CHAPTER 9

Cisco Trust Agent 802.1x Wired Client

The Cisco Trust Agent 802.1x Wired Client (802.1x Wired Client) is an authentication supplicant for creating secure user connections with an Ethernet switch. The 802.1x Wired Client provides a graphical user interface for monitoring authentication status and managing authorized network access that is protected by the IEEE 802.1x protocol.

The 802.1x Wired Client implementation allows end-user connectivity to the network only after successful client-server authentication via port access control on the 802.1x-enabled access device.

The 802.1x Wired Client is an integral part of the Cisco Network Admission Control (NAC) security environment. In this environment, the Cisco Secure Access Control Server (ACS) requests posture information about NAC-compliant applications running on the system from the Cisco Trust Agent (CTA). The 802.1x Wired Client returns that posture information for CTA.

The Cisco Trust Agent 802.1x Wired Client is available for Windows systems only.

This chapter contains the following sections:

- 802.1x Wired Client Features, page 9-3
- 802.1x Wired Client Administrative and Client Versions, page 9-4
- 802.1x Wired Client User Interface, page 9-4
  - Administrative 802.1x Wired Client Automatic Startup, page 9-4
  - Network Connection Status, page 9-5
  - 802.1x Wired Client System Tray Shortcut Menu, page 9-7
  - 802.1x Wired Client Window, page 9-7

802.1x Wired Client Features

The Cisco Trust Agent 802.1x Wired Client (802.1x Wired Client) has the following features:

- **Pre-Configured**: The 802.1x Wired Client operates automatically. The only input required for administrative use of the client is the initial, one-time entry of the administrator’s individual user credentials.
- **Wired**: The 802.1x Wired Client supports wired 802.3 Ethernet connections (up to a maximum of 4).
- **Auto-Connection**: Connection to the CTA network environment is automatic, once a physical Ethernet connection has been made between your computer system's wired adapter interface and the network itself. Both machine and user logon context connections are supported.
- **Network Profile**: The 802.1x Wired Client is predefined to support a single network profile, embodying an administrative user, his security credentials, the computer's wired interface adapter(s), an 802.1x Ethernet switch access device, and an authentication server.
- **DHCP Management**: The 802.1x Wired Client ensures IP connectivity after a connection is authenticated.
- **Client Deployment**: The administrative version includes a deployment wizard that allows for creation and pre-configuration of an end user client. Pre-configuring involves supplying a trusted server list and end user credential selection methods.
- **Single Sign-on**: Once deployed, the 802.1x Wired Client can perform user authentication using Single Sign-On for Microsoft and Novell Networks.

- **Request Password When Needed**: Once deployed the 802.1x Wired Client can perform user authentication by requesting the user's password.
- **Machine Authentication Only**. Once deployed, the 802.1x Wired Client can support machine authentication without user authentication.

802.1x Wired Client Administrative and Client Versions

The administrative version of the 802.1x Wired Client is the "out-of-the-box" version of the product. By default, the Administrative 802.1x Wired Client will authenticate its local network using both machine and user authentication. It is intended for use by the IT organization responsible for configuring and deploying the end-user versions of the 802.1x Wired Client.

Once the administrator defines connection policies and those policies are installed along with the 802.1x Wired Client on a user's workstation, the 802.1x Wired Client becomes the end-user version of the product.

Note Unless otherwise noted, the functions described in this chapter refer only to the administrative version of the 802.1x Wired Client and are not available to end-users running the client version of the 802.1x Wired Client. While end-users will be able to view authentication settings previously deployed by the administrator, they will not be able to configure the client.

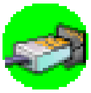
802.1x Wired Client User Interface

This section describes the elements of the 802.1x Wired Client interface that are visible to the administrative user.

Administrative 802.1x Wired Client Automatic Startup

After installation, the Cisco Trust Agent 802.1x Wired Client service starts automatically on startup of the Windows operating system. By default, the administrative 802.1x Wired Client is configured to automatically attempt to authentication the host using machine and user credentials. Confirmation that the 802.1x Wired Client has been successfully started is indicated by the presence of its icon in the Windows task bar icon tray.

Figure 9-1 802.1x Wired Client Icon



Network Connection Status

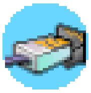
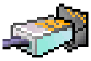
The 802.1x Wired Client icon in the Windows system tray changes color to reflect the state of the network connection.

Icon colors and their associated status indications are detailed in Table 9-1:

Table 9-1 Icon Status Color Codes

Icon Color	Status
Green 	The network adapter is connected and has been authenticated.
Yellow 	Authentication is taking place.
Red 	Authentication has failed.

Table 9-1 Icon Status Color Codes

Icon Color	Status
Blue 	The network adapter is connected but it does not require authentication. The connection is unauthenticated.
No color 	Connection is idle

Mousing-over the 802.1x Wired Client icon displays a summary connection status message.

Disabling the 802.1x Wired Client System Tray Icon

Step 1 Open the 802.1x Wired Client Interface

Step 2 From the Client menu, uncheck Show System Tray.

This configuration is made on individual clients and cannot be defined in a custom installation package.

802.1x Wired Client System Tray Shortcut Menu

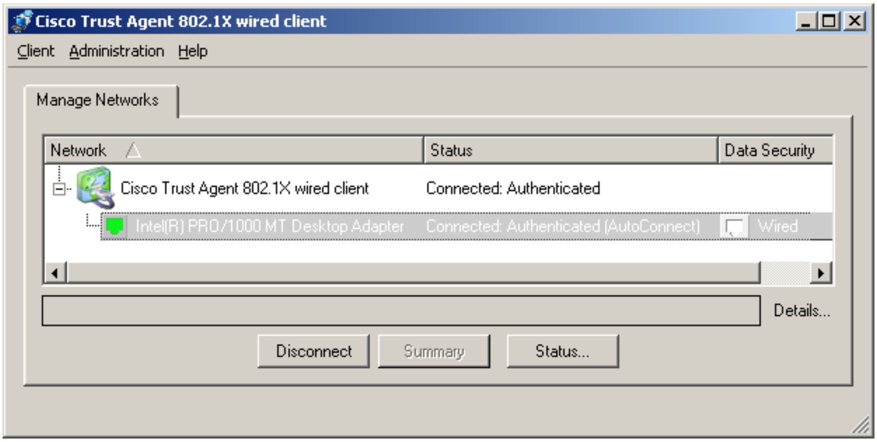
By right-clicking the 802.1x Wired Client status icon in the Windows system try you see a menu with three menu options.

Menu Choice	Description
Open	Allows you to launch the CTA 802.1x Wired Client interface.
Enable Client	Displays the state of the CTA 802.1x Wired Client, whether it is Enabled or Disabled. Checking the Enable Client menu option enables the 802.1x Wired Client. Unchecking the Enable Client menu choice disables the CTA 802.1x Wired Client. If **Enable** is checked the 802.1x Wired Client is active and can provide posture and credential information to authenticate the host. If **Disable** is checked, the 802.1x Wired Client can not provide posture and credential information to authenticate the host. Client:Enabled is the default state of the CTA 802.1x Wired Client.
About	Displays the version number and copyright information for the CTA 802.1x Wired Client.

