1X capability, providing a single authentication framework to manage user and device identity, as well as the network access protocols required to move smoothly from wired to wireless networks. Consistent with its VPN functionality, the Cisco AnyConnect Secure Mobility Client supports IEEE 802.1AE (MACsec) for data confidentiality, data integrity, and data origin authentication on wired networks, safeguarding communication between trusted components of the network.

Figure 1 shows a sample Cisco AnyConnect VPN configuration on Microsoft Windows.

**Figure 1.** Cisco AnyConnect Icon and Sample VPN Configuration on Microsoft Windows

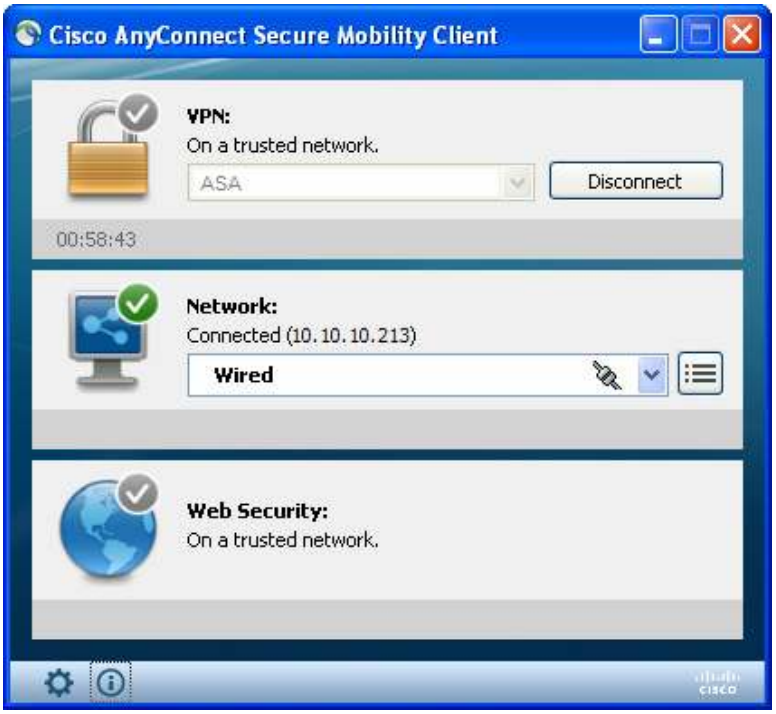
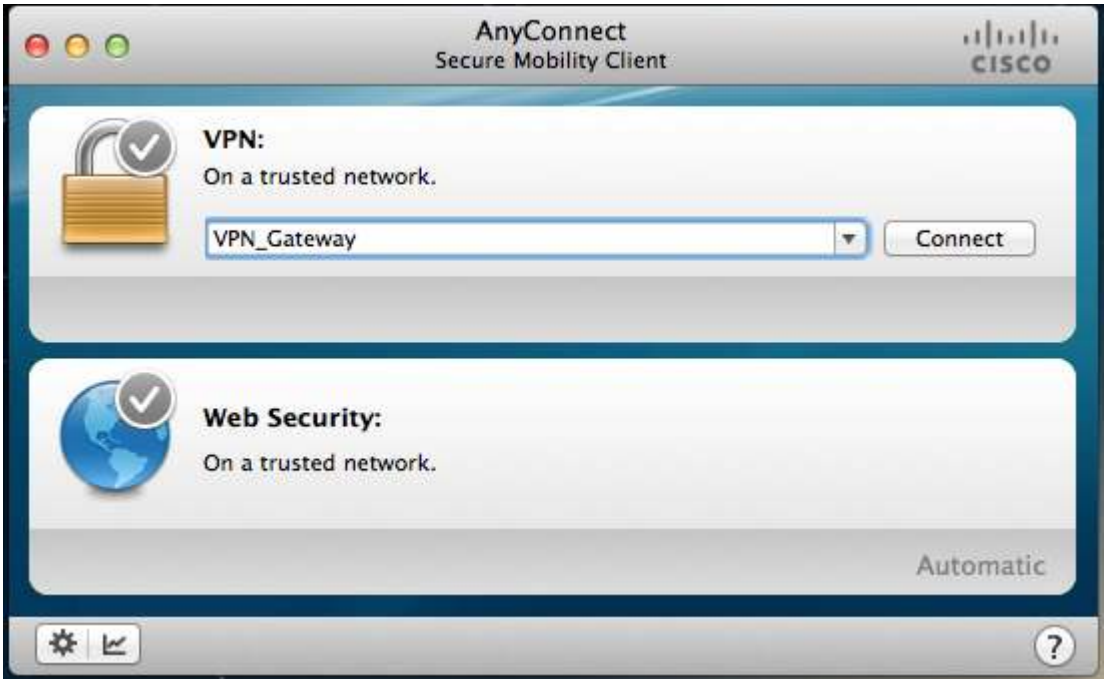



Figure 2 shows a sample Cisco AnyConnect VPN configuration on Apple OS X.

