Cisco Secure Services Client for Windows 2K/XP User Guide

Software Release 4.2.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13520-01

Cisco Secure Services Client Administrator Guide

The preface provides an overview of the *Cisco Secure Services Client User Guide* (OL-13520-01), references related publications, and explains how to obtain other documentation and technical assistance.

The following topics are covered in this section:

Audience and Scope

This publication is for both IT administrators and end-users interested in understanding the operation of the Cisco Secure Services Client (SSC) and the meaning of entries in the various windows and dialogs of the user interface. This guide also contains detailed descriptions on creating and managing networks from the user interface.

Conventions

This publication uses the following conventions to convey instructions and information:

- GUI window, window pane and tab names are in **Green** type.
- GUI elements are in **bold** type.
- GUI actions are in ***bold-italic*** type.
- Procedures are identified by a ***Procedure*** heading.
  Procedures are step-by-step instructions for completing a task.
- Notes and tips are identified by **Note** or **Tip**.
  Notes contain addition information for the subject at hand. Tips contain helpful suggestions.

Related Publications

For more information about Cisco Secure Services Client, refer to these publications:

- *Cisco Secure Services Client Administrator Guide* — Provides detailed information for the IT administrator on preconfiguring and deploying end-user versions of SSC.
- *Cisco Secure Services Client Release Notes* — Describes new features and the open and resolved caveats in each SSC release.

You can find these Cisco SSC technical documents at this URL:

www.cisco.com/en/US/products/ps7034/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Getting Started

Introducing Cisco Secure Services Client

The Cisco Secure Services Client is an 802.1X authentication supplicant (aka, Cisco SSC) for creating connections that also has a user interface for giving status and accepting commands to/from a user. It allows your computer to connect to and access a network that is protected by the IEEE 802.1X security protocol. Only after successful client-server authentication will the port access control on the 802.1X-enabled access device (the wireless access point or the wired ethernet switch) allow end-user connectivity to the network.

For short-hand notation, the term "**Client**" will often be used throughout this document to mean the ***Cisco Secure Services Client***.

Client Versions

Administrator/Out-of-the-Box Client Version:

SSC as downloaded from cisco.com (the out-of-the-box version) is not configured. The out-of-the-box version is intended for use by an IT organization that is responsible for configuring and deploying a derived, end-user version. This deployed version is appropriate for use by the various enterprise departments and organizations that you support. As the IT Administrator you have control over the user experience and the end-user's allowed choices and configuration options. The out-of-the-box version has a fully open policy that allows access to most features and requires configuring a network when initially started. However, only through a deployed distribution package file, that is, a SSC configuration file, does the IT Administrator have full access to all settings and network configurations.

See *Cisco Secure Services Client Administrator Guide* for details on out-of-the-box configurations and deploying end-user client versions.

Deployed End-User Client Versions:

The deployed end-user version has been pre-configured with a distribution package description, possibly with a restricted feature set, and deployed by you the IT/System Administrator. It most likely contains one or more pre-defined enterprise networks that allow instant connection to your enterprise networks. Two types are available as follows:

- **Configurable End-User Version:**

  This version allows your end-users to create new network profiles within the scope of your policy. It is an excellent choice for end-stations that will move out of the enterprise network to home or travel networks.

- **Preset End-User Version:**

  This version contains only your pre-defined network profiles that allow instant connection to your enterprise networks. It is an excellent choice for end-stations that will only encounter enterprise networks that you control.

Using a Configurable Client for Making Connections

Each Network is defined by its **Network Profile**.

For the ***End-User Client*** version the first task is to determine if one of these pre-defined profiles completely satisfies your needs or if you need to also create a specific one.

For the ***Administrator Client*** version the first task is to create an initial one.

Using a pre-defined network - *End-User Client*:

The pre-defined network profiles were setup by your IT/System Administrator with the required settings for your enterprise networks.

Note: *these are locked profiles and can not be modified.*

To ***use*** these networks see the following:

Viewing your Network Connections

Making Connections

For reference you can ***view*** the configuration of a pre-defined network from the following:

Viewing your Pre-defined Network Profile

Making a new network - *Administrator & End-User Clients*:

Step 1: Define a Network Profile

Note: *See Understanding Policy and Profiles for* ***default*** *descriptions.*

Setup Task: *determine profile content.*

A Network Profile has a user-friendly name and defines the following:

- the class of Network - ***sub-task:*** *determine the authenticating needs of this network from the following:*
  - personal class network - no authentication server (an open or shared key security network)
  - enterprise class network - requires authentication via your enterprise server
    - authentication credential storage environment - ***sub-task:*** *determine from the following*:
      - simple user name identification
      - using domains for complex user name identification
    - the EAP authentication protocols used - client supports a flexible suite of allowed protocols, ***sub-task:*** *choose a configuration method from the following:*
      - auto-select method - which inherits a comprehensive allowed list from the system default settings (as specified in the client policy) and then automatically determines a compatible protocol at the time of a connection attempt (allows for simple network profile creation).
      - advanced configuring method - which allows for overrides of the system defaults.
        Important Note: the client can not make unilateral choices - the configuration of the network is primarily determined by the policy of the authentication server and its associated access devices. The client must be configured appropriately to conform.

      See Understanding EAP Methods for details and requirements for additional support items.
    - the Credentials needed - the type of credential required varies according to the specific authentication method and the settings of the authentication server, ***sub-task:*** *determine the type of credentials and choose a collection method*.

See Providing Credentials for details - observe any user certificate companion installation requirements.

- the set of Access Devices that belong to the network - ***sub-task:*** *at least one must be specified at time of defining the network profile*.

  Note: *Remember that a network has a single set of user credentials, so all the access devices should be physically connected to the same end point computing facilities.*

  - for WiFi, the association and encryption modes supported, and, if static WiFi, then the WEP or WPA keys - client supports flexibility as to the amount of configuring required, ***sub-task:*** *choose a configuration method from the following*:
    - auto-detect method - which autonomously detects settings, when possible, at the time of network profile creation, and allows for simple network profile creation.
    - manual configuring method - which allows for overrides of the system defaults or autonomous settings.

Create Task: *Go to Creating a New Network for a detailed step-by-step procedure based on the above decisions.*

Step 2: **Configuring Authentication Server validation** (authenticating networks)

When using a mutual authenticating method, required for wireless WPA/2 compliance, a server validation is part of the authentication process. To support this the client maintains a Trusted Server List the contents of which are used during server validation.

> **Note**: server validation is the ***default*** mode for the out-of-the-box administrator client. Therefore not properly populating the Trusted Server List for these EAP methods will result in authentication failures, unless server validation was disabled for the particular authentication being used when you created the network (previous step).

Setup Task: *determine server validation needs of your authentication server. (see Understanding EAP Methods for more details)*

Create Task: *Go to Managing Trusted Servers for detailed step-by-step procedures.*

Using the Preset End-User Client for Making Connections

This deployed preset end-user version of the client has one or more pre-defined enterprise networks when initially started. Each Network is defined by its **Network Profile**.

Using a pre-defined network:

The pre-defined network profiles were setup by your IT/System Administrator with the required settings for your enterprise networks.

> **Note**: *these are locked profiles and can not be modified.*

To ***use*** these networks see the following:

> Viewing your Network Connections
>
> Making Connections

For reference you can ***view*** the configuration of a pre-defined network from the following:

> Viewing your Pre-defined Network Profile

Starting the Client

The Client runs as a Windows service and starts automatically on startup of the Windows operating system and takes over protocol management at the appropriate time (based on user-defined stored configuration parameters).

> **Tip**: manually stopping and starting the Cisco Secure Services Client service can be performed via the Windows Services dialog (Start > Control Panel > Administrative Tools > Services) - assuming you have Windows Administrative Privileges.

Confirmation that the Client has been successfully started is given by the presence of its icon in the Windows task bar icon tray. **Note**: *this is the initial **default** mode, but the presence of the task bar icon is user configured (see understanding Main Screen options).*

The graphical user interface (GUI), used to operate and manage the Client, is started by one of the following methods:

- opening via the **task bar icon**
- opening via the Windows **Start menu**
  - Start> All Programs> Cisco Secure Services Client> Cisco Secure Services Client Open

> **Note**: *attempting to open the GUI when the Cisco Secure Services Client service is not started will result in the display of an appropriate error message dialog.*

Related Topics:

> Operations Overview

The Main Screen

The Client opens in the **Connection Control** Main Screen.

Configurable Versions (Administrator/End-user)

The **Main Screen** allows for the following ***views***:

- Understand the Main Screen Views
  - Viewing your Networks and Access Devices
    - **Create Network** View
    - **Manage Network** View

The **Main Screen** allows for the following ***operations***:

- Main Functions - **Create Networks** tab
  - Create a new Network

    First time? See Getting Started.
- Main Functions - **Manage Networks** tab
  - View Connection Status of connected networks
  - Control the User Network Connections
  - Manage an existing Network's Configuration

- Manage Ancillary Functions
  - Manage the system's Network Adapters
  - Manage the system's Trusted Servers
  - Manage the system's Security Settings

- Support Functions
  - Manage a Log Report
  - Activate the client

Preset Version (End-user)

The **Main Screen** allows for the following ***view***:

- Understand the Main Screen View
  - **Manage Network** View

The **Main Screen** allows for the following ***operations***:

- Main Functions - **Manage Networks** tab
  - View Connection Status of connected networks
  - Control the User Network Connections
  - View Properties of Locked Networks

- Support Functions
  - Manage a Log Report

List of Procedures

Viewing your Networks and Access Devices

The Client's Networks and Access Devices can be viewed from two perspectives:

- Viewing configured networks perspective
  The **Manage Network** tab view provides a list of all of your Networks and their assigned Access Devices.
- Viewing available access devices perspective
  The **Create Networks** tab view provides a list of all available Access Devices - currently unassigned to a network.
  Note: *equivalent to a classical scan list.*
  (***Policy dependent*** - may not be present in a deployed End-User Client)

Note: *when Client opens in the **Connection Control** Main Screen, it does so by displaying the tab view that was last opened when the Client was closed. (The first-time, **default** view is the Create Networks view.)*

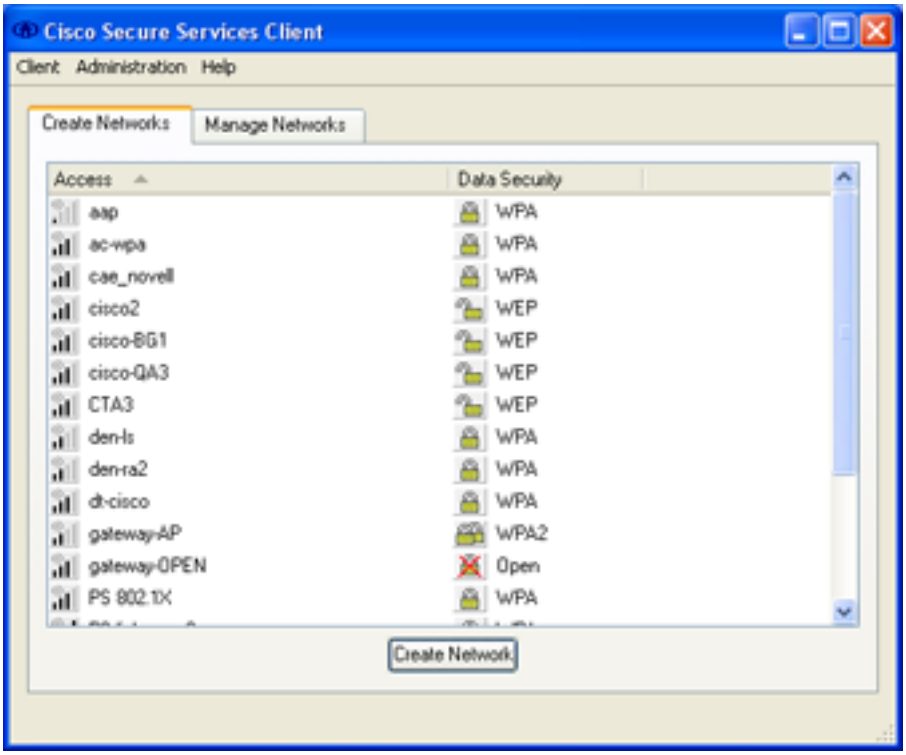
Related Topics:

Viewing Detailed Status

Viewing Available Access Devices

Connection Control Main Screen - Create Networks tab

(***Policy dependent*** - may not be present in a deployed End-User Client)



Selecting the **Create Networks** tab in the Client's **Connection Control Main Screen** ***displays*** the following:

- All scan-capable wireless Access Points not presently assigned to a configured Network and detected as locally available, where scan-capable is defined as follows:
    - access points that are issuing a beacon
    - access points that will respond to an active (broadcast) probe request
- All wired Access Devices not presently assigned to a configured Network.

Note: the display is periodically updated autonomously.

Note: *in a multi-wireless adapter environment, the scan lists are merged for the highest security reporting.*

Access Device List Fields:

Access Field:

- **Access Device Icon**
  The ***first***graphical icon on the left indicates the following:
    - **Media Type**
        - wired - designated by an ethernet connector port image
        - wireless - designated by a set of Signal Level bars

- **Signal Level** - wireless only
  - one partially colored bar: very low signal
  - one colored bar: low signal
  - two colored bars: medium signal
  - three colored bars: high signal
  - four colored bars: very high signal

  Note: a ? is overlayed for a hidden access when not selected for a connection.

- **Access Device Name** - assigned name for the access device

  *For **wireless**, the assigned access name is typically the SSID of the access point. Selecting reveals its BSSID (MAC Address).*

  *Furthermore, for the case of **multiple access points with the same SSID** a list entry represents a group of linked (for purposes of roaming) access points. (The number of detected access devices is indicated via appended text.) Selecting such an access device will display an expanded view of the individual members and the following information:*

  ***BSSID** (MAC Address)*
  ***Signal level** - categorized and displayed as Very Low, Low, Medium, High, Very High*
  ***Data Security** - detected value for this individual access point*

  Tip: *to deselect the expanded view, click in the white space of the next (empty) column (to the right, within the list table).*

  Note: *Access devices with modes not supported by the license, such as, WPA2, are filtered from the list.*

  *For **wired**, all wired (ethernet) adapters can only be applied to a single network. When available (link-up), all are displayed generically as a single <ethernet> grouped access device.*

Data Security Field:

- **Security Icon & Encryption Class**

  The ***second***graphical icon indicates the following for the best detected (supported) mode:

  - **Security Level (Wireless**) - configured data encryption method
    - **X overlay on Lock: *None*** - indicates there is an open connection - **no encryption**.
    - **1 open Lock: *Good*** - indicates that there is weak (known to be breakable) encryption. Used for **WEP**.
    - **1 closed Lock: *Better*** - indicates that there is secure encryption. Used for **WPA** (generally with TKIP).
    - **2 closed Locks: *Best*** - indicates that there is the best known encryption. Used for **WPA2** (generally with AES).
    - **? overlay with Lock**: ***Mixed*** - the multiple same-SSID members have different data security settings.
  - **Security Level (Wired)**
    - ***Placeholder Port*** - **Wired**. Data encryption not applicable for ethernet media type.

Related Main Screen Topics

Clicking the **Create Network** button allows for Creating a new Network and assigning Access Devices from a similar list display.

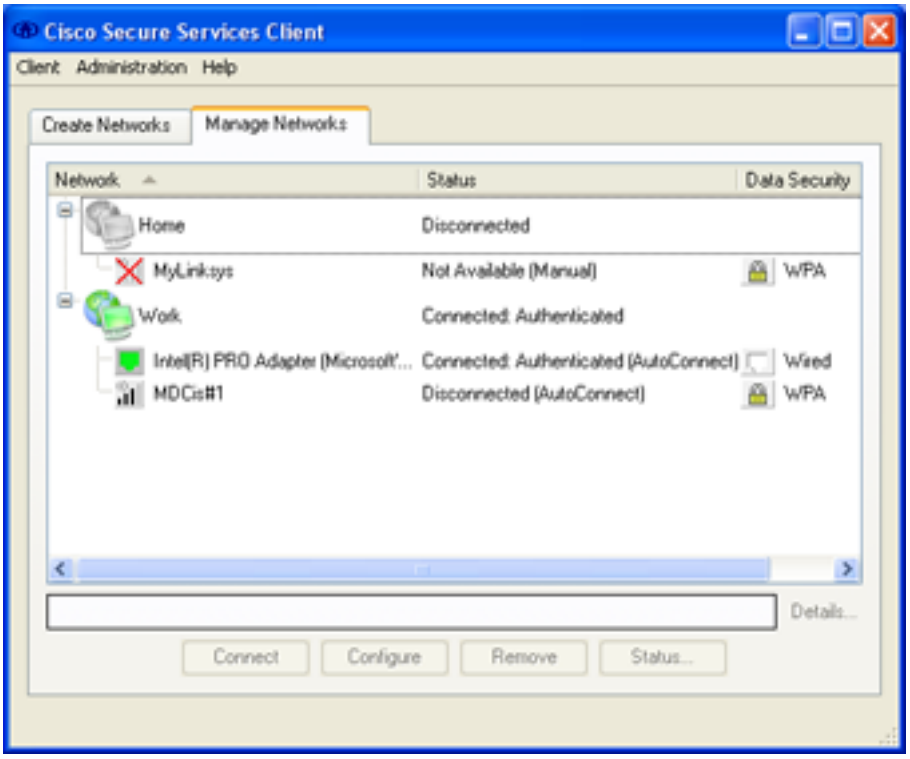
Additional Topics

View Networks & Network Connections

Additional Main Screen Options

Viewing Networks and Network Connections

Connection Control Main Screen - Manage Networks tab



Selecting the **Manage Networks** tab in the Client's **Connection Control Main Screen** ***displays*** the following:

- All named, configured Networks - expands to display:
  - All Access Devices configured within the listed Networks

Note: the display is periodically updated autonomously.

Network and Access Device List Fields:

Network Layer:

- **Network Icon**
  The graphical network icon on the left indicates the following:
  - **Icon Connection Status** - a station image with a set of colored overlays and a global network image, ordered as follows:
    - **Blue**: Connected - at least one access is in the '*Connected: Unauthenticated*' state
    - **Green**: Connected - otherwise, at least one access is in the '*Connected: Authenticated*' state
    - **Yellow**: Connecting - otherwise, at least one access in in the 'Connecting' state
    - Grey: Disconnected otherwise (not connected)
- **Network Field**
  - **Network Name** - assigned name for the network
  - **Profile Status** (appended textual indication) - indication of how configurable the profile is.
    - **Locked** - profile configuration fixed by the deploying administrator.

- (blank) - implies ***Unlocked***, profile may be modified by user.

- **Status Field**
  Note: *when applied to a Network, indicates a summation of its underlying access devices, ordered as follows.*
  - **Connected: Unauthenticated**: if any unauthenticating access device is connected.
  - **Connected: Authenticated**: else if only any authenticating access device is connected.
  - **Connecting**: else if no access device is connected and any access device is connecting.
  - **Disconnected**: else no access device is connected or connecting.

- **Data Security Field** - not used at network layer

Access Layer:

- **Access Device Icon**
  The graphical access icon on the left indicates the following:
  - **Media Type**
    - **wired** - designated by an ethernet connector port image
    - **wireless** - designated by a set of Signal Level bars
  - **Signal Level** - wireless only
    - one partially colored bar: very low signal
    - one colored bar: low signal
    - two colored bars: medium signal
    - three colored bars: good signal
    - four colored bars: very good signal

    Note: a ? is overlayed for a hidden access when not selected for a connection.
  - **Icon Connection Status** - a colored background overlay to both media type images
    - **Gray**: Disconnected (Not Connected)
    - **Yellow**: Connecting
    - **Green**: Connected with authentication
    - **Blue**: Connected without authentication
    - **Red**: Failed authentication attempt
    - X overlay: Not Available, No Adapter Available, Misconfigured, Not Capable

- **Network Field**
  - **Access Device Name** - assigned name for the access device
    Note: *For **wireless**, the assigned access name is typically the SSID of the access point.*
    *For **wired**, the assigned access name is typically the name of the ethernet adapter. (Unless all the members of the ethernet group are 'Not Available', in which case the name changes to its group '<ethernet>' name.)*
  - **Profile Status** (appended textual indication) - indication of how configurable the profile is.
    - **Locked** - profile configuration fixed by the deploying administrator.
    - (blank) - implies ***Unlocked***, profile may be modified by user.
  - **Scan-capable Status** (appended textual indication) - indication of wireless access's scanning type
    - **Hidden** - access device requires special active scanning method
      Note: *its availability can not be determined when in the 'No Adapter Available' state (it may in fact be physically present).*
    - (blank) - access device supports standard (typical) scan detection

- **Status Field**
  Note: *the connecting, connected and failed states may be augmented with a (**Machine**) suffix, indicating a machine connection.*
  - **Access Connection States**:
    - **Disconnected**: currently available but not attempting a connection (a transitory state for auto-connection).
    - **Connecting**: currently being used in an attempt to create a connection.
    - **Connected: Authenticated**: currently being used for an active connection and has an IP address (with 802.1x authentication).
    - **Connected: Unauthenticated**: currently being used for an active connection and has an IP address (without 802.1x authentication - not required).
    - **Not Available**: the configured access device is not presently detected.
    - **Failed (retrying)**: temporary state while attempting (N times) to authenticate and create a connection, but the last attempt failed.
      Similar to connecting status - manual disconnect control enabled.
    - **Failed**: authentication attempt(s) has failed (N trys were attempted).
      Selecting the access device will display the reason for the failure in the Message Status bar.

        - **Misconfigured Access**: access device is available, but the network profile configuration is not compatible with the associated access device. To aid in troubleshooting this condition, an expanded display conveys the following information:
            - **Capable for**: a list of association modes supported by the access device
            - **Configured for**: the configured association mode
        - **No Capable Adapter**: the adapter available for use with the access device is not compatible with (does not support) the network's configured mode.
        - **No Adapter Available**: access device is currently available but no extra adapters are free to connect to it.
          Note: *for a **hidden** access, no information can be obtained for the access device until an adapter becomes free (its availability is unknown).*
    - **Access Connection Type information**:
      The access devices's connection state is augmented (in parentheses) with auto connection status information. See controlling user connections for more details.
        - **Manual**: for networks in which user connections are not set for User AutoConnect.
        - **AutoConnect**: for networks in which user connections are set for User AutoConnect and a connection will be established as soon as an adapter is available.
        - **Suspended**: for networks in which user connections are set for User AutoConnect but the user has disconnected or canceled credentials or a connection attempt has failed and the access has been placed into a temporary manual-override condition; no connection will be established until the user intervenes.

- **Data Security Field**
  The ***second*** graphical icon and its text indicates the following for the configured mode:

    - **Security Level (Wireless**) - configured data encryption method
        - **X overlay on Lock: *None*** - indicates there is an open connection - **no encryption**.
        - **1 open Lock: *Good*** - indicates that there is weak (known to be breakable) encryption. Used for **WEP**.
        - **1 closed Lock: *Better*** - indicates that there is secure encryption. Used for **WPA** (generally with TKIP).
        - **2 closed Locks: *Best*** - indicates that there is the best known encryption. Used for **WPA2** (generally with AES).
    - **Security Level (Wired)**
        - ***Placeholder Port*** - **Wired**. Data encryption not applicable for ethernet media type.

Status Bar

Displays messages about the current activity of the client. Often used to clarify the reason for a failure, for example, why a connect attempt might have failed.

Display of Authentication Process:

Selecting a particular access device, enables the "**Details...**" activation text. ***Clicking*** on the "Details.." opens the **Information** dialog.

The **Information** dialog displays a real-time feedback of the individual steps of any (manual or auto) connection or disconnection process.

Note: the **Information** dialog is an independent window and will remain open while performing other operations from the main screen.

The messages are a subset of those recorded in the technical log (for example, the context modifiers and date are dropped for clarity). See understanding status messages for more details.

Selecting another access device or network, or using the **"Clear"** control clears the current display.

Related Main Screen Topics

Selecting the **Network** or **Access Device** allows it to be:

Manually Controlled by ***clicking***, when enabled, the **Connect / Disconnect** button.

Configured or Removed by ***clicking***, when enabled, the **Configure** and **Remove** buttons, respectively.
Note: not available in a Preset end-user client (Configure/Remove buttons not available).

Viewed by ***clicking***, when enabled, the **Summary** button.
Note: only applies to a locked, end-user network profile and its access devices.