802.1x Wired Client Window

The 802.1x Wired Client's main window contains a list of controlled networks. The single, pre-named, network connection expands to display all access devices configured within the network connection. In Figure 9-2 the network is named, "Cisco Trust Agent 802.1x wired client."

Figure 9-2 802.1x Wired Client Administrator's main window



Network	Status	Data Security
Cisco Trust Agent 802.1X wired client	Connected: Authenticated	
Intel(R) PRO/1000 MT Desktop Adapter	Connected: Authenticated (AutoConnect)	Wired

Network Connection Status

The color of the network connection's icon reflects the best connection status of all of the access device connections. The network connection icon in Figure 9-2 is named Cisco Trust Agent 802.1x Wired Client.

Table 9-2 Network Icon Status Information

Network Icon Display	Network Status	Description
Fully colored icon	Connected	Indicates that at least one of the access devices is connected and has been authenticated.
Grey icon	Connecting	Indicates that at least one of the access devices is connecting and is authenticating.
No color	Disconnected	Indicates that no access devices is connected or connecting and that no device has been authenticated.

Access Device Connection Status

The main window contains a list of access devices, which includes network adapters and network interfaces. In figure Figure 9-2 there are two access devices in the network:

- Intel(R) PRO/1000 CT Network Connection
- Intel(R) PRO/1000 MT Desktop Adapter

The assigned access device name is taken from the name of the network adapter associated with the access device. If all the members of the ethernet group are 'Not Available,' the name changes to its group '<ethernet>' name.

The color of the icon indicates the connection status of the access device.

Table 9-3 Access Device Icon Status Information

Access Device Icon Display	**Access Device Status**	**Description**
None	Disconnected	• The access device is currently available but not attempting a connection (a transitory state for auto-connection) • Auto-connection has been stopped, possibly caused by one of the following actions: – Credentials have been cancelled. See the "Credential Revalidation" section on page 9-23. – Connection has been stopped. See the "Manually Connecting To the Network" section on page 9-12.
Yellow	Connecting	The network adapter is attempting to make a network connection.
Green	Connected: Authenticated	The network adapter is connected to the network. The host has been authenticated.
Blue	Connected: Unauthenticated	The network adapter is connected to the network and does require authentication.

Table 9-3 Access Device Icon Status Information

Access Device Icon Display	Access Device Status	Description
Red	Failed (retrying)	This is a temporary state while attempting to authenticate the host and create a connection. The last attempt to authenticate failed.
Red	Failed	Authentication attempts have failed. Selecting the access device will display the reason for the failure in the Message Status bar.
X Overlays gray icon	Not Available	Access device is not available

The **Data Security field** is used only for access devices. It indicates that the security is based on a wired port.

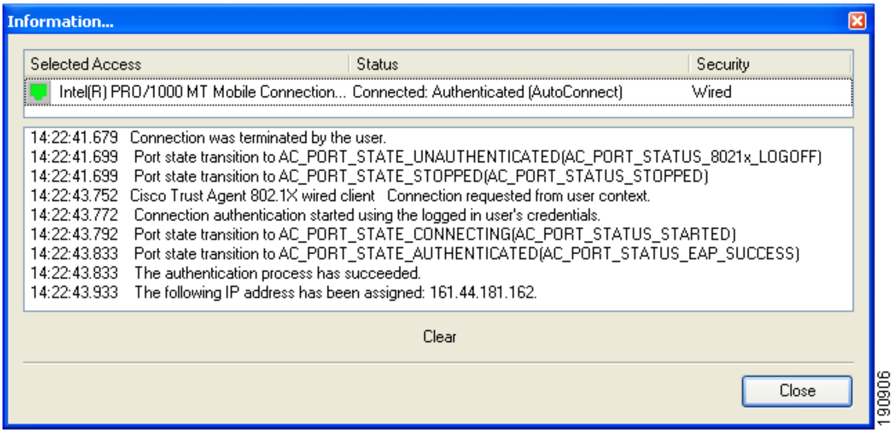
A single **Status Message display line** is located below the Access Port List and adds clarification to the current access status. Often used to clarify the reason for a failure, for example, why a connect attempt might have failed.

To the right of the Status Message display line is the **Details...** hot spot. Clicking the **Details...** hot spot launches the Information window. The Information window displays a real-time feedback of the individual steps of any (manual or auto) connection or disconnection process.

Selecting another access device, or using the “Clear” control clears the current display.

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

Figure 9-3 Network Adapter Information box



Information...

Selected Access	Status	Security
🟩 Intel(R) PRO/1000 MT Mobile Connection...	Connected: Authenticated (AutoConnect)	Wired

```
14:22:41.679  Connection was terminated by the user.
14:22:41.699  Port state transition to AC_PORT_STATE_UNAUTHENTICATED(AC_PORT_STATUS_8021x_LOGOFF)
14:22:41.699  Port state transition to AC_PORT_STATE_STOPPED(AC_PORT_STATUS_STOPPED)
14:22:43.752  Cisco Trust Agent 802.1X wired client  Connection requested from user context.
14:22:43.772  Connection authentication started using the logged in user's credentials.
14:22:43.792  Port state transition to AC_PORT_STATE_CONNECTING(AC_PORT_STATUS_STARTED)
14:22:43.833  Port state transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_EAP_SUCCESS)
14:22:43.833  The authentication process has succeeded.
14:22:43.933  The following IP address has been assigned: 161.44.181.162.
```

Basic 802.1x Wired Client Procedures

This section describes the tasks administrators perform from the main window of the 802.1x Wired Client.

Opening the 802.1x Wired Client

Use one of the following methods to launch the 802.1x Wired Client main window:

- Right-click the client icon in the system tray (as shown above in Figure 9-1,) to display the icon menu. Click **Open** to display the 802.1x Wired Client main window.
- Double-click the client icon in the system tray to directly open the 802.1x Wired Client main window.
- Use the Windows Start menu. Navigate Start > Programs > Cisco Systems, Inc. Cisco Trust Agent 802.1x wired client > Cisco Trust Agent 802.1x wired client

Manually Connecting To the Network

Step 1 From the 802.1x Wired Client main window, select the desired access device icon, displayed without color.

Step 2 Click **Connect**.

Manually Disconnecting From the Network

Step 1 From the 802.1x Wired Client main window, select the desired access device icon, displayed in full color.

Step 2 Click **Disconnect**.