**Figure 2.** Cisco AnyConnect Icon and Sample VPN Configuration on Apple OS X



## AnyConnect Secure Mobility Client Modules

The Cisco AnyConnect Secure Mobility Client is a lightweight, highly modular security client providing easily customizable capabilities based on the individual needs of the business. Features such as VPN, 802.1X, and integration with Cisco Cloud Web Security are available in separately deployable modules, allowing organizations to select the features and functionality most applicable to their secure connectivity needs. This keeps AnyConnect™ nimble and operationally efficient, while providing maximum flexibility and benefit to the organization.

## Features and Benefits

Table 1 lists the features and benefits of the Cisco AnyConnect Secure Mobility Client.

**Table 1.** Features and Benefits

| Feature | Benefit |
|---|---|
| **Remote-Access Virtual Private Networking (VPN)** | |
| **Broad Operating System Support** | • Windows 7 32-bit (x86) and 64-bit (x64)<br>• Windows Vista 32-bit (x86) and 64-bit (x64), including Service Packs 1 and 2 (SP1/SP2)<br>• XP SP2+ 32-bit (x86) and 64-bit (x64)<br>• Mac OS X 10.6 and later<br>• Linux Intel |
| **Software Access** | • Available on Cisco.com for customers with active Cisco SMARTnet® Service contracts on their Adaptive Security Appliances (ASA) |
| **Optimized Network Access - VPN Protocol Choice SSL (TLS and DTLS), and IPsec/IKEv2** | • AnyConnect now provides a choice of VPN protocols, allowing administrators to use whichever protocol best fits their business needs<br>• Tunneling support includes SSL (TLS and DTLS) and next-generation IPsec (Internet Key Exchange Version 2 [IKEv2])<br>• DTLS provides an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access<br>• TLS (HTTP over TLS/SSL) ensures availability of network connectivity through locked-down environments, including those using web proxy servers<br>• IPsec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPsec |
| **Optimal Gateway Selection** | • Determines and establishes connectivity to the optimal network access point, eliminating the need for end users to determine the nearest location |
| **Mobility-Friendly** | • Designed for mobile users.<br>• Can be configured so that the VPN connection remains established during IP address changes, loss of connectivity, and/or hibernation or standby<br>• Trusted Network detection enables the VPN connection to automatically disconnect when an end user is in the office and connect when a user is at a remote location |
| **Encryption** | • Supports strong encryption, including AES-256 and 3DES-168. (The security gateway device must have a strong-crypto license enabled.)<br>• Next-Generation Encryption, including NSA Suite B algorithms, ESPv3 with IKEv2, 4096-bit RSA keys, Diffie-Hellman group 24, and enhanced SHA2 (SHA-256 & SHA-384). (Only applies to IPsec IKEv2 connections. Cisco AnyConnect Premium license required.) |
| **Wide Range of Deployment and Connection Options** | Deployment options:<br>• Pre-deployment, including Microsoft Installer<br>• Automatic security gateway deployment (administrative rights are required for initial installation) via ActiveX (Windows only) and Java<br>Connection modes:<br>• Standalone via system icon<br>• Browser-initiated (Weblaunch)<br>• Clientless portal initiated<br>• CLI-initiated<br>• API-initiated |