Selecting a 'Connected' **Access Device** allows it to also be:

Viewed in detail by ***clicking***, when enabled, the **Status** button.

Additional Topics

View Available Access Devices

Additional Main Screen Options

Providing User Credentials

Controller User Connections

Viewing Detailed Connection Status

Connection Control Dialog

Selecting a ***connected*** Access Device in the **Manage Network** view enables the **Status** button and allows viewing its properties.

> **Note**: dynamic parameters will display real-time updates.

Connection Status Screen

Connection Details Tab:

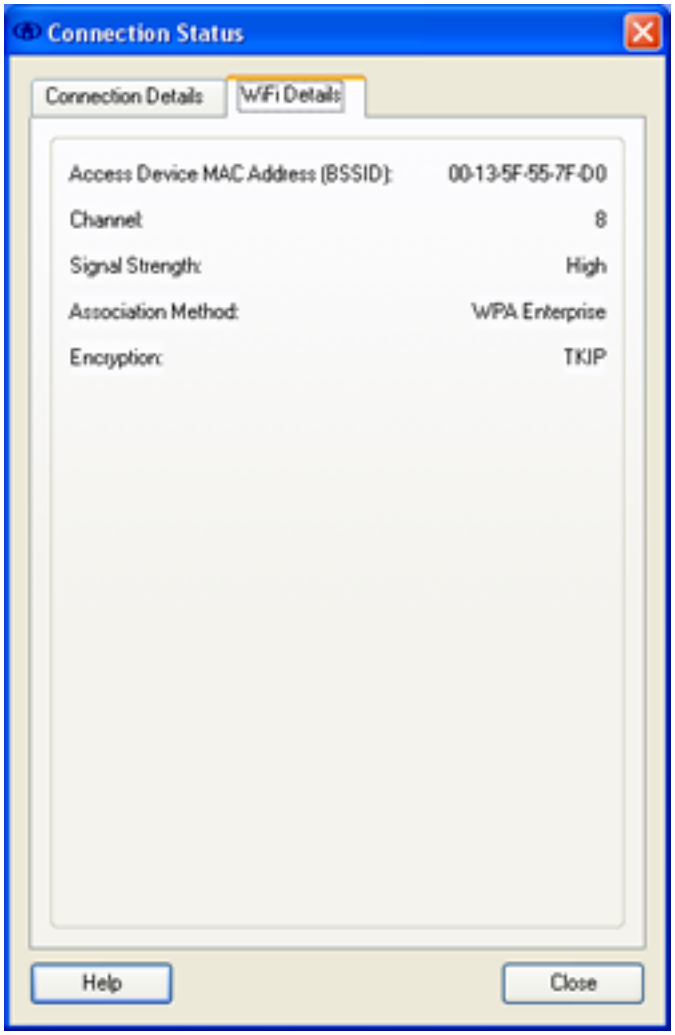
Displays details of the connection for the selected **Access Device**.

- **Status** - state of the connection (carried over from the Main Screen Access Port list)
- **Duration** - defines how long the connection has been operational
- **Network Profile** - friendly assigned name for the network
- **Network Adapter** - identifies the port's adapter name
- **Client MAC Address** - MAC address of the associated network adapter
- **Access Device** - assigned name for the access device
  Note: *For wireless, the assigned access name is typically the SSID of the access point.*

For wired, the assigned access name is the fixed generic name <ethernet>

- **Access Device MAC Address** - MAC address of the Access Point (wireless) or Switch (wired)
- **Transmitted packets** - actual number of layer 2 frames transmitted
  Note: *Windows displays the number of layer 3 data packets transmitted.*
- **Received packets** - actual number of layer 2 frames received
  Note: *Windows displays the number of layer 3 data packets received, which may be less.*
- **Speed** - indication of connection maximum data rate
- **Authentication Method** - Outer EAP Method used [Inner EAP Method used, as appropriate]
- **Authentication Server** - one of the following - augmented with an indication of either 'not verified' or 'trusted' (validation not performed or validation successful, respectively, as determined by policy)
  - the server certificate's name (for mutually authenticating EAP methods)
  - the server's FAST A-ID (for EAP-FAST)
  - 'unknown' (for non-mutually authenticating EAP methods)
  - blank when not performing 802.1x authentication
- **IP Address** - currently assigned value shown in standard x.x.x.x format

WiFi Details Tab:



Displays details of the wireless properties of the connection.

- **Access Device MAC Address (BSSID)** - MAC address (a.k.a. BSSID) of the wireless Access Point
  Note: *enables one to distinguish different access points with the same SSID.*
- **Channel** - The radio channel on which the network is communicating

  Note: *this can be used in conjunction with the speed to infer the 802.11 radio band, i.e., 802.11a, b or g.*

Radio	*Channel*	*Speed*
11b	1-11	11
11g	1-11	54
11a	36-64	54

- **Signal Strength** - five relative levels: very poor, poor, good, very good, excellent
- **Association Method** - indication of the WiFi association mechanism
  - WPA2-802.1X - most advanced key management and credential validation with an authentication server (2nd generation enterprise).
  - WPA2-PSK - most advanced key management and credential validation with a pre-shared key between client and access device (2nd generation home/small office).
  - WPA-802.1X - advanced key management and credential validation with an authentication server (enterprise).
  - WPA-PSK - advanced key management and credential validation with a pre-shared key between client and access device (home/small office).
  - Open - legacy 802.11 (with or without 802.1X).
  - Shared - legacy 802.11 with a shared static key between client and access device.
- **Encryption Method** - indication of the WiFi encryption mechanism
  - AES - (AES-CCMP) most advanced data security.
  - TKIP - advanced data security, entry level for WPA.
  - WEP - basic data security, disallowed by WPA.
  - None - no data security, disallowed by WPA.

Close Button:

Click the **Close** button to return to the **Connection Control** Main Screen.

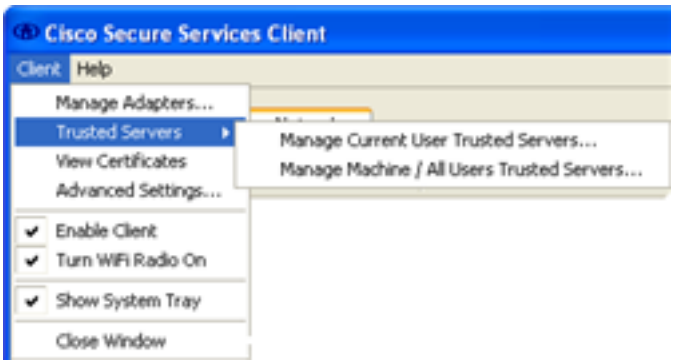
Related Topics:

Viewing the Network Connection

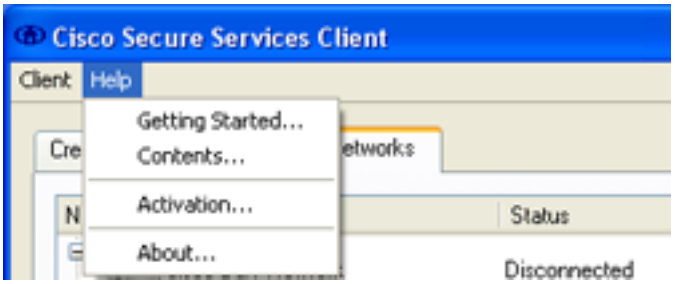
Understanding Main Screen Options

Main Menu

The Main Menu provides a convenient access to ancillary operations of the client:



(Manage Adapters, Trusted Servers,
Advanced Settings, WiFi Radio may not be present in end-user client)



(Activation may not be present in end-user client)

- **Client** Menu
  - **Manage Adapters** - configure an adapter's manage/unmanage state
    (***Policy dependent*** - may not be present in a deployed End-User Client)
  - **Trusted Servers** - configure servers and validation rules
    (***Policy dependent*** - may not be present in a deployed End-User Client)
    - **Manage User Trusted Server List** - associated with private profiles for current user connections.
    - **Manage Machine Trusted Server List** - associated with both public profiles for machine and all user connections and private profiles for current user connections.
      (***Policy dependent*** - locked in a deployed End-User Client - viewable only)
  - **View Certificates** - opens the **Certificates** dialog for viewing certificates.
  - **Advanced Settings** - Administrator options for global security settings - see managing advanced settings.
    (***Policy dependent*** - may not be present in a deployed End-User Client)
  - **Client:** - controls whether the Client is managing the adapters - see Client Option.
  - **WiFi Radio:** - controls the state of the radio for all managed wireless adapters - see WiFi Radio Option.
    (***Policy dependent*** - may not be present in a deployed End-User Client. Dependent on support for wireless media.)
  - **Show System Tray** check mark - controls display of client icon in the system tray.
    click on the current state to change states.
  - **Close Window** - closes the Client's user interface dialog.

- **Help** Menu
  - **Getting Started** - opens this **Help System** dialog at the Getting Started chapter.
  - **Contents** - opens this **Help System** dialog at the Main Screen Index of Operations.
  - **Activation** - opens the **Activate Product Features** dialog for access to viewing license status and ability to

add new licenses.
(***Policy dependent*** - may not be present in a deployed End-User Client)

- **About** - opens the **About Dialog** which provides the product name and version.
  Note: the client version has the format A.B.C.D (for example, 4.0.1.xxxx), where
  - A - denotes the product series.
  - B - incremented when significant feature and functionality enhancements are added to the previous version.
  - C - denotes bug fixes, with little or no added features and functionality.
  - D - internal build identifier for version A.B.C.

Allowed upgrades to your client, based on increments to fields B and C, are determined by your maintenance agreement.

Tip: **Shortcuts** - *with the Client window in focus, press the Alt key to enable displaying of the keyboard shortcuts for the menu bar items.*

System Tray Icon

Client Icon: 

Optional:
The use of the System Tray Icon is user optional and is controlled by the '**System Tray Icon**' client menu checkmark.

Usage:
The System Icon provides a convenient short-cut mechanism for opening the **Connection Control** Main Screen and other global adapter controls.

- **Left-click** or **right-click** - displays a pop-up menu with the following items.
  - **Open** - opens the Client's **Connection Control** Main Screen.
  - **About** - opens the **About Dialog** which provides the product name and version.
  - **Client:** - controls whether the Client is managing the adapters - see Client Option.
  - **WiFi Radio:** - controls the state of the radio for all managed wireless adapters - see WiFi Radio Option.
    (***Policy dependent*** - may not be present in a deployed End-User Client. Dependent on support for wireless media.)
- **Double-click** - automatically opens the Client's **Connection Control** Main Screen.

Connection Status:
The System Tray Icon has a circular colored background overlay indicating a summary connection status over the set of managed adapters, ordered as follows:

- **Blue**: Connected (no authentication required)
- **Green**: Connected (authenticated)
- **Yellow**: Connecting (authenticating)
- **Red**: Failed authentication
- **Gray**: Disconnected (idle/not connected) - rest state (when not in one of the above states)

Hovering over the system tray icon will display a summary connection status message over the set of managed adapters.

Global Client Options

Client Enable / Disable Control

Access via Main menu-**Client** or System Tray **Icon**.

Controls whether the Client is or is not managing the existing adapters (enabled/disabled) as follows:

- **[Checked] Enable Client** - Client is enabled and managing the configured network adapters
- **[Unchecked] Enable Client** - Client is disabled and Windows control of the adapters is re-established
  Note: new adapters added while in the disabled condition will be managed consistent with the client's policy.

click on the current state to change states.

Note: individual adapter management is still controlled via the Manage Adapter dialog.

Caution: when the client is re-enabled all adapters are managed by default.

WiFi Radio On / Off Control

Access via Main menu-**Client** or System Tray **Icon**.

Controls the state of the radio for all managed wireless adapters as follows:

- **[Checked] Turn WiFi Radio On** - Wireless adapter radio on.
  Note: when set to on, a scan is initiated to refresh the view of available wireless access devices and the connection process will re-start.
- **[Unchecked] Turn WiFi Radio On** - Wireless adapter radio off.
  Note: when set to off, any wireless access in the connecting/connected states will transition to disconnected.
  Note: while in the off state the **Status Bar** in the **Connection Control** Main Screen will indicate this condition.

click on the current state to change states.

Tips - ***auto turn-on*** of radio while **WiFi Radio** control set to **Off**:
If a particular adapter is 'unmanaged' via the **Manage Adapter** dialog, then the radio will be turned back on prior to unmanaging it.

If the **Client** control is set to 'Disabled', then the radio will be turned back on for all currently managed adapters.

If the Client Windows service is manually stopped, then the radio will be turned back on for all currently managed adapters.

Related Topics:

Understanding Connection Contexts

Connection Context Types

The Client provides for machine and user connections. Machine connections connect the machine to the network when there are no users logged onto the machine. User connections establish a network connection when a user is present on the machine.

Each network is configured to support one of following connection context combinations: (see also configuration summary)

User only Context Connection

Behavior:

Existence: User context connections are always enabled.
Connection initiation: Configurable option to select auto (at login - illustrated) or manual only (via desktop client - not illustrated) initiation.
Credentials: tied to current user.

System event	boot	login	logout	shutdown
	time ---------->			
Context Type		user		
Connection	no	yes	no	no
Credentials		user		

For configuring a normal User Context Connection see the procedure for creating a network.

Machine & User Context Connection

Behavior - Machine:

Existence: Requires setting configurable option to enable machine context connections.
Connection initiation: always auto, once enabled.
Credentials: tied to machine.

Behavior - User:

(Same as for User only Context)

System event	boot	login	logout	shutdown
	time ---------->			
Context Type	machine	user	machine	
Connection	yes	yes	yes	no
Credentials	machine	user	machine	

For configuring a normal Machine Context Connection see the procedure for configuring a machine connection.

Extended Machine only Context Connection

Behavior:

Existence: Requires setting configurable option to enable machine context connections and setting configurable option to automatically establish user connection.
Connection initiation: auto - based on above existence settings.
Credentials: tied to machine for both contexts

System event	boot	login	logout	shutdown
	time ---------->			
Context Type	machine	user	machine	
Connection	yes	yes	yes	no
Credentials	machine	machine	machine	

For configuring an extended Machine only Context Connection see the procedure for configuring an extended machine connection.

User only Machine Context Connection

Behavior:

Existence: User context connections are always enabled.
Connection initiation: always auto.
Credentials: tied to machine.

System event	boot	login	logout	shutdown
	time ---------->			
Context Type		user		
Connection	no	yes	no	no
Credentials		machine		

<return to beginning>

Machine and User Interactions:

If both machine and user context auto connections are enabled, then the following actions take place when moving from one context to another:

- **When the user logs on**
  The client will re-authenticate with the user's credentials and will test for IP (Layer 3) connectivity and obtain a new IP address if necessary.
- **When the user logs off**
  The client will re-authenticate with the machine credentials and will test for IP (Layer 3) connectivity and obtain a new IP address if necessary.

Note: If there are no valid credentials transitioning from machine to user or user to machine, the connection will be broken due to the failure to re-authenticate.

Note: If there is no IP connectivity then a DHCP renew is issued (to a specific address). If the renew does not succeed then a DHCP release / renew is issued (to a broadcast address). The connectivity check can take up to 20 seconds. The DHCP renew can take up to 30 seconds when it times out. The DHCP release / renew typically takes up to 10 seconds (unless there is no dhcp server).

<return to beginning>

Connection Context Configuration Summary

Connection Context Desired	**Network Profile Settings**		
	User Credentials (1)	**Automatically establish {Machine/User} connection** (2)	
		Machine	**User** (3)
User only	single sign-on | request	unchecked	checked | unchecked
Machine & User	single sign-on | request	checked	checked | unchecked
Extended Machine only	machine	checked	checked only
User only Machine	machine	unchecked	checked | unchecked

Notes:

(1) User Credentials are configured in the Network Profile>Network Authentication dialog
(2) Machine/User connections are configured in the Network Profile dialog.
(3) User context is always enabled - this setting is for determining auto connect (checked) or manual connect (unchecked)

<return to beginning>

Related Topics:

User Connections - Details

Machine Connections - Details

Controlling User Connections

Connection Control Main Screen

Auto Connect:

The Client will automatically attempt to establish a connection for any network that has been configured for "Automatically establish User connection" when the user logs on to the system. A restart of the auto-connection process occurs if:

- an existing connection is lost
- a connection attempt fails on one access device
- the set of available and configured Access Devices changes based on an updated wireless scan or wired link-up and there is a network adapter available
- a new adapter becomes available
- when the machine resumes (from hibernation or suspension)

Selection process: the connection process selects the correct auto-connect network profile, network adapter and access device to use based on environment (radio compatibility, etc.), policy (security level compatibility, etc.), available profiles and the preferred media type policy setting.

Once the *ranked list of potential connections* is established based on the above criteria, connections are attempted dependent on the current configuration of the **Simultaneous Connection** admin/policy setting. (***Policy dependent*** - may be preset and fixed in a deployed End-User Client)

Configured for **Multi-homed** connections:

A connection is attempted for all potential connections. For example, in a typical laptop environment with a single wired and a single wireless adapter, an auto-connect for one of its networks starts an authentication session on each of them. Therefore, assuming no authentication or other failures, two connections, one for each of the two different media types will be made.

Configured for **Single-homed** connections:

A connection is initially attempted only for the first-ranked potential connection. Only one connection is made at a time. For example, in a typical laptop environment with a single wired and a single wireless adapter, an auto-connect for one of its networks starts an authentication session on the wired port (**Note**: *wired is the preferred media type*). Furthermore, if the wired connection attempt fails, then the restart of the auto-connect process, as described above, will cause the client to start an authentication session on the wireless port. (See connection processing observations for additional behavioral comments.)

Connection failure: if an auto-connect attempt results in a failure, the associated access device is placed in a "temporary manual-override mode" and no further auto attempt to this access device will be made - see manual control below.

Note: *the status for the corresponding access device in the* ***Manage Networks*** *Main Screen will change from "AutoConnect" to "Suspended" to indicated this state.*

Exception - wired: The only exception is for a non-authenticating wired network. Windows will automatically establish a network connection in that case, independent of being in the auto-connect and/or single-homed modes. Therefore in order for ***single-homed*** to function properly, the wired connection must use an authenticating port. If a wired non-authenticating port is used, the client cannot control the connection, and therefore the system may become multi-homed, and proper single-homed operation is not supported.

<go back to creating a network profile>

Manual Control:

Manual control of the network connection is available for:

- making connections to non-auto-connect networks
- overriding of an auto-connected network with a manual selection
- re-connecting manually disconnected connections or failed connection attempts
- as a backup convenience (in case of some abnormal but plausible event) on auto-connect networks.

Note: manual network connection behavior for a multi-homed configured system is slightly different than for auto-connect, as described above, for example, in a typical laptop environment with a single wired and a single wireless adapter, a manual-connect for one of its (non auto-connect) networks only starts an authentication session on the adapter with the "highest signal" - which for this case, by definition, is the wired 'access' . Therefore, assuming no authentication or other failures, one wired connection will be made.

Note: All access devices within a network configured for manual user connections will have their status in the ***Manage Networks*** *Main Screen* indicated as "Manual".

Connect Button

Enabled when selected network or access device is 'Disconnected' or 'Failed'. ***Clicking*** causes the connection process to run on this selection.

When selecting a ***specific access device***, a connection attempt will be made to this device (independent of (overriding) auto-selection rules).

When selecting a ***network***, a connection attempt will be made to the access device as determined by the auto-selection rules within this network.

Disconnect Button

Enabled when selected network or access device is 'Connecting' or 'Connected'. ***Clicking*** causes a permanent disconnect.

When selecting a ***specific access device***, a disconnect for that device will be made.
Note: *the associated access device is now in "temporary manual-override mode" and no auto attempt to it will be made. However, any existing connection to another access device within this network will be maintained.*
The status for the corresponding access device in the ***Manage Networks*** *Main Screen will change from "AutoConnect" to "Suspended" to indicated this state.*

When selecting a ***network***, a disconnect for all devices within this network will be made.
Note: *the associated network is now in "temporary manual-override mode" and no auto attempt to any access devices within this network will be made.*

Note: for an auto-connect network, return to auto mode will be made after any of the following actions:
- re-configuration of the network or one of its access devices.
- manual connect (or disconnect/connect) operation (at parent network level).
- the client service is restarted or system reboot - on client startup no network profiles will be in the "temporary auto-exclusion mode".
- for single-homed environments, restart of the auto-connect process

Connection processing observations:

v **Connection attempt failures:**

In general a connection request will make N internal attempts to associate/authenticate.

- **Non-Interactive (N=1)**: for cases in which a user intervention would not help to correct the fault. In general, this applies to connection attempts not involving an **Enter Your Credentials** Pop-up, such as, a PSK mismatch, or all failures associated with a server certificate validation (invalid certificate chain, invalid or

missing CA certificate, or invalid trusted server rule).

- **Interactive (N>1)**: for cases in which a user intervention might correct the fault. In general, this applies to connection attempts involving user text entry or list selection associated with an **Enter Your Credentials** Pop-up, to allow for user corrections.

(***Policy dependent*** - for both cases, the value of 'N' is admin configurable and is preset and fixed in a deployed End-User Client)

Once a connection request moves to the ***Failed*** state, selecting the associated access device will display the reason for the failure in the **Message Status** bar. (The network will automatically be expanded, if not already, with the failed access selected - thereby forcing the reason-for-failure display.) A subsequent manual connect request will clear the failure and start the connection process over.

v **Single-homed connections:**

For single-homed to function properly, all wired connections must use an authenticating port. If a wired non-authenticating port is used, the client cannot control the connection, and therefore the system may become multi-homed, and proper single-homed operation is not supported.

Auto media preference:
If an auto-connection exists to the wireless (non-preferred) media type and the environment changes making the wired (preferred) media type of connection available (for example, plugging in of Ethernet cable), a change in connection will be attempted and this will cause a disruption in the network connectivity (disconnect before re-connect). The inverse is not true - a connection to the wired (preferred) media type will not change when environment changes make the wireless media available. Only a loss of the wired connection will cause a re-connect attempt on the wireless.

v **'No Authenticate' networks:**

'No Authenticate' configured networks consist of access devices that also either do not have any data encryption (a completely open network) or do utilize one of the shared-key data encryption protocols (WEP or PSK). Therefore there is always a small delay in connecting to these networks in order to first transmit 802.1X EAPOL-Start messages. These are sent to improve the end-user experience. These are to detect when the end station is connected to an authenticating NAS and inform the end-user why the client is unable to connect to that network.

A connection attempt in which there is an error in the shared key will fail since it will not be able to properly obtain an IP address.

v **Connection loss:**

When a connection is broken because of service shutdown, un-managing an adapter or the computer is being shutdown, the client will send an EAPOL-logoff and disassociate for WiFi connections.

v **Support for Remote Desktop:**

Restricted support for Windows Remote Desktop allows an administrator to remotely take over a local user session. The SSC user interface (UI) will migrate onto the remote desktop, allowing the administrator full control. When the remote user (administrator) logs out or the local user forces the remote user to log out, SSC will migrate back to the local user. .

Authentications take place as follows:

- On the transition between the local user and the administrator, SSC will not trigger any 802.1X authentication. However, if re-authentication is triggered by the network, SSC will use the administrator's credentials.

- Once the administrator logs out, SSC will trigger a machine re-authentication as usual. When the local user logs in, SSC will trigger a user re-authentication as usual.

Restrictions for this scenario to work include:

- The client must be configured to support both machine and user auto-connect and the administrator must have valid credentials to do the 802.1X authentication.

- Remote desktop may not be configured to allow the local machine to ask permission from the currently logged-in user

to be interrupted/logged out by a remote session. If configured with this feature, the SSC tray icon does not show up on the remote desktop and does not show up on the local desktop after a local login. Restoring the icon on the local desktop requires a local logout and login.

- **Support for IPv6:**

  If an adapter has only the Microsoft TCP/IP version 6 protocol enabled and the IPv4 protocol disabled, the client indicates it is unable to obtain a valid IP address.

Related Topics:

Viewing the Network Connection

Providing Credentials

Configuring Simultaneous Connections

Providing User Credentials

Credentials are assigned on a per Network basis - all Access Devices configured for that network use the same credentials. Credentials are part of the associated Network Profile.

Topics:

User Credential Types

The authentication methods used by the Client allow for the following types of user credentials:

- Mandatory Elements
  - **Identity**
    An Identity has a Network Access Identifier (NAI) format and takes the following generalized form: **UserName [@ Domain]**, where the use of the '@ domain' (a.k.a. realm) is optional - based on the requirements of the specific authentication server.

