AT&T Global Network Client

Administrator's Guide

10.7.0

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of publication. However, information is subject to change.

Microsoft Public License

The Application uses Open Source Software that is licensed under the Microsoft Public License (the "License"). You may not use this file except in compliance with the License. You may obtain a copy of the License at http://dotnetzip.codeplex.com/license. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Notice 2
Microsoft Public License 2
Overview 9
Using this Document 9
Related Documents 9
Your Network Service 10
Managed Virtual Private Network Services 10
AT&T Global Network Client Firewall 10
Lightweight Policy Enforcement 10
Authentication Types 10
AT&T Authentication Server 11
RADIUS 11
Authentication Providers 11
LDAP/Digital Certificates 11
AT&T Global Network Client Overview 12
Preparing for Installation 13
System Requirements 13
Requirements for Installation & Use 14
Installation 15
AT&T Global Network Client Installation Packages 15
Obtaining the AT&T Global Network Client 16
Distribution 16
Local Installation 16
Group Policy Distribution 16
Upgrading Previous Releases 17
Selecting Your Language Support 17
Configuration 18
The Connection Sequence 18
Advanced Configuration 20
Central Configuration 20

Profile Management 20
Login Properties 20
Profile Manager 21
Network Services 22
Servers 22
Preferences 23
Autostart 23
Post Connection Script 24
Proxy 25
Timeouts 26
Connection Features 27
Persistent Connections 27
Configuration for AT&T Services (AT&T VPN or Business Internet Services) 27
User Preference 27
Persistent Connection Mode 28
AutoReconnect 28
Prevent Multi-Homing 29
Configuration 29
User Preference 29
AutoConnect Feature 29
Software Updates 31
User Permissions 31
Hotspot Directory Updates 31
Automated Check for Updates 31
Manual Check for Updates 32
Uninstall 33
Local Uninstall 33
Uninstall 33
Remove Warning 36
Remote Uninstall 36

Command Line Uninstall 36
Customizations 37
Advanced Customizations Using Windows Installer 37
AT&T Global Network Client Features 37
Public Properties 39
Shortcuts 44
Common Windows Installer Properties 44
Using the Command Line to Customize Installation 44
Example Command Line Customizations 45
Creating a Windows Installer Transform 45
Tools to Create a Transform 46
Common Changes Customized via a Transform 46
Things That Must Be Avoided 47
Recommended Actions via a Transform 47
Adding Files 47
Updating Files 48
Customizing Your Password Rules 48
Changing the Installation Directory 48
Changing the Application Name 48
Making the Transform Apply To Future Versions 48
Customization Using a config.xml File 49
Global Customizations (FastPath Replacement) 49
Trusted Domain Customization 49
Trusted Domain Configuration 50
Trusted Domain Customization Limitations 50
Client Profiles Customization 50
Client Profiles Configuration File 50
Other Commonly Requested Customizations 53
Network Login Option Customizations 53
Hide Options Button 53

Use Digital Certificates 53
Password Format 54
Other Network Login Options 54
Limiting Connections Per Operating System 55
Profile Customization Limitations 55
Controlling the AT&T Global Network Client Firewall 55
Network Awareness Customization 55
Defining Networks and Corresponding Actions 57
Approved Mobile Device Customization 58
Approved Connection Type Customization 59
Secondary Method of Customizing Network Login Options 59
Customizing Default Login Options 60
Customization Services 61
SDK Prioritization 61
Accessibility Features 61
Visual Display of Screen Element in Focus 61
Keyboard Navigation 62
AT&T Lightweight Policy Enforcement 63
Asset Based Connection Prevention 63
Operating System 63
Application Monitoring 64
Types of Applications Monitored 64
Limitations 65
Lightweight Policy Enforcement Customization Examples 65
AT&T Global Network Client Firewall 70
Overview 70
Operating Modes 70
Default 71
Trusted Domains 71
User Controlled 71

Disabled 71
Firewall Settings Window 71
Managed VPN Access Control Lists 72
Limitations 73
AT&T VPN Services 74
Using Managed IPSec VPN Services 74
Local Resources 74
Sharing Local Resources 74
Registering VPN IP Address with Dynamic DNS 74
Encryption for IPSec VPN connections 75
Co-existence with Microsoft IPSec 75
NAT Traversal 75
Configuring UDP Encapsulation 76
Cisco Passwords 76
Using Managed SSL VPN Services 76
Network Layer Solution 76
Security/Authentication 77
Configuring the AT&T Global Network Client to Establish a VPN Connection through a Proxy 77
Importing a Proxy File for SSL connections 77
Proxy.ini File 77
proxy.ini Field Information: 78
Importing the Proxy.ini file 79
Dynamically VPN Connect 79
IPv6 Support 80
IP version preference 81
IP version failover 81
Integrating with Third Party Software 83
ThinkVantage® Access Connections™ 83
WireShark® and Microsoft Network Monitor 83
Help/Customer Support 84

Support Forum 84
Contact AT&T 84
Frequently Asked Administration Topics 85
Using Digital Certificates for Authentication 85
Troubleshooting Installation 85
Appendix A: Central Configuration 86
Central Configuration Values 86
AT&T Administration Server Client Configuration Values 87
Additional Service Information 94
Appendix B: Third-Party Firewall Support 95
Network Firewalls 95
SMX List 96
Personal/Client Firewalls 96
Hotspot Directory and Dynamic Customization Updates 97
SLA data collection 97
Appendix C: Using the Command Line Program 98
AT&T Client 98
Parameters: 98
AT&T Global Network Client Firewall 102
Index 103

Overview

The AT&T Global Network Client is a program that enables your Windows computer to easily connect to the Internet or your company's private network.

Using this Document

This document is intended for IT professionals that are deploying the AT&T Global Network Client to their employees, or IT professionals that wish to gain a better understanding of the administration of AT&T remote access services.

The reader is assumed to be an IT administrator with a technical knowledge of Microsoft Windows® and computer networking and is referred to in this document as the customer account administrator.

Related Documents

AT&T Global Network Client User's Guide

http://www.corp.att.com/agnc/windows/documentation/usersguide.pdf

AT&T Domain Login Guide

http://www.corp.att.com/agnc/windows/documentation/domainlogonguide.pdf

Your Network Service

AT&T enterprise mobility consists of a portfolio of managed services for remote access, VPN, and endpoint security. AT&T provides the service and the support for your managed network service; however, account administration and user configuration is controlled by you, the Customer Account Administrator, for all users associated with your account. AT&T provides you with central tools to manage and configure your individual account and user experience, storing the settings in the AT&T administration server. The AT&T Global Network Client interfaces with the AT&T administration server to receive configuration information.

Your administration of the AT&T Global Network Client requires basic knowledge of the features of your network service.

Managed Virtual Private Network Services

Managed Virtual Private Network (VPN) Services provide a remote computer with connectivity to a private Intranet.

AT&T IP-VPN Services use the AT&T Global Network Client to perform all aspects of the network service, including establishing and maintaining the VPN connection.

AT&T Global Network Client Firewall

The AT&T Global Network Client Firewall is a component of the AT&T Global Network Client which provides basic firewall capabilities. The AT&T Global Network Client Firewall uses the Windows firewall engine for the firewall and fencing.

Lightweight Policy Enforcement

AT&T Lightweight Policy Enforcement (LPE) is an optional service which performs basic application monitoring and can be customized by the Customer Account Administrator at installation time.

Authentication Types

AT&T allows each customer to select the type of authentication engine implemented for users of their account.

AT&T Authentication Server

Many customers allow AT&T to manage their user authentication via the AT&T authentication server (a.k.a. AT&T Service Manager). You, as the Customer Account Administrator, can define and administer the users within your account using central tools.

RADIUS

It may be possible for the AT&T authentication server to interface with your RADIUS server for user authentication. User accounts are defined in the AT&T authentication server for administration and all authentication requests proxy to your RADIUS server via the AT&T authentication server for validation.

Authentication Providers

Several authentication options are supported with the AT&T Global Network Client. Both hardware token as well as software token solutions are supported. RSA SecurID®, RSA SoftToken, SafeWord, CryptoCard, Defender, and other multi-factor authentications are all supported via RADIUS. Most multi-factor solutions should be supported. Please open a change request or contact the AT&T account team if you find a solution that is not working as expected.

LDAP/Digital Certificates

AT&T offers the use of Entrust and Microsoft digital certificates to authenticate users for Internet and AT&T IP-VPN services. **Use of certificates may require custom software development at a cost to our customers. Contact your AT&T account team to engage product management for assistance.**

AT&T Global Network Client Overview

The AT&T Global Network Client is software that allows Windows computers to easily access the Internet and your company's private network from many locations around the world. It provides a simple, powerful interface designed to automatically detect and connect over mobile, Wi-Fi, and broadband networks. It also is designed to provide security policy enforcement, offline hotspot and directory browsing, detailed connection history, and in-depth diagnostic logging.

The AT&T Global Network Client is available in two installation packages. The AT&T Global Network Client installation package includes all required and optional features and can be used for the majority of installations. The AT&T Global Network Client for Export installation package does not contain VPN encryption software for use in countries which restrict the import of such technology. More information about the AT&T Global Network Client installation packages can be found in the Installation Chapter of this document.

As we request and require customers to upgrade AGN Client versions 10.3 and older they may experience problems with connectivity in China with the more recent AGN Client versions. Recent AGN Client versions, such as 10.7, are using the TLS protocol for authentication. AGN Client connections originating from within China may be more likely to have their connection attempt blocked by the Chinese firewall due to use of TLS. There is no immediate solution to work around this situation, nor is it predictable as to when users may experience trouble.

Preparing for Installation

System Requirements

The AT&T Global Network Client and its components are supported* on the following operating systems and hardware. (The AT&T Global Network Client may function properly on other operating systems and lesser hardware, but it is not formally tested or supported):

Operating System	Software	Hardware
Windows 8.1®	Windows Installer 3.5 or later	IBM PC or 100% compatible
Windows® 10	.Net Framework 4.6 or later	1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
	MSXML 3 or 4	2 MB RAM or higher recommended
		250 MB free disk space
		Wi-Fi connection: wireless adapter that adheres to NDIS 5 specifications and tested by AT&T
		Mobile connection: PC Mobility Card

Administrator Rights

Required: The user must have administrator rights when the installation is executed.

Requirements for Installation & Use

Before starting the AT&T Global Network Client installation and setup, verify you have the information required in the following checklist. If you are missing any information, please contact your Customer Account Administrator.

- Administrator rights to install or upgrade
- Your Windows install media (CD or installed MSI files) may be required.
- Hardware/Equipment necessary to establish basic network connectivity. For example, an existing Internet connection via cable or DSL, Wi-Fi, or Mobile modem/card.

For connections which require credentials:

- Account
- User ID
- Password, passcode, or PIN and token

Installation

The AT&T Global Network Client installation is packaged using Microsoft Windows Installer and InstallShield® 2015 SP1[1] and can be installed and updated locally. Terminology specific to Windows Installer is used in this document and a basic knowledge of Windows Installer is useful when administrating the installation of the AT&T Global Network Client package. More information about Windows Installer can be found by consulting the "Roadmap to Windows Installer Documentation" at http://msdn.microsoft.com/en-us/library/aa371366(VS.85).aspx

AT&T Global Network Client Installation Packages

The AT&T Global Network Client is available in two installation packages. The AT&T Global Network Client installation package should be used for the majority of installations. The AT&T Global Network Client for Export installation package is available for use in countries that prohibit the import of VPN encryption technology.

An overview of the installation package to be used with each service is shown in the table below.

	AT&T Global Network Client	AT&T Global Network Client for Export
Remote Access Services	✓	✓
AT&T VPN Services	✓	
AT&T Global Network Client Firewall	✓	✓
Lightweight Policy Enforcement	✓	✓

Figure 1: AT&T Global Network Client Installation Packages

[1] Flexera Software, AdminStudio, FlexNet Connect, InstallShield, and InstallShield Professional are registered trademarks or trademarks of Flexera Software LLC in the United States of America and/or other countries.

Obtaining the AT&T Global Network Client

The AT&T Global Network Client is distributed through a public Internet download. If you have previously installed from a private FTP/Intranet download location you may be using a custom version of the AT&T Client; contact your Customer Account Administrator to request an updated version.

Users of Custom Versions: Do not manually download new releases. Contact your AT&T Account Representative to request an updated customversion.