| Feature | Benefit |
| --- | --- |
| **Wide Range of Authentication Options** | • RADIUS<br>• RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM)<br>• RADIUS one-time password (OTP) support (state/reply message attributes)<br>• RSA SecurID (including SoftID integration)<br>• Active Directory/Kerberos<br>• Embedded Certificate Authority (CA)<br>• Digital Certificate/Smartcard (including Machine Certificate support), auto- or user-selected<br>• Lightweight Directory Access Protocol (LDAP) with Password Expiry and Aging<br>• Generic LDAP support<br>• Combined certificate and username/password multifactor authentication (double authentication) |
| **Consistent User Experience** | • Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience<br>• Multiple delivery methods help ensure broad compatibility of Cisco AnyConnect<br>• User may defer pushed updates to Cisco AnyConnect<br>• Customer experience feedback option |
| **Centralized Policy Control and Management** | • Policies can be preconfigured or configured locally, and can be automatically updated from the VPN security gateway<br>• Application Programming Interface (API) for AnyConnect eases deployments through webpages or applications<br>• Checking and user warnings for untrusted certificates<br>• Certificates can be viewed and managed locally |
| **Advanced IP Network Connectivity** | • Public connectivity to/from IPv4 and IPv6 networks<br>• Access to internal IPv4 and IPv6 network resources over SSL (v6 internal requires TLS/DTLS)<br>• Administrator-controlled split/all-tunneling network access policy<br>• Access control policy<br>IP address assignment mechanisms:<br>• Static<br>• Internal pool<br>• Dynamic Host Configuration Protocol (DHCP)<br>• RADIUS/Lightweight Directory Access Protocol (LDAP) |
| **Preconnection Posture Assessment (Premium license required)** | • In conjunction with Cisco Secure Desktop, HostScan verification checking seeks to detect the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access<br>• Administrators also have the option of defining custom posture checks based on the presence of running processes<br>• Cisco Secure Desktop can detect the presence of a watermark on a remote system. The watermark can be used to identify assets that are corporate-owned and provide differentiated access as a result. The watermark-checking capability includes system registry values, file existence matching a required CRC32 checksum, IP address range matching, and certificate issued by/to matching<br>• An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications |
| **Client Firewall Policy** | • Added protection for Split Tunneling configurations<br>• Used in conjunction with Cisco AnyConnect Secure Mobility Client to allow for local access exceptions (for example, printing, tethered device support, and so on)<br>• Supports port-based rules for IPv4 and network/IP access control lists (ACLs) for IPv6.<br>• Available for Windows XP SP2, Vista, and Windows 7, and Mac OS X |
| **Localization** | In addition to English, the following language translations are included:<br>• Czech (cs-cz)<br>• German (de-de)<br>• Latin American Spanish (es-co)<br>• Canadian French (fr-ca)<br>• Japanese (ja-jp)<br>• Korean (ko-kr)<br>• Polish (pl-pl)<br>• Simplified Chinese (zh-cn) |

| Feature | Benefit |
|---|---|
| **Ease of Client Administration** | • Allows an administrator to automatically distribute software and policy updates from the head-end security appliance, thereby eliminating administration associated with client software updates<br>• Administrators can determine which capabilities to make available for end-user configuration<br>• Administrators can trigger an endpoint script at connect/disconnect time when domain login scripts cannot be utilized<br>• Administrators can fully customize and/or localize end-user visible messages |
| **AnyConnect Profile Editor** | • AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM). |
| **Diagnostics** | • On-device statistics and logging information<br>• View logs on device[1]<br>• Logs can be easily emailed to Cisco or an administrator for analysis |
| **Federal Information Processing Standard (FIPS)** | • FIPS 140-2 Level 2 Compliant (platform, feature and version restrictions apply) |
| **Secure Mobility** | |
| **Cisco Cloud Web Security Integration** | • Uses Cisco Cloud Web Security, the largest global provider of software-as-a-service (SaaS) web security, to keep malware off corporate networks and control and secure employee web usage<br>• Gives organizations flexibility and choice by supporting cloud-based services in addition to premises-based<br>• Cisco Web Security Appliance<br>• Cloud hosted configurations and dynamic loading<br>• Secure Trusted Network detection |
| **Cisco AnyConnect Secure Mobility Premium license or Cisco Web Security Appliance Secure Mobility license required)** | • Enforces security policy in every transaction, independent of user location<br>• Requires always-on secure network connectivity with a policy to permit or deny network connectivity if access becomes unavailable<br>• Hotspot/Captive Portal detection<br>• Optimized for use with Cisco Web Security or Cisco Cloud Web Security |
| **Telemetry** | • Provides feedback from endpoints to the web filtering infrastructure using information about the origin of malicious content causing infections<br>• Enhances web security protection levels by working to strengthen the filtering algorithm, and improve the accuracy of the URL reputation database by analyzing and correlating the endpoint data<br>• Supported on Windows 7, Vista, and XP SP2+ |
| **Broad Operating System Support** | • Windows 7 32-bit (x86) and 64-bit (x64)<br>• Windows Vista 32-bit (x86) and 64-bit (x64)<br>• XP SP2+ 32-bit (x86) and 64-bit (x64)<br>• Mac OS 10.6.x, 10.7.x and 10.8.x |
| **Network Access Manager and 802.1X** | |
| **Media Support** | • Ethernet (IEEE 802.3)<br>• Wi-Fi (IEEE 802.11a, 802.11b, 802.11g, 802.11n)<br>• Mobile Broadband 3G/4G (requires Windows 7 and adapter supporting an NDIS interface) |
| **Network Authentication** | • IEEE 802.1X-2001, 802.1X-2004, and 802.1X-2010<br>• Enables businesses to deploy a single 802.1X authentication framework to access both wired and wireless networks<br>• Manages the user and device identity and the network access protocols required for secure access<br>• Optimizes the user experience when connecting to a Cisco unified wired and wireless network |
| **Extensible Authentication Protocol (EAP Methods)** | • EAP-Transport Layer Security (TLS)<br>• EAP-Protected Extensible Authentication Protocol (PEAP) with the following inner methods:<br>  ◦ EAP-TLS<br>  ◦ EAP-MSCHAPv2<br>  ◦ EAP-Generic Token Card (GTC)<br>• EAP-Flexible Authentication via Secure Tunneling (FAST) with the following inner methods:<br>  ◦ EAP-TLS<br>  ◦ EAP-MSCHAPv2<br>  ◦ EAP-GTC<br>• EAP-Tunneled TLS (TTLS) with the following inner methods: |