    The identity specified may contain up to 63 ASCII characters and is case sensitive.

    Note: ***Domain Details***
    All EAP methods send an unprotected identity as a response to the initial EAP Request/ Identity.
    In the following details, no processing is done on [domain]. So regardless of whether it is a domain alias (not fully qualified) or a fully qualified domain name, what is entered is sent.
    For tunneled methods see configure unprotected identity for substitution of [userName] with "anonymous" in the following details.

    For Single-Sign-on credential collection:
    If one types [domain]/[userName] for the identity in the SSO text entry box, [userName]@[domain] will be sent.

    If one types [userName]@[domain] for the identity in the SSO text entry box, [userName]@[domain] will be sent.

    If one types [userName] and then select a [domain] from a SSO drop-down list, [userName]@[domain] will be sent.

    For Prompt credential collection:
    If one types [userName]@[domain] for the identity in the Prompt for Credential text entry box, [userName]@[domain] will be sent.

    Tip: When using the single-sign-on credential collection method, be aware that Windows is not case sensitive and will allow logon to Windows accordingly. This will lead to inconsistencies and possible incorrect behavior because the Windows logon userName and the network authentication identity will not match. *Always logon to Windows with the same case syntax as your authentication identity.*

- Optional Elements (at least one method required)

- **Password**
  It may contain up to 80 ASCII characters and is case sensitive.

- **User Certificate**
  A user certificate is ***obtained*** from either the appropriate **Windows Certificate Store** (Personal Certificate Store for the currently logged in Windows user) or, additionally, from a **SmartCard** through any detected smart card reader.
  - **SmartCard:**
    Supports both local and domain login environments.
    Limitation: *only a single (the first one detected) smartcard reader is supported.*
    PIN support (two-factor authentication) - prompted when required via **Enter Your Credentials** Pop-up dialog or SSO GINA. The allowed maximum length is 63 characters.
    PIN behavior is dependent on the assigned user credential collection method.
    - Desktop Request&Save: PINs are not stored - independent of the configured "store" mode and therefore will be subsequently requested again under certain situations, such as, whenever a server initiated re-authentication is required (unless the EAP method is configured for fast session resumption), roaming, a failed re-authentication, lost association, resumption from hibernate.
    - SSO: PINs are stored for the duration of the logon session. Therefore, subsequent pop-up requests are, in general, avoided.

    Note: the Client only supports SmartCards that support the Microsoft CryptoAPI and SCard interfaces (interfaces to Cryptographic Service Provider functionality). Furthermore, any smartcard reader and smartcard combination must inter-operate via the PC/SC interface to provide low level support for these same CSP functions.

    Note: Multiple certificates from a single SmartCard are supported.

  - **Windows Certificate:**
    Note: *if a Windows user certificate is required as part of the authentication process, it must be appropriately pre-installed as a separate task.*
    Tip: see Microsoft certificate management.

    Limitation: not supported with domain login environments - see understanding domain login.
    Restriction: when configured for 'Automatically establish user connection', a certificate with 'strong private key protection' will fail at logon and should not be used. Certificates with this property are only supported when configured for always making manual connections at desktop.

    The identifying information for the selected certificate in the selection pull-down list is obtained from the various fields of the certificate as follows:
    - text box name - Subject: CN (Common Name)
    - Issued to: - Subject: CN (Common Name)
    - Issued by: - Issuer: CN (Common Name)
    - Alternative Name: - Subject Alternate Name: DNSName
    - Expires: - Valid to
    - Extended Key Usage - Extended Key Usage

    Validity check: Only valid certificates are displayed for selection. Expired certificates are not listed. Also, valid certificates that are about to expire contain a warning that shows how many days left before the certificate expires.

    Extended Key Usage Filtering: (***Policy dependent*** - the network policy in a deployed End-User Client may restrict the choice of acceptable certificates based on Extended Key Usage values.)

  Procedure: **Viewing Client Certificates**

  Step 1: from the **Client** menu, ***select*** **View Certificates** to open the **Certificates** dialog.

  Step 2: ***view*** all the stored certificates in the **Certificates** display pane.
  Disallowed certificates will display an explanation, such as, Expired or Filtered by Policy Rules, in the **Notes** column.

  Step 3: ***select*** a displayed certificate to view its detailed information in the **Certificate Details** pane.
  The detailed information for the selected certificate consists of the following:
  - Issued to: - Subject: CN (Common Name)
  - Issued by: - Issuer: CN (Common Name)
  - Alternative Name: - Subject Alternate Name: DNSName
  - Expires: - Valid to

- Extended Key Usage - Extended Key Usage

- **PAC**
  Only used with EAP-FAST authentication method, whose protocol provides for creating and client provisioning. (See an EAP methods overview for more details.)

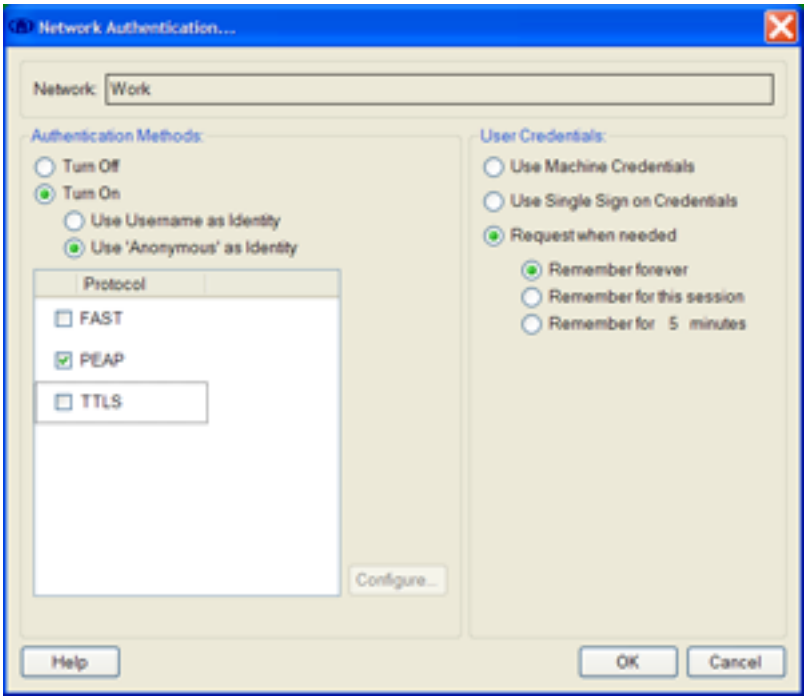
  Note: A tunnel (user) PAC is stored such that it is tied to the user for which it was created. Only a user that logs in to the account with the same username/password will be able to use it.

Note: *a set of credential optional elements will be associated with a particular network, which may have several wired and wireless access devices. If a particular type of credentials is requested by a supported authentication method (protocol), and they have been provisioned, they will be used. If they have not been provisioned then the user will be asked for them.*

The type of credential required for a specific authentication session is determined by the settings of the authentication server and is automatically processed by the Client.

<return to configuring the network profile authentication>

User Credential Collection Methods



Credentials can be configured as part of the **Network Authentication** dialog to be obtained via the following methods:

- **Single-Sign-on**
  Credentials, specifically user-name/passwords, entered by a user for the operating system logon (typically in a pop-up dialog) will also be used for authentication. No client provisioning is required.
  For example, if authentication should be based on the user's Windows or Novell logon name and password.

- **Request *when needed* and Store** (***default***)
  on-demand- requested by the client at the appropriated time during its first connection attempt for the network. A series of appropriate **Enter Your Credentials**Pop-up dialogs are progressively displayed to the user with prompts and mechanisms for entering the desired information.
  Note: *canceling a request for credentials will cause the network to revert to the idle (no connection) state, even if designated as auto-connect. After which a manual connect operation is required to initiate another connection attempt.*

Tip - password Enter Your Credentials dialog:
The Client will retrieve any password prompt message that the network is passing along for viewing by the user and will substitute it for the generic "Please enter your credentials". For example, one common invocation of the password format when using EAP-GTC to support ***token cards*** (two-factor authentication) is a concatenation of the user's static PIN + the time-limited Token. A server provided text would be displayed to make it clear to the user what needs to be entered into the "password" textbox.

Credentials will be encrypted and ***stored***as follows:
choosea save-for duration to **Remember credentials**. (***Policy dependent***- how long credentials may be saved may not be selectable or have a limited set of options in a deployed End-User Client)

- **Forever** (***default***) - essentially equivalent to providing static credentials.
  Note: The identity and password are stored (encrypted) such that they are tied to the user for which it was created.
- **For the User Session** - saved only while the connection lasts - until the user logs out. The credentials will be forgotten after the connection session is ended.
- **For *specified* Time** - saved only for configured time (in minutes) interval. (***Policy dependent*** - actual time is set by the policy.)
  After the time-out, re-authentication requests will force the user to re-enter the credentials via the pop-up (which will restart the duration timer). The credentials will be forgotten after the time interval is ended.
  The specified time must be between 1 - 3600 (1 minute to approximately 2 1/2 days).
  Note: *since the specific time is set in the policy, it therefore applies to (is the same for) all network profiles.*

- **Use Machine Credentials**
  Special option used to support the extended machine only connection context in which the use of unique user credentials (either of the above options) is replaced by the machine credential. (Therefore all users essentially are not differentiated and are presumed to be authenticated via another method, such as, at layer 3.) See machine credentials as part of configuring an extended machine only connection.

<return to configuring the network profile authentication>

Initial Credential Provisioning

Typically during the first connection attempt to a new network, specific user credential information will be required to be provisioned. It is requested by the client at the appropriated time during its first connection attempt. A series of appropriate **Enter Your Credentials** Pop-up dialogs are progressively displayed to the user with prompts and mechanisms for entering the desired information.

Note: ***canceling*** a credential request in the **Enter Your Credentials** Pop-up dialogs is treated the same as a **Disconnect** operation and converts the network to the 'temporary manual-override mode', as appropriate (see controlling user connections for related information).

Note: a ***smart card*** provided certificate usually has a PIN associated with its access. It is also requested, on-demand, by the client at the appropriated time during its first connection attempt, via a PIN **Enter Your Credentials** pop-up. At that point the user is given the opportunity to remember (save forever) it, avoiding any future prompting.

Ongoing Credential Changing

Policy Initiated:
Where credentials are not stored forever after initial entry, re-prompting of the user via the appropriate **Enter Your Credentials** Pop-ups will occur when a re-authentication takes place after the temporary save period.

Server Initiated:
During an authentication attempt, in addition to cases where the credentials fail to be accepted by the server, the server may employ policies such as password aging that will also automatically cause re-prompting of the user via the appropriate **Enter Your Credentials** Pop-ups.

Note: tunneled MSCHAPv2 supports password change, tunneled GTC does not (even if "allowed" by the server).

User Initiated:

For a locked, deployed end-user network, the user can manually force a re-prompting for different credentials by the following procedure:

***Procedure:* Clear Credentials**

Step 1: ***select*** on the **Connection Control (Network View)** Main Screen, the Locked Network of interest.
Step 2: ***click*** the **Summary** button » to open the **Network Configuration Summary** screen.
Step 3: click the **Clear Stored Credentials** button to force a re-prompt for user credentials on the next connection attempt.
Note: the control is enabled if the credentials are remembered. When the user clears the credentials, the control will become disabled.

Tip: for an administrator or configurable end-user network, credentials are cleared when ever the network profile's advanced settings are modified.

***Procedure:* Re-configure Credentials**

Step 1: ***select*** on the **Connection Control (Network View)** Main Screen, the Locked Network of interest.
Step 2: ***click*** the **Configure** button » to open the **Network Profile Configuration** screen.
Step 3: ***click*** the **Modify** button » to open the **Network Authentication** screen.
Step 4: ***click*** **OK**, then **OK** again, to return to the **Connection Control** Main Screen without modifying the profile but indirectly clearing any stored credentials.

Tips:

v **Errors while entering your credentials**

With the **Enter Your Credentials** dialog displayed but before completing entering your information, if the client detects the absence of the targeted access point (due to a borderline signal), then either a "connection unexpectedly terminated" or a "credentials request has expired" error message dialog will appear, depending on where in the association/authentication process the loss is detected.

An error of "no certificate in personal store" also applies to the case of no smartcard in its reader (a smartcard will appear as a Windows personal certificate store entry).

v **Windows Certificate Management**

The Client uses the Microsoft Certificate Store as the local certificate repository for the client certificates.

To check the field of a client/user certificate associated with the current user, open the Internet Options Control Panel (either Settings> Control Panel> Internet Options> Content> Certificates, or from Internet Explorer, open the Tools menu and select Internet Options> Content> Certificates).

To check the field of a machine certificate associated with the local computer, open the Microsoft Management Console (Start> run> open: mmc). The appropriate “snap-in” is added through the Console> Add/Remove Snap-in> Add> Certificates> Add> Computer account> Next> local computer> Finish.

In both cases, choose the correct certificate and click View, after the certificate screen appears, click the Details tab and click the appropriate field item.

Understanding Domain Log-in

Logging in to a domain environment where the login credentials are verified remotely by the network domain server requires that an authenticated network connection be established before the domain login process. Additionally, the client often needs to provide network connectivity early enough so that OS and 3rd-party processes and services (which may or may not contribute directly to the domain login process) that require network connectivity shall have one.

Domain vs. Authentication Credentials

The user domain credentials and 802.1x authentication credentials may or may not be the same and are configured via the **User Credentials** pane of the **Network Authentication** dialog (p/o Network Profile configuration) - see credential collection methods for more information.

- **Use Single Sign on Credentials** - (***typical***) use the domain login credentials also for network authentication.
- **Request when needed** - (supported) configure unique user credentials for network authentication.

Microsoft Active Directory Domain

Connection Configurations

One or both of the Network Profile's automatic connection settings must be enabled.

- **Automatically establish Machine connection** - only option

  No additional configuring required - see configuring machine connections for more information.

- **Automatically establish User connection** - only option

  Further configuration to clarify the order of domain login and network connection is required.

  Network connection first: ***typical case - (default)***.

  Requires ***checking*** the Network Profile's (Automatically establish User connection) '**Before user account (supports smartcard/password only)**' check-box.

  Requires password or smartcard user credential types.
  Note: a client certificate is not supported because the client cannot obtain access to the client certificate in the Microsoft certificate store until AFTER domain login. A smartcard, although technically a client certificate, acts like a machine certificate since it is available externally to the operating system and are not stored in the user's Windows profile.

  1. Login Window - user types their identity and password into the Microsoft Windows login screen and clicks 'OK'.
  2. User Network Connect - the client intercepts and holds off the login process while it carries out its required network authentication processing.
  3. Windows Domain Login - once the connection is completed the client will allow the normal windows login procedure to continue. At this point access to user registry and importing of User Group Policy can take place.

  Domain login first: rare case - limited environment.

Requires Microsoft ***cached credentials***.

Requires ***unchecking*** the Network Profile's (Automatically establish User connection) '**Before user account (supports smartcard / password only**)' check-box.

Allows for user certificate (from the Windows certificate store) user credential type.

1. Login Window - user types their identity and password into the Domain login screen and clicks 'OK'.
2. Windows Domain Login - normal login process takes place locally on the machine but User Group Policy is not available yet.
3. User Network Connect - the client carries out its required network authentication processing. Only at this point can importing of User Group Policy take place.

- **Automatically establish Machine & User connection** - both options

Further configuration to clarify the order of domain login and network connection is required.
Note: *for password and smartcard user credentials the setting of the '**Before user account** ..' may be configured either way - depending on the details of any Group Policy processing, as described below.*

Unchecking the Network Profile's (Automatically establish User connection) '**Before user account (supports smartcard / password only**)' check-box.

Allows for all user credential types, including user certificate (from the Windows certificate store).

Allows for User Group Policy processing via the network connection via machine as long as no IP change is required when transferring between the machine and user contexts, as follows:

1. Machine Network Connect - an early network connection is created using the machine credentials.
2. Login Window - user types their identity and password into the Microsoft Windows login screen and clicks 'OK'
3. Windows Domain Login - once the connection is completed the client will allow the normal windows login procedure to continue. At this point access to user registry and importing of User Group Policy can take place.
4. User Network Connect - the client re-authenticates the network connection using the user credentials.

Checking the Network Profile's (Automatically establish User connection) '**Before user account (supports smartcard / password only**)' check-box.

Allows for User Group Policy processing via the network connection via user and an IP change if required when transferring between the machine and user contexts, for example, if accompanied by a VLAN change, as follows:

1. Machine Network Connect - an early network connection is created using the machine credentials.
2. Login Window - user types their identity and password into the Microsoft Windows login screen and clicks 'OK'.
3. User Network Connect - the client intercepts and holds off the login process while it carries out its required network authentication processing (and change of IP, if necessary).
4. Windows Domain Login - once the connection is completed the client will allow the normal windows login procedure to continue. At this point access to user registry and importing of User Group Policy can take place.

Novell Domain

On system startup the user will be presented with the normal Novell logon screen. After appropriately supplying the Novell credentials logon will proceed. However the process will first be diverted to the Client to authenticate to the network and establish layer 2 connectivity and then, following a successful authentication, allow the Novell Client to login the user to the Novell network.

Novell modes of operation are limited as follows:

- Supported modes of operation:
  - Normal (Context and Tree specified) Login
  - LDAP Contextless Login - Context is missing and the Server and Tree are used to locate and calculate the username.
- Non-supported modes of operation:
  - Treeless Login
  - DSCAT Contextless Login - must be disabled in the Novell Client Configuration

To support this functionality the following setup procedures must be applied:

Novell configuration:

- If the Novell contextless mode of operation is desired, the following settings are required.
  - The Novell Client must be configured to have all LDAP modes of operation disabled (both Treeless and Contextless).
    - It must be configured through the Novell Client Configuration screen, temporarily, enabling the appropriate modes to enable setting up the tree and server information only. Then disabling all LDAP modes after configuration is complete. (All of the '**Enable LDAP ....**' checkboxes must be unchecked when done configuring.)
      Note: the Novell Client must be set up to authenticate to the Novell network as if the context is always specified. The Novell Contextless LDAP username lookup will be filtered to the contexts configured in the appropriate Novell registry.
      Note: Cisco Secure Services Client selects the Novell mode by detecting whether or not the context text field on the Novell GINA is filled in or not. If it's blank, then contextless login is performed.
  - ***enable*** '**Clear Current Connections**' (This allows you to clear all previous connections when you create a new connection to the network.)
    - enable the "Clear Current Connections Box" (Advanced Login › Clear Connections) - this will allow access to the 'Clear Connections' checkbox in the GINA.
      or
    - check the 'Clear Current Connections' checkbox (Location Profiles › Default › Properties › Login Service › Properties › NDS)
  - context caching:
    - if the end station will be used for multiple users, ***turn off*** the '**Save last successful login**' feature. (Otherwise later users will not be aware that they need to change their context and the Novell login will fail.)
    - if the end station will be used only by a single user, ***turn on*** the '**Save last successful login**' feature. (It is beneficial to have context cached so that LDAP searches are not performed every time.)
- If the Novell normal mode (default) of operation is desired, no further configuring is required. The context, tree and server information must be supplied in the Novell GINA.
- Authentication support:
  It is recommended that the following setting be configured for all EAP methods, but especially if using EAP-FAST and could ever have an expired PAC.
  - ***set* to 0** the '**Bad Address Cache Timeout**' parameter - located on the Advanced Setting tab of the Novell Client Configuration dialog.

Cisco Secure Services Client configuration:

The Network Profile must be configured as follows:

- **Connection configurations**:
  - always ***check*** the '**Automatically establish User connection**' checkbox
    - always ***check*** the associated '**Before user account (supports smartcard/password only)**' check-box.
  - optionally configure the ' **Automatically establish Machine connection**' as required.
- **Authentication credentials**:
  - if '**Use Single Sign on Credentials**' is configured, then the authentication credentials are taken from the Novell GINA (the Microsoft GINA is not used for authentication).
- **User credential types**:
  - only passwords and smartcards are supported (user client certificates from the Windows certificate store are not supported for Novell login).

Notes:

v **Tree or Server not found**
If you are experiencing the "Tree or Server not found" error there is a patch on the Novell web site that should address this.

v **Limitations**:
As a result of this sequencing, some of the familiar functions on the Novell logon screen will not work. The tree, contexts, and servers buttons cannot perform a lookup without network connectivity.

v **Novell "Workstation only" mode**
If the "Workstation only" checkbox is enabled in the Novell login window, then network authentication will take place but without any Novell login. For example, this allows for support of both a "work" network profile which would be used for Novell network connectivity in the work location and a "home" network profile which, when used in conjunction with checking the "Workstation only" checkbox, would be used for local network connectivity in the home location.

v **Novell Login when recovering from Standby or Hibernate**
When recovering from standby or hibernate, the Novell GINA may appear before the client can restore the network connection (there is no Novell indication available to delay the GINA's appearance). The user can enter the correct Novell user name and password, but the machine cannot find the Novell server. You need to wait approximately 20-30 seconds to permit the client to establish a wireless connection. Then attempt to log into the Novell server and the desktop again.

v **Cisco Secure Services Client and Novell Client Installation**
The Novell Client may be installed prior to or after the installation of the Cisco Secure Services Client. However if the Novell client is ever uninstalled and then subsequently re-installed, then the Cisco Secure Services Client must also be uninstalled and re-installed in order to have the proper registry entry hierarchy in place.

Machine Connections

Machine Credentials

Machine credentials consist of the following supported types (EAP method dependent):

- **Machine certificate** - uses the Microsoft Active Directory provided machine certificate, or equivalent, with a TLS-based EAP method.
  A machine certificate must be in the appropriate **Windows Certificate Store** (Personal Certificate Store for the Local Computer). (See also, certificate key permissions.)

  Restriction: Normally only a single certificate will be stored here. However, for cases when multiple certificates are present (e.g., temporary overlap while provisioning a newer certificate to replace an old one or provisioning from different certificate authorities) the first valid certificate found is used.
  Restriction: The certificate must not require a PIN or have strong private key protection.

  Note: *the machine identity is provisioned from the machine certificate (the 'dnsName' field of the Subject Alternative Name).*
  Note: *Another aspect of machine authentication is that the domain controller containing the computer must be performing the machine authentication. The policy for the computer must automatically enroll the computer for a machine certificate.*

- **Machine Password** - uses the Microsoft Active Directory provided machine password with a password-based EAP method, such as, EAP-MSCHAPv2.

- **Machine PAC** - only used with EAP-FAST and only supported in newer versions of authentication servers (e.g., ACS 4 or later) which have been upgraded to support EAP-FAST v1a.

  Note: A machine PAC is stored such that it is tied to the specific end station. If it is copied off to another end station, it will not be usable.

  Tip: You can not access stored machine PACs after reinstalling Windows - new PACs must be reprovisioned.

Configuring Normal Machine Connections

A normal machine connection is one that takes place in the background whenever a user is not logged in. (See understanding connection contexts.)

Note - Machine GPO: When using Microsoft's machine group policies, see Tips.

Machine connections are also subject to the **simultaneous connection** admin/policy setting of either multi-homed or single-homed, see configuring simultaneous connections. (***Policy dependent*** - preset and fixed in a deployed End-User Client)

Configured for **Multi-homed** connections:
A connection is attempted for all potential connections. For example, in a typical laptop environment

with a single wired and a single wireless adapter, an auto-connect for one of its networks starts an authentication session on each of them. Therefore, assuming no authentication or other failures, two connections, one for each of the two different media types will be made.

Configured for **Single-homed** connections:

A connection is initially attempted only for the first-ranked potential connection. Only one connection is made at a time.
Note: ranking is dependent on wired/Ethernet being the preferred media type and wireless signal strength.

Configuring for normal machine connectivity simply requires that the network be modified to enable the feature.

Note: ***Policy dependent*** - a deployed end-user client may only create machine connections with non-authenticating network connections (PSK, WEP) since only the deploying administrator is permitted to create machine trusted server rules.

Configure a **Network Profile** for Machine connectivity via the following procedure:

Procedure: Configuring a Machine Connection

Step 1a: when **creating** a network: from the **Connection Control (Create Networks)** Main Screen, by ***clicking*** the **Create Network** button » to open the **Network Profile Configuration** dialog.
or
Step 1b: when **modifying** a network: from the **Connection Control (Manage Networks)** Main Screen, by ***selecting*** the Network of interest, and ***clicking*** the **Configure** button » to open the **Network Profile Configuration** dialog in the advanced mode.