Two different installation packages are available for download. The single file executable (.exe) installation package is used for most user based installations. The single file executable has the benefit of detecting previous AT&T Global Network Client installations and automatically performing the correct upgrade. The compressed single file MSI (.msi) installation package is useful if you wish to use a software distribution technology to push software updates out to your users.

Package	Downloads
AT&T Global Network Client	http://www.corp.att.com/agnc/windows/agnc.exe http://www.corp.att.com/agnc/windows/agnc.msi
AT&T Global Network Client for Export	http://www.corp.att.com/agnc/windows/agnc_export.exe http://www.corp.att.com/agnc/windows/agnc_export.msi

Figure 2: Download Location Table

Distribution

The AT&T Global Network Client is distributed for local installation. Customization and pre-installation configuration are supported. Microsoft Windows Administrator rights are required when the AT&T Global Network Client is installed.

Local Installation

A local installation is initiated by the user on the target machine by executing one of the AT&T Global Network Client installation packages.

Administrator Rights Required:

The user must have Microsoft Windows Administrator rights/privileges when the installation is executed.

Group Policy Distribution

When installing the AT&T Global Network Client using an Active Directory Group Policy you must define a new object in your Group Policy manager and define the Software Installation Package with the

full network path to the installation files, not the local path to the files. The installation files must be copied to the local machine to do the installation.

Upgrading Previous Releases

If you already have the AT&T Global Network Client (version 7 or later) installed on your workstation, the installation can perform an upgrade to version 9.x. During the upgrade, the previous AT&T Global Network Client will be uninstalled, the workstation may be rebooted, and then the new AT&T Global Network Client will be installed. Administrators can suppress the reboot after the previous AT&T Global Network Client has been uninstalled by setting the installation property "SUPPRESS_UPGRADE_REBOOT=1" for the installation package but this feature is not recommended and will require detailed testing on your part prior to selection. For more information, refer to the chapter titledAdvanced Customizations Using Windows Installer."

As part of the upgrade process, the user's data and AT&T Global Network Client customizations will be preserved whenever possible. This is accomplished by renaming, then restoring the user's data directory and the custom data directory. Installation package customizations, such as a custom desktop icon, will not be preserved. More information about customizations can be found in the Customizations chapter of this guide.

Selecting Your Language Support

The AT&T Global Network Client automatically installs support for running in English, French, German, and Spanish. If the installation is being performed on a Japanese version of the operating system, the installation will also install support for running in Japanese[2].

Installing the files necessary to support English is required. Support for other languages is configurable using the Custom installation path.

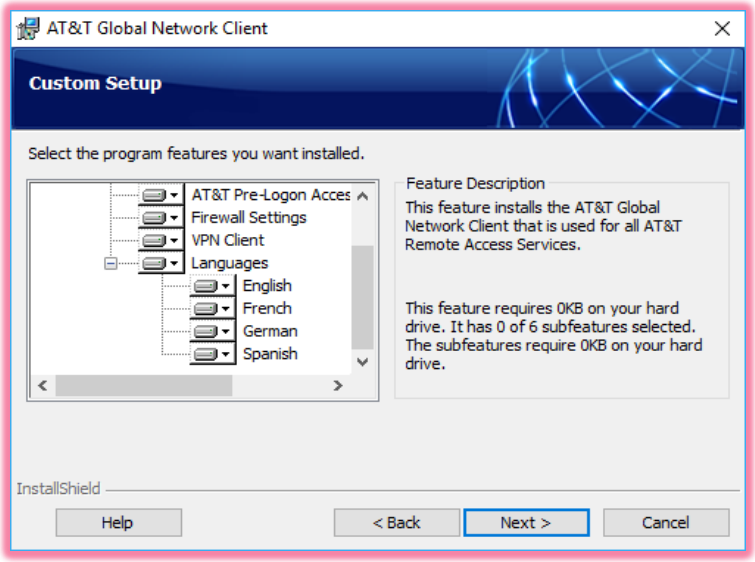


Figure 3: Select Your Language

The default language for the installation dialogs is English. To display the installation dialogs in French, German, Japanese or Spanish, or to automatically configure the languages installed for use by the AT&T Global Network Client, an installation Transform can be used. For more information on customizing the AT&T Global Network Client installation program, see the section titled Advanced Customizations Using Windows Installer

[2] Japanese is only supported if installed on a Japanese version of the Microsoft Windows Operating System.

Configuration

Most users are able to establish a connection with no manual configuration prior to their first connection attempt, benefitting from the AT&T Global Network centralized administration and the AT&T Global Network Client automatic connection feature.

AT&T Global Network Client basic configuration is achieved through automatic prompting; advanced configuration is performed using central configuration settings or manually using the **Login Properties**.

The Connection Sequence

The AT&T Global Network Client attempts to connect using each of the available connectivity methods in the order they are shown on the main window.

Figure 4: Connection Sequence

If a connectivity type is unavailable, the panel for that connectivity type will be disabled and will appear grayed out.

Figure 5: Connection Panel with Unavailable Connection Methods

If you would prefer to select a specific connectivity method to use for the connection attempt, click on the smaller green **Connect** button beneath the method desired, e.g. Wi-Fi.

Figure 6: Network Login Window

Once entered, your Account and User ID will automatically be stored for future connections. Your Password will be stored only if you click the checkbox next to Save Password. Customer Account Administrators can customize the AT&T Global Network Client so the Save Password option is not available. Refer to the chapter on Customizations on page 37 of this guide for additional information on hiding the **Save Password** option. Click **change…** to change your password. Click **OK** to continue.

Hardware Token Users: If you are using an authentication type which requires a PIN and token, enter your PIN immediately followed by the current token in the Password field.

Figure 7: Network Login Window – PIN and Token

Advanced Configuration

Central Configuration

Central Configuration Simplifies Client Administration: Review all centrally configured values prior to distribution of the AT&T Global Network Client.

The AT&T Global Network Client interfaces with the AT&T administration server to retrieve values set by you, the Customer Account Administrator.

Configuration of the values can be done by your AT&T representative or by you, via an AT&T provided administration tool. Refer to Appendix A on page 86 of this guide for additional information on central configuration.

It is recommended that you review the list of values supported by the AT&T Administration Server in Appendix A on page 86 of this guide and set values prior to the distribution of the AT&T Global Network Client to your users.

Profile Management

AT&T Global Network Client profiles store user information. A profile includes:

- Account
- User ID
- Advanced Login Properties (Service, WINS, DNS, Domain Suffix)
- Service

Most users connect with the same information a majority of the time and will only require one profile.

Users that connect with different user IDs may want to define profiles for their common user combinations to easily switch between them. AT&T Global Network Client profiles can be assigned common names to help you remember when to use them, for example, 'My Internet Profile' or 'VPN Servers – Germany'.

Login Properties

To access **Login Properties** click the **Settings** Menu > **Login properties** on the main window of the AT&T Global Network Client.

The AT&T Global Network Client - **Login Properties** window allows you to configure the settings and properties for your current connection. It is recommended you use the default values and values defined in the AT&T administration server.

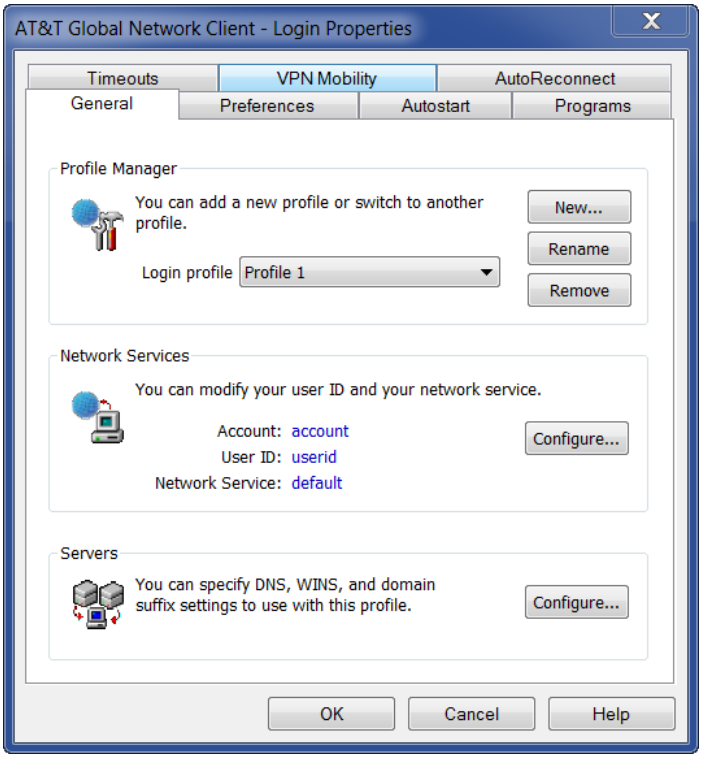


Figure 8: Login Properties Window

Profile Manager

Use the drop down box to activate an existing profile. Click **New…** to create a new profile. Click **Rename** to rename a profile. Click **Remove** to delete a profile.

Network Services

Click **Configure…** to change the Account, User ID, or Network Service. Your default network service is the service defined in the AT&T administration server for your specified Account and User ID. If you override the network service in the AT&T Global Network Client, you must be authorized for the new service in the AT&T administration server for a successful connection.

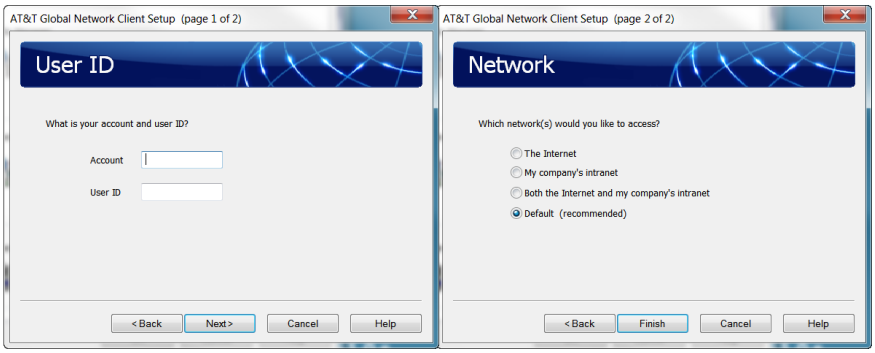


Figure 9: Configure Network Services Screens

Servers

DNS, **WINS**, and **Domain Suffix** configuration information is normally stored in the AT&T administration server. The AT&T Global Network Client automatically retrieves the values and updates the device to use the supplied values throughout the connection. Click **Configure…** to to verify or define your server information.

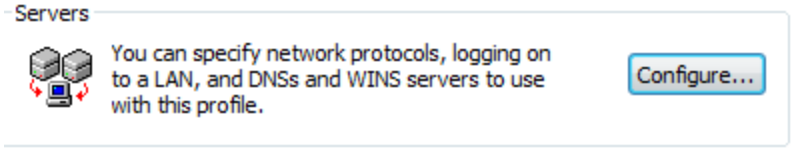


Figure 10: Servers Configure Button

To override the values defined in the AT&T administration server select **Use the following manual settings** and enter the corresponding values.

For **WINS** and **Domain Suffix** you also have the ability to select **Do not update** and the AT&T Global Network Client will not alter the specified settings when connected**.**

Preferences

Preferences define the settings for your connection. Preferences are organized by AT&T Global Network Client Profile. For more information about profiles see Profile Management in this guide.