[1] This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).

| Feature | Benefit |
| --- | --- |
| | ◦ Password Authentication Protocol (PAP)<br>◦ Challenge Handshake Authentication Protocol (CHAP)<br>◦ Microsoft CHAP (MSCHAP)<br>◦ MSCHAPv2<br>◦ EAP-MD5<br>◦ EAP-MSCHAPv2<br>• Lightweight EAP (LEAP) - Wi-Fi only<br>• EAP-Message Digest 5 (MD5) - Administrative Configured, Ethernet Only<br>• EAP-MSCHAPv2 - Administrative Configured, Ethernet Only<br>• EAP-GTC - Administrative Configured, Ethernet Only |
| **Wireless Encryption Methods (Requires corresponding 802.11 NIC support)** | • Open<br>• Wired Equivalent Privacy (WEP)<br>• Dynamic WEP<br>• Wi-Fi Protected Access (WPA) Enterprise<br>• WPA2 Enterprise<br>• WPA Personal (WPA-PSK)<br>• WPA2 Personal (WPA2-PSK)<br>• CCKM (requires Cisco CB21AG Wireless NIC) |
| **Wireless Encryption Protocols** | • Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) using the Advanced Encryption Standard (AES) algorithm<br>• Temporal Key Integrity Protocol (TKIP) using the Rivest Cipher 4 (RC4) stream cipher |
| **Session Resumption** | • RFC2716 (EAP-TLS) Session Resumption using EAP-TLS, EAP-FAST, EAP-PEAP, and EAP-TTLS<br>• EAP-FAST Stateless Session Resumption<br>• PMK-ID Caching (Proactive Key Caching/Opportunistic Key Caching) - Windows XP only |
| **Ethernet Encryption** | • Media Access Control - IEEE 802.1AE (MACsec)<br>• Key Management - MACsec Key Agreement (MKA)<br>• Defines a security infrastructure on a wired Ethernet network to provide data confidentiality, data integrity, and authentication of data origin<br>• Safeguards communication between trusted components of the network |
| **One Connection at a Time** | • Only allow a single connection to the network disconnecting all others<br>• No bridging between adapters<br>• Ethernet connections automatically take priority |
| **Complex Server Validation** | • Support “ends with” and “exact match” rules<br>• Support for in excess of 30 rules for servers with no name commonality |
| **EAP-Chaining** | • Differentiate access based on enterprise and non-enterprise assets<br>• Validate users and devices in a single EAP transaction |
| **Enterprise Connection Enforcement (ECE)** | • Ensures that users connect only to the correct corporate network<br>• Prevent users from connecting to a third party access point to surf the Internet while in the office<br>• Prevent users from establishing access to the guest network<br>• Eliminates cumbersome blacklisting |
| **Suite B** | • Supporting the latest cryptographic standards<br>• Elliptic Curve Diffie-Hellman Key Exchange<br>• Elliptic Curve Digital Signature Algorithm (ECDSA) Certificates |
| **Credential Types** | • Interactive user passwords or Windows passwords<br>• RSA SecurID tokens<br>• One-time password (OTP) tokens<br>• Smartcards (Axalto, Gemplus, SafeNet iKey, Alladin)<br>• X.509 certificates<br>• Elliptic Curve Digital Signature Algorithm (ECDSA) Certificates |
| **Remote Desktop Support** | • Authenticate remote user credentials to the local network when using Remote Desktop Protocol (RDP) |
| **Federal Information Processing Standard (FIPS) 140-2 Level 1 (Windows XP only)** | • Requires purchase of separate drivers for a complete FIPS 140-2 Level 1 client solution<br>• Many popular Intel, Broadcom, and Atheros Wi-Fi chipsets supported<br>• FIPS mode includes support EAP-TLS, EAP-FAST and EAP-PEAP methods |