Step 2: **Auto Connect** settings:

- ***check*** the **Automatically establish Machine connection** checkbox to enable machine context connections. (The ***default*** is unchecked.) This will also enable the **Available to all users (public profile)** checkbox to allow this network to have a machine connection.

Step 3: if using authentication, ***ensure*** that a compatible machine credential type has been pre-configured:

See machine credential types above.

Step 4: if using authentication, ***ensure*** that one of the following compatible EAP methods is enabled:

Note: *for a certificate credential, the authentication method must support the use of a certificate to provide machine client credentials.*

EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS
Note: *for any of the tunneled methods (FAST, PEAP, TTLS) the server must be appropriately configured to call for an inner tunnel method of TLS.*

Note: *for a password credential, the authentication method must support the use of a password to provide machine client credentials.*

Note: the client autonomously seeks the correct credential type based on the EAP method initiated by the authentication server.

Step 5: ***click*** the **OK** button to accept the changes to the Network and return to the **Connection Control** Main Screen.
(Or ***click*** the **Cancel** button to return without modifying the Network.)

Tips:

- **Windows store key permission for machine certificates**

The *Key Container file* must have full access for SYSTEM, and read access for local admin.

> **Note**: The key container file is a file that has the name <certificate hash>_<MachineGuid> and resides in the MachineKeys directory which can be found at: "C:\Documents and Settings \All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys\".
>
> If the MachineKeys directory doesn't exist then autoenrollment creates the directory with the following permissions for "everyone":
> - List Folder / Read Data
> - Read Extended Attributes
> - Create Files / Write Data
> - Create Folders / Append Data
> - Write Attributes
> - Write Extended Attributes
> - Read Permissions

If the permissions for the MachineKeys directory are not set correctly then the key container file will be created with incorrect permissions which prevents applications from accessing it. The client will not be able to access the key store and therefore not be able to send the machine certificate, resulting in failure of the authentication attempt.

<go back to creating a network profile>

<go back to modifying a network profile>

Machine only Connections

Configuring Extended Machine only Connections

An extended machine only connection is one that takes place permanently in the background independent of any user differentiation. With this type of connection context configuration it is presumed that any user authentication is taking place via another mechanism, such as, at layer 3. (See understanding connection contexts.)

Note - Machine GPO: When using Microsoft's machine group policies, see machine certificate tips.

Configuring for extended machine only connectivity requires that the network be configured for a specific set of machine and user options.

Note: ***Policy dependent*** - a deployed end-user client may only create machine connections with non-authenticating network connections (PSK, WEP) since only the deploying administrator is permitted to create machine trusted server rules.

Configure a **Network Profile** for Machine connectivity via the following procedure:

Procedure: Configuring an Extended Machine Connection

Step 1a: when **creating** a network: from the **Connection Control (Create Networks)** Main Screen, by ***clicking*** the **Create Network** button » to open the **Network Profile Configuration** dialog.
or
Step 1b: when **modifying** a network: from the **Connection Control (Manage Networks)** Main Screen, by ***selecting*** the Network of interest, and ***clicking*** the **Configure** button » to open the **Network Profile Configuration** dialog in the advanced mode.

Step 2: **Auto Connect** settings:

- ***check*** the **Automatically establish Machine connection** checkbox to enable machine context connections. (The ***default*** is unchecked.) This will also enable the **Available to all users (public profile)** checkbox to allow this network to have a machine connection.
- ***check*** the **Automatically establish User connection** checkbox to ensure a continuous connection independent of user login/logout. (The ***default*** is unchecked.)
    - ***uncheck*** the **Before user account** checkbox (not required for this scenario). (The ***default*** is checked.)

Step 3: if using authentication, ***ensure*** that a compatible machine credential type has been pre-configured:

See machine credential types.

Step 4: ***initiate*** advanced configuring by ***clicking*** the **Modify** button » to open the **Network Authentication** dialog.

Step 5: **Authentication Methods**: if using authentication, ***ensure*** that one of the following compatible EAP methods is enabled:

Note: *for a certificate credential, the authentication method must support the use of a certificate to provide machine client credentials.*

EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS

Note: *for any of the tunneled methods (FAST, PEAP, TTLS) the server must be appropriately configured to call for an inner tunnel method of TLS.*

Note: *for a SID credential, the authentication method must support the use of a password to provide machine client credentials.*

Note: the client autonomously seeks the correct credential type based on the EAP method initiated by the authentication server.

Step 6: **User Credentials**:

- ***select*** the **Use Machine Credentials** (special) option - this setting is required for this scenario.

Step 7: ***click*** the **OK** button to accept the changes to the Network Authentication and return to the **Network Profile** dialog.

Step 8: ***click*** the **OK** button to accept the changes to the Network and return to the **Connection Control** Main Screen.
(Or ***click*** the **Cancel** button to return without modifying the Network.)

<go back to machine connections>

Viewing a Machine only Connection:

When viewing the **Connection Status** in the **Connection Control** Main Screen or in the **Connection Status/Connection Details** screen, the connecting, connected and failed states will be augmented with a (Machine) suffix, indicating a machine connection.

Managing Networks

A single Network is defined by its **Network Profile**. A Network Profile has a user-friendly name, defines the set of credentials needed, the set of Access Devices (wireless access points or physical ports) that belong to the network, the EAP authentication methods used, and for WiFi, the association and encryption modes supported, and, if static WiFi, then the WEP or WPA keys.

Managing Network Profiles consists of the following ***operations***:

Creating new Networks

Create a Network

Modifying existing Networks

Re-configuring a Network
Re-configuring an Access Device
Removing a Network
Removing an Access Device

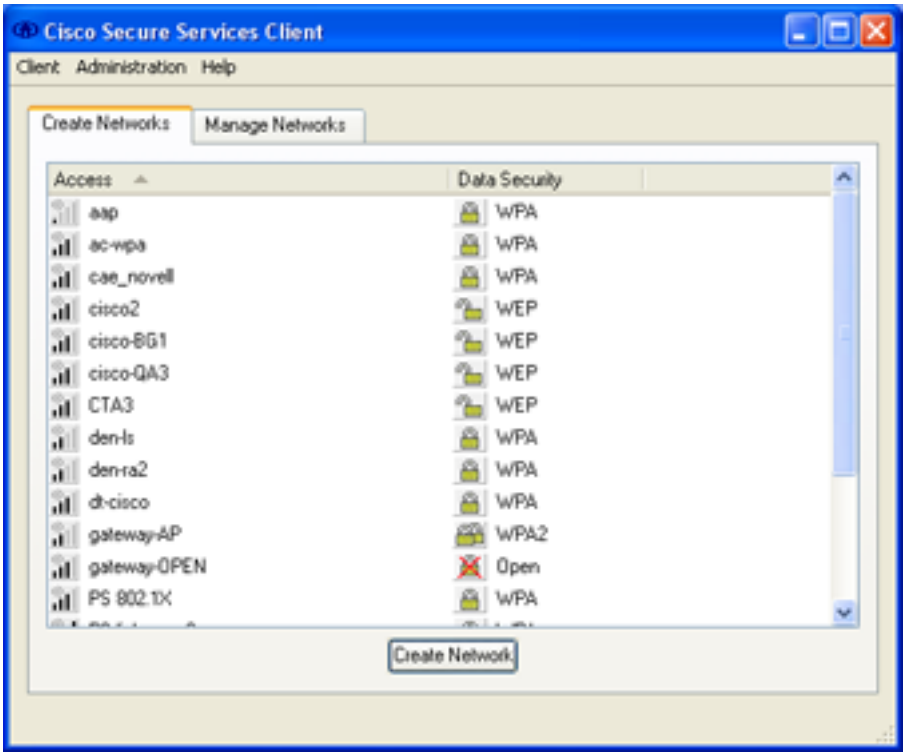
Locked Networks

Viewing a locked Network

Creating a new Network

Network creation is performed from the **Create Networks** tab in the Client's **Connection Control Main Screen**.

See viewing available access devices for an overview.



Network Creation

Create a **Network Profile** via the following procedure:

> **Important Note**: the client can not make unilateral choices - the configuration of the network is primarily determined by the policy of the authentication server and its associated access devices. The client must be configured appropriately to conform.
>
> **Tip - server certificate dependency**:
> When creating an auto-connect network that requires server certificate validation, consider first configuring the associated Trusted Server rule, otherwise the connection that is attempted as soon as the network profile has been created will fail.
>
> **Tip**: See understanding connection contexts for an overview of when and how you can establish network connectivity.

Procedure: Create a Network

Step 1: ***click*** the **Create Network** button (available from the **Create Networks** tab only) » to open the **Network Profile Configuration** dialog.
Note: *the dialog opens with only the basic **Network** settings, enabling simple profile creation for non-authenticating networks.*

Step 2: ***name*** the Network by editing the **Name** text box.
Note: *this is a user-friendly name used only for display purposes throughout the client's various dialogs.*

Step 3: **Connection scope:**
click the **Available to all users** checkbox only if you want this Network Profile to be available to everyone - all users of this machine will see this Network in their Main Screen Network display list (individual user credentials are however treated separately).

Step 4: **Automatic connection** settings:

- ***check*** the **Automatically establish User connection** checkbox only if you want to instruct the auto user context connection process to include this Network in its network selection algorithm - user context connections are always enabled (i.e., they can always be initiated manually, independent of this option). (The ***default*** is to auto connect.)
  For **Related Information**, see Controlling the Network Connection - auto connect.
  - ***check*** the **Before user account (supports smartcard/password only)** only if this network is going to be used in a domain login environment and an early network connection is required. (See understanding domain login for more details on settings for specific Microsoft Active Directory and Novell environments.)
    Note: as stated, only password and smartcard credentials are supported with auto-connection in this type of network arrangement. (See understanding user credential types for more information.)
  - ***uncheck*** the **Before user account (supports smartcard/password only)** if this network is not going to be used in a domain login environment (allows for no restrictions on credential types, including support for user certificates in the Windows User-Personal Store) or this network is going to be used in a domain login environment but an early network connection is not required. (See understanding domain login for more details on settings for specific Microsoft Active Directory and Novell environments.)
- ***check*** the **Automatically establish Machine connection** checkbox only if you want to enable machine context connections. (The ***default*** is to not support.)
  Note: *machine connections require a public profile - the appropriate setting will be automatically configured.*
  See Configuring and Making Machine Connections for more details.

Step 5: **Network Configuration** settings:

Network Configuration Summary pane - lists an overview of the default Authentication and Credential modes, as follows.

- **Network Authenticating Method** - one of two types will be displayed
  - Authentication **Off** - represents a network geared for home or travel use - does not employ an authentication server.
  - Authentication **{List of EAP Methods}** - represents a network geared for the enterprise, complete with server authentication.
- **Credential Collection and Storage methods -** only applicable for an authenticating network

These settings are ***inherited*** from the system defaults. (***Policy dependent*** - may vary in a deployed End-User Client)

- For the **administrator/power-user** client version, the mode ***defaults*** to creating open or shared-key, non-authenticating networks.
  The **Authentication** text will be **Off**.
- For a **deployed end-user** client version, the ***default*** mode may be restricted to one of the authenticating options.
  The **Authentication** text will be **Off** or contain a list of the inherited authentication methods and a credential method.

If these need changing, ***initiate*** advanced configuring by ***clicking*** the **Modify** button » to open the **Network Authentication** dialog.

See managing authentication methods for details if the default settings need to be changed.

Step 6: ***assign*** an Access Device to the Network.
Initially the **Access Devices** pane will be empty. ***click*** the **Add** button » to open the **Add Access Device** dialog.
See adding an access device.
Note*: This supports all ways of specifying associated access devices - whether they are currently available (in the Access Device View scan list) or not.*

Step 7: ***click*** the **OK** button to accept the new Network and return to the **Connection Control** Main Screen.
(Or ***click*** the **Cancel** button to return without creating a network.)

<chapter menu>

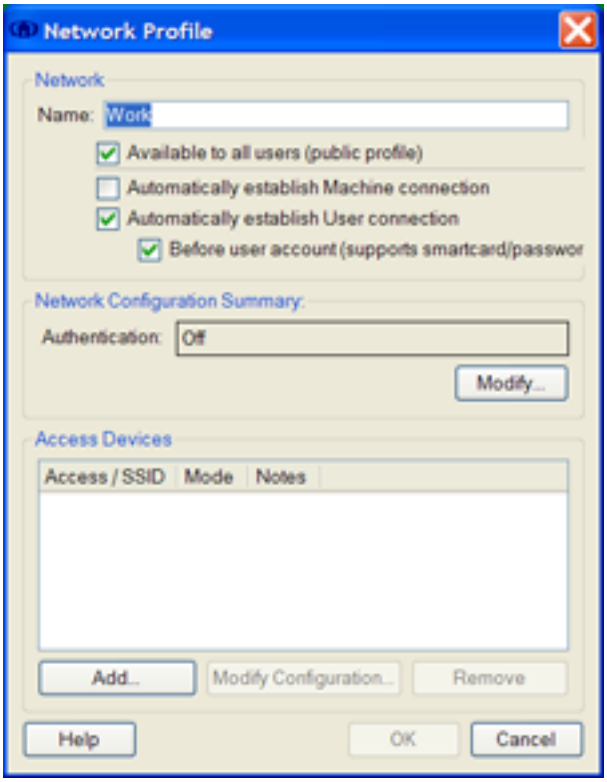
Modifying an existing Network

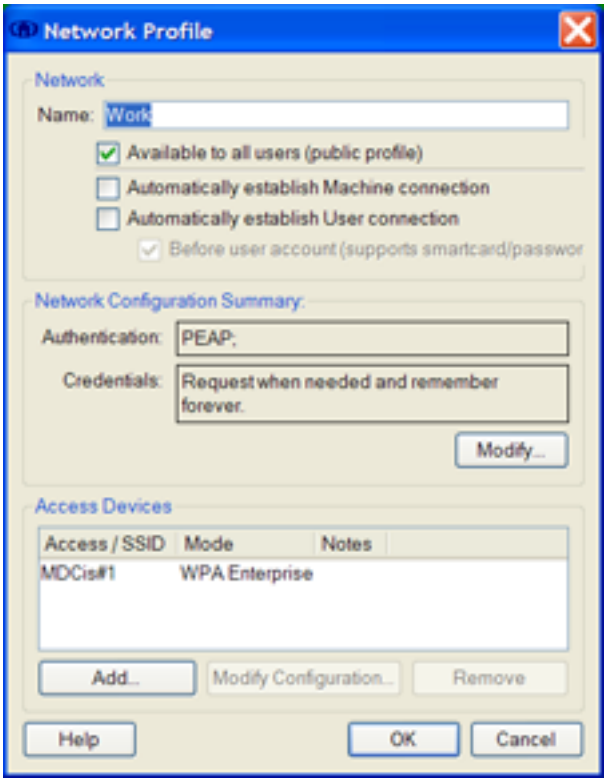
Network management is performed from the **Manage Networks** tab in the Client's **Connection Control Main Screen**.

See viewing networks & network connections for an overview.

Configuring a Network Profile

The behavior of an existing Network can be modified via the configuration of its Profile's settings.





Configure a **Network Profile** by overriding the client's default profile settings or changing your current configuration via the following procedure:

Procedure: Configuring a Network Profile

Step 1: from the **Connection Control (Manage Network)** Main Screen, by ***selecting*** the Network of interest, and ***clicking*** the **Configure** button » to open the **Network Profile Configuration** dialog.
Note: a network must not be connected or locked in order to be reconfigured.

Step 2: ***Basic*** **Network** settings and controls:

- **Settings**:
  - **Name**
    edit the **Name** text box to change the user-friendly display name of the Network
  - **Connection scope**
    check the **Available to all users** checkbox if expanding the scope of the Network to either allow access to all users or allow machine connections.
    or ***uncheck*** the checkbox if removing both availability of this network profile to all other users and machine connection capability.
  - **Connection methods**
    check the **Automatically establish ...** checkbox if changing the connection initiation to **auto**
    or ***uncheck*** the checkbox if changing the connection initiation to **manual**
    Note: *See Configuring and Making Machine Connections for details on machine connections.*
    - **Credential domains** - User connection only
      check the **Before user account (supports smartcard/password only**) checkbox if changing the network to use domain login and early user network connectivity is required.
      Note: in this mode, user client certificates from the Windows certificate store are not supported.

      or ***uncheck*** the checkbox if changing the network to not use domains or changing domain login to a configuration that no longer requires early user network connectivity.

Caution: Changing this is not likely since it is fundamental to how your enterprise network is architected for its credential storage (its authentication environment).

Important: *see understanding domain login for more detailed information.*

- **Access Devices Display:**

  - **Access ID** - lists all access devices assigned (configured) to this network
    Note: *if the access device was added as 'hidden' (marked via the **Actively search for ...** check-box) it will have this noted at the end of the access identifier's name.*
  - **Mode** - Association/Encryption setting assigned to this access device.
    Note: *See port mode settings for details on options.*

- **Access Devices Controls**:

  - **Add** an Access Device (or Re-Add an existing Access Device so as to modify its 'hidden' attribute)
    see adding an access device
  - **Modify Configuration** of an Access Device (wireless)
    see configuring an access device
  - **Remove** an Access Device
    see remove an access device

Step 3: ***Advanced*** **Network** settings:

Network Configuration Summary pane - lists an overview of your current Authentication and Credential modes.

If these need changing, ***initiate*** advanced configuring by ***clicking*** the **Modify** button » to open the **Network Authentication** dialog.

Advanced network settings consist of the following items:

- **Network Authenticating Method** - your network has already been assigned to one of the following basic classifications
  - **Turn Off** authentication - represents a network geared for home or travel use - does not employ an authentication server.
  - **Turn On** authentication - represents a network geared for the enterprise, complete with server authentication.

    Caution: Changing this is usually not recommended since it most likely changes the whole scope of the network and probably invalidates the existing set of access devices, requiring you to reselect/ reconfigure them. It may be simpler to remove this network and create a new one. See configuring authentication methods for details.

    - For authenticating (Turn On) networks: **Authentication Protocols**

      You may have a need to adjust which EAP methods (a.k.a. protocols) are allowed for this network. But this would most likely only follow changes to your authentication server. See configuring authentication protocols for details

    - For authenticating (Turn On) networks: **Credential Collection and Storage**

      Caution: Changing the collection method is not likely since it is fundamental to how your enterprise network is architected. However, you

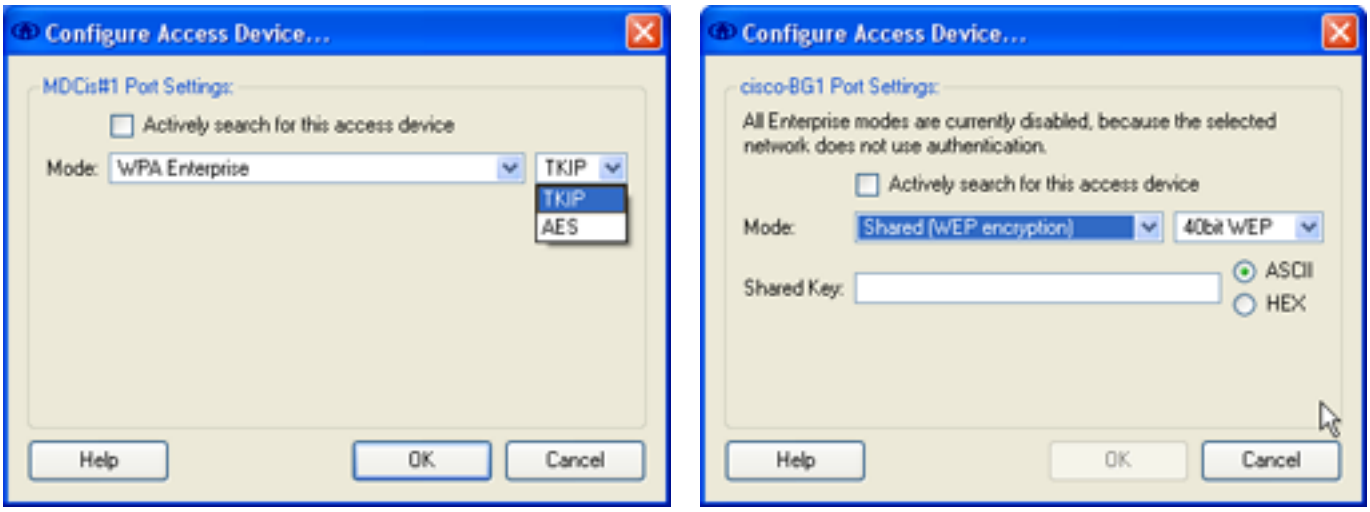
may have a need to adjust the storage mode for credentials that are obtained on demand. See configuring credentials for details.

Step 4: ***click*** the **OK** button to accept the changes to the Network and return to the **Connection Control** Main Screen.
Note: *if any of the advanced settings are modified, any stored credentials will be cleared, invoking a subsequent* ***Enter Your Credentials*** *pop-up dialogs.*
(Or ***click*** the **Cancel** button to return without modifying the Network.)

<chapter menu>

Configuring an Access Device

The behavior of an individual, configured (that is, already assigned to a network) Access Device (wireless only), as retained by its parent's Network Profile, can be modified through the configuration of the access device's advanced settings.



Configure a more complex **Access Device** by overriding the client's default profile settings via the following procedure:

Procedure: Configuring an Access Device

Step 1a: from the **Connection Control (Manage Network)** Main Screen, by ***selecting*** the configured wireless access device of interest, and ***clicking*** the **Configure** button » to open the **Configure Access Device** dialog.
or
Step 1b: from the **Network Profile Configuration** dialog, by ***selecting*** the wireless access device of interest from the network's **Access Device** list, and ***clicking*** the **Modify Configuration** button » to open the **Configure Access Device** dialog.

Step 2: **Access Device Port Settings**: Beaconing status

The **Actively search for ...** check-box settings:

> ***checked*** - only for the class of non-scan-capable access devices (non-beaconing and non-probe response access point).
> **Note**: *the access device will be categorized as "hidden".*
>
> ***unchecked*** - for standard beaconing access devices.

Step 3: **Access Device Port Settings**: Association/Encryption **Mode**

The **Configure Access Device** dialog displays the currently configured port mode setting.

Background: An attempt was made to ***automatically determine*** the operating values of the WiFi association and encryption through information internally obtained from the Access Point at the time that the access device was assigned to its network (during create network). If successful, then the value pre-populated in the selection box is the preferred mode. Otherwise the settings may have to be manually updated as detailed here.

Association / Encryption Mode options (***Policy dependent*** - the allowed set may be limited in a deployed End-User Client.)
Note: *the set of allowed encryption methods is dependent on the Association method and the allowed combinations are displayed as options.*

- ***WiFi Protected Access*** (WPA) - the security solution of the WiFi Alliance and counters the known shortcomings of both the legacy 802.11's encryption method, Wired Equivalent Privacy (WEP), and the 802.1X's subsequent enhancement, dynamic WEP. WPA's strength comes from an integrated sequence of operations that encompass 802.1X/EAP mutual authentication and sophisticated key management and encryption techniques. WPA2 is a recent upgrade based on the full 802.11i standard. WPA2 is Wi-Fi Alliance branding for 802.11i interoperability. WPA2 is not being released to address any flaws in WPA. The major aspect of WPA2 is the mandating of a new and stronger encryption cipher (AES). WPA2 also introduces subtle improvements in the association request/response messaging and in the key exchange messaging.
  WiFi Protected Access mandates authentication before key exchange and uses 802.1X authentication or Pre-Shared Keys in order to provide encryption seeds for key exchange.
  - ***802.1X mode*** (Enterprise) - uses an authentication server for credential storage and generation of encryption seeds.
    - **WPA2 Enterprise**
    - **WPA Enterprise**
  - ***PreShared Key*** (PSK) ***mode*** (Personal) does not require an authentication server, in this case the access point and the client must both know the same PSK pass-phrase, which is used to seed encryption for the keys. The personal mode was developed primarily for the home/small office environment.
    - **WPA2 Personal**
    - **WPA Personal**

    A **Shared Key** text entry will be enabled for either of the WPA/WPA2 Personal options.
    - **enter now** - the format of the key determines how many characters can be entered in each field.
      - Entry **Format** selection menu
        - ASCII - it must contain at least 8 characters and may contain up to 63 and is case sensitive. (ASCII decimal 32-126 only)
        - HEX - it must contain 64 characters.