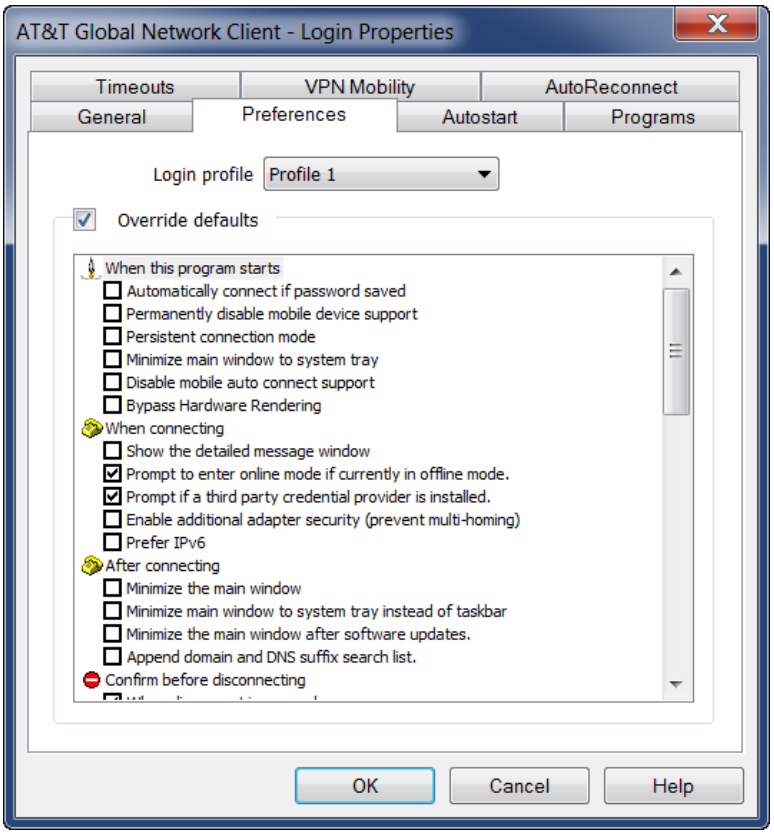


Figure 11: Login Properties - Preferences Window

Autostart

Autostart allows you to define programs to automatically launch at any of the following times:

- Before Connecting
- After Connecting
- Before Disconnecting
- After Disconnecting

Autostart settings are organized by AT&T Global Network Client Profile. For more information about profiles see Profile Management earlier in this chapter of this guide.

Click the checkbox next to **Override defaults** to change any of the settings.

Click the **Add…**, **Change…**, and **Remove** buttons to configure the program information. Click on the arrow buttons to move a program up and down in the launch order.

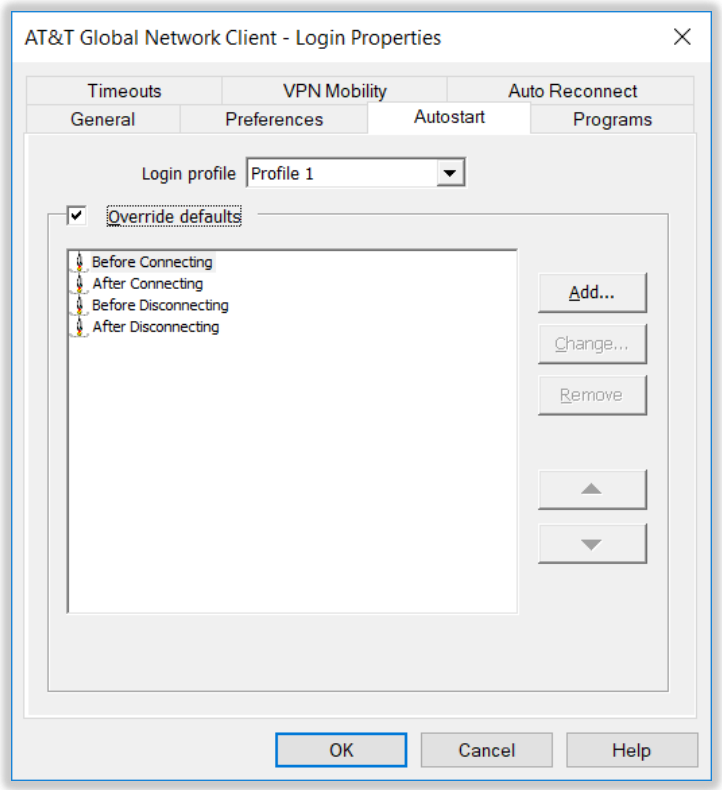


Figure 12: Login Properties - Autostart Window

Post Connection Script

In addition to starting the programs configured in the Autostart Preferences, the AT&T Global Network Client has been designed to automatically run a custom VBScript after connecting if provided by the Customer Account Administrator. The application will run a VBScript file named *PostConnectScript.vbs* if it is present in the directory in which the AT&T Global Network Client is installed. The system administrator may have to give execute permissions to this file. By having a script file (PostConnectScript.vbs), you have the flexibility to do a variety of common post connection tasks such as:

- Drive Mapping
- Launch your own VPN Client
- Launch messages to the User
- Record AT&T Global Network Client usage data

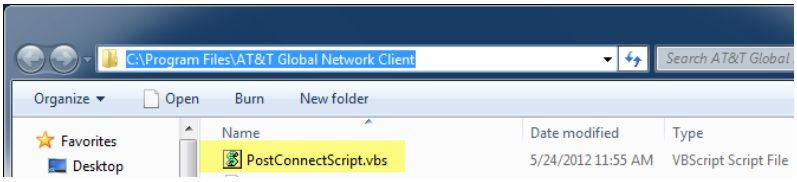


Figure 13: VBScript File Location and Name

Proxy

The **Proxy** tab allows you to specify proxy configured when connected to the network. Temporary updates are useful to eliminate or reduce the manual configuration needed before using the programs. The update values can be defined in the AT&T administration server by the Customer Account Administrator. No values are defined by default.

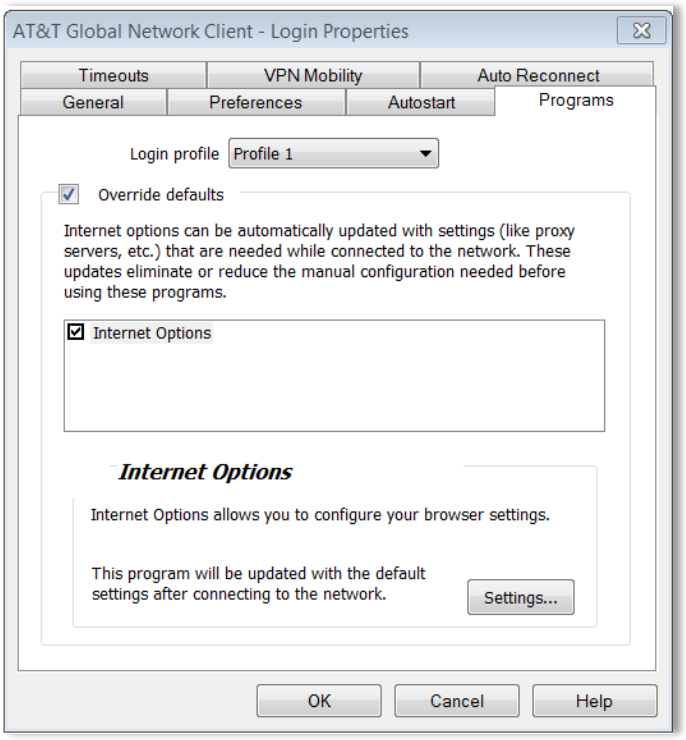


Figure 14: Login Properties - Programs Window

To prevent the use of the values from the AT&T administration server or to define new values, click **Override defaults** and select the program you wish to change. Click **Settings** to review the values and make any changes.

For example, using the Programs tab, you can remove Microsoft Internet Explorer proxy settings while connected by clicking **Override Defaults**, selecting **Internet Options**, clicking **Settings**, clicking to highlight **Auto-Proxy URL**, clicking **Manually update to**, and leaving the **Auto Proxy URL to use** field blank.

Timeouts

The AT&T Global Network Client supports two variations of **Timeouts** which can be configured by clicking **Override defaults**.

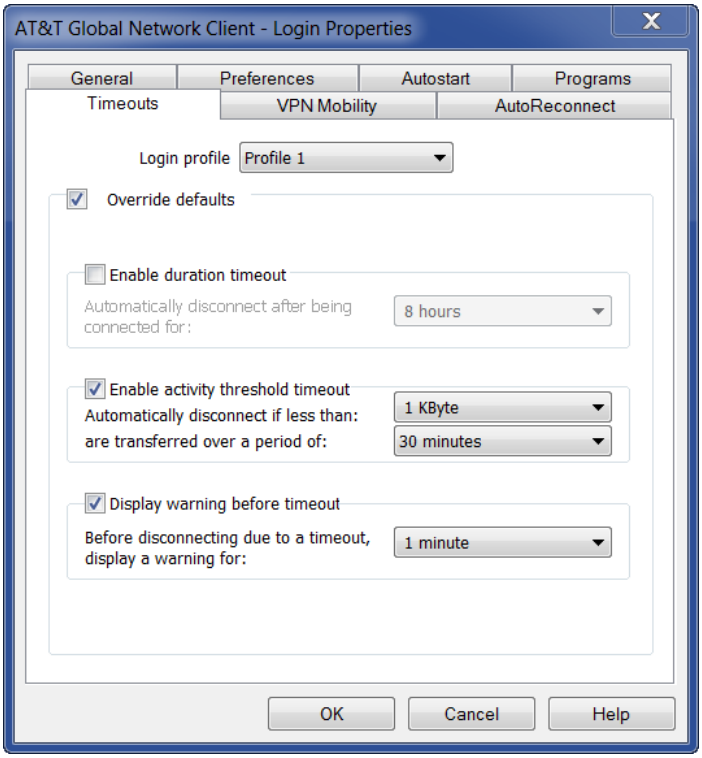


Figure 15: Login Properties - Timeouts Window

Connection Features

The AT&T Global Network Client accommodates common transitions in network connectivity when users roam between networks or locations.

Persistent Connections

When enabled, the Persistent Connections feature will automatically connect or reconnect the AT&T Global Network Client with little or no user interaction. Persistent Connections can be used with all AT&T services. For AT&T services, it must be configured both in the AT&T Global Network Client and the AT&T administration server.

One example of the Persistent Connection advantage is a user with an active AT&T Global Network Client connection whose machine enters hibernation state, automatically disconnecting the AT&T Global Network Client connection. When the user returns and resumes their work, the AT&T Global Network Client enabled with Persistent Connections is designed to automatically initiate a connection attempt to establish connectivity, without action from the user. If the **Save Password** option is enabled, no user interaction is required to establish the new connection.

Persistent Connections does not maintain the current connection; when enabled, a new connection is established when necessary.

Configuration for AT&T Services (AT&T VPN or Business Internet Services)

The Persistent Connections feature requires:

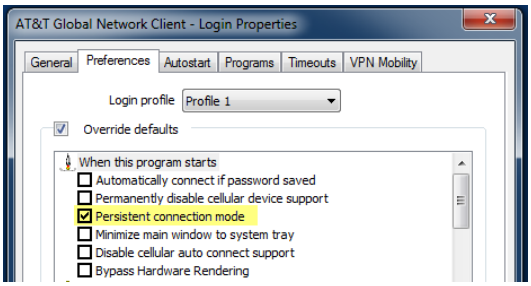
- The **Persistent Connection** option must be enabled in the AT&T administration server. See Appendix A Central Configuration for additional information.
- The "Persistent connection mode" must be checked in the Login Properties of the AT&T Global Network Client.

User Preference

The user can be given the option to disable the use of Persistent Connections for one or more profiles using the **Allow Persistent Connections** property on the **Preferences** tab of the **Login Properties** dialog.

Persistent Connection Mode

When the **Persistent connection mode** property in the Login Properties dialog is disabled, a Persistent Connection will not be supported regardless of the value of the Persistent Connection Mode option in AT&T administration server.



The **Persistent connection mode** uses broadband, Wi-Fi or Mobile connections.

AutoReconnect

The AT&T Global Network Client supports connecting and reconnecting sessions for connection drops or for switching to AT&T Wi-Fi or AT&T Partner Hotspots when connected with a Mobile connection. These settings can be specified by your Customer Account Administrator in the AT&T Service Manager.

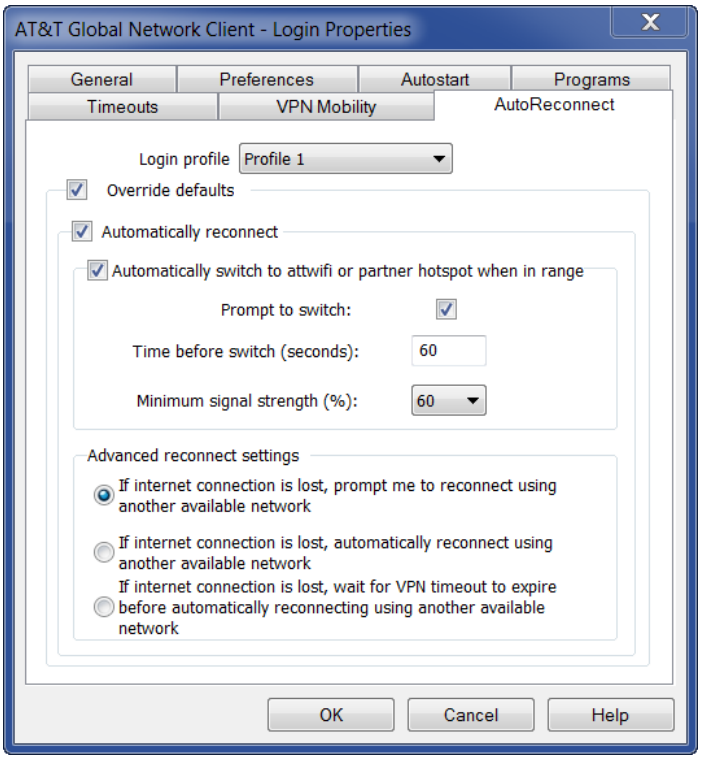


Figure 16: Login Properties – AutoReconnect Window

By setting the **Automatically reconnect** option, the existing connection will be re-established with another available connection. VPN sessions can also be re-established without having to re-enter credentials.