| Feature | Benefit |
|---|---|
| **Operating Systems Supported** | • Windows 7 (32-bit and 64-bit)<br>• Windows Vista (32-bit and 64-bit)<br>• Windows XP SP2+ (32-bit)<br>• Windows Server 2003 (32-bit) |

## Platform Compatibility

- The Cisco AnyConnect Secure Mobility Client is compatible with all Cisco ASA 5500 Series Adaptive Security Appliance models (running Cisco ASA Software Release 8.0(4) and later).
- Additional compatibility information may be found at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

## Cisco AnyConnect Secure Mobility Client Licensing Options

Table 2 lists licensing options for the Cisco AnyConnect Secure Mobility Client.

**Table 2.** Cisco AnyConnect Secure Mobility Client Licensing Options

| License Requirements (each license below is required) | Description |
|---|---|
| **Cisco ASA Platform License** | **Cisco AnyConnect Essentials**[2] (P/N: (L-ASA-AC-E-55**=) 05, 10, 20, 40, 50,80, 85)<br>• Highly secure remote-access connectivity<br>• Single license per ASA device model (not a per user license); enables maximum simultaneous users on platform<br>• Full-tunneling access to enterprise applications |
| | **Cisco AnyConnect Premium**[3] (P/N: (L-ASA-SSL-***=) 10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10,000<br>• Also provides support for clientless SSL VPN and capabilities available on desktop AnyConnect platforms including Cisco Secure Desktop HostScan and always-on VPN connectivity<br>• License is based on number of simultaneous users, and is available as a single device or shared license (part number above is for a single device license) |
| **Cisco AnyConnect Mobile License**[5]<br>P/N: (L-ASA-AC-M-55*=)<br>05, 10, 20, 40, 50,80, 85 | • Enables Mobile OS platform compatibility<br>• Single license per ASA device model (not a per user license) is required in addition to Essentials or Premium licenses |

## Electronic License Delivery

Most licenses are available for electronic delivery; this significantly speeds up license fulfillment time. To order a license electronically, be sure to order part number(s) that begin with “L-.” If you have any questions regarding licensing or would like evaluation licenses, please contact ac-mobile-license-request (AT) cisco.com and include a copy of the results of the “show version” command from your Cisco ASA appliance.

If you already have an Essentials or Premium ASA license, you may use the automated license request tool at: https://tools.cisco.com/SW IFT/Licensing/PrivateRegistrationServlet?FormId=717.

## Warranty Information

Find warranty information at the Cisco Product Warranties page.

[2] Replace ** with the appropriate last two digits of the ASA model number.
[3] Replace *** with the number of total number of license seats.

## Ordering Information

To place an order for a security gateway license, visit the Cisco Ordering Home Page. See Table 1 for compatible platforms and software access information.

Security gateway licenses are required to enable connectivity. Please refer to the Cisco AnyConnect Licensing Options section above for additional information on the available options. For a list of available licensing options that enable connectivity with Cisco AnyConnect, please refer to the Cisco AnyConnect Secure Mobility Client Features, Licenses, and Operating Systems webpage.

## Acknowledgements


- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: (http://www.openssl.org).
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This product incorporates the libcurl HTTP library: Copyright © 1996-2006, Daniel Stenberg, (Daniel@haax.se).


## For More Information

Cisco AnyConnect Secure Mobility Client homepage: http://www.cisco.com/go/anyconnect

Cisco AnyConnect documentation:
http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

Cisco ASA 5500 Series Adaptive Security Appliance Licensing Information:
http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

AnyConnect End User License Agreement and Privacy Policy:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm


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 C78-527494-05 09/12