  An ***encryption option*** is also available for the WPA/WPA2 modes.
  - **AES** - highest data security -normally linked to WPA2 association but may be available in some WPA compliant access devices.
  - **TKIP** - standard method for WPA association, also allowed with WPA2 association for backwards compatibility.

- ***Legacy 802.11*** - the legacy security solution which provided a low-level mechanism for a basic, but easily breakable, authentication and data privacy capability between the client and access device. These legacy methods are supported for backwards compatibility but are not viewed to be an integral part of an enterprise-level security solution.
  - ***Open*** association supports 3 levels of data encryption - none (no security and therefore no credentials required), static WEP (basic security) and dynamic WEP (an earlier interim improvement over static, made possible by the 802.1X introduction of an authentication server). WEP provides lower data security and is disallowed by WPA.
    - **Open** (***default*** when not deterministic)
      No key used - no encryption.
    - **Static WEP**
      Key source - Key entry required.
      Note: *choose this option if the access point only supports static WEP (older legacy hardware).*
      Tip: *if unsure, select dynamic WEP, since this is the most prevalent mode.*
    - **Dynamic WEP** (***default***)
      Key source - Network will provide a key.
      Note: *the access point must support dynamic WEP.*

  - ***Shared*** association requires the use of a static WEP key pre-defined in both the client and access point.
    - **Shared**
      Key source - Key entry required.

  A **WEP Key** text entry will be enabled for the above 'key entry required' cases.
  - **enter now** - the size and format of the key determines how many characters can be entered in each field.

Tip: *5 ASCII characters, or 10 hex characters, for a 40 bit key. 13 ASCII characters, or 26 hex characters, for a 128 bit key.*

- **Key size** selection menu
  - 40 bit
  - 128 bit
- Entry **Format** selection menu
  - ASCII
  - HEX

Note: *The length of a WEP key is not available from the information elements in the 802.11 broadcast advertisements, just that the encryption is WEP, and therefore it is not automatically populated in the selection menu. You must explicitly set both the length and the key to match the key set on the AP.*

Note: *WEP keys are used for both association and authentication. Use of static WEP keys for association only is not supported.*

Critical Note: *the Network Key (PSK/WEP) entered into the client must be the same as the network key that is configured on the access device.*

Note: If there are multiple choices available from the access device for setting the association/encryption mode, the client will always choose the most secure. The ordered list from most secure to least secure is: WPA2-Enterprise, WPA-Enterprise, WPA2-Personal, WPA-Personal, Dynamic WEP, Static WEP, Shared, Open. (The list is also tempered by the advertised capability of the adapter performing the scan.)

Note: *For WiFi Protected Access compatible access points, their announced modes allow for definitive binning within the client's authentication methods. For Legacy access points, this is not fully supported. Here the client only distinguishes between Open and any of the WEP modes (static, dynamic or shared). Furthermore the set 'open, static and shared' are typically associated with a non-authenticating network (they appear in the mode pull-down list for Authentication Off). But since there is no protocol enforcement of this (pre-802.1X) they also appear in the mode pull-down list for Authentication On for compatibility with old, atypical networks.*

Tip - Misconfigured: *If re-configuring from a 'Misconfigured' condition, remember that the auto-detected mode(s) is still visible in the **Capable for** list in the expanded text view of the selected access device on the **Main Screen**.*

Caution: *for the case of multiple access devices with the same SSID. In this case the value for the network's consolidated access device may not be the preferred one, especially if the set of access points have **mixed** security. It may be easier for this special case to remove the access device from the network and reassign it again. In doing so, while non-configured, you have access to viewing the announced modes of all of the SSID member accesses, giving you a better picture of your environment.*

Caution: *When there is a misconfiguration in WPA/WPA2 due to encryption there is no explicit indication in the 'Capable for' list of encryption detected. You need to confirm that the configured value shown in this **Configure Access Device** dialog is consistent with your access point configuration.*

***Remember**: a 'Misconfigured' status can result from several factors, as follows:*

correctable via client

client configuring: your original choice (override or not) was incorrect.

not correctable via client

policy limitation: you are making selections not allowed by the client's policy.

access point configuring: you are making choices known to be correct but the access device itself is misconfigured.

Note - Not Available: *When an access device is 'Not Available' or 'No Adapter Available', then the value visible in the **Data Security** column on the **Main Screen** is still the configured mode.*

Step 3: ***click*** the **OK** button to accept the changes to the Access Device and return to the **Connection Control** Main Screen. (Or ***click*** the **Cancel** button to return without modifying the Access Device.)

<chapter menu>

Removing a Network

Once a Network is no longer needed it can be removed via the following procedure. All Access Devices currently configured as assigned to this Network will be released and returned to the **Non-configured Access Devices** category.
Note: *a 'Connected' or 'locked' Network can not be removed.*

Note: ***Policy dependent*** - not available in a Preset end-user client (Remove button not available).

Procedure: Remove a Network

Step 1: ***select*** on the **Connection Control (Manage Network)** Main Screen, the Network of interest.
Step 2: ***click*** the **Remove** button » the button will become **Undo Removal**.
Step 3a: ***make*** another selection (or take another action) » to cause a permanent removal
or
Step 3b: ***click*** the **Undo Removal** button » to restore the Network.

<chapter menu>

Removing an Access Device from an Existing Network

Once an Access Device is no longer needed within a Network it can be removed via the following procedure. The Access Device currently configured as assigned to the associated Network will be released and returned to the **Non-configured Access Devices** category.

Note: *a 'connected' or 'locked' or the last Access Device can not be removed. (A network must contain at least 1 access device.)*

Note: ***Policy dependent*** - not available in a Preset end-user client (Remove button not available).

Procedure: Remove an Access Device from an Existing Network

Step 1a: while viewing a Network, ***select*** on the **Connection Control (Manage Network)** Main Screen, the Access Device of interest.
Note: *a wired access can only be removed via step 1b, where the entire <ethernet> grouped access device is displayed.*
or
Step 1b: while modifying a Network Profile, ***select*** on the **Network Profile Configuration** dialog, the Access Device of interest.
Step 2: ***click*** the **Remove** button » the button will become **Undo Removal**.
Step 3a: ***make*** another selection (or take another action) » to cause a permanent removal
or
Step 3b: ***click*** the **Undo Removal** button » to restore the Access Device.

<chapter menu>

Tips:

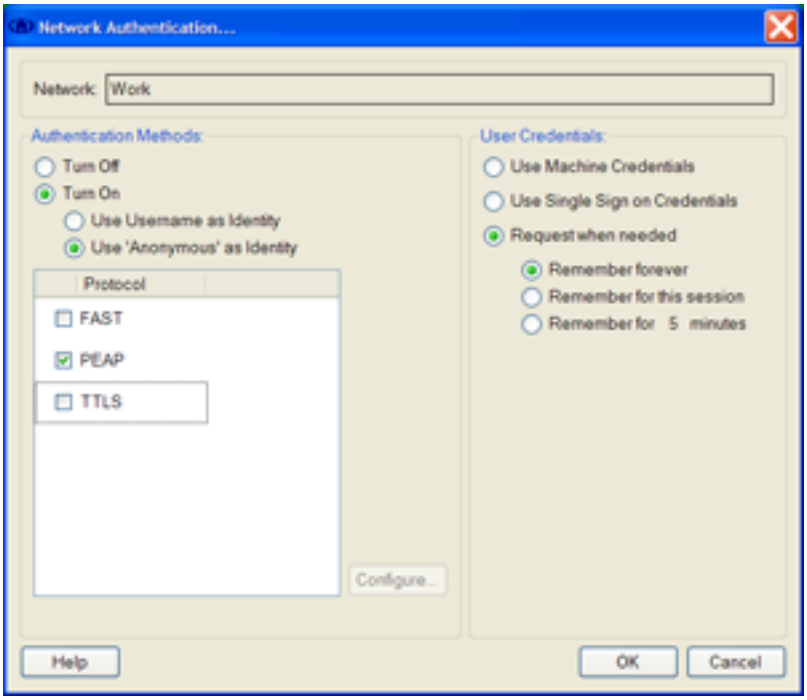
v **Configuring the Client**

- **Naming restrictions**
  User named entities, such as, SSIDs and trusted server rules, have limitations for using numerical characters.
  Workaround: Avoid defining names that start with 0 (zero) or contain greater than 19 all-numeric characters.

- **Connection attempt during configuring**
  The client may attempt to connect when being configured.
  Workaround: Exit configuring dialogs, clear any "Enter your credentials" pop-up(s), disconnect any "connecting" state (which converts auto-connect to manual control), and re-start your re-configuring task.

<chapter menu>

Managing Authentication Methods



User Credentials pane:

Password / Certificate Options:

Credential Collection methods - see configuring Credential Collection for details.

Authentication Methods pane:

Authentication Methods selection (***Policy dependent*** - may be fixed or limited in a deployed End-User Client)

- ***check*** the **Turn Off** Authentication option (***default***) to restrict the operating mode to one that does not use an authentication method or an associated authentication server. This limits one to the following modes:
  - Open and no encryption (no security)
  - Shared key for encryption between the client and the access point

  This represents a network geared for small office, home or travel use.

- ***check*** the **Turn On** Authentication option to allow for all of the EAP Authentication methods and settings specified by the client's policy.

  This represents a network geared for the enterprise.

Choose an ***Authentication Protocol class*** as follows - make choices on:

Tunneled usage for authentication protocol
Identity usage for phase 1 outer (unprotected) tunnel of tunneled EAP methods - with or without domain routing

Note: *just [UserName] will always be sent for the EAP Identity of any phase 2 inner tunnel (protected identity).*

Note: *the correct behavior required is a function of the authentication server.*

Tip: see Understanding EAP Methods for more details.

- ***check*** the **Use Username as Identity** option (***default***) to allow all EAP methods and to send the UserName in all EAP Identity responses.
  In this mode the client will send ***UserName@Domain*** for the Identity, even for the outer identity (phase 1) of any included tunneled methods. That is, *the user identity (user name) is sent in the clear.*
  - **Tip - Microsoft server:** *In general, a Microsoft AAA server using its PEAP method will require th*is setting.

- ***check*** the **Use 'Anonymous' as Identity** option to further restrict the set of allowed authentication methods to those that utilize tunneling and to restrict sending the UserName in the EAP Identity response of the outer (unprotected) tunnel.
  In this mode the client will send **anonymous@*Domain*** for the Identity.
  - **Tip - Cisco ACS server:** *If using domains with ACS 3.3 AAA server you must use this setting.*

Caution: changing from one authentication mode to another will reset the settings and configurations of the items in the **EAP Method (Protocol)** list.

EAP Method (Protocol) display

Any protocol configured for a Network Profile will be permitted for connections to all Access Devices associated with that profile.

Use the settings to refine and re-configure EAP method behavior, such as listed below.

- restrict an EAP method's usage
- control optional client certificate usage
- control fast session resumption
- limit inner tunnel methods to a specific one

Background Note: *During the EAP negotiation phase of authentication process, if the client receives a request from the server for a particular EAP method that it is not configured to support, it will respond with a list, as indicated in the display, of alternate EAP methods that it will support. The server will sequence through the list, in its own order, to search for an acceptable alternate. If it finds one, it will re-negotiate with the mutually agreed to method, otherwise authentication will fail.*

Policy dependent -The EAP Methods list is pre-populated and will display all supported EAP methods as determined by the client's license and deployed policy and the previously-made choice of authentication method.
Note: *the pre-populated set of methods for the out-of-box administrator/power-user client is inherited from the client's license.*

Method Usage - For each method there is an enabling ***checkbox***.
Note: *any selected protocol can be used for either wired or wireless connections.*

- ***check*** to enable the method
- ***uncheck*** (***default***) to disable the method

Tip: *if there are EAP methods that allow client certificates then it is assumed that a client certificate can be requested. Therefore if client certificates are not supported, then uncheck EAP-TLS, if present.*

Configure - ***click*** to open the **Configure EAP Method** dialog in order to further define the method's

optional settings as over viewed above.
Note: enabled only when a configurable EAP method is selected.

<return to chapter beginning>

<return to modifying a network>

<return to creating a network>

Related Topics:

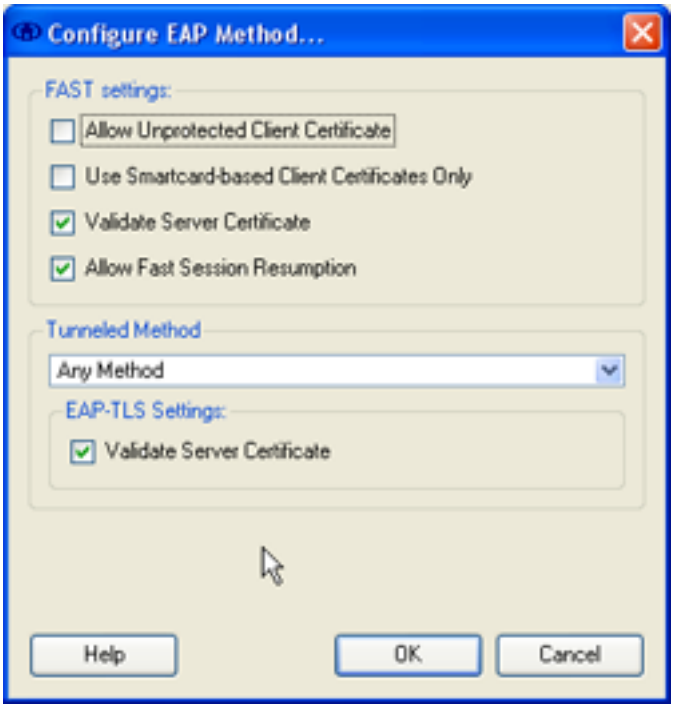
Understanding EAP Methods

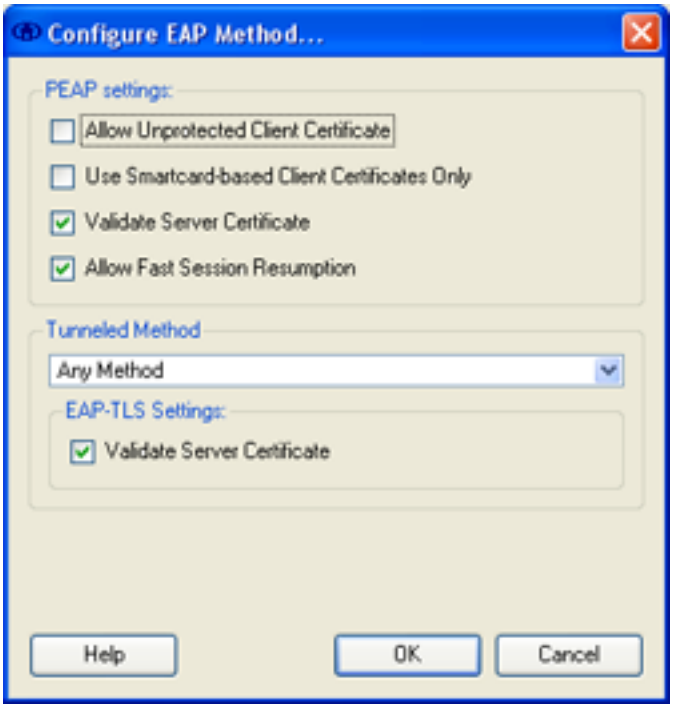
Managing EAP Methods

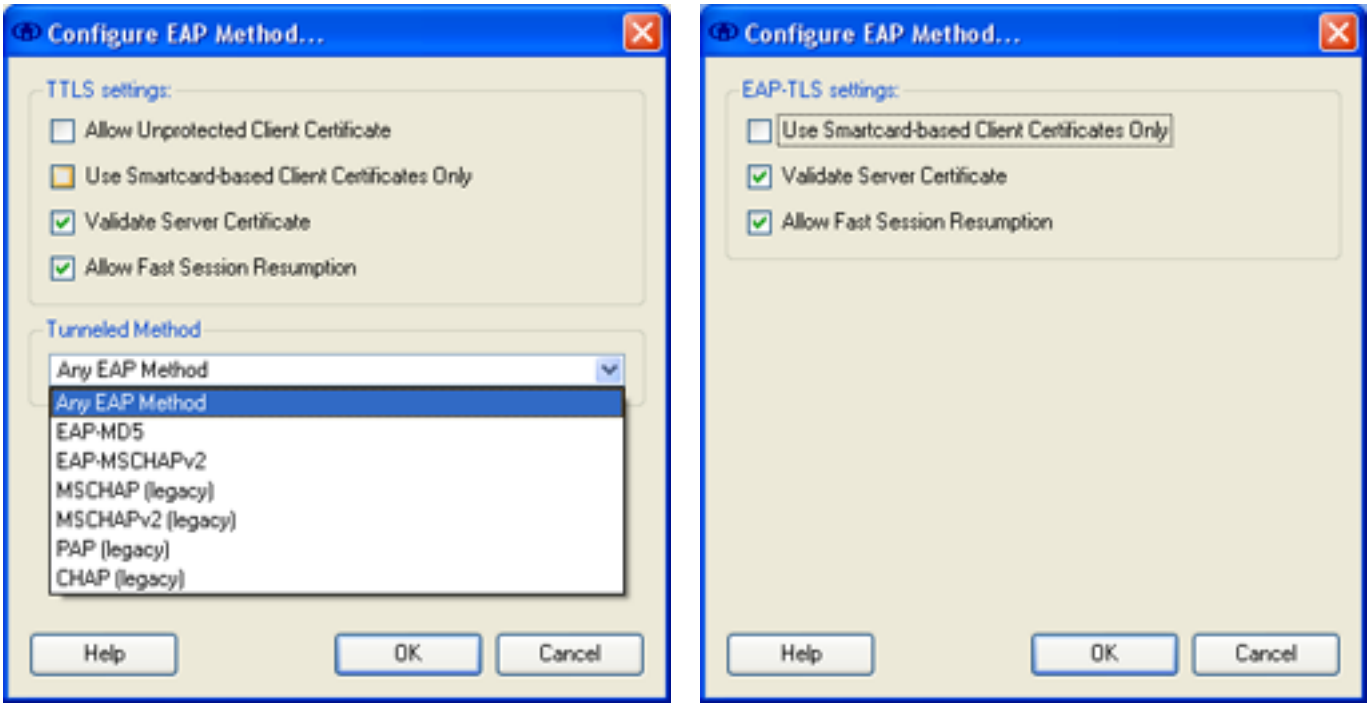
The set of applicable configuration settings is dependent on the selected EAP method, per the following table.

Applicability of Settings to EAP Methods				
Configurable Setting	**PEAP**	**FAST**	**TTLS**	**TLS**
Use Client Certificate - Connection authentication	yes	-	yes	-
Use Client Certificate - PAC Provisioning	-	yes	-	-
Validate Server Certificate	yes	yes	yes	yes
Allow Fast Session Resumption	yes	yes	yes	yes
Allow Fast Session Resumption	yes	yes	yes	yes

EAP Method Settings







Client Certificate response: The protocols that use this setting support the optional use of a client certificate as part of the authentication process. However, the use (i.e., if a client certificate is requested as part of the authentication messaging) is solely determined by the configuration of the authentication server, not the client. The option is referring to whether or not the supplicant should send a certificate unprotected and not necessarily, whether or not to ever use a certificate.

If the server is configured to request a client certificate, then how the client reacts to this request is controlled by the value of this element. It may force a client certificate to be selected and made available to the authentication server for certification or it may force the client to not respond with a client certificate.

The detailed behavior is as follows:

- **Allow Unprotected Client Certificate** checkbox (PEAP & TTLS)
  - ***check*** to **disable** protection
    When requested by the server for a client certificate during the Phase 1 portion of the protocol:
    - If there is a client certificate available, it will be sent.
    - If there is no client certificate, none will be sent and the server policy will determine if authentication continues or fails.
  - ***uncheck*** (***default***) to **enable** protection
    When requested by the server for a client certificate during the Phase 1 portion of the protocol:
    - The client certificate will never be sent to the server (since there is no way to send a client certificate protected for these EAP methods). Server policy will determine if authentication continues or fails.

  Note: *it's important to configure the client compatible with your server settings.*

- **Allow Unprotected Client Certificate** checkbox (FAST)
  - ***check*** to **disable protection**
    When requested by the server for a client certificate during the unprotected (phase 1) portion of FAST PAC provisioning:
    - If there is a client certificate available, it will be sent.
    - If there is no client certificate, none will be sent and the server policy will determine if authentication continues or fails.
  - ***uncheck*** (***default***) to **enable protection**
    When requested by the server for a client certificate during the unprotected (phase 1) portion of FAST PAC provisioning:
    - The client refuses at this point to send any certificate (it's allowed this option) because it will wait for the protected Phase 2 of the protocol (actually, a tunnel will first be established, based on the server's certificate, and the supplicant will send its certificate before Phase 2 begins, sort of a Phase 1 1/2, for lack of a better term).

  Note: *this checkbox has no affect on the use of a client certificate during the protected (phase 2) portion of FAST PAC*

provisioning. If the server is configured to request the sending of the client certificate within the secure tunnel, the client will always attempt to use one. If none is available and not sent, the connection attempt will fail.

Client Certificate source restriction: If the use of client certificates is required by the server, control over its source is configurable.
Note: client certificate always required for TLS.

- **Use Smartcard-based Client Certificates Only** checkbox (FAST, PEAP, TTLS & TLS)
  - ***check*** to **restrict** the certificate selection to be from a smartcard only. Thus prohibiting the use of locally stored certificates.
  - ***uncheck*** (***default***) to allow certificates from smartcards and the appropriate Windows Certificate Store.
    Note: *For user connections the store of interest is the Personal Certificate Store for the currently logged in Windows user.*

Server Certificate usage: (***Policy dependent*** - may not be present in a deployed End-User Client)
Note: the use of server certificates must be supported by:

1) an entry in the client's Trusted Servers List
and
2) the CA certificate used to trust the server certificate must be placed in the proper Windows Certificate Store
Note: For user connections the stores of interest are the User-Trusted Root Store or User-Intermediate Certification Authorities.

- **Validate Server Certificate** checkbox (All methods)
  - ***check*** (***default***) to **validate** the server certificate.
  - ***uncheck*** to **not validate** the server certificate.
    Important Note: this option is ***not recommended*** and is usually only used for debugging (to help determine if the server certificate is responsible for a failed authentication) because it reduces the level of security. Using this option implies that you are not WiFi compliant for the associated wireless network.

Fast Session Resumption setting: for mutual authenticating EAP methods that involve creation of an SSL session, an authentication fast session resumption is performed with cached credential information. (Applies to both outer and inner tunnel methods.)
Note: For a network profile that allows multiple EAP methods of this type, if Fast Session Resumption is enabled for any one of these methods, then Fast Session Resumption will be enabled for all the configured methods associated with this network profile regardless of their individual settings.

- **Allow Fast Session Resumption** checkbox (All methods)
  - ***check*** (***default***) to **allow** Fast Session Resumption.
  - ***uncheck*** to **disallow** Fast Session Resumption.

Tunneled Method selection (FAST & PEAP): (***Policy dependent*** - the set of pre-defined inner tunnel methods is fixed by the client's policy)

select one of the following:

- **Any Method** (***default***) - support **all** inner EAP methods
- **specific method** - support **limited** to the **one** selected method

If the tunneled method is **TLS** (or 'Any Method' list which includes TLS), the following additional settings for the Inner TLS method are available:

- **Validate Server Certificate** - same setting descriptions as above for the outer tunnel method.
- **Use Smartcard-based Client Certificates Only** - same setting descriptions as above for the outer tunnel method.

Tunneled Method selection (TTLS): (***Policy dependent*** - the set of pre-defined inner tunnel methods is fixed by the client's

policy)

The use of Legacy and EAP methods inside the EAP-TTLS are mutually exclusive and can not be simultaneously specified.

select one of the following:

- **Any EAP Method** (***default***) - support **all** inner EAP methods only (the use of one of them will be negotiated with the server)
  Not applicable for Legacy inner authentication methods.
- **specific method** - support **limited** to the **one** selected method
  Must be used for Legacy inner authentication methods (server non-negotiable, only one should be specified).
  Optional for EAP inner authentication methods.