The **Automatically Switch to attwifi...** option will switch your connection over to one of AT&T's free Wi-Fi hotpots or partner hotspot when connected with a Mobility connection. The target hotspot must have a "strong" signal of at least 60% before the client will switch to Wi-Fi. The **Time before switch** option is a safeguard against switching to AT&T's Wi-Fi in a drive-by/drive away siutation and losing your existing session altogether. The switch can be automatic or prompted depening on the **Prompt to switch** setting.

Advanced reconnect settings allow you to control how the Autoreconnect will happen: Automatically, Prompt or after the VPN session times out.

Prevent Multi-Homing

When enabled, the Prevent Multi-Homing feature prevents the ability for other network interfaces to be made available once a connection has been established through the AT&T Global Network Client. For example, this feature prevents an Ethernet or Wi-Fi connection from becoming active while connected over a mobile connection.

Additionally, the user will not be able to install or enable any new network interfaces through the Windows Control Panel while connected.

Prevent Multi-Homing Feature insures all traffic flows through the active connection established by the AT&T Client: Use it if you have multiple connections and need additional adapter security.

Configuration

The Prevent Multi-Homing feature can be enabled by the user unless the option to do so is disabled by the Customer Account Administrator through customization. See the chapter on Customizations for more information on public properties of the AT&T Global Network Client.

User Preference

The user can be given the option to enable the Prevent Multi-Homing feature for one or more profiles using the **Enable additional adapter security (prevent multi-homing)** property on the **Preferences** tab of the **Login Properties** dialog.

AutoConnect Feature

Certain Mobile devices allow the AT&T Global Network Client to monitor the Connected state. When supported by the mobile device, if the AT&T Global Network Client recognizes a mobile connection is

active, and the default Profile is Internet, the AT&T Global Network Client will reflect the Connected state when the AT&T Global Network Client is launched.

Software Updates

The AT&T Global Network Client is designed to automatically attempt to update the following components after initial installation and on regular intervals thereafter:

- Hotspot Directory (Wi-Fi locations)
- Dynamic customizations files

Depending on your Operating System, Microsoft Windows Administrator Rights may be required for automatic software update of the AT&T Global Network Client software.

User Permissions

Hotspot Directory updates can be applied without Administrator rights. However, Dynamic customization updates require Administrator rights.

Hotspot Directory Updates

Updates to the Hotspot Directory are downloaded from http://eaccess-cdn.att.com. The update service attempts to download the current version file from the server directly, without using any proxy settings. If the attempt fails, the update service will attempt to retrieve the version file using the proxy settings stored in Microsoft Windows Internet Options. If the file was successfully retrieved using the attempt through the proxy server, future attempts will automatically be retrieved using the proxy.

The available versions are compared against the installed versions of the Hotspot Directory to determine if a newer version is available.

Automated Check for Updates

A service that periodically checks for updates to all AT&T Global Network Client software components is installed with the AT&T Global Network Client and runs in the background when your Windows machine boots up. It does not require the AT&T Global Network Client to be running.

If an update is available, the download is initiated. Downloads in the background run at low priority and only occur when the workstation is idle.

The software update service will check for new updates for all software components every 14 days. The interval between updates can be customized by the Customer Account Administrator.

If the Hotspot Directory or Dynamic customizations files are newer than the installed files, the updates will be automatically downloaded and installed without prompting the user.

Manual Check for Updates

To manually initiate a check for updates, click **Check for Updates** from the **Help** panel on the left-hand side of the main window. This triggers the update process and launches **Software Updates** window.

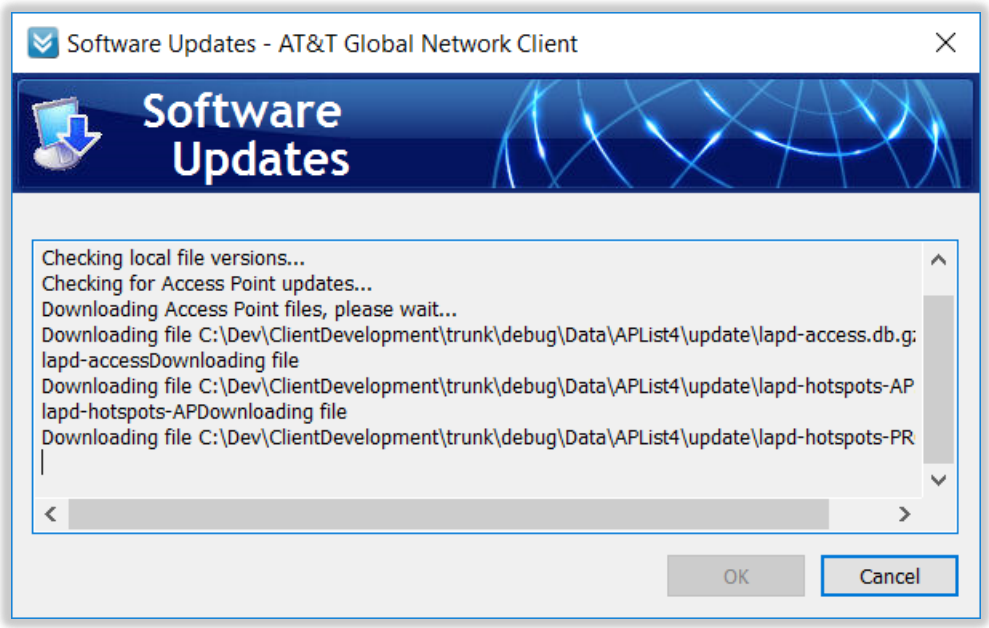


Figure 17: Software Updates Window

The **Software Updates** window shows the detailed status while the updates are being downloaded. **Cancel** button can be used to cancel the updates while updates are being downloaded. This can be useful in case download process takes too much time because of slow response from server. In that case, updates can be checked at a later time.

Uninstall

Local Uninstall

The AT&T Global Network Client is removed via the **Windows Control Panel**, **Programs and Features** option.

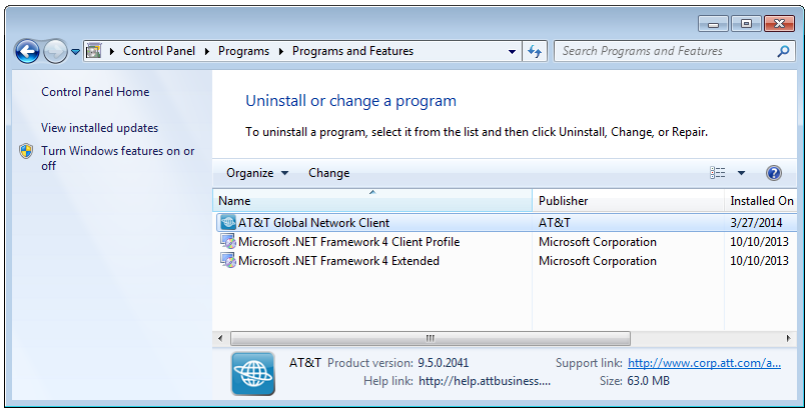


Figure 18: Programs and Features Window

Uninstall

The Programs and Features Uninstall option is not supported for the AT&T Global Network Client; to uninstall click Change and follow the directions below.

Change

Click **Change** on the **Programs and Features** window list to **Modify**, **Repair** or **Remove** the AT&T Global Network Client program

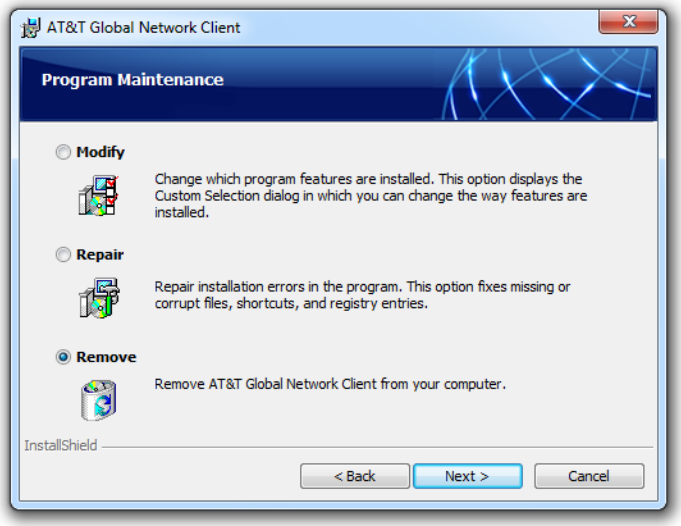


Figure 19: Modify, Repair, Remove Welcome

Click **Remove** and click **Next>** to continue.

Program files will be removed. You can also select which user settings are removed. Select **Leave all user settings on the computer. (default)** to leave user information such as account and user ID as well as profile information on the computer. Select **Remove only my user settings** to remove only the settings stored for the current user. Select **Remove settings for all users on this computer** to remove all AT&T Global Network Client user settings on the computer. Click **Next>** to continue.

Figure 20: Program Maintenance Window

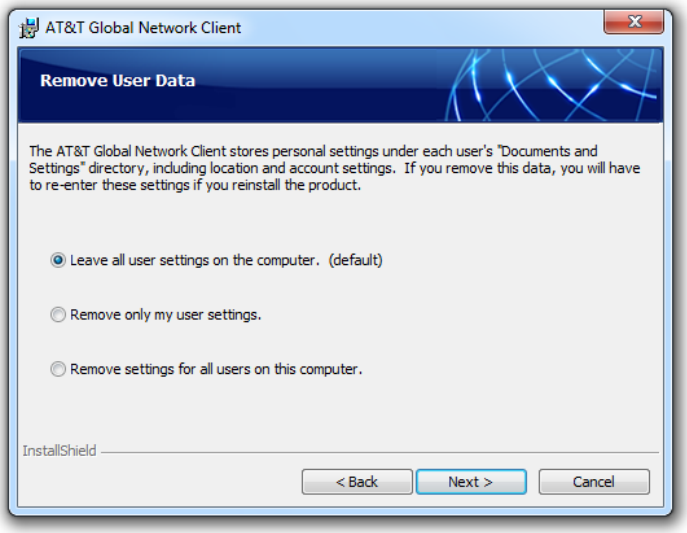


Figure 21: Remove User Data Window

Click **Remove** to continue.

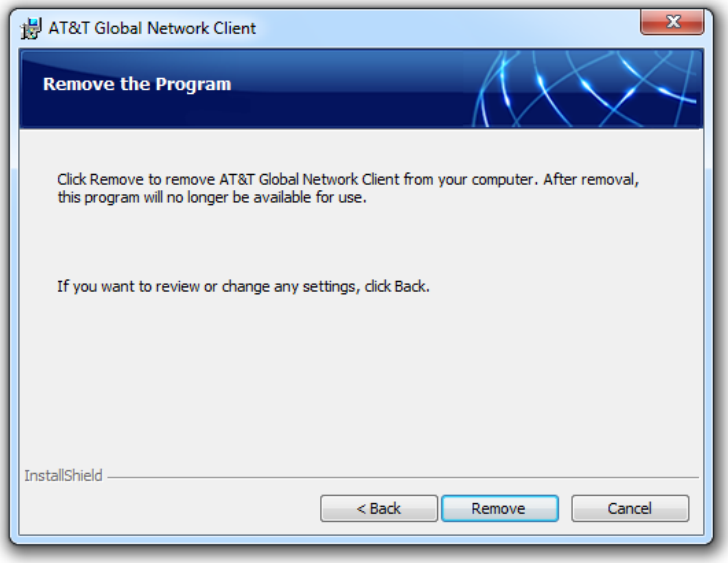


Figure 22: Remove the Program Warning

Click **Finish**.