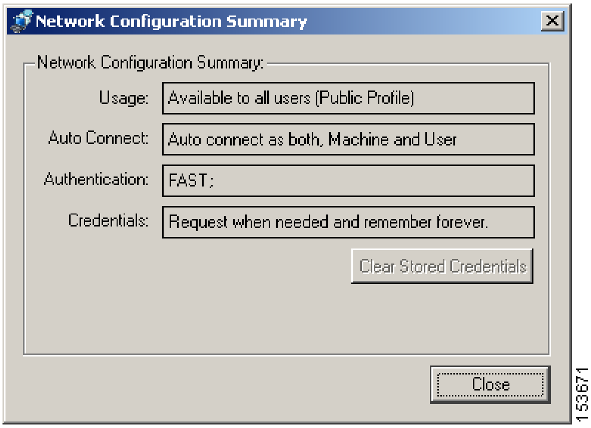
Viewing Network Summary

A summary of the policy that governs the connection and authentication of the host to the network can be viewed but it cannot be modified.

Step 1 In the 802.1x Wired Client main window, select the network for which you want to view the policy summary.

Step 2 Click **Summary**. The Network Configuration Summary dialog opens.

Figure 9-4 Network Configuration Summary dialog



Network Configuration Summary

Network Configuration Summary:

Usage: Available to all users (Public Profile)

Auto Connect: Auto connect as both, Machine and User

Authentication: FAST;

Credentials: Request when needed and remember forever.

Field	Description
Usage	802.1x Wired Client profiles are always public
Auto Connect	Indicates if the host connects using machine or user authentication.
Authentication	802.1x Wired Client always uses EAP-FAST authentication
Credentials	Describes where and how user credentials are obtained.
Clear Stored Credentials	Clicking this button allows users to delete their stored credentials and force a re-validation of their credentials.

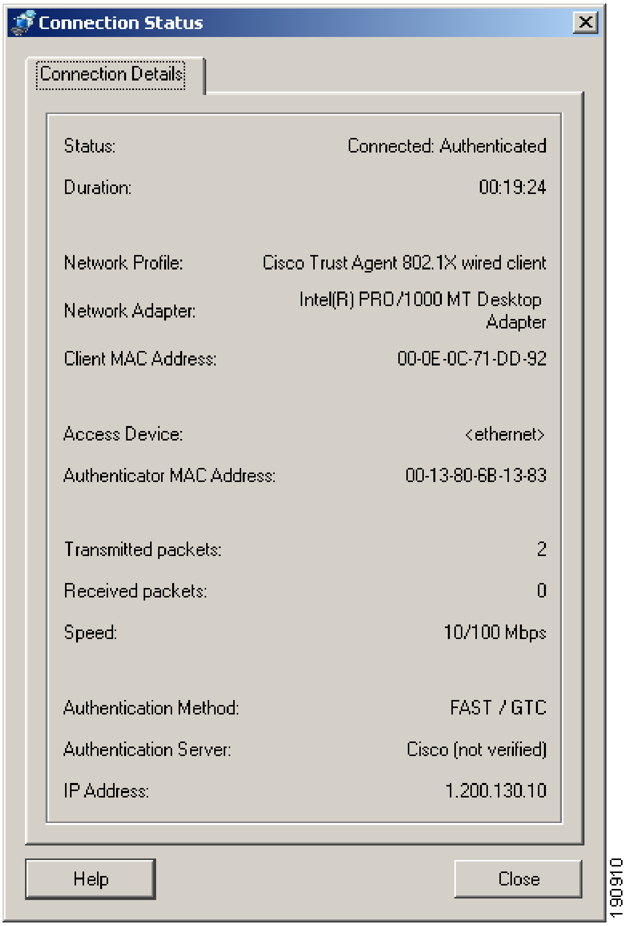
Viewing Access Device Status

This option displays the Connection Details window, which contains specific information about the access device’s network connectivity.

Step 1 In the 802.1x Wired Client main window, select the desired access device icon, for which you want to view the connection status.

Step 2 Click **Status**...The Connection Details window opens.

Figure 9-5 Connection Details Window



Status: Connected: Authenticated

Duration: 00:19:24

Network Profile: Cisco Trust Agent 802.1X wired client

Network Adapter: Intel(R) PRO/1000 MT Desktop Adapter

Client MAC Address: 00-0E-0C-71-DD-92

Access Device: <ethernet>

Authenticator MAC Address: 00-13-80-6B-13-83

Transmitted packets: 2

Received packets: 0

Speed: 10/100 Mbps

Authentication Method: FAST / GTC

Authentication Server: Cisco (not verified)

IP Address: 1.200.130.10

Field	Description
Status	State of the connection. This is derived from the Main Screen Access Port list
Duration	Defines how long the connection has been operational
Network Profile	Fixed generic name
Network Adapter	Identifies the port's adapter name
Client MAC Address	Displays the MAC address of the associated network adapter.
Access Device	Fixed generic name
Authenticator MAC Address	MAC address of the switch.
Transmitted packets	Actual number of layer 2 frames transmitted
Received packets	Actual number of layer 2 frames received
Speed	Indication of connection maximum data rate
Authentication Method	The authentication method may be EAP-FAST, EAP-GTC, or EAP-TLS. If the field is blank then authentication is not required because the host is not connected to a 802.1x configured port.
Authentication Server	The field shows either the server certificate's name or the server's FAST A-ID - augmented with an indication of either 'not verified' or 'trusted'. 'Not verified' only exists for the case of an empty Trusted Server List. (See the "Trusted Server Validation Area" section on page 9-29 for more information on trusted servers.)
IP Address	IP Address of host

Getting Started with 802.1x Wired Client Functions

Administrative 802.1x Wired Client Overview

This administrative version of the client has one pre-defined enterprise network when initially started. A Network is defined by its Network Profile. (See "Understanding Policies and Profiles" section on page 9-24 for more information on network profiles.)

The 802.1x Wired Client utilizes EAP-FAST (the Flexible Authentication via Secure Tunneling method of the Extensible Authentication Protocol). 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.

Authentication Methods Overview

The 802.1x Wired Client authenticates machines and users so that they may connect to the network. Successful user authentication establishes a network connection after a user logs onto the machine. Successful machine authentication connects the machine to the network once the machine's credentials have been authenticated. User and machine authentication may also be used together.

Note

- Some applications may not be appropriate choices to provide posture credentials during machine authentication. Such applications may be slow to start, for example, and they will not be ready to provide posture credentials immediately for machine authentication.

  In this case, machine authentication could fail, not because of a security problem but because the application was not available to provide its posture credentials in time.

- In order to perform machine authentication, the EAP-FAST Configuration in ACS must allow machine authentication.
- Machine authentication can only be performed on networks where Windows Active Directory is in use.

Each deployed end-user 802.1x Wired Client is configured to support one of the following methods of authentication for network access:

- User authentication only
- Machine and user authentication
- Machine authentication only

The administrative 802.1x Wired Client is pre-configured to connect the host to the network only after authenticating machine and user credentials.

Overview of FAST Connections in a User Logon Context

Initial User Connections - Before the PAC Has Been Provisioned

During the initial authentication session, the FAST protocol provides for the automatic provisioning of the administrative user's unique PAC.

There are two methods of automatically provisioning a user’s PAC. The first is a basic automatic provisioning feature that does not require a server certificate to be installed on the host. The second is a more secure automatic provisioning feature that uses a server certificate for providing initial authentication.