<return to advanced configuring of a network profile>

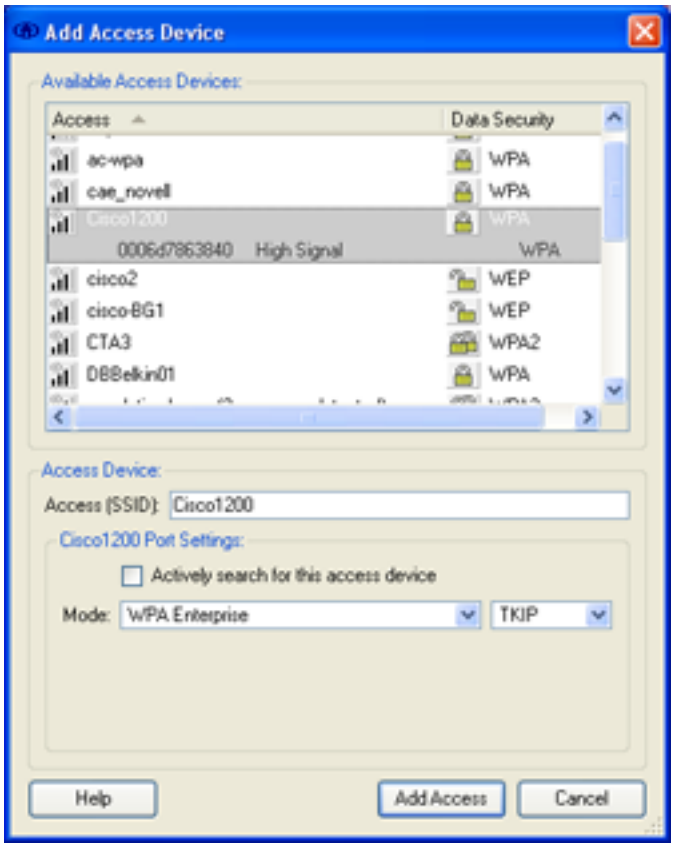
Related Topics:

Understanding EAP Methods

Adding an Access Device to a Network

Add an **Access Device** to a Network via the following procedure:
Note: *the client will support up to 10 access devices.*

Note: The same SSID can not be configured in multiple networks - including across multiple private networks associated with different users.



Procedure: Add an Access Device to a Network

Step 1: From the **Network Profile Configuration** dialog, ***click*** the **Add** button » to open the **Add Access Device** dialog.

Step 2: ***select*** the desired Access Device from one of the following [two] techniques:

- Entry method 1: WiFi access device present or ethernet
- Entry method 2: WiFi access device not present

Step 3a: [method 1] the **Available Access Devices** pane will initially contain the list of all of the available (i.e., detected through scanning), non-configured (i.e., unassigned to a network) access devices or an available access device already configured for an existing network (i.e., assigned to this network).

> **Note**: *the first set represents the non-configured Access Devices displayed in the **Connection Control (Create Network)** Main Screen.*
>
> **Clarification - Wireless**: *the Available Access Devices list displays Access Points by SSID. Selecting reveals its BSSID (MAC Address).*
> *Furthermore, for the case of **multiple access points with the same SSID** a list entry represents a group of linked*

(for purposes of roaming) access points. (The number of detected access devices is indicated via appended text.) Selecting such an access device will display an expanded view of the individual members and the following information:

***BSSID** (MAC Address)*
***Signal level** - categorized and displayed as Low, Medium, High*
***Data Security** - detected value for this individual access point*

Note: *Access devices with modes not supported by the license, such as, WPA2, are filtered from the list.*

Clarification - Wired: *all wired (ethernet) adapters can only be applied to a single network. When available, all are displayed generically in the Available Access Devices list as a single <ethernet> grouped access device.*

Select the desired Access Device, if it is present (otherwise go to Step 3b).

Selecting an Access Device will automatically populate the lower **Access Device** pane.

- The **Access (SSID)** will be automatically filled in and should be left as is.
- The Association/Encryption **Mode** will normally be ***automatically determined*** and populated at the time of the profile creation through information internally obtained from the Access Point and should normally be left as is.
  (See understanding association/encryption for more background information.)
  Tip: *mode is implied by the displayed* **Data Security** *level.*
  Note: *the allowed choices are viewable in the pull-down list and are determined by the configured authentication mode of the network and the allowed settings of the client policy.*

  Note: *if this information is not detected or not compatible with the client policy, then the settings default to the first allowed list item (Open association and No encryption, for the administrator client) - which may have to be manually updated . (See configuring an access device's port for a detailed description of the options.)*

  Caution: *a warning message will appear if the underlying network is configured for 'no authentication' and the access device being added is configured for an 'enterprise level mode'. However, a* **Force Enterprise** *checkbox will also appear that, when clicked, will accept the device at the 'enterprise level mode' and mark it in red when returned to the* ***Network Profile*** *dialog as a reminder that the network profile's authentication mode must be appropriately edited (via the* **Modify** *control). The device may not be accepted (the 'OK' button is disabled).*

  Caution: *overriding the detected state should be done with care. Selecting a mode not supported by either the allowed WiFi settings as determined by the network configuration and client policy or by the access device will most likely result in its status being set to 'Misconfigured' when returning to the* ***Connection Control*** *Main Screen.*

  Special Multiple SSID Case: if not all the access devices in the group have matching security (i.e., association/ encryption) then the group's security will be shown as '**Mixed**'. The value assigned to the network's port mode is then determined as follows:
  selecting the group, arbitrarily sets the network mode to one of the group member's value. **Tip**: This *must be set manually* by selecting the desired value from the pull-down menu choices.
- The **Actively search for ...** check-box should be left ***unchecked*** for access devices obtained from the Non-configured Access Devices list. ***Proceed*** to Step 4. (It's disabled for wired access devices.)

Step 3b: [method 2] Else if the desired Access Device is not present in the list for one of the following reasons:

- **scan-capable** - (issues beacons or responses to active probe) but is known not to be available (that is, not physically within detection range).
- **non-scan-capable** - not configured to be detectable via a scan and therefore may or may not be physically within detection range.

then ***manually enter*** the access device by entering its SSID in the textbox of the lower **Access Device** pane.

Note: SSIDs are limited to 32 characters.

Tip: *attempting to enter and assign a SSID already configured to an existing network will result in a warning message - a given SSID may only be assigned to a single network.*

Note: a **Wired** access device may be configured by entering "<ethernet>". (*This means that an SSID of '<ethernet>' is not supported and will be filtered from the available access device scan lists.*)

The **Access Device Port Settings** must be manually configured for this case.

- The Association/Encryption **Mode** must be configured by selecting the appropriate mode from the pull-down menu. See configuring an access device's port for a detailed description of the options.
- The **Actively search for ...** check-box must only be ***checked*** for the class of **non-scan-capable** access devices (non-beaconing and non-probe response access point).
  Note: *the access device will be categorized as "hidden".*

  Proceed to Step 4.

Step 4: ***Click*** the **Add Access** button to close this dialog and return to the **Network Profile Configuration** dialog where the Access Device will now appear in the **Access Devices** pane.
(Or ***click*** the **Cancel** button to return without assigning an Access Device.)

<return to creating a new Network *Procedure*>

<return to modifying an existing Network *Procedure*>

Related Topics

Managing Networks

Managing Locked Networks

Viewing a Locked Network

A ***locked*** Network Profile can not be modified (re-configured). However its configuration can be viewed via the following procedure.

> **Note**: *only an end-user client can have a locked profile - created as part of the IT administrators deployment process.*

Procedure: View a Locked Network

> **Step 1**: ***select*** on the **Connection Control (Network View)** Main Screen, the Locked Network of interest.
> **Step 2**: ***click*** the **Summary** button » to open the **Network Configuration Summary** screen.

Additional Topics

> Clearing credentials

Reference Information

This chapter contains generic background information relating to creating and managing networks - applicable to individual versions of the Client subject to its policy.

It contains these subchapters:

Understanding Policies and Profiles

Client Behavior

An individual client behaves and creates connections based on:

- Its ***base features*** that are defined by its ***license***, consisting of the following capabilities:
  - life time and maintenance support
    - shipped with a 90-day trial license
  - operating system support
  - supports wired (802.3) and/or wireless (802.11) network media types
  - plugin support
    - plugin type and the client's dependency on it (optional or required) when licensed
      Note: current plugins: Cisco Trusted Agent feature
  - authentication methods supported
  - WPA2/802.11i support
  - Smartcard support

- Its ***current operational environment*** that is defined by a set of configuration files, consisting of the following capabilities and out-of-the-box values:

  Note: *In a multi-user system, individual users may have different profiles, but everyone shares the same policy.*

  The ***client policy*** defines the capabilities and user experience of the client and allow OEM and IT Administrators to customize these (within the limits set by their license):

  - Authentication methods on how network connections may be created.
    - Supported WiFi & Wired EAP Methods:
      - EAP-FAST with inner methods of EAP-MSCHAPv2, EAP-GTC, EAP-TLS
      - EAP-PEAP with inner methods of EAP-MSCHAPv2, EAP-GTC, EAP-TLS
      - EAP-TTLS with inner methods of EAP-MSCHAPv2, MSCHAPv2, EAP-MD5, MSCHAP, CHAP, PAP
      - LEAP
      - EAP-TLS
      - EAP-MSCHAPv2 (typically restricted to wired)
      - EAP-MD5 (typically restricted to wired)
      - EAP-GTC (typically restricted to wired)
  - For wireless, association and encryption methods on how connections may be created and behave.
    - Allowed Association Methods:
      - WPA2-8021X
      - WPA-8021X
      - WPA2-PSK
      - WPA-PSK
      - Open
      - Shared
    - Allowed Encryption Methods:
      - AES
      - TKIP
      - AES
      - None
  - User interface configuration variations
    - User type
      Note: *the out-of-the-box type (Cisco Systems web store download) is Administrator/Power-user (allows the administrative functionality of end-user client deployment). The out-of-the-box license is a trial one.*
    - allows direct activation (licensing) from the client
      Note: *when activated through the Cisco Systems web store, the client type becomes Power-user and loses the trial functionality of the administrator functionality of end-client deployment. Licensing of an Administrator client is handled through Cisco Systems Sales.*

- Connection behavior
  - supports both machine and user originated connection types
  - allows auto and manual connection
- Network profile usage
  - allows users to create public (shared) profiles (required for machine connections)
- Credential types, collection methods and storage criteria
  - allowed credential types
    - passwords
    - certificates
  - allowed collection methods
    - single sign-on
    - request when needed
  - allowed storage times
    - duration of connection session
    - specified period of time
    - forever (static)
- Trusted Servers List which defines how to validate the credentials of servers during mutual EAP authentications.
  - allows full management of the Trusted Server List
  - allows choice of server validation for each network
- Adapter List which defines what media types of network adapters are supported.
  - supports wired (802.3) and wireless (802.11) network media types
- Security Settings for the following
  - support for use of older wireless network adapters with WPA, but not fully compliant
  - control of number of simultaneous connections (multiple/single)

The ***network profile*** defines the specific behavior of a single network, inherits capabilities from (limited by) the policy and allows for setting specific choices for multi-valued, allowed capabilities, as follows: (The default values for the out-of-the-box base network profile are indicated.)

- Credential types
  - ***default*** set to password and/or certificates
- Set specific methods for collecting credentials
  - ***default*** set to 'request when needed' and save 'forever'
- Connections
  - machine connection ***defaults*** to disabled
  - user connection ***defaults*** to 'auto connect'
- Network profile usage
  - ***defaults*** to public
- Authentication methods
  - ***defaults*** to no authentication and the policy-defined set when enabled
  - ***defaults*** to 'validate server certificate'
  - ***defaults*** to allowing fast session resumption
  - ***defaults*** to not requiring optional client user certificates
- WiFi Association and Encryption methods
  - ***defaults*** to auto-detect at time of network profile creation.

The administrator controls the end-user experience and allowed choices through the deployment of a distribution package (configuration) xml file. The distribution package xml file contains the following:

The client policy.
The network profiles.

See the *Cisco Secure Services Client Administrator Guide 4.1* for complete details of creating and deploying the distribution package xml file.

Related Topics:

Understanding Authentication Methods

Understanding Authentication Methods

EAP Methods - classification and certificate / pac usage

EAP Method	Method Feature			
	Client Certificate	Server Certificate	PAC	Class
Wireless / Wired				
EAP-FAST - connection	N/A	N/A	required	mutual / tunneled
EAP-FAST - provisioning v1	N/A	N/A	N/A	one-way / tunneled
EAP-FAST - provisioning v1a	optional	required	N/A	mutual / tunneled
EAP-PEAP	optional	required	N/A	mutual / tunneled
EAP-TTLS	optional	required	N/A	mutual / tunneled
LEAP	N/A	N/A	N/A	mutual
EAP-TLS	required	required	N/A	mutual
Wired				
EAP-MSCHAPv2	N/A	N/A	N/A	mutual
EAP-MD5	N/A	N/A	N/A	one-way
EAP-GTC	N/A	N/A	N/A	one-way

EAP Methods - classification aspects

- Secure for WiFi network
  - choose: PEAP, FAST, TTLS, TLS
- Authenticate the server's identity
  - choose: PEAP, FAST, TTLS, TLS, LEAP, MSCHAPv2
- Protect my identity from snooping
  - choose: PEAP, FAST, TTLS

EAP Methods Support

Items that need to be prepared, disseminated and/or setup by the network administrator prior to initial startup:

- **Credentials** (all EAP methods) - see providing credentials for details of what information must be known.
  - **Client (User) Certificates** - see providing user credentials
    The client certificate must be independently pre-installed and placed in the proper Windows Certificate Store (User- Personal Store).
  - **Client (Machine) Certificates** - see providing machine credentials
    Active directory provided machine certificate or password (SID (Security IDentifier)) must be available.
- **Server Certificate**
  - Authentication server setup - configured with server certificate.
  - Knowledge of the authentication server's name - needed to populate client's trusted server list.
    Note: *the server's name is taken from one of the following certificate fields: Subject Alternate Name: DNSName, Subject: CN (Common Name), list of Subject: DC (Domain Component).*
  - The certificate authority (CA) certificate(s) used to trust the server certificate must be independently pre-

installed in the client system and placed in the proper Windows Certificate Store (For user connections: User-Intermediate CA and Trusted Root CA Stores; for machine connections: Local computer-Intermediate CA and Trusted Root CA Stores).

- **PAC** (EAP-FAST)
  - Authentication server setup - configured for either auto provisioning (and auto tunnel (user) and/or machine PAC creation) or manual PAC creation/provisioning.
  - Knowledge of the Authority Identity (A-ID) of the FAST authentication server - needed to populate client's trusted server list.
    Note: *if provisioning via the server certificate method, the client, when initially accepting the provisioned PAC, will autonomously add the A-ID to its Trusted Server list - transferring the "trust" in the server certificate to the server's A-ID.*
    Note: *if provisioning via the basic mode, the client's use of a trusted server list for A-ID acceptance adds back some degree of security for this method which otherwise would allow an unauthenticated server to provide the initial PAC.*

EAP Methods Overview

EAP-FAST - Flexible Authentication via Secure Tunneling (Cisco initiative) is an extensible framework that enables mutual authentication. However EAP-FAST differs from the other major industry standard mutual authenticating tunneled EAP methods in that it does not, for a normal authentication exchange, use a server certificate for validating of the server by the client.

EAP-FAST establishes a protected TLS (Transport LAN Service) tunnel using a pre-shared secret. The pre-shared secret is referred to as the Protected Access Credential, or PAC. (A master key that is kept by the authentication server is used to generate a unique PAC for each user.) The PAC also serves to establish the server's identity to the client. The tunnel is then used to protect weaker authentication methods, typically based on a password such as EAP-GTC or EAP-MSCHAPv2, in which the client authenticates itself to the server. In this way, mutual authentication is achieved. It is also possible that mutual authentication can also be achieved during the tunnel creation if the client provides a client certificate via the TLS protocol.

In order to initially provide the PAC to the client two automatic provisioning methods are possible.

- Basic mode:
  In FASTv1, an unauthenticated server provides the initial PAC. Because of this, only mutually authenticated methods (MSCHAPv2, TLS) are allowed to be used for the inner tunnel method.
- Server Certificate mode:
  In FASTv1a an authenticated server provides the initial PAC. This is accomplished through the use of a server certificate. Because of this, the restriction of requiring a mutual authenticating method within the inner tunnel for automatic provisioning is no longer applicable.

The provisioning of a Machine PAC which is needed for machine context connections is only supported with the server certificate method. A machine certificate, pre-installed on the client system must be used to provide the client credentials.

Note: For a machine connection, if a machine certificate is not supported, then an initial machine connection can not be made and the machine PAC provisioning will wait until the initial user logon connection is made. At which point both machine and user (tunnel) PACs will be provisioned.

If a machine certificate is supported, then an initial machine connection may be made and the machine PAC provisioning may take place depending on whether or not it is supported and configured by the authentication server. Otherwise the machine PAC provisioning will wait until the initial user logon connection is made. At which point both machine and user (tunnel) PACs will be provisioned.

In either provisioning case, the client maintains a persistent store of the PAC for later retrieval during a connection attempt.

Note: For an unauthenticated provisioning, the initial user authentication session may in fact take several authentication cycles to complete because the provisioning session is declared a failure by the server. This can also be true for an authenticated provisioning depending on the configuration of the server (here the protocol allows for rejection or acceptance). The Client, however, makes this invisible to the user since it differentiates between an actual failure and a failure-following-successful-PAC-provisioning. In the latter case the Client will

autonomously try to create the connection again.

Furthermore, the PAC is update and aging managed as part of the EAP-FAST protocol. As a result the PAC may be dynamically re-provisioned to a client as part of the EAP-FAST protocol. The maintenance update, or refresh, mechanism is, however, done in a secure manner.

Supported inner tunnel authentication protocols:

- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS

EAP-PEAP - Protected Extensible Authentication Protocol (Microsoft & Cisco initiatives) is an example of a tunneled method that mandates the use of a certificate for validation of the server. Tunneled EAP Methods create a secure private tunnel within which a less-secure authentication mechanism may be run, protected by the tunneled EAP Method, to pass the client credentials. EAP-PEAP only allows EAP Methods within their secured channel (tunnel). PEAP allows for the use of a client certificate during the tunnel establishment phase. However most authentication servers do not call for it.

Supported inner tunnel authentication protocols:

- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS/smartcard

EAP-TTLS - Tunneled Transport Layer Security (Funk initiative) is an example of a tunneled method that mandates the use of a certificate for validation of the server. Tunneled EAP Methods create a secure private tunnel within which a less-secure authentication mechanism may be run, protected by the tunneled EAP Method, to pass the client credentials. EAP-TTLS allows legacy (non-EAP Methods), in addition to EAP Methods, within their secured channel (tunnel). TTLS allows for the use of a client certificate during the tunnel establishment phase. However most authentication servers do not call for it.

Supported inner tunnel authentication protocols:

- Legacy methods
  - PAP
  - CHAP
  - MSCHAP
  - MSCHAPv2
- EAP methods
  - EAP-MSCHAPv2
  - EAP-MD5

EAP-TLS - Transport Layer Security is an example of a method that mandates the use of certificates for validation of both the client and server.

LEAP -Light Extensible Authentication Protocol (Cisco initiative) is an example of a proprietary authentication method that uses a shared secret between the client and server to provide mutual authentication.

EAP-MSCHAPv2 - Microsoft Challenge-Handshake Authentication Protocol v2 is an example of a method that uses a one-way cryptographic hash of the password and random data with two-way challenge, thereby supporting mutual authentication. The hash method is defined by the protocol itself. Authentication is accomplished by creating a matching "hashed value of the password".

EAP-MD5 - Message Digest 5 is an example of a method that uses a password that must be available on both ends to allow the server to verify the client in a non-mutual authentication.

EAP-GTC - Generic Token Card is an example of a method that allows the exchange of clear-text authentication, which has the added property of being a one-use, time limited password. It was standardized primarily to support token cards.

Tips for Creating Networks

Multiple Networks within the same physical location

Premise: Your enterprise environment has an access point that beacons two SSIDs (which you have named Private and Public). Because these are the same radio, the signal strength on both is the same.

Solution:
Create two network profile, one for each SSID.

Since the Private network is the preferred network, it should be configured for auto-connect. While the Public network should be set to manual connect.

When the user wishes to connect to the less preferred network they will manually disconnect from Private and then manually connect to Public.

Mixed Access Point hardware within the same physical location

Premise: Your enterprise environment has a mix of access point hardware where you might have some existing pre-WPA access devices and would like to add newer WPA-compliant devices.

Solution: The client does not support mixed security in a single SSID, it's recommended that you assign the WPA devices to a different SSID. Both SSID access device groups may be configured into the same network profile.

Networks with domain login

Premise: Your enterprise environment consists of having your end station users logon to a domain.

Solution: See understanding domain login for more details on settings for specific Microsoft Active Directory and Novell environments.

Machine connections

Premise: Your enterprise network uses a machine connection prior to user logon.

Solution: Since the authentication method must support the use of a certificate to provide the machine client credentials, ensure that one of the following compatible EAP methods is enabled:

- EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS

> **Note**: *for any of the tunneled methods (FAST, PEAP, TTLS) the server must be appropriately configured to call for an inner tunnel method of TLS.*

Smartcards

Premise: Your enterprise network uses Smartcards for end user logon.

Solution: Since the authentication method must support the use of a certificate to provide the user client credentials, ensure that one of the following compatible EAP methods is enabled:

- EAP-TLS, EAP-FAST/TLS, EAP-PEAP/TLS, EAP-TTLS/TLS

Authentication Server

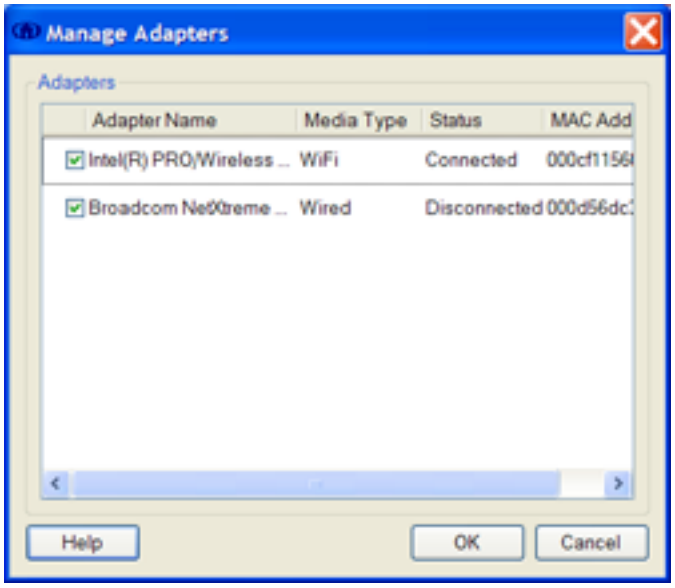
Premise: Your authentication server uses EAP v1 which can only issue a single default authentication method method and can only receive a single counter suggestion back from the client.

Solution: It is recommended if the client can not accept the server default then it should be configured for a single EAP method in the **Network Authentication** dialog of the network profile configuration.

Managing Adapters

The set of network adapters that are controlled by the Client can be configured by the following procedure:

> **Note - number supported**: *the client will support connecting and maintaining connections for up to four (4) network adapters simultaneously with two being wireless adapters and two being wired adapters.*



Procedure: Managing the Network Adapters

Step 1: from the **Client** menu, ***select*** **Manage Adapters** to open the **Manage Adapters** dialog.

Step 2: ***view*** the available adapters from the **Adapters** display pane.

The display will contain a list of all network adapters physically equipped. The list is automatically updated to ***dynamically*** show the current set. (For example, plugging in an external adapter and then later unequipping it will cause the adapter to appear and disappear from the list, respectively.)

- **Adapter Name** - a user friendly name for the network adapter hardware
- **Media Type**
  - **WiFi** - 802.11 wireless adapter
  - **Wired** - 802.3 ethernet adapter
- **Status** - an indication of the current connection status of the adapter
  - **Managed** adapters (***checked***)
    - **Disconnected** - not currently being used for a connection.
    - **Connecting** - currently being used in an attempt to create a connection.
    - **Connected** - currently being used for an active connection.
  - **Unmanaged** adapters (***unchecked***)
    - **Disconnected** - connection status not known.
    - **Used by Another Client** - when detected as managed by another application.
    - **Adapter Failure** or **Bad Driver** - when the Client detects a serious error and unmanages the adapter.
    - **Unlicensed Adapter** - media type not supported by Client's license.
    - **Restricted by Policy** - media type not supported by deployed policy.
- **MAC Address** - address of the adapter

Step 3: ***adjust*** the **Managed / Unmanaged** checkbox to take control of the adapter or not.