Figure 23: Removal Complete

Reboot May Be Required: You will be prompted if you must reboot your workstation after removing the AT&T Client.

Remove Warning

The AT&T Global Network Client cannot be removed while it is running. If you attempt to remove the AT&T Global Network Client when it is running you will receive an error.

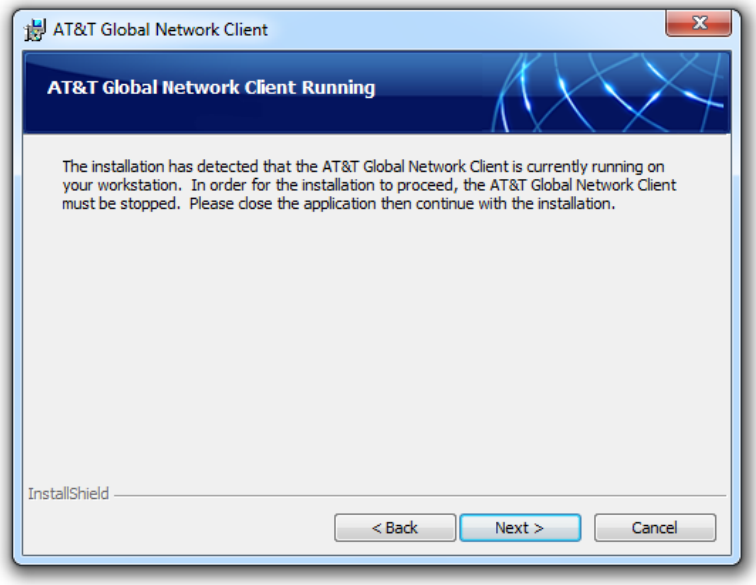


Figure 24: Client Running, Remove Warning Window

Remote Uninstall

If you used a desktop software management server to distribute the AT&T Global Network Client, you may be able to use the server to remove the package. You must initiate a reboot or have users manually restart or shutdown after the AT&T Global Network Client is removed to confirm the software is fully uninstalled.

Command Line Uninstall

Advanced users can uninstall using the command line. When using the command line, Windows Installer public properties can be used to control the type of uninstall performed. More information can be found in the Public Properties table on page 39; reference the REMOVE_USER_SETTINGS property.

Customizations

The AT&T Global Network Client can be customized by you, the Customer Account Administrators to streamline setup and define specific features for your users.

Advanced Customizations Using Windows Installer

The AT&T Global Network Client installation is packaged using Microsoft Windows Installer and InstallShield® 2015 SP1. The installation of the AT&T Global Network Client can be customized. A number of Windows Installer public properties are available to specify details of the installation. Additionally, Windows Installer provides native capabilities that can be used to specify features to be installed and to control the installation experience.

AT&T Global Network Client Features

The AT&T Global Network Client contains a number of Windows Installer Features. Each Feature defines a required or optional component of the AT&T Global Network Client. The AT&T Global Network Client Ffeatures are described below.

Feature	Description
Net_Client	Installs the AT&T Global Network Client that is used for all AT&T Services. This feature is required.
Firewall_GUI	Allows a user to turn the AT&T Global Network Client Firewall on and off while the AT&T Global Network Client is not running.
VPN_Client	Installs VPN software for connecting to your company's private network. **NOTE**: Not available in the installation package used for export
APD_NA	Hotspot Directory Database for North America
APD_EMEA	Hotspot Directory Database for Europe, Middle East and Africa
APD_SA	Hotspot Directory Database for South America

APD_AP	Hotspot Directory Database for Asia Pacific
APD_PRC	Hotspot Directory Database for People's Republic of China
PLAP	Provides the ability to connect to the network before logging onto Windows 8.1. This feature can be seen by selecting Custom Installation Path in any Edition.
LPE	Installs the Lightweight Policy Enforcement Feature and provides for the visibility of the Security Status portion of the AT&T Global Network Client Main Window.
Languages	Installs English, French, German, Japanese, and Spanish language support. Each language is a sub-feature under the Languages feature. English is required, other languages are optional.

Public Properties

The installation packages contain a number of public properties that can be set on the command line or within a transform. The properties in the table below govern some behaviors of the setup.

Important Note: Some public properties ***should not*** be used along with the CONFIG_FILE public property. Some public properties (noted with "Use XML") will generate a config.xml which will be overwritten by the CONFIG_FILE. If using CONFIG_FILE, please include all customizations in the config.xml only.

Property	Use XML	Intended Use & Value Information
ACCOUNT	X	This property can be set to pre-configure the account used to connect to the network
AUTOCONNECT_CONTROL_ALLOWED	X	Set this property to "yes" to show the Automatic Mobile Connection option on the Mobile Menu. Default: "yes"
CERT_SHOW	X	Set this property to "Y" to set the AT&T Global Network Client to show the "Login using a Digital Certificate or Smart Card" checkbox on the User ID panel of the Setup Wizard. Default: blank (not set)
CERT_SHOW_SET	X	Set this property to "Y" to select the "Login Using a Digital Certificate or Smart Card" checkbox for all new user profiles. Default: blank (not set)
CERT_DEFAULT_USE		Set this property to "1" to make the AT&T Global Network Client look for certificates only on the Smart Card. Default: blank (not set)
CONFIG_FILE		This property can be set to the name of an xml file which contains the settings for a Trusted LAN configuration or Client Profiles configuration. If a full path is not specified, the installation package will look for a file in the same directory as the installation source. See page 49 for customizations in the CONFIG_FILE section for more information. Default: blank (not set)

Property	Use XML	Intended Use & Value Information
CUSTOM_APN		Set this property if you are using a custom APN to connect with your Mobility device.
CUSTOM_APN_USERNAME		Set this property if you are using a custom APN and need a user name to connect with your Mobility device. * Only do so if directed by your AT&T Account Representative
CUSTOM_APN_PASSWORD		Set this property if you are using a custom APN and need a password to connect with your Mobility device. * Only do so if directed by your AT&T Account Representative
DEFAULT_AUTOCONNECT_MODE		Set this property to "ENABLE" to enable auto-connect on client start if the detected hardware supports the autoconnect feature. Set to "DISABLE" to disable the autoconnect feature when the AT&T Global Network Client starts. Default: "NOCHANGE"
DESKTOP_SHORTCUT		Set this property to "1" to install a desktop shortcut. Set it to an "" (empty string) (i.e. `DESKTOP_SHORTCUT=""`) to not install a desktop shortcut. Default: "1"
FIREWALL_STATE		Set this property to "on", "off" or "disabled" on the command line to control the initial state of the AT&T Global Network Client Firewall. Setting the state to "on" defaults the AT&T Global Network Client Firewall on causing it to discard unsolicited traffic. Setting the state to "off" causes the AT&T Global Network Client Firewall to allow all traffic. Setting the firewall to "disabled" makes it so the AT&T Global Network Client Firewall will not be used as a firewall.

Property	Use XML	Intended Use & Value Information
HIDE_SAVE_PASSWORD	X	Set this property to "1" to hide the Save Password or Save Pin option on the Network Logon dialog. See Figure 6 for the checkbox option described. Default: "0"
INTERNET_ONLY	X	Set this value to "1" to allow the users to connect directly to mobile and Wi-Fi (private and free) Internet networks without entering AT&T Global Network credentials (Account, User ID, and Password). Default: "0"
LAUNCHPROGRAM		Set this value to "1" to pre-select the launch program checkbox on the setup complete dialog of the installation. Default: "1"
LPE_COMPLIANCE_THRESHOLD		Set this value to the number of failed compliance checks allowed before the AT&T Global Network Client performs the compliance failure action; with a default value of "0", the AT&T Global Network Client will immediately handle compliance failures.
LPE_FILE	X	Set this value to prevent connections if a specificied file does not exist on the system. Example: LPE_FILE=C:\Windows\compid.txt Note: The LPE *feature* does not need to be installed.
LPE_OS_RANGE	X	Set this value to prevent connections on specific Operating Systems. Use the numeric version of an Operating System(s) you wish to block. Example: Windows Vista through Windows 7 RTM: LPE_OS_RANGE=6.0.6000-6.1.7600 Note: The LPE *feature* does not need to be installed.
LPE_REG	X	Set this value to prevent connections if a specificied registry hive does not exist in the HKEY_LOCAL_MACHINE branch. Example: LPE_REG="SOFTWARE\YourCompany\Asset" Note: The LPE *feature* does not need to be installed.

Property	Use XML	Intended Use & Value Information
MULTIHOMING_CLIENT_ADDITIONS		Specifies the VPN Clients to exclude when preventing multi-homing: Cisco Client: Cisco All Cisco Clients: CiscoAll Juniper Client: Juniper CheckPoint Client: Checkpoint Example: MULTIHOMING_CLIENT_ADDITIONS=Cisco
NS_FROM_VPN_SERVER		Use the name servers supplied by the VPN server instead of the values supplied from the Service Manager
PASSWORD	X	Used to specify the password for a pre-configured profile
PROFILENAME	X	Used to specify the profile name for a pre-configured profile
PROGRAM_GROUP		Set this property to full path to the start menu program group (i.e. C:\Documents and Settings\<Username/All Users>\Start Menu\Programs\Group Name) in order to specify an alternate Program Group for the installation. Default: <blank>
REMOVE_USER_ SETTINGS		This property controls whether to remove user settings during uninstallation. Specifying "None" causes the setup to leave user settings on the computer. Specifying "Me" causes the setup to delete the entire [LocalAppDataFolder]AGNS directory. Specifying "All" causes the setup to remove the entire [LocalAppDataFolder]AGNS for every user account on the computer. Default: "None"

Property	Use XML	Intended Use & Value Information
SHARED_SETTINGS		Set this to "1" for the AT&T Global Network Client to use the Common Application Data folder on the workstation, instead of the users application data folder for settings and profiles. This enables all users on a workstation to share the same settings and profiles. This value is automatically set to "1" for new installations that include the GINA feature. Default: "0" ("1" for new PLAP installations)
SKIPWINLOGONCHECK		Set this property to "1" to bypass the check for the install running on the WinLogon desktop. Default: <blank>
SUPPRESS_UPGRADE_REBOOT		Set this property to "1" to suppress the upgrade reboot when installing a new version of the AT&T Global Network Client to a system which already has a previous version installed. Set to "0" to allow a reboot during upgrade. Default: "0"
TRUSTED_DOMAINS		Set this property to a comma delimited list of Connection-specific DNS Suffixes for which the firewall should be disabled for the Trusted Domain Configuration
USERID	X	This property can be set to pre-configure the User ID used to connect to the network.
VNIC_CON_NAME		This is the name of the network connection that will be show in the Windows Network Connections window. *Ideally this value SHOULD NOT be changed*. Default: "AT&T Global Network Virtual Network Adapter"

Shortcuts

Name	Location	Target File
AT&T Global Network Client	Desktop	NetClient.exe
AT&T Global Network Client	[ProgramMenuFolder]AT&T Global Network Client	NetClient.exe
Customer Support	[ProgramMenuFolder]AT&T Global Network Client	NetHelp.exe
Firewall Settings	[ProgramMenuFolder]AT&T Global Network Client	NetFW.exe

Common Windows Installer Properties

Network administrators frequently deploy applications via a command line or with a transform. Properties can be set in a transform and on the command line, as well.

Property	Example	Intended Use
ADDLOCAL	ADDLOCAL=PLAP	List the features you want to install locally, separated by commas.
INSTALLDIR	INSTALLDIR=C:\Program Files\AT&T Global Network Client	The main installation directory for the product.
PRODUCTNAME	AT&T Global Network Client	The name of the application.

Using the Command Line to Customize Installation

Using the Public Properties and understanding the Features available in each AT&T Global Network Client Edition, you can customize your installation package using command line switches and parameters.

When using command line customization, any default parameters normally set by the AT&T Global Network Client installation are superceded by the parameters set on the command line. If using command line customization you must replicate the default parameters normally set by the AT&T Global Network Client program (such as generation of an installation log).