Note The initial authentication session may take several authentication cycles to complete depending on the method used and the configuration of the server.

The basic automatic provisioning feature prompts users for their user credentials only.

The automatic provisioning feature that uses a certificate also requires user credentials and the CA certificate used to trust the server certificate must be stored in the proper Windows Certificate Store (User-Trusted Root Store) of the host.

For both the basic or certificate-based automatic provisioning, the FAST authentication server must be configured for auto creation of the administrator's unique user PAC information.

The user credentials needed for the basic and certificate-based automatic provisioning are requested on an as-needed basis. See the "User Credentials" section on page 9-20 for more information.

These are the user credentials that may be required:

- Identity. The format of the information is *UserName@Domain*, where the use of the domain, also referred to as a "realm," is optional.
- Password. This credential is optional.
- User Certificate Identifier. This credential is optional.

Subsequent User Connections - After the PAC Has Been Provisioned

Once the user (tunnel) PAC has been provisioned and the user's credentials saved, subsequent connections are autonomously made using the PAC data to create the secure tunnel used for passing the user's credentials for authentication. No user intervention is required and authentication is automatic.

Overview of FAST Connections in a Machine Credentials Context

Initial Machine Connections - Before the PAC Has Been Provisioned

The provisioning of the Machine PAC, which is needed for machine context connections, is accomplished using the server certificate or machine security identity (SID). Machine PACs are only supported in newer versions of authentication servers (ACS 4.0 or later) which have been upgraded to support EAP-FAST v1a.

To make a make a machine connection before the PAC has been provisioned, the CA certificate used to trust the server certificate must be placed in the proper Windows Certificate Store (Local Computer-Trusted Root Store).

The host must also provide these machine credentials:

- Active Directory provided machine certificate. The authentication method must support the use of a certificate to provide machine client credentials - the server must be appropriately configured to call for an inner tunnel method of TLS.
- Active Directory provided SID (password). The authentication method must support the use of a password to provide machine client credentials.

Finally, the FAST authentication server must be configured for auto creation of administrator's unique machine PAC information.

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

Note If a machine certificate or *machine password* (SID) is not *initially pre-installed on the machine*, 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.

Note If a machine certificate/password 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.

Subsequent Machine Connections - After the PAC Has Been Provisioned

Once the machine PAC has been provisioned, subsequent connections are autonomously made using the PAC data exclusively and authentication is automatic.

User Credentials

The EAP-FAST method used by the 802.1x Wired Client supports the following types of user credentials:

- **User identity**. This is a mandatory element.
- **User password or user certificate**. The use of one of these elements is required.

The single Network Profile of the 802.1x Wired Client is pre-configured to accommodate both types, as needed. 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 802.1x Wired Client.

Initial Credential Provisioning

After the 802.1x Wired Client is deployed to an individual end-user, specific user credential information may be required to be provisioned. However, there is no pre-provisioning of this information. Rather it is requested, on-demand, by the client at the appropriated time during its first connection attempt after initial startup. A series of appropriate Credential Request Pop-up Dialogs are progressively displayed to the user with prompts and mechanisms for entering the desired information.

Identity Credentials

One of the following identity credential methods has been pre-configured:

- Operating System login (Single-Sign-On) credentials - no provisioning required.
- Request & Store - initial text input provisioning through Enter Your Credentials Pop-ups, encrypted and stored for automatic use thereafter.

  An Identity has a Network Access Identifier (NAI) format and takes the following generalized form: *UserName@Domain*, where the use of the domain, also referred to as a "realm," is optional. The identity specified may contain up to 63 ASCII characters and is case sensitive.

Password Credentials

One of the following password credential methods has been pre-configured:

- Operating System login (Single-Sign-On) credentials - no provisioning required.
- Request & Store - initial text input provisioning through Enter Your Credentials Pop-ups, encrypted and stored for automatic use thereafter. The password specified may contain up to 80 ASCII characters and is case sensitive.

Certificate Credentials

The request and store configuration method for certificates credentials has been pre-configured:

- Request & Store - Initial file selection provisioning through Enter Your Credentials Pop-ups, stored for automatic use thereafter.

  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)
  - Expired: Valid to

Note The certificate must not have strong private key protection, since this will cause the connection authentication to fail at logon.

Note The administrator version is pre-configured to support "Request & Store" only.

Machine Credentials

Depending on the EAP method you use, there are two types of machine credentials.

Pre-PAC or no-PAC Provisioning

- **Machine certificate** - This 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).

  There are two restrictions to this method:

  - There can only be a single certificate stored here - which is the normal usage condition.
  - The certificate must not require a PIN or have strong private key protection.

Note The machine identity is provisioned the “dnsName” field, of the Subject Alternative Name, of the machine certificate.

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 SID** - This uses the Microsoft Active Directory provided machine SID (Security IDentifier) with a password-based EAP method, such as, EAP-MSCHAPv2.

Note The SID acts as a machine password.

Post-PAC Provisioning

A Machine PAC is 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.

Credential Revalidation

Credentials may expire in which case the server may initiate a revalidation of the credentials or the user may clear the credentials and force a revalidation.

Server-Initiated Credential Revalidation

In addition to cases where the credentials fail to be accepted by the server, the server may employ policies such as password aging that automatically re-prompts the user for their credentials using the appropriate “Enter Your Credentials” pop-up.

User-Initiated Credential Revalidation

The user can manually force a re-prompting for authentication credentials. The re-prompting clears any stored user credentials which causes a new sequence of credential request pop-up dialogs to appear during the next authentication attempt.

Note The control is enabled if the credentials are remembered. When the user clears the credentials, the control will become disabled.

Note This is not valid for Single-Sign-On credentials.

To clear existing credentials, follow this procedure:

Step 1 Launch the 802.1x Wired Client interface.

Step 2 In the Connection Status dialog box, select the network that you want to re-prompt for credentials.

Step 3 Click **Summary**.

Step 4 Click **Clear Stored Credentials**.

Understanding Policies and Profiles

The 802.1x Wired Client is part of a family of 802.1x connection clients. An End-user 802.1x Wired Client creates network connections based on its base features and its operational environment, which is defined by a set of configuration documents.

The 802.1x Wired Client's base feature is that it is limited to a wired (802.3) network media type.

The authentication policies used by the 802.1x Wired Client are based on two configuration documents:

- 802.1x Wired Client policy file
- 802.1x Wired Client network policy file

802.1x Wired Client Policy File

The 802.1x Wired client policy file, policy.xml, which is installed in the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies** directory defines these aspects of the operational environment:

- **Authentication methods on how network connections may be created.** 802.1x Wired Client is limited to an EAP-FAST "outer method" with "inner methods" of EAP-TLS, EAP-MSCHAPv2, EAP-GTC
- **User interface configuration variations.** The 802.1x Wired Client is limited to one network profile.
- **Trusted Servers List** which defines how to validate the credentials of servers during mutual EAP authentications.