The set of Media Types controllable by the Client is ***policy dependent*** - one or the other of a media type class of adapters may not be enabled.

The managed/unmanaged adapter's state will always be ***remembered***. However the user will not be able to remove (or forget) those settings if the adapter is not present anymore. If the adapter is missing, it will simply disappear from the list.

- **check** - Client is in control of the adapter and it will be available to be used by Networks for making a connection. Checking will bind the Cisco driver (Meetinghouse 802.1x Protocol) to the adapter.
- **uncheck** - Client is not in control of the adapter

Note: *unchecking an adapter while in the connected state will break the connection.*

Tip: *unchecking and checking any wireless adapter will initiate an access device scan and* ***manually refresh*** *the list of non-configured Access Devices. A "Searching ...." transient pop-up message appears while the scanning and updating takes place.*

Tip: *clicking the Esc key will clear the "Searching ...." window, if necessary.*

Note: The Client will automatically take control over any new adapters (contingent on its media type being allowed by the policy).

Step 4: ***click*** the **Apply** button to accept the current set of checkbox values and return to the **Connection Control** Main Screen. (Or ***click*** the **Cancel** button to return without modifying the Adapter Management.)

Tips:

v **Cisco Protocol Conflicts**

Applications based on Cisco Network Adapter Protocol Driver
When taking control of an adapter that is already controlled by another 'Cisco'-based EAPOL client application (i.e., OEM applications based on the Cisco Core Supplicant Services API & Cisco Protocol driver), the Client will indicate via a pop-up message that another application is in control of the adapter and will release the adapter from being managed by the client.
Note: The Cisco network adapter protocol driver is labeled "Meetinghouse 802.1x Protocol".

v **Third party 802.1X applications**

Note: 3rd party applications include applications based on Cisco Protocol.

The Client will co-exist with any other 802.1X clients which operate on adapters that it does not control (i.e., unchecked in the Client's **Manage Adapter** dialog).

Caution: multiple client applications, beyond this Client, should not be configured to control an access point with the same SSID. (Allowing multiple applications to carry out write operations (as well as carry on EAPOL conversations required for making a connection) through the same network adapter will confuse both applications - resulting in unpredictable behavior in both client applications.)
If you must configure two applications with the same network, you must disable all but one of the client applications and use the one enabled client to make connections. Disabling this Client can be done easily from the Manage Adapter dialog or from the system icon. Disabling other 3rd party clients may or may not be a simple operation. In some cases where a simple disable of another client is not supported, such a dual, switched application environment can not be supported.

v **Windows Wireless Zero Configuration (WZC)**

The client disables WZC for the adapter when taking control and restores it to its original (saved) state when relinquishing control.

v **Windows Adapter Control**

The checkbox status is also a reflection of the Windows controls.

- **Adapter Network Connection - enable/disable**
  Window's Network Connection Enable/Disable functions actually stop operation of the adapter. A Windows disabled adapter will have its manage/unmanage checkbox unchecked.

  To view and edit an adapter's connection state in Windows, use the following:
  Start> **Control Panel**> **Network Connections**. ***Select*** the wireless adapter of interest and ***right-click***, in the resulting pop-up menu ***click*** either disable or enable, as appropriate, to change its state.

- **Adapter protocol binding**
  The Windows binding status determines whether or not client control of the wireless adapter is permitted. If the Cisco Protocol is bound to the adapter, then the Client, or another 'Cisco' branded client, has access to the adapter. (See above for protocol conflict resolution.)

  To view and edit an adapter's protocol driver binding in Windows, use the following:
  Start> **Control Panel**> **Network Connections**. ***Select*** the wireless adapter of interest and ***right-click*** **Properties**, this opens the **Wireless Network Connection Properties** dialog for the adapter. Find the 'Meetinghouse 802.1x Protocol' entry in the table and verify the binding checkbox status to its left. A check indicates that Cisco Protocol is bound to the adapter and an empty box indicates unbound. To change the state, check/uncheck the box and click OK.

v **Virtual adapters**

Virtual adapters, for example, for a VPN client, are not managed and therefore not bound to by the Client's protocol driver.

v **Managing adapters with Windows property dialog open**

If attempting to manage an adapter (normally takes control of the adapter from Windows WZC), but the Windows network properties dialog for the adapter is open, then the client will not be able to fully disable WZC and both clients will be interfering with each other.
Workaround: close the Windows network properties dialog, and from the client un-manage (unselect) and re-manage (re-select) the adapter either from the Manage Adapter dialog (individual control) or from the system tray icon (all adapter control), the client will then be properly managing the adapter(s).

Managing Trusted Servers

User Management

Background

The Client's Trusted Server List acts as a repository of authentication servers that the client is authorized to exchange information with. Information (validation rules) about these servers is stored in the client in order to allow the client to be able to validate, at the appropriate point in the authentication process, that a particular server is one that is indeed "trusted". There are two fundamental categories of server information type, as follows:

- **Server Certificates** - used during mutual authentication scenarios. During mutual authentication EAP message exchanges, in addition to the server validating the identity of the client, the client must similarly validate the identity of the server.

  Server certificates are employed for the following two end purposes:
  - **Normal Connections** - authentication using these EAP methods: EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-FAST

    Note: *EAP-FAST also supports an atypical "non-PAC" connection authentication based just on the server certificate (FAST server optionally configured not to provision the PAC).*

    Note: *enabling server validation for one of the above methods at the outer level also applies to any inner mutual authenticating method, for example EAP-PEAP/TLS.*

- **Autonomous PAC Provisioning** - during the initial phase of EAP-FAST server authentication may be used to support the download of the client's (users and/or machine) FAST PAC, which, in turn, is subsequently used during the EAP-FAST normal connection authentication process.

Note: Server certificate validation processing

The internal steps to validate a server certificate consist of the following:

- Validate the signature (certificate chain) against the trusted root store.

  The server certificate received during negotiation may be issued directly by a trusted root certificate authority or by one of its trusted intermediate certificate authorities whose certificate must exist in the server certificate chain. Intermediate or subordinate certification authorities are trusted only if they also have a valid certification path from a trusted root certification authority.

  The certificate authority (CA) certificate(s) used to trust the server certificate must be independently pre-installed and placed in the proper Windows Certificate Store. CA storage location follows the same structure as for the different Trusted Server types, as described below (For both all machine connections and user connections (public profile): Local computer-Intermediate CA and Trusted Root CA Stores; For user connections (private profile): Current User or Local computer-Intermediate CA and Trusted Root CA Stores).

  So, if you do not have the proper CA certificate in a CA store then a connection attempt will fail.

- Verify one or more fields within the certificate against the trusted server list (server issuer).

  So, if you do not have the proper server rule in the trusted server list then a connection attempt will fail.

- Ensure the server is who he claims to be by ensuring that the server actually possess the private key that matches the public key indicated in the server certificate that was just validated and verified by running the TLS protocol. (This step is performed autonomously without intervention or configuration by the user.)

Note: ***Self-signed certificates***
A server certificate may be signed by itself (having a certificate chain length of 0). The Client will trust such certificates if they appear in the list of trusted root entities in the appropriate store.

- **FAST Server Identification** - used only in EAP-FAST for normal connection authentication or while accepting and saving a user's (or machine) PAC sent by the FAST server (whether requested by the client or autonomously sent by the server) to validate the identity of the PAC's source.

Note: *the client, when initially accepting a provisioned PAC via the server certificate method, will autonomously add the FAST Server Identification (A-ID) to the Trusted Server list - transferring the "trust" in the server certificate to the server's A-ID. This means that when using the standard FAST v1a methodology of provisioning the client's PAC via a server certificate it is sufficient to only populate the Trusted Server List with the server certificate rule. Note: this auto-created PAC rule will not, however, be displayed in the list of Trusted Server Definitions - only manually created rules are visible.*

However, when using the older FAST v1 methodology of unauthenticated provisioning the Trusted Server List must be populated with a PAC rule.

Note: PAC validation processing

The internal steps to validate a PAC consist of the following:

- Verify the AID from the server against the trusted server list.
- Ensure the server has the key and opaque that goes with the verified AID. (This step is performed autonomously without intervention or configuration by the user.)

<return to top>

User Management

The set of trusted servers that are used by the Client can be manually configured by the following procedures:
(***Policy dependent*** - the ability to populate and edit the list may not be enabled in a deployed End-User Client.)

Adding to the List of Trusted Servers

Removing a Trusted Server

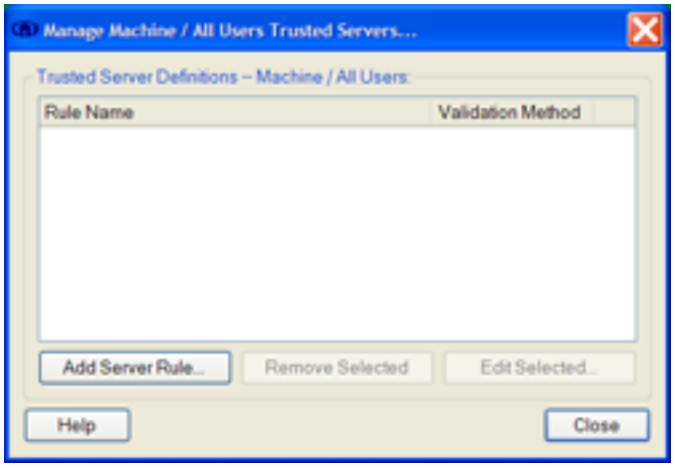
Editing a Trusted Server's Rules

Trusted Server List types:

- Trusted Server definitions for ***machine and all users*** (public profile)
  - used for server validation for the following connection types:
    - all machine connections
    - all user connections (public profile)
    - user connections (private profile) - trust is inherited from the machine's list.
  - required for acceptance (and storage) of a received-via-provisioning machine PAC.

- control (add, edit, remove) available for the following client types and operations.
  (***Policy dependent***- where available in a deployed end-user client, it is limited to viewing only)
  - administrator client version
  - administrator's deployment distribution package (only the administrator can define machine trust) (All deployed trusted servers are of this type.)

- Trusted Server definitions for ***current users*** (private profile)
  - used for server validation for the following connection types:
    - user connections (private profile) - trust is based on the union of the two trusted server lists.
  - acceptance (and storage) of a received-via-provisioning user (tunnel) PAC is based on the union of the two trusted server lists.
  - control (add, edit, remove) available for the following client types and operations.
    - administrator client version
    - configurable end-user client version (***Policy dependent*** - where enabled)



***Procedure*: Adding to the List of Trusted Servers**

Step 1: from the **Client** menu, ***select*** one (User or Machine) of the **Trusted Servers** sub-menu items » to open the appropriate **Manage <Current User | Machine / All Users> Trusted Servers** dialog.

Step 2: ***view*** the list of Trusted Servers from the **Trusted Server Definitions** display pane.

> **Note**: *in the out-of-the-box Administrator/Power-User client, the Machine / All User Trusted Server list will initially be empty. In a deployed End-User client it must be pre-populated by the IT administrator, if required.*

The display contains a list of all currently trusted servers.

- **Server Name** - a user-friendly name chosen at the time of entry for ease of identification - it is not used for any validation, simply a reference.
- **Validation Method** - identifies the category of server information type .
  - **Certificate** - information stored is the validation rules for the server certificate.
  - **PAC** - information stored is the FAST A-ID (Authority Identification) of the FAST server.

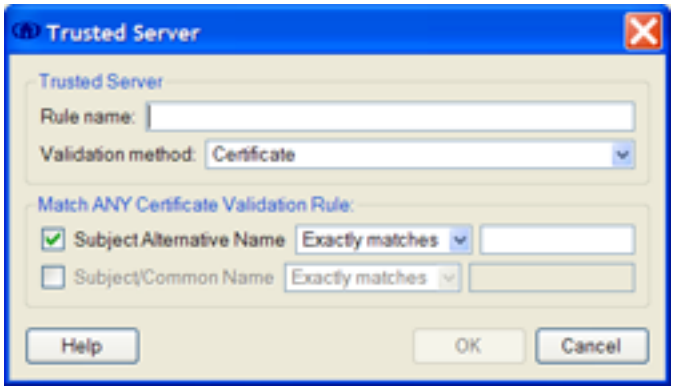
Step 3: ***click*** the **Add Server Rule** button » to open the **Trusted Server Rule** dialog.

Step 4: in the **Trusted Server** pane, provide the following:

- **Rule name** - enter a user-friendly name that allows for easy identification of the specific server.
- **Validation method** - select from the pull-down menu the type of server information being added. This changes the second pane of the dialog for the correct detailed rule entry.

Step 5: Server Rule type

Step 5a: For ***Certificate***:



Initially the ***Match ANY Certificate Validation Rules*** list will be empty.
Add a Rule:
1) **Select** a certificate field:
Since certificates are allowed to use different sets of optional attributes, you may specify the specific certificate attribute (s) to use in the validation rule from the following list of acceptable certificate attributes: Choose either or both.

- ***Subject Alternative Name*** - searches the following certificate fields (attributes):
  - Subject Alternate Name: DNSName
    Note: *typically this takes the form of a Fully Qualified Domain Name (FQDN)*
- ***Subject Common Name*** - searches the following certificate fields (attributes):
  - Subject: CN (Common Name)
    Note: *typically a simple ASCII string.*
    Note: *if multiple Common Names are specified, all those listed in the certificate are searched.*
  - Subject: DN (Domain Name) - a composite of a set of DC (Domain Component) attributes
    Note: *for example, a DC set of DC=Mycompany, DC=com, results in a Domain Name of Mycompany.com.*

2) **Select** a validation comparison rule:

- ***Exactly matches*** - the certificate field must contain the full contents of the text box
- ***Ends with*** - the certificate field must end with the contents of the text box
  Note: *typically used to quantify a FQDN - for example, if the text box contains "mycompany.com", certificates with the following Subject Alternate Names would be considered trusted, engr.mycompany.com, mkrt.mycompany.com.*

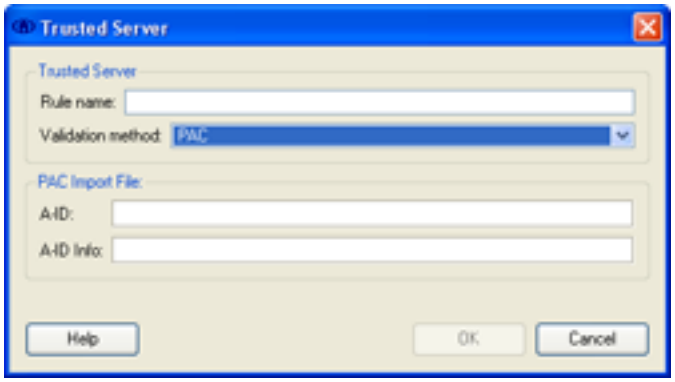
3) **Enter** the text: acceptable formats are:

- ***label*** - <string>
- ***realm*** - <string> . <string> etc.

or

Step 5b: For ***PAC***

Note: PAC *rules are not generally required to be manually created - see background discussion above.*



1) Obtain the ***PAC Import File*** information from the Cisco ACS server.
   - **A-ID** (required) - Authority Identification (the actual FAST server identifier) - typically this can be a somewhat cryptic expression and is HEX formatted.
   - **A-ID Info** (optional) - a user-friendly name for the A-ID

2) Enter the information into the appropriate ***PAC Import File*** text box.

Step 6: ***Click*** the **OK** button, to accept the addition and return to the **Manage Trusted Servers** dialog.
(Or ***click*** the **Cancel** button to return without modifying the Trusted Server list.)

<return to user management>

Procedure: Removing a Trusted Server

Step 1: from the **Client** menu, ***select*** one (User or Machine) of the **Trusted Servers** sub-menu items » to open the appropriate **Manage <Current User | Machine / All Users> Trusted Servers** dialog.

Note: a deployed Trusted Server rule is locked and can not be removed.

Step 2: ***select*** a Trusted Server from the **Trusted Server Definitions** display pane.

Step 3: ***click*** the **Remove Selected** button to remove the specific trusted server.

<return to user management>

Procedure: Editing a Trusted Server

Step 1: from the **Client** menu, ***select*** one (User or Machine) of the **Trusted Servers** sub-menu items » to open the appropriate **Manage <Current User | Machine / All Users> Trusted Servers** dialog.

Note: a deployed Trusted Server rule is locked and can not be modified. (All deployed rules are Machine / All User Trusted Server rules.)

Step 2: ***select*** a Trusted Server from the **Trusted Server Definitions** display pane.

Step 3: ***click*** the **Edit Selected** button to open the pre-populated **Trusted Server Rule** dialog for the specific trusted server.

Step 4: ***edit*** the validation rules appropriately. (See above for detailed explanations of validation fields.)

Step 5: ***Click*** the **OK** button, to accept the changes and return to the **Manage Trusted Servers** dialog.
(Or ***click*** the **Cancel** button to return without modifying the Trusted Server.)

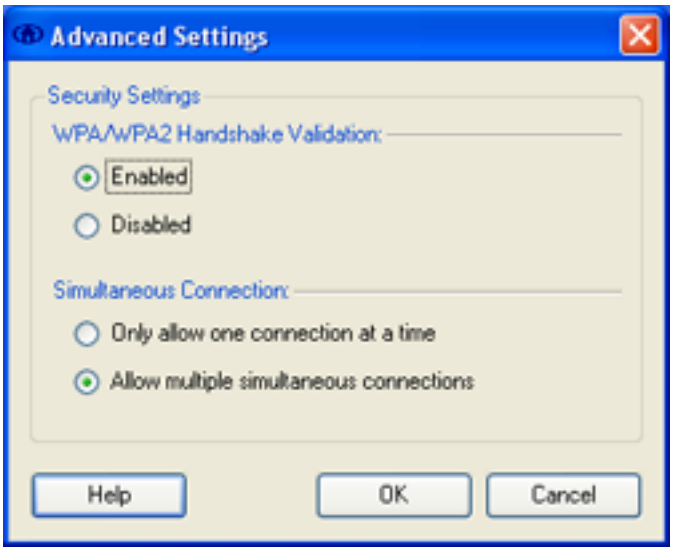
<return to user management>

<return to top>

Managing Advanced Settings

Managing Client Advanced Settings consists of the following topics:

Global administrator options for the Client can be configured with the following dialog:



(***Policy dependent*** - may not be present in a deployed End-User Client.) When deploying end-user clients the administrator will most likely set these options to a fixed configuration for the deployed client.

Managing Security

WPA/WPA2 Handshake Validation

Background: WPA's sophisticated key management requires driver capabilities that may not all be available in older embedded network adapters. In order to support situations where it is not practical to update a large base of older adapters, the Client provides a security bypass capability for WPA/WPA2 so that no RSN probe response/beacon IE verification is required in the 4-Way Handshake.

Procedure: Managing the Adapter WPA Security

Step 1: from the **Client** menu, ***select*** **Advanced Settings** to open the **Advanced Settings** dialog.

Step 2: in the **WPA/WPA2 Handshake Validation** portion of the **Security Settings** pane

- choose **Enabled** for all WPA/WPA2 fully-compliant wireless adapters, as required by the standards.
- choose **Disable** (***out-of-box default***) only for special cases in which your wireless adapter's driver is known to have this deficiency.

Step 3: ***click*** the **OK** button to accept the new setting and return to the **Connection Control** Main Screen.
(Or ***click*** the **Cancel** button to return without changing the security setting.)

Simultaneous Connections

Setting the preference for controlling whether or not simultaneous connections are allowed across multiple access devices (either within a network or between networks) can be configured by the following procedure:

> **Note**: *Multiple connections require the end station be equipped with multiple network adapters (wired and/or wireless).*

See controlling user connections or managing machine connections for additional behavioral descriptions for these settings.

Procedure: Managing Simultaneous Connections

Step 1: from the **client** menu, ***select*** **Advanced Settings** to open the **Advanced Settings** dialog.

Step 2: in the **Simultaneous Connection** portion of the **Security Settings** pane

- choose **Only allow one connection at a time** to restrict the Client to creating only a single connection (prevent multi-homed configurations).
  > **Note**: the preference of the media type is fixed for wired/Ethernet, when both types are available within a network.
- choose **Allow multiple simultaneous connections** (***out-of-box default***) to allow multi-homed network connections.

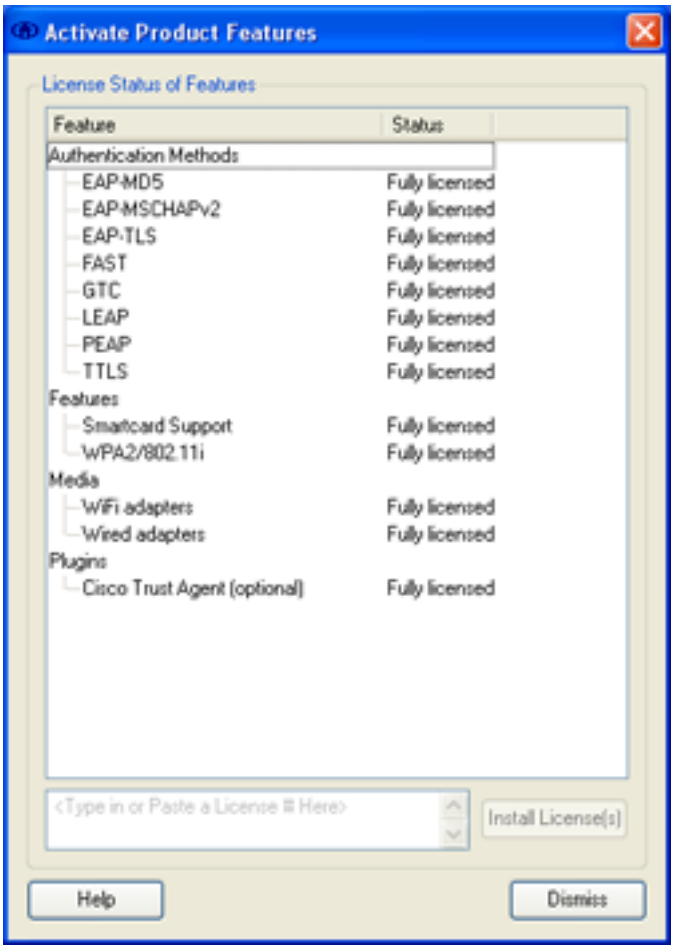
Step 3: ***click*** the **OK** button to accept the new setting and return to the **Connection Control** Main Screen.
(Or ***click*** the **Cancel** button to return without changing the security setting.)

> **Note**: the changes will not take effect until the next connect action.

Understanding Client Licenses

The ***base features*** of the Client are defined by its ***license***.

See understanding policies and profiles for an overview of licensable features.



License Status

The current status of the client's licensable features can be viewed via the following procedure:

(***Policy dependent*** - may not be present in a deployed End-User Client)

***Procedure*: Viewing the License**

Step 1: from the **Help** menu, ***select*** **Activation** to open the **Activate Product Features** dialog.

The **License Status of Features** pane displays a table of **Features** with their corresponding license **Status**.

- **Status** types
  - **Unlicensed** - feature is not enabled in client
  - **Trial License** - feature is enabled for a particular duration

        - Termination is displayed via an indication of "**N days left**" - after which the client will no longer operate.

    - **Fully Licensed** - feature is enabled indefinitely
      A full license may be accompanied by a ***maintenance agreement*** which allows for certain free upgrade privileges - contact Cisco Systems Sales/Support for detailed information.
        - After maintenance termination the client will still continue to operate but will lose its upgrade privileges.

    - **Timed License** - feature is enabled for a specific lifetime
        - Lifetime termination is displayed via an indication of "**N days left**" - after which the feature will no longer operate.

    - **Expired** - feature is no longer enabled
      Note: *applies to Trial and Timed License cases.*

Tip - Expiring License:

Within 15 days of a license expiring, a warning message is displayed when a user logs on to the machine. The message dialog also contains a link to the **Activate Product Features** dialog to allow for changing the license.