Windows Installer command line switches are described on the Microsoft MSDN site at: http://msdn2.microsoft.com/en-us/library/aa367988.aspx

Example Command Line Customizations

Example	Command
Silent installation with a Desktop Shortcut	msiexec /i agnc.msi /qb
Silent installation with No Desktop Shortcut	msiexec /i agnc.msi DESKTOP_SHORTCUT="" /qb
Completely Silent Installation[3]	msiexec /i agnc.msi /qn
Installation with logging	msiexec /I agnc.msi /l*v install.txt
Executable installation with logging	agnc.exe /v"/l*v install.txt"
Interactive Hook Mode GINA installation	msiexec /i agnc.msi ADDLOCAL=ALL
Silent installation without AT&T Global Network Client Firewall	msiexec /i agnc.msi ADDLOCAL=Net_Client,VPN_Client,PLAP /qb
Silent Uninstallation Using the MSI Package	msiexec /x agnc.msi /qb
Suppress Reboots	msiexec /i agnc.msi REBOOT=ReallySuppress

Creating a Windows Installer Transform

A transform is available if you are unable to create the customization you desire using only command line options. A transform provides advanced customization which is applied to the standard installation package at the time of installation.

One important capability of a transform is that if done properly, it can be written to apply to several versions of the AT&T Global Network Client Installer packages. Also, patches that are created for the

[3] Beginning with Version 8.0, using the /qn option for a silent installation will remove the user interface from the AT&T Global Network Client installation and will persist and chain to any subsequent additional features or third party installations included with the AT&T Global Network Client installation package

standard AT&T Global Network Client Installer package should also apply to AT&T Global Network Client packages that have been customized with a transform if the transform has been implemented correctly.

To preserve as much as possible of the typical behavior of the standard Windows Installer package, your transform should make as few changes as possible. That means that you should first try to accomplish the modification by changing values in the Property table, rather than by making more extensive changes in the MSI database. It is recommended all changes are done with a minimalist approach to avoid unintended consequences.

Tools to Create a Transform

Microsoft Windows Platform SDK contains tools which can assist you in creating a transform. You must obtain and install the Windows Platform SDK relevant to your operating system to have access to the tools.

The Microsoft tool named Orca can open and edit MSI transform files. When Orca is installed as part of the Windows Platform SDK, you can right click on MSI files and select the option **Edit with Orca**.

When viewing an AT&T Global Network Client MSI file with Orca the public properties will be shown in the Orca Property Table. Properties not listed in the Orca Property Table, but listed in this document can be added to the Orca Property Table for editing. Select **Add Row** in the Orca Property Table to add fields and corresponding values.

Common Changes Customized via a Transform

Item	Notes
INSTALLDIR property	When specified during an upgrade, the installation package will honor an installation directory change for a Major Upgrade. Minor updates must install to the same directory as a previous installation.
PACKAGE_ID property	The default value is "default". This change also requires additional database files provided by AT&T via a customization that must be included with the package.
PACKAGE_VERSION	An optional revision number for packages which have used the same PACKAGE_ID. This change also requires additional database files provided

Item	Notes
	by AT&T via a customization that must be included with the package.
ProductName property	
Start menu folder	
Names of shortcuts	
The selection states of features, such as GINA	
Whether various dialogs appear in the UI	
Captions on the dialogs	This change also requires additional database files provided by AT&T via a customization that must be included with the package.
The installation of additional files (i.e. Data\Custom)	These files should be "new" files that are not in the original setup.

Things That Must Be Avoided

Performing any of the following using a transform will make future patches and upgrades difficult or potentially impossible.

- Renaming the original MSI package.
- Using a transform to deploy updated files that the MSI package already deploys. (There is one exception for passwordrules.chm.)
- Removing any components.
- Changing the ProductCode, UpgradeCode, or Package Code.
- Changing the ProductVersion property.

Recommended Actions via a Transform

If you are going to perform any of the following, the recommended approach is to use a Windows Installer Transform.

Adding Files

Only add new files in a transform. Do not remove any key files from any existing components.

Updating Files

Use patches or upgrades to update files that exist in the original setup. Do not use a transform to cause the setup to install newer files than were in the original setup because that will make the transform invalid for future versions of the setup.

Customizing Your Password Rules

Password rules are contained in the file **"passwordrules.chm"**. The **"Never Overwrite"** property for the component that installs the file **"passwordrules.chm"** has been set to **"Yes"**. Therefore, it is possible to include a different version of this single file in a transform and replace the file that is deployed in the original MSI package. Since this file will never be overwritten, it will be preserved during upgrades and patches.

Changing the Installation Directory

Change the installation directory in the setup by modifying the value of **INSTALLDIR** in the Directory table. When specified during an upgrade, the installation package will honor an installation directory change for a Major Upgrade. Minor updates must install to the same directory as a previous installation.

Changing the Application Name

You can change the name of the application name by modifying the **ProductName** property in the **Property** table. You can modify the names of the shortcuts by changing the values in the **Name** field in the **Shortcut** table.

Making the Transform Apply To Future Versions

Transforms offer several validation checks that can occur before the installation begins. The validation can occur on the **UpgradeCode**, **ProductCode**, **ProductVersion**, and **ProductLanguage** properties. To make the transform apply to future versions of the product, you should eliminate the validation checks or check only the **ProductCode**.

The Project Settings dialog in InstallShield configures which validation checks occur at runtime. To open this dialog, click **Project** then **Settings** from the menu.

Customization Using a config.xml File

If you require more than a few simple customizations for your deployment which can all be accommodated using Windows Installer public properties, you can use a config.xml file to specify all of your customization and configuration. If you are using a config.xml file for your customization, place all of your customizations in the file and do not use Windows Installer public properties at the same time.

Global Customizations (FastPath Replacement)

There are several configuration options which are not tied to a profile and change the fundamental behavior of the application. These configuration options are specified in the global_customizations section of the file.

XML Comments explaining each customization are shown in red.

```
<?xml  version="1.0" encoding="UTF-8"?>
<agnclient>
  <global_customizations>
    <!-- Means that the Save Password checkbox will be hidden -->
    < flag name="HideSavePassword" value="Y" />
    <!-- Means that the Save Password checkbox will be checked by default -->
    <flag name="DefaultSavePasswordOn" value="Y" / >
    <!-- Means that the Pin and Token is shown and not the password field -->
    <flag name="InitiallyShowPinAndToken" value="N" / >
  </global_customizations>
</agnclient>
```

Figure 25: Fastpath Replacement Configuration File Example

Trusted Domain Customization

The Trusted Domain Customization allows Customer Account Administrators to define a list of trusted domain suffixes at installation time. When the AT&T Global Network Client with the AT&T Global Network Client Firewall component is installed using a Trusted Domain list, the firewall is enabled by default unless the workstation is actively connected and assigned a Connection-specific DNS Suffix in the Trusted Domain list. This customization is commonly used for mobile laptop users that transition between public networks and a trusted Intranet office environment. The Trusted Domain Customization defines the trusted Intranet environment when the AT&T Global Network Client Firewall may inhibit productivity or prevent remote management tools from functioning properly.

The list is defined at installation time and once the trusted domains have been configured, there is no method to dynamically update them.

There is one exception to the Trusted Domain Configuration; regardless of the Connection-specific DNS Suffix, if a VPN session is established the firewall is enabled on all interfaces.

Trusted Domain Configuration

The Trusted Domain Customization uses a Windows Installer public property to specify the list of Trusted Domains. Set the TRUSTED_DOMAINS Windows Installer public property to a comma delimited list of domain suffixes you want to be trusted when the installation package is deployed to your workstations. See the Advanced Customizations Using Windows Installer section on page 37 for examples of using Windows Installer public properties.

Trusted Domain Customization Limitations

The Trusted Domain Customization is an install time only configuration and cannot be updated on demand. There is one exception to the Trusted Domain Configuration; regardless of the Connection-specific DNS Suffix assigned, if a VPN session is established the firewall is enabled on all interfaces.

Client Profiles Customization

The Client Profiles Customization allows customer account administrators to define a list of client profiles at installation time. When the AT&T Global Network Client is installed using a Client Profile list, the client profiles are created at installation time rather than manually by the user after installation.

The list is defined at installation time and once the profiles have been configured, there is no method to dynamically update them.

Client Profiles Configuration File

The Client Profiles Customization requires a Configuration File be present during AT&T Global Network Client installation. The name of the configuration file must be defined via the **CONFIG_FILE** public property of the installation package (see the chapter on Customizations for more information on public properties of the AT&T Global Network Client). The Trusted LAN, Trusted Domain customization and Client Profiles Customization can be defined in the same configuration file.

The Configuration file uses the standard XML file format. The Client Profiles information is specified with two "tables" definitions for each profile, **"Profile"** and **"ConfigSettings"**.

In the example below **Profile**, define a basic profile. **Name** defines the name of the profile.

- **Account** defines the AT&T account of the user
- **UserId** defines the AT&T user ID. **Note**: That you can use **$(UserName)** to use the Windows loged on user's name as the User Id.

It is recommended you do not customize profile properties that are configurable using the AT&T administration server (such as network service). Because of the ability to update the value at connect time, it is recommended to use the AT&T administration server to centrally define values when possible.

Following is an example of a Client Profile using all the public properties that might conflict with the "CONFIG_FILE" configuration file. Feel free to use this file and remove the sections you do not need:

XML Comments explaining some of the customizations are shown in green.

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
agnclient attributes is where the package id is set for config enforcement.  The package id is limited to
eight characters.  If you update the package version after the config.xml has been processed the
config.xml will be reprocessed.  New to 10.5.0 you can also add the global action to delete all profiles
before processing the config.xml file.
-->

<agnclient package_id="Package" package_version="20210315-153604" global_actions="DeleteAllProfiles">

   <!--
   NOTE!!! This XML file has all the possibilities where there could be conflicts with PUBLIC PROPERTIES.
   You need to look at this XML and remove what is not appropriate to your installation
   -->

   <global_customizations>
      <!-- This means that the Save Password checkbox will be hidden -->
      <flag name="HideSavePassword" value="Y" />
      <!-- This means that the Save Password checkbox will be checked by default -->
      <flag name="DefaultSavePasswordOn" value="Y" />
   </global_customizations>

   <tables>
      <table name="profiles">
         <!-- Define the default profile -->
         <profile>
            <Action>add</Action>
            <!-- this would be the PROFILENAME Public Property -->
            <Name>My First Profile</Name>
            <Account>Account1</Account>
            <!-- $(UserName) can be used to use the current loged on user for the UserId -->
            <UserId>$(UserName)</UserId>
            <!-- Make this profile the default profile -->
            <Default>Yes</Default>
            <!-- Hide the Save Password checkbox on the Network Logon Screen -->
            <!-- this would be the same as HIDE_SAVE_PASSWORD=1 Public Property -->
            <HideSavePassword>Yes</HideSavePassword>
         </profile>

         <!-- Define the second profile -->
         <profile>
            <Action>add</Action>
            <Name>My Second Profile</Name>
            <Account>Account2</Account>
            <UserId>MyUserId</UserId>
            <!-- Use Certificates from the local store -->
            <UseDigitalCertificates>LocalStore</UseDigitalCertificates>
         </profile>

         <!-- Example of changing a profile -->
         <profile>
            <Action>change</Action>
            <Name>Profile that you want to change</Name>
            <UseDigitalCertificates>SmartCardOnly</UseDigitalCertificates>
         </profile>
```

```
        <!-- Example of deleting a profile -->
        <profile>
          <Action>delete</Action>
          <Name>Profile that you want to delete</Name>
        </profile>

    </table>

    <!-- This section is an example on how to set preferences for a profile. -->
    <!-- this is an optional section  -->
    <table name="preferences">
        <preference>
          <Action>add</Action>
          <!-- The profile name from above -->
          <ProfileName>My First Profile</ProfileName>
          <!-- Minimize Main window after connecting -->
          <MinimizeMain>True</MinimizeMain>
          <!-- Minimize to System Tray when minimizing the main window -->
          <MinimizeSysTray>True</MinimizeSysTray>
        </preference>
        <preference>
          <Action>add</Action>
          <ProfileName>My Second Profile</ProfileName>
          <ConfirmDisconnect>False</ConfirmDisconnect>
          <ConfirmClose>False</ConfirmClose>
        </preference>
    </table>

    <!-- This section is an example on how to set auto start applications for a profile. -->
    <!-- this is an optional section  -->
    <table name="autostarts">
        <!-- After connecting start Outlook -->
        <autostart>
          <Action>add</Action>
          <ProfileName>My First Profile</ProfileName>
          <FSMState>AfterConnecting</FSMState>
          <NameId>Microsoft Outlook</NameId>
        </autostart>

        <!-- After connecting start Microsoft Edge -->
        <autostart>
          <Action>add</Action>
          <ProfileName>My First Profile</ProfileName>
          <FSMState>AfterConnecting</FSMState>
          <NameId>Microsoft Edge</NameId>
        </autostart>