Note The administrator version is pre-configured with an empty Trusted Server List and therefore never performs server validation.

802.1x Wired Client Network Policy File

The network policy file, **networks.xml**, which is installed in the **Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\networks** directory defines these aspects of the operational environment:

- **Methods for collecting user credentials**. The 802.1x Wired Client supports single sign-on or request authentication-unique password user credentials.

  Note The administrator version is pre-configured to support “Request & Store” only.

- **Origination of connections**. The 802.1x Wired Client supports both machine and user originated connection types.
- The administrative version of the 802.1x Wired Client is pre-configured to support “Machine and User authentication.”
- **Use of client certificates**. The 802.1x Wired Client can be configured to require the use of client certificates for machine and user connection types.

  Note The administrative version of the 802.1x Wired Client is pre-configured to not require a client certificate for both machine and user authentications.

- **Authentication protocols.** 802.1x Wired Client can be configured for the Identity used for the phase 1 outer (unprotected) tunnel of the EAP-FAST method.

  Note The administrative version of the 802.1x Wired Client is pre-configured to use “Anonymous” as the identity.

Using the Administrative 802.1x Wired Client, a system administrator uses the Deployment Package Wizard to create the 802.1x Wired Client policy.xml file and network.xml policy file based on the administrator’s input.

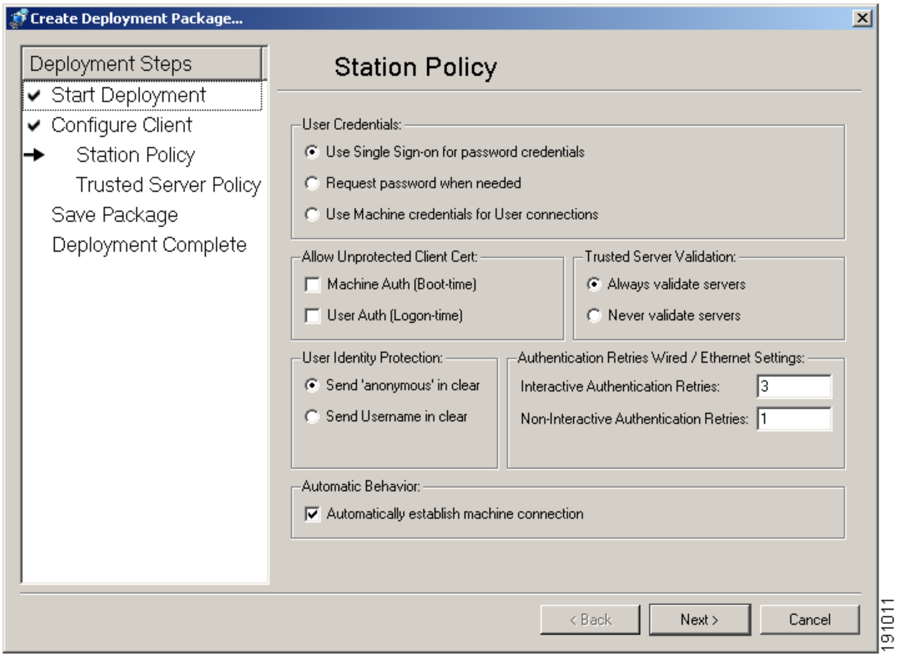
The names for the policy.xml and network.xml files are standardized so that they may be easily recognized and distributed to the appropriate hosts.

Create Deployment Package Wizard

The Create Deployment Package wizard provides an interface which allows you to configure the network connection context. The deployment package you create using the wizard consists of a **policy.xml** and a **networks.xml** file which contain the connection context information. See "Understanding Policies and Profiles" section on page 9-24 for more information about these files and their roles.

The Station Policy window of the Create Deployment Package wizard displays the settings which are configured to create the policy.xml and networks.xml file.

Figure 9-6 Station Policy Window



Create Deployment Package...

Deployment Steps
- ✓ Start Deployment
- ✓ Configure Client
- → Station Policy
- Trusted Server Policy
- Save Package
- Deployment Complete

Station Policy

User Credentials:
- ● Use Single Sign-on for password credentials
- ○ Request password when needed
- ○ Use Machine credentials for User connections

Allow Unprotected Client Cert:
- □ Machine Auth (Boot-time)
- □ User Auth (Logon-time)

Trusted Server Validation:
- ● Always validate servers
- ○ Never validate servers

User Identity Protection:
- ● Send 'anonymous' in clear
- ○ Send Username in clear

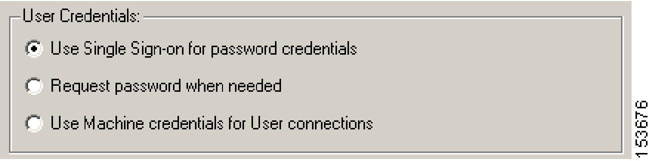
Authentication Retries Wired / Ethernet Settings:
- Interactive Authentication Retries: 3
- Non-Interactive Authentication Retries: 1

Automatic Behavior:
- ☑ Automatically establish machine connection

User Credentials Area

The User Credentials area of the Station Policy window defines which user credentials are used to authenticate the host to the ACS server. Radio buttons provide three options.

Figure 9-7 User Credentials area



User Credentials:

● Use Single Sign-on for password credentials

○ Request password when needed

○ Use Machine credentials for User connections

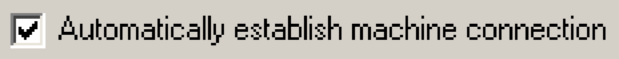
Radio Button	Description
Use Single Sign-on for password credentials	This option uses the user's Windows Operating System password. The user is not prompted for this password.
Request password when needed	This password is recorded in ACS. It is the password defined to authenticate a client to the ACS server. This may be the Windows operating system password or it may be another. The user is prompted for this password.
Use Machine credentials for user connections	This option replaces user credentials with machine credentials. Choose this radio button when performing machine authentication only.

Automatically Establishing Machine Connection

The **Automatically establish machine connection** check box should be checked when you are performing machine authentication or machine and user authentication.

If the box is checked, the client automatically attempts to authenticate itself during boot up. If the box is not checked, machine authentication does not occur until after the GINA (Graphical Identification and Authentication) login.

Figure 9-8 Automatically establish machine connection check box.



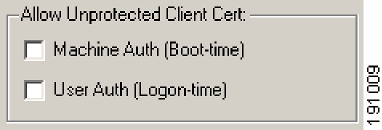
☑ Automatically establish machine connection

Allow Unprotected Client Cert Area

This area allows you to enable the use of client credentials during the unprotected phase of FAST PAC provisioning. The use of client credentials is optional.

These settings refer to whether or not the 802.1x Wired Client should send a certificate unprotected and not necessarily, whether or not to ever send a certificate.

Figure 9-9 Allow Unprotected Client Cert Area



Allow Unprotected Client Cert:

□ Machine Auth (Boot-time)

□ User Auth (Logon-time)

- **Machine Auth (Boot-time)**: This method authenticates the host to the ACS using the Microsoft Active Directory provided machine certificate.
- **User Auth (Logon-time)**: This method authenticates the host to the ACS using a pre-deployed user certificate.