Tip - Fully Expired License:

*When all features of the client expire, when started the client will display an indication of such via a popup message window. (You can also check the technical log for expired license warning messages.) The message dialog also contains a link to the **Activate Product Features** dialog to allow for changing the license. Alternately, you can invoke the **Activate Product Features** dialog by selecting the **Activation** menu item from the system tray icon's modified pull-down menu list.*

Changing the License

The client's license may be changed after installation for a number of reasons, including the following:

- convert a trial license to a full license
- add or remove individual feature support
- add maintenance support
- extend the lifetime of a client

License Processing

A trial license requires an activation process consisting of the following:

- **Acquisition** - process by which a customer provides a 'payment' and a license is created that represents what the user has paid for.
    - responsibility of the IT Administrator for an administrator client and deployed end-user clients and performed through Cisco Systems Sales.
- **Activation** - process of installing the license into the product.
  (***Policy dependent***- may not be present in a deployed End-User Client)
    - direct through the client via the following procedure.
    - indirect as an integral part of the deploying of an End-User Client (see deploying an end-user client).
- **Validation** - process of reading one or more licenses, ignoring invalid licenses and enforcing the feature set indicated by the valid licenses.
    - performed autonomously by the Client.
      Note: *if, after processing all license strings, there are no features licensed then the Client service will simply exit silently.*

Procedure: Changing the License - via the Client

Step 1: from the **Help** menu, ***select*** **Activation** to open the **Activate Product Features** dialog.

Step 2: enter your license string in the text box.
Tip: *cut & paste from your email notification (full) or cisco.com (trial). Avoid any leading or trailing white space when entering the license.*

Note: *the license string is a 70, ASCII character, encrypted and encoded, representation of the license features and their status.*

Step 3: ***click*** the **Install License** button.

The license will be processed and
if ***valid***, the **Feature - Status** display will be updated accordingly
or
if ***invalid***, one of the following messages will be displayed:
For failure in string format: "Invalid license code, please double-check code." (double-check your inputted string)
For failure in content: "Invalid license options, please obtain new license."

Note - checking for license / profile inconsistencies:
Redeploying a new license may cause existing network profiles to become incompatible (invalid) or existing capabilities to become disallowed. Therefore when a new license is accepted by the client it will perform a consistency check. Any conflicts with the license will be resolved by modifying the network's behavior (or removing it). Manual reconfiguring may be required.

***Procedure*: Changing the License - outside the Client**

The IT Administrator can initialize or update a deployed end-user client through the distribution package (configuration) xml file.

See the *Cisco Secure Services Client Administrator Guide 4.1* for complete details of creating and deploying the distribution package xml file.

Troubleshooting the Client

In the event of operational problems, with local hardware, with a network access device or authentication server, or internally, the following diagnostic features are available that aids a user or support technician to debug an unexpected event in the client.

- **Technical log** of status and error activity messages

  The technical log file is a time-stamped, Unicode text file that is the destination for log messages capable of being viewed with Notepad (or equivalent) on Windows 2K/XP. Detailed characteristics are as follows:

  - the "file" is actually a series of files. The client stops using the current log file and creates a new log file whenever the client starts up or the maximum file size is reached (1MB).
  - the set of files have a maximum amount of allocated non-volatile (disk) space of approximately 5 MB. When the maximum storage level is reached, the oldest log file is deleted.
  - the current log file has the format: log_current.txt.
  - each archived file has the following naming format: log_<date>_<time>.txt, where <date> has the format YYYY-MM-DD, where YYYY is the year, MM is the month and DD is the day and <time> has the format: hh.mm.ss, where hh is the hour, mm is the minute and ss is the second.
    The date/time indicates when the file was archived - archived files therefore contain events prior to this time.
  - the set of files are located in a folder named ‘log’, below the main install folder. This would be 'Program Files\Cisco Systems\Cisco Secure Services Client\log' for the default install folder.
  - each log file contains a list of single line entries, where each entry defines a single log event.

  The technical log level is intended for those users who have training in 1X, .11i, EAP, EAP methods, PKI and understand the profiles/policies of the client.

  See understanding messages for details and a complete listing.

- **System Report**

  A separate utility that provides end user’s a simple way to automatically gather data needed by support personnel to troubleshoot any problems. It captures the following information:

  - current end-user technical log contents.
  - current internal application activity log (usable only by client developers)
  - information on the machine's hardware and software environment.

  See managing a report for detailed instructions on its use and operation.

Tips:

v **Conflicts with Antivirus software**

When using any antivirus software with the client, it is best to configure the antivirus software, if possible, to ignore scanning/processing current "active" log files in order to avoid consuming processing resources during an authentication.

Cisco SSC generates log files during authentication. The virus checkers detect this disk activity and produce high CPU usage while checking the log files, which are being written continuously. When there is high CPU usage during WPA/WPA2 authentication, Cisco SSC may not have sufficient access to the processor to complete the protocol handshake within the period permitted by the access point. This will cause the access point to dissociate the end station immediately after the 802.1X authentication, preventing establishment of the connection.

Configure the anti-virus software to not check the directory where the Cisco SSC logs are written. The most critical directory is c:\Program Files\Cisco Systems\Cisco Secure Services Client\system\log, which contains Cisco Systems support logs and where the most file writes occur. The second directory of interest is c:\Program Files\Cisco Systems \Cisco Secure Services Client\log, which contains the technical log discussed here.

Understanding Status and Error Messages

This section describes the format and contents of the Technical Log status and error messages.
Note: see technical log diagnostics for an overview.

Technical Log message format

Every log entry has the format:

<date & time> [process] <log message id> <log message class> <context IDs> <grammatical log message>

where:

- <***log message class***> determines the type of log message and is one of the following:
  - **I** – informational log message - used to indicate a client state that is part of normal processing.
  - **W** – warning log message - used to indicate a client state that is insecure or unexpected but which still allows processing.
  - **E** – error log message - used to indicate an exception that prevents normal processing.
- <***log message id***> is the unique number for the log message.
- <***date & time***> in the format MM/DD/YYYY HH:mm:SS.sss, where:
  - MM - numeric month (01-12)
  - DD - numeric day (01-31)
  - YYYY - numeric year (e.g. 2005)
  - HH - numeric hour on a 24 hour clock (00-23)
  - mm - numeric minutes past the hour (00-59)
  - SS.sss - numeric seconds with SS being seconds, and sss being fractions of a second.
- <***context IDs***> conveys zero or more identifiers to define the context of this log event. Each has the following format:
  - <code><unique string/number> where:
    - < code> is a two letter code that indicates the class of the term.
    - < unique string/number> is string or number that is guaranteed to be unique.
  - ***Adapter Identifier*** - **AD**<MAC address in hexadecimal for the adapter>
  - ***Access Identifier*** - **AC**<MAC/BSSID for the access device>
  - ***Media Type Identifier*** - ***MT***<Ethernet | WiFi> (**Note**: *MT may or may not be explicitly indicated*)
  - ***Connection Identifier*** - **CN**<an incrementing integer>
  - ***Profile Identifier*** - **PR**<network profile name truncated to 16 characters>
- <***grammatical log message***> is a sentence that describes the event. It may also contain a <value>, where:
  - <***value***> is a placeholder for a variable value to be placed in the message.
- [***process***] - internal process identifier, only important to developers.

Technical Log message content

Note: <value> definitions are listed after the message table.

Class	ID	Context IDs	Message
Client processing messages			
I	1		Client Service Auto Started. <Client's service name>, <version number>, <OS Name>
I	101		Client Service Manually Started. <Client's service name>, <version number>, <OS Name>
I	2		Client Service Normal Shutdown. <Client's service name>, <version number>, <OS Name>
E	133		Client Service Fatal Error Shutdown. <Client's service name>, <version number>, <OS Name> *Action*: manually stop and start the service or in extreme cases, uninstall and reinstall the client (your configuration files will be maintained).

I	3		Boot processing initiated.
Client environment processing messages			
I	85		Entering power save mode. *Note*: entering standby/hibernate mode.
I	86		Exiting power save mode (automatic) *Note*: exiting standby mode - will be followed with Error Msg #87.
I	87		Exiting power save mode. *Note*: exiting standby mode if preceded by Error Msg #86, otherwise exiting hibernate mode.
User logon processing messages			
I	4		User logon processing initiated.
I	134		Manual user <logon type> logon processing initiated by user <user id>.
I	129		User single sign-on credentials obtained from Novell GINA
I	130		User single sign-on credentials obtained from Microsoft GINA
I	5		User logoff processing initiated
Adapter processing messages			
I	6	AD< > MT< >	Adapter Detected.
I	8	AD< >	Adapter Controlled.
E	30	AD< >	Adapter startup failed because driver is in use. *Action*: manually disable competing utility.
I	13	AD< >	Wireless Zero Config automatically deactivated for adapter.
I	132	AD< >	Wireless Zero Config automatically reactivated for adapter.
I	14	AD< >	Control has been released for this adapter.
I	135	AD< >	Wired Access device disappeared.
I	136	AD< >	WiFi Access device disappeared. <ssid>
W	137	AD< >	WiFi access device has invalid channel number: <ssid>, <channel>
W	138	AD< >	Filtering out ssid '<ethernet>', it is not supported by this product. *Note*: '<ethernet>' is reserved for the wired access device class.
I	7	AD< >	Adapter Removed.
I	95	AD< >	User: User requested client to manage adapter
I	96	AD< >	User: User requested client to not manage adapter
Access device processing messages			
I	15	AC< >	Wired Access device detected.
I	102	AC< >	WiFi Access device detected. <ssid>, <signal>, <type>, <association>, <encryption>
Connection processing messages			
I	16	CN< > PR< > AD< > AC< >	Connection Requested automatically from machine context.
I	103	CN< > PR< > AD< > AC< >	Connection requested automatically from user context.
I	104	CN< > PR< > AD< > AC< >	Connection requested by user from user context.
I	94	PR< >	The user has initiated a network disconnect.
I	17	CN< >	Connection was terminated by user request.
I	105	CN< >	The service has been shut down. *Note*: any existing connection will be terminated.
I	106	CN< >	The adapter has been removed. *Note*: any existing connection will be terminated.

I	107	CN< >	The link is down. *Note*: any existing connection will be terminated (access device disappeared).
E	108	CN< >	The connection has terminated due to an internal error. *Action*: manually stop and start the service.
Connection processing - association messages			
I	18	CN< >	Connection association started using encryption mode <WiFi Association/Encryption Mode>.
I	19	CN< >	Connection association succeeded.
E	22	CN< >	Connection association failed. *Action*: verify network profile configuration with that of the access device.
Connection processing - key management messages			
I	80	CN< >	Adapter encryption key set. *Note*: part of the WiFi key exchange.
E	81	CN< >	Failed to set adapter key set. *Note*: the WiFi protocols for key exchange have succeeded, but the client has been unable to deliver the key to the network adapter for use. *Action*: update your network adapter to the latest adapter version.
W	139	CN< >	A pre-shared key is required but could not be found in the profile.
Connection processing - IP specific messages			
I	82	CN< > AD< >	Sending DHCP <action type> request.
E	84	CN< >	The IP address request (DHCP) has timed out. *Action*: verify network readiness - failure outside of client.
E	110	CN< >	A failure occurred while trying to get an IP address. *Note*: DHCP server responded with failure. *Action*: verify network readiness - failure outside of client.
E	111	CN< > AD< >	A failure occurred while trying to get an IP address. *Note*: Unknown DHCP failure has occurred. *Action*: verify network readiness - failure outside of client.
I	78	CN< > AD< >	The following IP address has been assigned: <IP Address>.
Authentication processing messages			
I	23	CN< > AD< >	Connection authentication started in machine context.
I	109	CN< > AD< >	Connection authentication started using the logged in user's credentials.
I	24	CN< > AD< >	Identity has been requested from the network.
I	25	CN< > AD< >	Identity has been sent to the network.
I	26	CN< > AD< >	The server has requested using authentication type: <Authentication Method name>. *Note*: EAP method suggested by server.
I	27	CN< > AD< >	The client has requested using authentication type: (<Authentication Method name>, …, <Authentication Method name>). *Note*: EAP methods requested by client
I	28	CN< > AD< >	Authentication method started using method type: <Authentication Method name>, level <tunnel depth>.
I	29	CN< > AD< >	Port state transition to <Port State>(<Port status>).
I	76	CN< > AD< >	The authentication process has succeeded.
E	77	CN< > AD< >	The authentication process has failed. *Action*: verify consistency of client, access point and server configuration.
I	57	CN< >	Attempting to resume TLS session number <session ID>
EAP Notification messages			
I	143	CN< >	EAP Notification message received from: AC< > <EAP Notification>
Authentication processing - FAST specific messages			

W	125	CN< >	Unauthenticated provisioning is supported for FAST.
I	55	CN< >	Phase one tunnel established using FAST. *Note*: using anonymous diffie-helman for unauthenicated provisioning of the PAC.
Authentication processing - server validation specific messages			
W	72	CD< >	Trusted Server list empty, server can not be validated.
I	73	CN< >	Validating the server: <Authentication Server Id>.
I	74	CD< >	The server <Authentication Server Id> has been validated.
W	142	CD< >	Profile does not require server validation.
E	75	CD< >	The server certificate could not be validated due to an unknown certificate authority. *Action*: verify that the correct CA certificate is in the Windows trusted root certificate store.
E	115	CD< >	The server certificate is invalid, the common name <CN name from server cert> does not match. *Action*: verify the server validation rule configuration - see managing trusted servers.
E	116	CD< >	The server certificate is invalid, the domain component name <DC name from server cert> does not match. *Action*: verify the server validation rule configuration - see managing trusted servers.
E	117	CD< >	The server certificate is invalid, the alternative name <Alternative name from server cert> does not match. *Action*: verify the server validation rule configuration - see managing trusted servers.
I	140	CN< >	The server authority identifier <AID-info> has been validated.
E	141	CN< >	The server could not be validated because the authority identifier <AID-info> did not match. *Action*: verify the server validation rule configuration - see managing trusted servers.
User profile configuring - manage trusted servers messages			
I	97		User: User added certificate based trusted server <Rule name>: <certificate-based trusted server rule>
I	112		User: User added pac based trusted server rule <Rule name> with AID: <AID-info>
I	98		User: User removed all trusted servers.
I	99		User: User modified trusted server list, <certificate-based trusted server rule>.
License processing messages			
I	89		Licensing: License file found.
E	90		Licensing: License file not found. *Action*: verify existence of the <install folder>\licenseTransport.txt file.
I	91		Licensing: License read: <License string>.
W	92		Licensing: License invalid because trial period expired <License string>, <trial period>.
W	118		Licensing: License invalid because termination date reached: <License string>, <termination date>.
W	119		Licensing: License invalid because operating system mismatch: <License string>, <licensed os>.
W	120		Licensing: License invalid because product id does not match: <License string>, <licensed product id>.
W	121		Licensing: License invalid because OEM id does not match: <License string>, <licensed OEM id>.
W	122		Licensing: License invalid because maintenance date reached: <License string>, <maintenance date>.
W	123		Licensing: License invalid due to unknown problem: <License string>, <termination date>.
W	131		Licensing: Ignoring trial license. Tampering detected: <License string>.
I	93		Licensing: License is valid and accepted: <License string>.
Internal messages			

W	0		Technical log message ID[<msgId>] not found.

Additional message <value> descriptions:

- <***Client's service name***>: The Windows service name for the client.
- <***version number***>: The version number of the client.
- <***OS Name***>: The operating system for which the client was built: Windows 2K/XP.
- <***logon type***>: Novell, Windows
- <***user id***>: user id for user logging on to endpoint.
- <***ssid***>: The SSID for the access device.
- <***channel***>: The 802.11 radio channel number.
- <***signal***>: The adapter received signal level: very poor, poor, good, very good, excellent.
- <***type***>: The 802.11 radio type: A, B, G.
- <***association***>: A comma separated list, where the list may contain one or more of: Open, Shared, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise.
- <***encryption***>: A comma separated list, where the list may contain one or more of: None, WEP, TKIP, AES.
- <***error number***>: An internal error number.
- <***error text***>: If the <error number> has a text equivalent.
- <***WiFi Association/Encryption Mode***>: Open, Shared 40 bit key, Shared 128 bit key, Static WEP 40 bit key, Static WEP 128 bit key, Dynamic WEP 40 bit key, Dynamic WEP 128 bit key, WPA-Personal TKIP encryption, WPA-Personal AES encryption, WPA-Enterprise TKIP encryption, WPA-Enterprise AES encryption, WPA2-Personal TKIP encryption, WPA2-Personal AES encryption, WPA2-Enterprise TKIP encryption, WPA2-Enterprise AES encryption.
- <***Authentication Method name***>: EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-LEAP, EAP-MD5, EAP-GTC, EAP-FAST, EAP-SIM, EAP-MSCHAPv2, MSCHAPv2, MSCHAP, CHAP, PAP.
- <***tunnel depth***>: A number indicating authentication tunnel depth starting at 0 for outer most and 1 for the inner nested method.
- <***sequence number***>: A number indicating where in a chain of authentications this authentication is beginning.
- <***port state***>: The adapter authentication AC_PORT_STATE values: _STOPPED, _CONNECTING, _AUTHENTICATING, _AUTHENTICATED, _REAUTHENTICATING, _UNAUTHENTICATED, _AUTH_NOT_REQD.
- <***port status***>: More detailed information on the success/failure of the authentication (and other associated state changes). It often acts as a sub-status of a particular AC_PORT_STATE. Values are listed below in a separate table.
- <***AID-info***>: The AID (Authority/Server Identifier) in the PAC.
- <***Authentication Server Identifier***>: The fully qualified domain name for the server or the PAC info field truncated to 16 characters.
- <***EAP Notification***>: Unsolicited messages from the authentication server.
- <***IP Address***>: IP address that the end station will use in the standard IP format xxx.xxx.xxx.xxx.
- <***rule name***>: Trusted server rule name.
- <***certificate-based trusted server rule***>: Defines the trusted server rule.
- <***License string***>: The license string read from the license file.
- <***trial period***>: The number of days in trial period.
- <***termination date***>: Date in format yyyy-mm-dd that the license expired.
- <***licensed os***>: The name of the operating systems that the license allows.
- <***licensed product id***>: The product id that the license allows.
- <***licensed OEM id***>: The OEM id that the license allows.

Port Status values:

```
AC_PORT_STATUS_UNKNOWN,
AC_PORT_STATUS_STOPPED,
AC_PORT_STATUS_STARTED,

/* status codes related to link state */
AC_PORT_STATUS_LINK_DOWN,
AC_PORT_STATUS_LINK_UP,
AC_PORT_STATUS_LINK_RESET,

/* status codes related to 802.1x state machine */
AC_PORT_STATUS_8021x_START,
AC_PORT_STATUS_8021x_FAILED,
AC_PORT_STATUS_8021x_ACQUIRED,
AC_PORT_STATUS_8021x_LOGOFF,
AC_PORT_STATUS_8021x_TIMEOUT,

/* error/status codes during 802.1x authentication */
```

```
AC_PORT_STATUS_ERR_CLIENT_EAP_METHOD_REJECTED,
AC_PORT_STATUS_ERR_CLIENT_GENERIC_REJECTED,
AC_PORT_STATUS_ERR_CLIENT_IDENTITY_REJECTED,
AC_PORT_STATUS_ERR_CLIENT_TLS_CERTIFICATE_REJECTED,
AC_PORT_STATUS_ERR_CHALLENGE_TO_AP_FAILED,
AC_PORT_STATUS_ERR_ROGUE_AUTH_TIMEOUT,
AC_PORT_STATUS_ERR_SERVER_TLS_CERTIFICATE_REJECTED,
AC_PORT_STATUS_ERR_UNKNOWN,
AC_PORT_STATUS_ERR_RESTRICTED_LOGON_HOURS,
AC_PORT_STATUS_ERR_ACCT_DISABLED,
AC_PORT_STATUS_ERR_NO_DIALIN_PERMISSION,
AC_PORT_STATUS_ERR_CHANGING_PASSWORD,
AC_PORT_STATUS_ERR_INVALID_TLV,
AC_PORT_STATUS_ERR_UNKNOWN_TLV,
AC_PORT_STATUS_ERR_TLV_NAK_RECEIVED,
AC_PORT_STATUS_ERR_INVALID_CMAC,
AC_PORT_STATUS_ERR_NO_CRYPTO_BINDING,
AC_PORT_STATUS_EAP_FAST_PROVISIONING,
AC_PORT_STATUS_ERR_EAP_FAST_INVALID_PAC_OPAQUE,
AC_PORT_STATUS_ERR_EAP_FAST_INVALID_PAC_KEY,

/* status codes related to EAP */
AC_PORT_STATUS_EAP_FAILURE,
AC_PORT_STATUS_EAP_SUCCESS,
AC_PORT_STATUS_WRN_CLEARTEXT_EAP_FAILURE,
AC_PORT_STATUS_WRN_CLEARTEXT_EAP_SUCCESS,

/* status codes related to credentials */
AC_PORT_STATUS_ERR_WRONG_PIN,
AC_PORT_STATUS_ERR_PIN_REQUIRED,
AC_PORT_STATUS_ERR_NO_DEVICE,
AC_PORT_STATUS_ERR_NO_CARD,
AC_PORT_STATUS_ERR_SIM_FAILURE,

/* status codes related to keys */
AC_PORT_STATUS_REKEY,
AC_PORT_STATUS_PAIRWISE_KEY,
AC_PORT_STATUS_GROUP_KEY,
AC_PORT_STATUS_INVALID_KEY,
AC_PORT_STATUS_WEP_TIMEOUT,

/* status codes related to WPA/11i */
AC_PORT_STATUS_RSN_REQUESTING_PAIRWISE_KEY,
AC_PORT_STATUS_RSN_REQUESTING_GROUP_KEY,
AC_PORT_STATUS_RSN_COUNTERMEASURES_START,
AC_PORT_STATUS_RSN_COUNTERMEASURES_STOP,
AC_PORT_STATUS_RSN_MULTIPLE_FIRST_MESSAGE,
AC_PORT_STATUS_RSN_DISCONNECT,
AC_PORT_STATUS_RSN_FIRST_MIC_FAILURE,

/* status codes related to CCX */
AC_PORT_STATUS_POSSIBLE_ROGUE_AP_START,
AC_PORT_STATUS_POSSIBLE_ROGUE_AP_STOP,
AC_PORT_STATUS_CCX_CCKM_ROAM
```

Related Topics:

Troubleshooting the Client

Managing a Log Report

System Report provides end user's a simple way to gather data needed by support personnel to troubleshoot any problems.

- Executable utility that is external and separate from the Client - operates whether the Client is currently active or not.
- Packaged with the Client and automatically installed with the Client.
- Creates a single file, the System Report, that contains information about the end station's hardware and software environment and Client as well as the gathered technical and developer logs.
  - a consolidated and compressed collection of files
  - non-configurable file name: Cisco_SSCSysRep<YYYYMMDD_hhmm>.zip, where YYYY is the year, MM is the month, DD is the day, hh is the hour and mm is the minutes.
  - non-configurable file location: Microsoft Windows Desktop
- Also creates a companion 'System Report log' text file which allows one to view what end station environment information was collected. This file is part of the System Report. It will be overwritten each time the utility is run with the same date.
  Note: in the event of a failure during the creation of the System Report zip file, this file serves as a means of reporting this.
  - non-configurable file name: Cisco_SSCSysRepLog<YYYYMMDD>.txt, where YYYY is the year, MM is the month, DD is the day, hh is the hour and mm is the minutes.
  - non-configurable file location: Microsoft Windows Desktop
- Accessible via the Windows start menu.
  All Programs › Cisco Secure Services Client › Cisco Secure Services Client System Report

Executing **Cisco Secure Services Client System Report** opens the **SysReport** dialog.

- ***check*** the **Protect sensitive data with following password** to encrypt some of the collected files, such as, your configuration files, license, etc., during the zip consolidation and compression process.
  - ***enter*** your password in the text box
    Note: *you will need to provide this password to the recipient of the System Report file.*
    Tip: *not all "unzip" utilities support a null password (empty password textbox) - it's recommended that you supply one.*
- ***click*** the **Collect Data** button to initiate the information gathering - this will take approximately 1/2 a minute or so.
- Once the report is saved, the user will see statement that "Report generation done ... Log file has been archived" and the following buttons are enabled:
  - **Copy To Clipboard** - copies the contents of companion System Report Log file to the Windows clipboard.
  - **Locate Report File** - opens Windows Explorer at the desktop with the desired zip file selected (highlighted).
- You can now email the System Report zip file to your support staff.

Related Topics:

Troubleshooting the Client