        <!-- Update  an existing Auto Start Notepad++ -->
        <autostart>
          <Action>change</Action>
          <ProfileName>My First Profile</ProfileName>
          <FSMState>AfterConnecting</FSMState>
          <Name>Notepad++</Name>
          <File>C:\Program Files\Notepad++\notepad++.exe</File>
          <Directory>C:\Program Files (x86)\AT&amp;amp;T Global Network Client\dyn_cust</Directory>
          <Parameters>config.xml</Parameters>
        </autostart>
    </table>

  </tables>
</agnclient>
```

Figure 26: Client Profiles Configuration File Example

Other Commonly Requested Customizations

The following are some common configurations and customizations. The details of implementing these customizations are provided.

Network Login Option Customizations

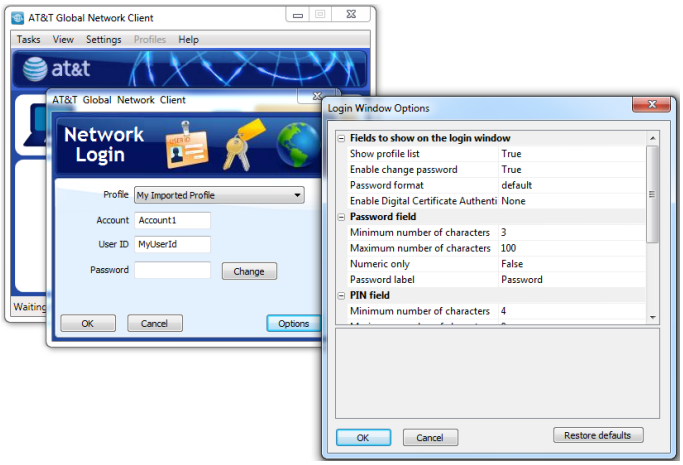


Figure 27: Network Login Options

Many customers need to set the options for the login properties dialog. The following is a list of customizations to add the CONFIG_FILE Public Property xml file:

Hide Options Button

```
<agnclient>
<registry_customizations>
        <registry type=”string”>
                <branch>HKEY_LOCAL_MACHINE\SOFTWARE\AGNS\NetClient\Settings\LoginOptions</branch>
                <field>HideOptionsLink</field>
                <value>1</value>
        </registry>
</registry_customizations>
</agnclient>
```

Use Digital Certificates

In Figure 26: Client Profiles Configuration File Example here are the vailid

Value options are:

- “None” for no certificates.
- “LocalStore” for Local store
- “SmartCardOnly” for Smart Cards

Password Format

Value options are:
"1" for Regular Password
"2" for Pin and Token

```
<agnclient>
<registry_customizations>
        <registry type="string">
                <branch>HKEY_LOCAL_MACHINE\SOFTWARE\AGNS\NetClient\Settings\LoginOptions</branch>
                <field>PasswordFormat</field>
                <value>2</value>
        </registry>
</registry_customizations>
</agnclient>
```

Other Network Login Options

PasswordMinChars	To set the password minimum characters option. Any valid numeric can be used. (Default value is 3)
PasswordMaxChars	To set the password maximum characters option. Any valid numeric can be used. (Default value is 100)
PINMinChars	To set the PIN minimum characters option. Any valid numeric can be used. (Default value is 4)
TokenMinChars	To set the Token minimum characters option. Any valid numeric can be used. (Default value is 4)
PINMaxChars	To set the Pin maximum characters option. Any valid numeric value can be used. (Default value is 8)
TokenMaxChars	To set the Token maximum characters option. Any valid numeric can be used. (Default value is 8)
PasswordPrompt	To customize the text of the password label. Any valid text/string can be used. *Note: Making it too long will cut off text.*
PINPrompt	To customize the text of the PIN label. Any valid text/string can be used. *Note: Making it too long will cut off text.*

Limiting Connections Per Operating System

If more than one range of Operating systems need to be defined, then the config.xml will have to be used instead of the LPE_OS_RANGE public property. The following example would allow Windows 7 SP1 through Windows 10.

```
<agnclient>
  <user_interface>
    <checkforos lowervalue="6.1.7601" uppervalue="6.1.7600" />
    <checkforos lowervalue="10.0.10240" uppervalue="10.0.99999" />
  </user_interface>
</agnclient>
```

See http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx for more information.

Profile Customization Limitations

The Client Profile Customization is an install time only configuration and cannot be updated on demand.

Controlling the AT&T Global Network Client Firewall

The state of the AT&T Global Network Client Firewall is "on", "off", or "disabled" and the initial state is set by specifying the **FIREWALL_STATE** public property. If it is set to "disabled" you must also request that your AT&T representative update your Firewall Setting in the AT&T Administration Server to "N".

NOTE: The FIREWALL_STATE public property sets the initial state only. Once the user connects to the network, this property may be overridden by the central firewall configuration downloaded from the AT&T Administration Server.

Network Awareness Customization

The Network Awareness customization provides the ability to define an AT&T Global Network Client action to be performed when a user connects to a defined network.

The following actions are currently supported using Network Awareness:

- No AT&T Global Network Client connection required, immediately disconnect the AT&T Global Network Client
- No AT&T Global Network Client connection required, immediately prompt the user to disconnect the AT&T Global Network Client
- Minimize the AT&T Global Network Client

When the user connects to a network defined to not require an AT&T Global Network Client connection, the AT&T Global Network Client connect button will be disabled.

Figure 28: Disabled Connect Button

If the user is connected to the internet and then connects to their corporate network, they can be prompted to disconnect their VPN session.

Figure 29: Prompt to Disconnect when Work Network is detected

Defining Networks and Corresponding Actions

The Network Awareness customization requires central configuration; the Network Awareness field in the AT&T administration server must be set to "**Y**". Refer to Appendix A: Central Configuration for additional information about central configuration.

This customization requires you to define the network(s) by creating a NetworkAwarness.xml file. Working knowledge of XML is recommended to perform this customization. The NetworkAwarness.xml file is read when the AT&T Global Network Client is launched and any subsequent changes are not effective until the AT&T Global Network Client is shutdown and restarted. Please note that xml style comments are not supported in the file at this time.

The XML file must be found at the following path:

"%ALLUSERSPROFILE%\AGNS\NetClient\NetworkAwareness.xml"

Following is an example of a Network Awareness XML configuration file:

```
<network_location>
        <description>the AT&amp;amp;T network</description>
        <active>Y</active>
        <action>IMMEDIATELY_DISCONNECT</action>
        <action>MINIMIZE_CLIENT</action>
        <subnet>135.0.0.0,255.0.0.0</subnet>
        <subnet>129.1.0.0,255.0.0.0</subnet>
        <wins_server_list>2.2.2.2,3.3.3.3</subnet>
        <operator>OR</operator>
</network_location>
```

The table below defines the settings configurable using the NetworkAwareness.xml.

Stanza	Description
network_location	A brief description of network – this is displayed on the AT&T Global Network Client user interface so the name should be kept short to preserve readability. **ONLY ONE network_location stanza may be defined in the NetworkAwareness.xml file**.
Active	Set to "**Y**" for the AT&T Global Network Client to actively look for and perform an action for this network location. Set to "**N**" to perform no action.
Action	Set to one or more available actions:

Stanza	Description
	IMMEDIATELY_DISCONNECT PROMPT_TO_DISCONNECT MINIMIZE_CLIENT
Subnet	Set to one or more IP address/subnet mask combinations to define the network. Multiple subnets can be defined by repeating this stanza within the network location stanza.
dns_suffix_list	Set to DNS suffix to identify network location. Multiple suffix's can be defined by separating suffix's with a comma. Multiple suffixes within the list are combined using "**OR**".
dns_server_list	Set to DNS Server IP Addresses to identify network location. Multiple IP Address's can be defined by separating IP Address's with a comma. Multiple IP Addresses within the list are combined using "**OR**".
wins_server_list	Set to WINS Server IP Addresses to identify network location. Multiple IP Address's can be defined by separating IP Address's with a comma. Multiple IP Addresses within the list are combined using "**OR**".
Operator	Set to "**OR**" or "**AND**" to determine how to combine multiple types of identifiers (subnet, dns_suffix_list, wins_server_list). Default: "**OR**"

Approved Mobile Device Customization

The Approved Mobile Device customization provides the ability to define a list of approved mobile devices with which your users can connect using the AT&T Global Network Client.

The following registry key is required:

HKLM\Software\AGNS\NetClient\WAN\AllowedDevices

The key must be created as a multi-string registry key at installation time. Multiple devices can be defined; each device should be listed on a separate line of the registry key. This is an allow list, only devices in the list will be supported.

The items in the list are compared against the installed mobile device model name for a match. If a match is not found, the user will receive a pop-up warning them the device cannot be used. The mobile icon will be disabled and mobile connection will have a status of **disabled** in the Connection Sequence window.

The AT&T Global Network Client must be restarted after the device is removed for the mobile icon to be enabled.

Approved Connection Type Customization

Beginning with Version 9.1, Customer Account Administrators can select to show or hide the Wi-Fi or Mobile connection types. Customizing the visibility of connection types requires a custom installation package created by AT&T. Please contact dl-AGNC_custom@att.com for additional information.

By default Ethernet/Existing, Wi-Fi and Mobile connection types are shown. WiFi and Mobile connection types can be hidden through customization. Hiding a connection type will hide ALL subtypes of that connection type by default.

Connection Type Which Can Be Hidden
WiFi
Mobile

Secondary Method of Customizing Network Login Options

The fields and functionality of the Network Login window can be configured by clicking the "Options" button on the Network Login window. The Login Options window shows the features that can be configured.

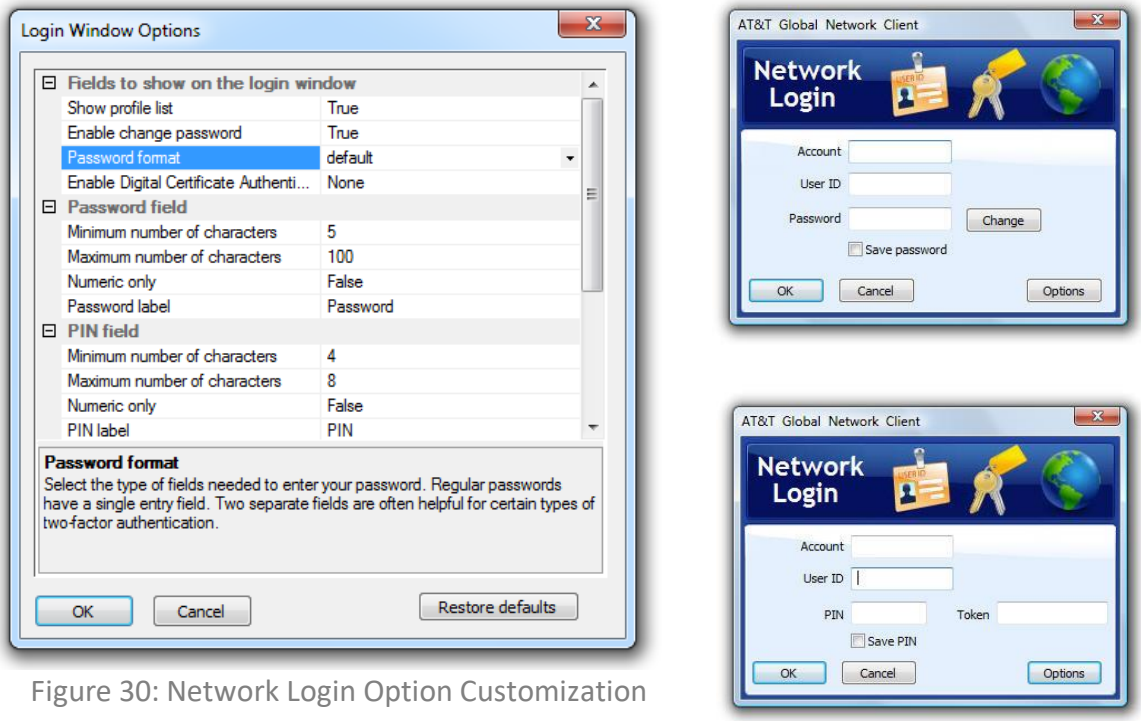


Figure 30: Network Login Option Customization

Customizing Default Login Options

The default login options can be customized by configuring them in the Windows registry. Default login options can be stored in the `HKEY_LOCAL_MACHINE` registry branch. User modified options are stored in the `HKEY_CURRENT_USER` registry branch and take precedence over the default values. (See the Hiding Login Options section for instructions on how to prevent users from changing the login options.)

Customizing Default Login Properties

1. Run the AT&T Global Network Client and configure the login options as desired.
2. Run regedit.exe and export the following branch to a file called LoginOptions.reg:
   HKEY_CURRENT_USER\Software\AGNS\NetClient\Settings\LoginOptions
   **Note: The branch will not exist until after the first login attempt.
3. Edit LoginOptions.reg and change HKEY_CURRENT_USER to HKEY_LOCAL_MACHINE.
4. Merge LoginOptions.reg into the registry to store the defaults.

Figure 31: Customizing Default Login Properties Table

Customization Services

A customized AGN Client may be required to enable certain features, for example: Lightweight Policy Enforcement or a drop down menu that makes it easier to select among many available profiles. Please contact DL-AGNClientCustomTeam@att.com to reach the team responsible for such customization.

SDK Prioritization

You are able to change the prioritization of the Windows Mobile Broadband SDK relative to other mobile SDKs.

Windows Mobile Broadband is only available in Microsoft Windows 8.1, and Windows 10

Accessibility Features

The AT&T Global Network Client complies with US regulations to support accessibility for persons with disabilities, including Section 508 regulations.

Visual Display of Screen Element in Focus

The AT&T Global Network Client screen element in focus is depicted by a gray highlighted box surrounding the control. When first launched, the Connect button is in focus as shown below.

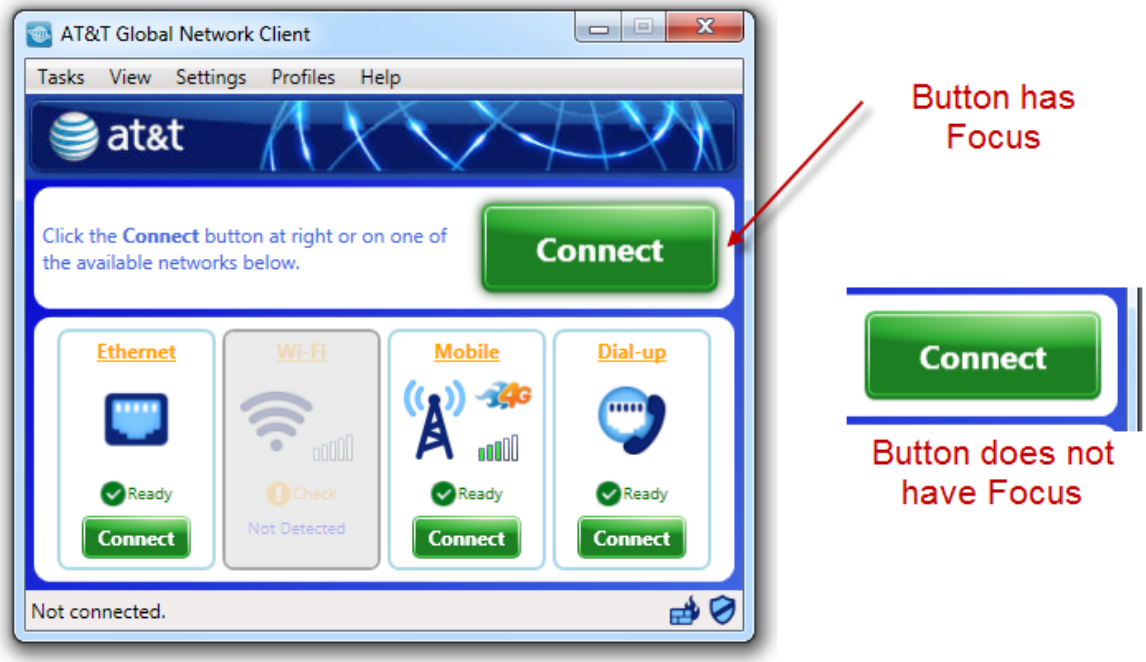


Figure 32: Main Window

Keyboard Navigation

The AT&T Global Network Client can be navigated and utilized exclusively using a keyboard.

The controls can be operated either by pressing the space bar or the Enter key.

To move between controls, use the tab key to navigate forward or shift key and tab key in unison to navigate backward. To simulate a right mouse click, use the menu key or the shift key in unison with the F10 key.

AT&T Lightweight Policy Enforcement

AT&T Lightweight Policy Enforcement (LPE) is an optional service available to AT&T customers using the AT&T Global Network Client for connectivity. AT&T Lightweight Policy Enforcement performs basic application monitoring and can be customized by the Customer Account Administrator at installation time.

Installation of the Lightweight Policy Enforcement feature is optional. Customer Account Administrators can use control Lightweight Policy Enforcement definitions using the XML CONFIG_FILE Public Property at installation time or the Windows Installer ADDLOCAL and REMOVE properties to control installation of the feature for all users. See the Customizations Chapter on page 37 of this guide for more information about installation customization.

Asset Based Connection Prevention

Beginning in 9.6, connections can be prevented based on

- Operating System/Service Packs
- A specified file
- A registry hive in HKEY_LOCAL_MACHINE

Operating System

Allow range of Operating Systems to be used

With the AGNC_LPE_OS_RANGE public property, the lowest allowed, highest allowed, or lowest and highest together. For

Allow range of Operating Systems to be used

To prevent connections based on obsolete or unsupported Operating Systems or Service Packs, you can do so by using the Public Property, LPE_OS_RANGE at install time. By specifying the numeric value range of the Operating System, connections will not be allowed. For example, if the company policy is to prevent connections on Windows Vista, you would specify:

LPE_OS_RANGE=6.0.6000-6.0.6002

6.0.6000 is Vista RTM and 6.0.6002 is Vista Service Pack 2.

For more information on Operating System build numbers, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

For multiple ranges, the config file should be used instead of public properties.

The following example would allow Windows 7 SP1 through Windows 10.