Configuring Unprotected Client Cert Area Settings

Checking Machine Auth (Boot-time) or User Auth (Login-time)

Checking either checkbox disables protection for the specific connection time. When requested by the server for a client certificate during the unprotected portion of FAST PAC provisioning:

- If there is a client certificate available the 802.1x Wired Client will sent it unprotected or “in the clear.”
- If there is no client certificate, none will be sent and the server policy will determine if authentication continues or fails.

Not Checking Machine Auth (Boot-time) or User Auth (Login-time) checkboxes

Leaving these checkboxes unchecked enables protection for the specific connection time.

When the server requests a client certificate during the unprotected portion of FAST PAC provisioning, the client refuses to send any certificate. The client may do this because it is waiting for the protected phase of the protocol.

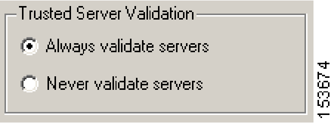
However, before the second phase of the protocol starts, a tunnel is established based on the server’s certificate. The 802.1x Wired Client will send its certificate through this tunnel before phase 2 authentication begins.

Note These check boxes have no effect on the use of a client certificate during the protected portion of FAST PAC provisioning. If the server is configured to request the sending of the client certificate within the secure tunnel (e.g., FAST/TLS), the client will always attempt to use one. If none is available and not sent, the connection attempt will fail.

Trusted Server Validation Area

The Trusted Server Validation area allows you to specify the authentication servers the End-user 802.1x Wired Client can trust with their user and machine credentials.

Figure 9-10 Trusted Server Validation area



Trusted Server Validation

● Always validate servers

○ Never validate servers

- Select **Always validate servers** to require authentication server validation during credential authentication. This is the most secure setting and it is the default setting.

  Note If you select **Always validate servers** and deploy a client profile with an empty Trusted Servers list, authentication will fail.

- Select **Never validate servers** to ignore authentication server validation during credential authentication. This is the least secure setting.

Warning **The "Never validate servers" option is not recommended because it reduces the level of security.**

Note There is an exception to the warning against using the "**Never validate servers**" radio button in the Trust Server Validation area.

The administrative version of the 802.1x Wired Client is the "out-of-the-box" version of the product. By default, the Administrative 802.1x Wired Client will authenticate itself to the local network using both machine and user authentication. It is intended for use by the IT organization responsible for configuring and deploying the end-user versions of the 802.1x Wired Client.

In order to specify a Trusted Server for a client, you need to create a deployment package and install it on the client. Once you install a deployment package on the client running the Administrative 802.1x Wired Client, the 802.1x Wired Client looses its Administrative capabilities and becomes and ordinary 802.1x Wired Client. That is, after the deployment package is installed, the 802.1x Wired Client will no longer be able to create authentication profiles or other deployment packages.

For that reason, the administrative version of the 802.1x Wired Client is pre-configured to support **Never validate servers** only.

Deploying Trusted Servers

Before you begin deploying trusted servers, the identification of the trusted server(s) that support the initial FAST PAC provisioning of the host needs to be configured. Two server validation methods are supported:

- Basic - requires knowledge of the Authority Identity of the associated Cisco Secure ACS.
- Server Certificate - requires pre-creation of certificate and storage on the associated server.

Initially the Trusted Servers list will be empty.

Note If you select **Always validate servers** in the Trusted Server Validation area of the Station Policy window, and deploy a client profile with an empty Trusted Servers list, authentication will fail.

Step 1 After clicking **Next** in the Station Policy window, the Trusted Server Policy Window opens.

Step 2 Click **Add Server Rule** to open the Trusted Server Dialog.

Step 3 Enter a name in the **Rule name** field. This can be any user-friendly name; it is not used for validation.

Step 4 In the **Validation method field**, select **Certificate**. This implies that the host will initially provision the PAC using a server certificate. (The PAC validation method is not supported.)

Note The client, when initially accepting the provisioned PAC, will autonomously add the A-ID to the deployed Trusted Server list - transferring the “trust” in the server certificate to the server's A-ID.

Step 5 Initially the “Match ANY Certificate Validation Rules” list will be empty. You will need to add a rule by configuring the fields in the Match ANY Certificate Rules area.

a. 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 Domain** - searches the DNSName field attribute.
- **Subject Common Name** - searches the following certificate fields (attributes):
  - Subject: CN (Common Name)

    Note If multiple Common Names are specified, only the first one listed in the certificate is used.

  - Subject: DN (Domain Name) - a composite of a set of DC (Domain Component) attributes

b. 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.

c. Enter the text: acceptable formats are:

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

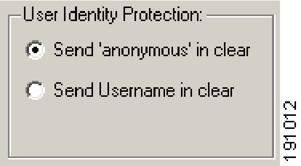
Step 6 Click **OK**, to return to the Trusted Server Definition Dialog.

Step 7 Click **Next** to continue creating a deployment package.

User Identity Protection Area

The **User Identity Protection** area defines what information is sent during an EAP Identity request.

Figure 9-11 User Identity Protection



User Identity Protection:

● Send 'anonymous' in clear

○ Send Username in clear

Radio Button	Description
Send 'anonymous' in clear	Select the "Send 'anonymous' in clear" option to send anonymous as the EAP-FAST outer identity. In this mode the host sends *anonymous@Domain* for the identity. This is the default setting.
Send Username in clear	Select the Use Username as identity option to send the *UserName* as the EAP-FAST outer identity. This could be used for login attempt auditing on the switch. In this mode, when also using "Use Single Sign-on for password credentials" for User Credentials, the client sends *UserName@Domain* for the identity. This information is sent in the clear. If not using "Single Sign-on for password credentials" for User Credentials, the client sends *UserName* for the identity. This information is also sent in the clear. ⚠ **Caution** This radio button choice is not compatible with ACS 4.0 installations or earlier. Support for this feature will be available in a future release of ACS.

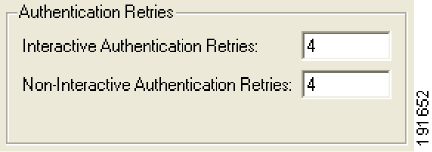
Note This setting does not affect the credentials sent during user and machine authentication. If user credentials are required for authentication ***UserName@Domain*** will be sent.

Note This authentication choice also needs to be configured on the ACS.

Authentication Retries Wired / Ethernet Settings

Some network access devices have the ability to open a port but switch the user into a special vlan after a failed connection attempt. In order to support these access devices, the client provides the administrator with the capability of adjusting the number of connection retries before disconnecting, allowing the access device to make intelligent decisions based on multiple authentication failures.

Figure 9-12 Authentication Retries Wired / Ethernet Settings Area



Authentication Retries

Interactive Authentication Retries: 4

Non-Interactive Authentication Retries: 4

Interactive Authentication Retries: Applies for cases in which a user intervention might correct the failed authentication attempt. In general, this applies to connection attempts involving user text entry or user list selection associated with an “Enter Your Credentials” pop-up window, to allow for user corrections. The default setting is four attempts.

Non-interactive Authentication Retries: Applies for cases in which a user intervention would not help to correct the failed authentication attempt. In general, this applies to connection attempts not involving an “Enter Your Credentials” pop-up window, such as, single-sign-on, or all failures associated with a server certificate validation. The default setting is four attempts.

Note Making changes to the default settings is not recommended without a thorough understanding of the impact on connection performance and knowledge of any special needs and features of your enterprise access devices. Any changes should be comprehensively tested before general end-user deployment.

- Increasing the **Interactive Authentication Retries** count will result in more user dialog prompts.
- Increasing the **Non-Interactive Authentication Retries** count will add a delay to the machine boot/user logon connection to the Windows System in cases where network connectivity fails.

When you decide on the proper settings for these fields, the values of these fields must be at least one greater than the value of the max-attempts value for the "auth fail vlan" feature on your switch. For example, if max-attempts value for "auth fail vlan" is 3 on the switch, both values must be set to 4.

Deploying End-User 802.1x Wired Clients

Deploying the End-user 802.1x Wired Clients requires that you perform three procedures:

Step 1 Create a Deployment Package. In this step you create a deployment package based on one of these authentication strategies:

- User Authentication only
- Machine and User Authentication
- Machine Authentication only

See "Creating Deployment Packages" section on page 9-36 for these procedures.

Step 2 Installing Server Certificates on the Host. See "Installing Server Certificates on the Host" section on page 9-42.

Step 3 Installing the End-user 802.1x Wired Client and the Deployment Package on the host. See "Installing Deployment Packages on Hosts" section on page 9-43 for this procedure.

Creating Deployment Packages

This section describes creating these different authentication packages:

- Creating a User Authentication Deployment Package, page 9-36
- Create a Machine and User Authentication Deployment Package, page 9-38
- Creating a Machine Authentication Only Deployment Package, page 9-40

Creating a User Authentication Deployment Package

If you want to provide network access only after a user has logged on to a machine, authenticate user credentials only.

Step 1 Open Cisco Trust Agent 802.1x Wired Client.

Step 2 From the Administration menu, click **Create Deployment Package**.

Step 3 At the Welcome window, click **Start**. The Station Policy window opens.

Step 4 In the Automatic Behavior area at the bottom of the window, uncheck the **Automatically establish machine connection** check box. See the "Automatically Establishing Machine Connection" section on page 9-27 for more information on this checkbox.

Step 5 In the User Credentials area, select either of these radio buttons:

- **Use Single Sign-on for password credentials**. This option passes the username and password from the Windows logon to the ACS.
- **Request password when needed**. This option prompts users for their username and password when they are trying to connect to the network. This username and password may be different from the Windows logon information. This value is configured in ACS.

See the "User Credentials Area" section on page 9-27, for more information on these radio buttons.

Step 6 In the User Identity Protection area, select the "Send 'anonymous' in clear radio button. See the "User Identity Protection Area" section on page 9-32 for more information about the radio buttons in this area.

Step 7 (Optional) In the Allow unprotected Client Cert area, check **User Auth (Logon-time)** if you want to use a client certificate during Phase 1 of FAST PAC provisioning. See the "Allow Unprotected Client Cert Area" section on page 9-28 for more information about this radio button.

Step 8 (Optional) In the Authentication Retries Wired/Ethernet Settings area, specify the number of interactive or non-interactive authentication retries. See the "Authentication Retries Wired / Ethernet Settings" section on page 9-34 for more information about these fields.

Step 9 (Optional) In the Trusted Server Validation area, select one of these options:

- Always validate servers
- Never Validate servers

See the "Trusted Server Validation Area" section on page 9-29 for more information about these radio buttons.

Step 10 Click **Next**. The Trusted Server Policy window opens.

Step 11 Add a trusted server rule, if it is appropriate:

- If you chose to Always validate servers in the Trusted Server Validation area, add a server rule at this time. See the "Deploying Trusted Servers" section on page 9-31 for this procedure.
- If you chose Never Validate servers in the Trusted Server Validation area, click **Next**.

Step 12 In the Save Package window, you can accept the default location in which to save the new deployment package .xml files or click **Browse** to store the files in a new or existing directory.

Step 13 In the Deployment Package filename field, specify a filename. This name is incorporated in all the authentication profile files. For the sake of an example, we will name the file "common-auth".

Step 14 Click **Save**. The deployment package is created and the file names and locations are listed in the Deployment Complete window. For the sake of this example, these were the files that were created:

- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-policy.xml**
- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-networks.xml**

- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-credentials.xml**

Step 15 Click **Close**.

Step 16 Install the authentication server certificates on the host using the "Installing Server Certificates on the Host" section on page 9-42.

Create a Machine and User Authentication Deployment Package

This configuration provides network access only after both the user and the machine credentials have been authenticated.

Step 1 Open the Cisco Trust Agent 802.1x Wired Client.

Step 2 From the Administration menu, click **Create Deployment Package**.

Step 3 At the Welcome window, click **Start**. The Station Policy window opens.

Step 4 In the Automatic Behavior area at the bottom of the window, uncheck the **Automatically establish machine connection** check box. See the "Automatically Establishing Machine Connection" section on page 9-27 for more information on this checkbox.

Step 5 In the User Credentials area, select either of these radio buttons:

- **Use Single Sign-on for password credentials**. This option passes the username and password from the Windows logon to the ACS.
- **Request password when needed**. This option prompts users for their username and password when they are trying to connect to the network. This username and password may be different from the Windows logon information. This value is configured in ACS.

See the "User Credentials Area" section on page 9-27, for more information on these radio buttons.

Step 6 In the User Identity Protection area, select the **Send 'anonymous' in clear** radio button. See the "User Identity Protection Area" section on page 9-32 for more information about the radio buttons in this area.

Step 7 (Optional) In the Use Client Certificate During area, check **User Authentication** if you want to use a client certificate during Phase 1 of FAST PAC provisioning. See "Allow Unprotected Client Cert Area" section on page 9-28 for more information.

Step 8 (Optional) In the Authentication Retries Wired / Ethernet Settings area, specify the number of interactive or non-interactive authentication retries. See the "Authentication Retries Wired / Ethernet Settings" section on page 9-34 for more information.

Step 9 (Optional) In the Trusted Server Validation area, select one of these options:

- Always validate servers
- Never Validate servers

See, "Trusted Server Validation Area" section on page 9-29 for more information.

Step 10 Click **Next**. The Trusted Server Policy window opens.

Step 11 Add a trusted server rule, if it is appropriate:

- If you chose to Always validate servers in the Trusted Server Validation area, Add a server rule at this time. See "Deploying Trusted Servers" section on page 9-31 for this procedure.
- If you chose Never Validate servers in the Trusted Server Validation area, click **Next**.

Step 12 In the Save Package window, you can accept the default location in which to save the new deployment package .xml files or click **Browse** to store the files in a new or existing directory.

Step 13 In the Deployment Package filename field, specify a filename. This name is incorporated in all the connection context files. For the sake of an example, we will name the file "common-auth".

Step 14 Click **Save**. The deployment package is created and the file names and locations are listed in the Deployment Complete window. For the sake of this example, these were the files that were created:

- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-policy.xml**
- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-networks.xml**
- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-credentials.xml**

Note The credentials.xml file is created but it is only meaningful when it is used in a wireless network environment. The CTA 802.1x Wired Client is only used in wired network environments.

Step 15 Click **Close**.

Step 16 Install the authentication server certificates on the host using the "Installing Server Certificates on the Host" section on page 9-42.

Creating a Machine Authentication Only Deployment Package

This procedure creates a policy for machine authentication only. For machine authentication, the machine credentials are substituted for user credentials. The machine connection to the network may be made automatically or manually.

During an automatic machine authentication, the host boots and the machine credentials are immediately submitted for authentication.

During a manual machine authentication, the host boots but its machine credentials are not submitted for authentication. Machine credentials are sent after the user logs on.

Step 1 Open the Cisco Trust Agent 802.1x Wired Client.

Step 2 From the Administration menu, click **Create Deployment Package**.

Step 3 At the Welcome window, click **Start**. The Station Policy window opens.

Step 4 In the User Credentials area, select **Use Machine credentials for User Connections** radio button. See "User Credentials Area" section on page 9-27 for more information.

Step 5 Make the machine connection automatic or manual:

- To establish the machine connection upon boot, **check** the **Automatically establish machine connection** check box in the Automatic Behavior area at the bottom of the window.
- To establish the machine connection after GINA login, **uncheck** the **Automatically establish machine connection** check box in the Automatic Behavior area at the bottom of the window.

Step 6 In the User Identity Protection area, select the **Send 'anonymous' in clear** radio button. See the "User Identity Protection Area" section on page 9-32 for more information about the radio buttons in this area.

Step 7 (Optional) In the Use Client Certificate During area, check **User Auth (Logon-time)** if you want to use a client certificate during Phase 1 of FAST PAC provisioning. See "Allow Unprotected Client Cert Area" section on page 9-28 for more information.

Step 8 (Optional) In the Authentication Retries Wired / Ethernet Settings area, specify the number of interactive or non-interactive authentication retries. See the "Authentication Retries Wired / Ethernet Settings" section on page 9-34 for more information.

Step 9 (Optional) In the Trusted Server Validation area, select one of these options:

- Always validate servers
- Never Validate servers

See, "Trusted Server Validation Area" section on page 9-29 for more information.

Step 10 Click **Next**. The Trusted Server Policy window opens.

Step 11 Add a trusted server rule, if it is appropriate:

- If you chose to Always validate servers in the Trusted Server Validation area, Add a server rule at this time. See "Deploying Trusted Servers" section on page 9-31 for this procedure.
- If you chose Never Validate servers in the Trusted Server Validation area, click Next.

Step 12 In the Save Package window, you can accept the default location in which to save the new deployment package .xml files or click **Browse** to store the files in a new or existing directory.

Step 13 In the Deployment Package filename field, specify a filename. This name is incorporated in all the connection context files. For the sake of an example, we will name the file "common-auth".

Step 14 Click **Save**. The deployment package is created and the file names and locations are listed in the Deployment Complete window. For the sake of this example, these were the files that were created:

- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-policy.xml**

- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-networks.xml**
- C:\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\ **common-auth-credentials.xml**

Note The credentials.xml file is created but it is only meaningful when it is used in a wireless network environment. The CTA 802.1x Wired Client is only used in wired network environments.

Step 15 Click **Close**.

Step 16 Install the authentication server certificates on the host using the "Installing Server Certificates on the Host" section on page 9-42.

Installing Server Certificates on the Host

Install server certificates on the host in order to support machine connections or user connections.

After the server certificate have been installed on the host, continue with the "Installing Deployment Packages on Hosts" section on page 9-43.

Machine Connection Support

If the 802.1x Wired Client for the end-user is using the Server Certificate method of initially provisioning the machine PAC, then perform these two steps:

Step 1 The CA certificate used to trust the server certificate must be deployed and placed in the proper Windows Certificate Store (Local Computer-Trusted Root Store).

Step 2 The end-user 802.1x Wired Client should be configured to be using the Microsoft Active Directory method of providing the machine certificate.

Note If a machine certificate is not supported, then no initial machine connection will be made and the machine PAC provisioning will wait until the initial user logon connection is made.

User Connection Support

If the end-user client is using the Server Certificate method of initially provisioning the end-user's PAC, then the CA certificate used to trust the server certificate must be deployed and placed in the proper Windows Certificate Store (User-Trusted Root Store).

Installing Deployment Packages on Hosts

Before you begin, test the deployment package before distributing it to the end-users. It is recommended to load the deployment package on an alternate machine so as to maintain the administrator version of the client on the current machine.

Note If you must test on the same machine, be sure to save the administrator configuration files, so that you can reconstruct the administrator version after the test.

Step 1 Install Cisco Trust Agent with the 802.1x Wired Client on the host that you want to use this connection context. Do not restart the host when prompted.

Step 2 Copy the deployment package files you created to the host.

Step 3 Copy the policy file to the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies** directory. (In our example the policy file is named common-auth-policy.xml.)

Step 4 Copy the networks file to the **Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\networks** directory. (In our example the network file is named common-auth-networks.xml.)

Step 5 The credentials.xml file is not required for the CTA 802.1x Wired Client.

Step 6 Reboot the host.

Changing Deployment Packages on Hosts

Changing the deployment package on an End-user 802.1x Wired Clients is very similar to deploying the original package.

Step 1 Create a new deployment package. Create a deployment package based on **one** of these authentication strategies:

- Creating a User Authentication Deployment Package, page 9-36
- Create a Machine and User Authentication Deployment Package, page 9-38
- Creating a Machine Authentication Only Deployment Package, page 9-40

Step 2 Follow the Replacing a Deployment Package on a Host procedure.

Replacing a Deployment Package on a Host

Using this procedure you can change the way a host authenticates itself to the network.

Step 1 Open the Windows Services window and stop the Cisco Trust Agent 802.1x Wired Client.

Step 2 Delete the policy file from the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies** directory. (In our example the policy file is named common-auth-policy.xml.)

Step 3 Copy the policy file from the new deployment package to the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies** directory.

Step 4 Delete the networks file from the **Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\networks** directory. (In our example the network file is named common-auth-networks.xml.)

Step 5 Copy the networks file from the new deployment package to the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\networks** directory.

Step 6 Delete the user PAC from the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\users directory. This file is named *UserName@hostname*.xml**

Step 7 Delete the user PAC from the **\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies\users\allusers** directory. The file is named **machineSettings.xml.**

Step 8 Reboot the host or restart the Cisco Trust Agent 802.1x Wired Client in the Windows Services window.