```
<agnclient>
  <user_interface>
    <checkforos lowervalue="6.1.7601" uppervalue="6.1.7601" />
    <checkforos lowervalue="10.0.10240" uppervalue="10.0.99999" />
  </user_interface>
</agnclient>
```

This example would allow

Specified File

To prevent connections based on whether a specific file exists on the user's system, use the LPE_FILE Public Property at install time. If the specified file does not exist, then a connection will not be allowed.

Registry hive in HKEY_LOCAL_MACHINE

To prevent connections based on whether a specific file exists on the user's system, use the LPE_REG Public Property at install time. If the specified registry hive does not exist, then a connection will not be allowed. For example, if you have company defined asset information entry in the HKEY_LOCAL_MACHINE hive, that would not be on a non-asset system, you can use that information to prevent a connection, e.g. LPE_FILE="SOFTWARE\MyCompany\Asset\Identifier"

Application Monitoring

The application monitor feature allows a Customer Account Administrator to specify configuration policies to monitor antivirus programs, firewalls and anti-spyware programs. The rules are configured through a custom kit. Some basic Lightweight Policy Enforcement rules can be enforced by a using the XML based CONFIG_FILE Public Property at installation time.

A threshold value indicating the number of failed compliance checks allowed before the AT&T Global Network Client performs the compliance failure action can be configured by the Customer Account Administrator through customization. See the LPE_COMPLIANCE_THRESHOLD public property in the chapter on Customizations for more information.

Types of Applications Monitored

Pre-defined antivirus, firewall, and anti-spyware applications can be monitored. The following table shows the types of applications that can be monitored, as well as what is monitored.

Application Type	Items Monitored
Firewall	• Whether Process is Running • Product Version

Application Type	Items Monitored
Anti-Mileware	• Whether Process is Running • Product Version • Virus Definition File Timestamp
Drive Encryption	• Whether Process is Running • Product Version
Data Loss Prevention	• Whether Process is Running • Product Version
Patch Management	• Whether Process is Running • Product Version • Is Patch installed

For a complete list of applications see the web site at http://www.corp.att.com/agnc/windows/

The Lightweight Policy Enforcement firewall monitoring is used to determine if a firewall is enabled prior to checking for and connecting to free Wi-Fi hotspots. The AT&T Global Network Client will allow the association to potentially free hot spots if any known firewall is running, thus allowing customers to use their own corporate or personal firewall software instead of the AT&T provided firewall.

Limitations

The application monitoring rules are determined at installation time and cannot be dynamically updated. If a user is out of compliance with the policy, the connection is rejected. The user is given a generic error message. The user must make the necessary changes to return to compliance with the policy manually, and without a connection using the AT&T Global Network Client.

Lightweight Policy Enforcement Customization Examples

The AT&T Global Network Client Lightweight Policy Enforcement Customization allows customers to create their own enforcement policy using the CONFIG_FILE public property.

Using CONFIG_FILE Public Property with XML

To set the Lightweight Policy Enforcement for the login properties dialog. The following is a list of customizations to add the CONFIG_FILE Public Property xml file:

LPE for a Generic Firewall

```
<?xml version="1.0" encoding="UTF-8"?>
<agnclient>
    <tables>
        <table name="lpe_rules">
            <rule>                                                  <!-- Firewall -->
                <GroupId>before_connecting</GroupId>                <!-- before connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                 <!-- Product Type firewall -->
                <PassNextRule>0</PassNextRule>                      <!-- next rule done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>       <!-- Fail message -->
            </rule>
            <rule>                                                  <!-- Firewall -->
                <GroupId>after_connecting</GroupId>                 <!-- after connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                 <!-- Product Type firewall -->
                <PassNextRule>0</PassNextRule>                      <!-- done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>       <!-- Resource message -->
            </rule>
        </table>
    </tables>
    <lpe_rules>
        <!-- Check every 60 seconds and once a minute after connecting -->
        <rule_group when="before_connecting" poll_frequency="60"/>
        <rule_group when="after_connecting" poll_frequency="60"/>
    </lpe_rules>
</agnclient>
```

Example 1 Generic Firewall

LPE for a Generic Anti-Malware

```
<?xml version="1.0" encoding="UTF-8"?>
<agnclient>
    <tables>
        <table name="lpe_rules">
             <rule>                                                 <!-- Anti-malware -->
                <GroupId>before_connecting</GroupId>                <!-- before connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>              <!-- ProductType Antimalware -->
                <PassNextRule>0</PassNextRule>                      <!-- done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>AntimalwareNotRunning</FailMessage>    <!-- Fail message -->
            </rule>
             <rule>                                                 <!-- Anti-malware -->
                <GroupId>after_connecting</GroupId>                 <!-- after connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>              <!-- ProductType Antimalware -->
                <PassNextRule>0</PassNextRule>                      <!-- done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>AntimalwareNotRunning</FailMessage>    <!-- Resource message -->
            </rule>
        </table>
    </tables>
    <lpe_rules>
        <!-- Check every 60 seconds and once a minute after connecting -->
        <rule_group when="before_connecting" poll_frequency="60"/>
        <rule_group when="after_connecting" poll_frequency="60"/>
```

```
    </lpe_rules>
</agnclient>
```

Example 2 Generic Anti-Malware

Lightweight Policy Enforcement for Generic Anti-Malware or Firewall not running.

```
<?xml version="1.0" encoding="UTF-8"?>
<agnclient>
    <tables>
        <table name="lpe_rules">
             <rule>                                                <!-- Anti-malware -->
                <GroupId>before_connecting</GroupId>               <!-- before connecting -->
                <RuleId>1</RuleId>                                 <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                     <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>             <!-- ProductType Antimalware -->
                <PassNextRule>2</PassNextRule>                     <!-- next rule 2 -->
                <FailNextRule>0</FailNextRule>                     <!-- done -->
                <FailAction>Disconnect</FailAction>                <!-- Disconnect -->
                <FailMessage>AntimalwareNotRunning</FailMessage>   <!-- Fail message -->
            </rule>
            <rule>                                                 <!-- Firewall -->
                <GroupId>before_connecting</GroupId>               <!-- before connecting -->
                <RuleId>2</RuleId>                                 <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                     <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                <!-- Product Type firewall -->
                <PassNextRule>0</PassNextRule>                     <!-- next rule done -->
                <FailNextRule>0</FailNextRule>                     <!-- done -->
                <FailAction>Disconnect</FailAction>                <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>      <!-- Fail message -->
            </rule>
             <rule>                                                <!-- Anti-malware -->
                <GroupId>after_connecting</GroupId>                <!-- after connecting -->
                <RuleId>1</RuleId>                                 <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                     <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>             <!-- ProductType Antimalware -->
                <PassNextRule>2</PassNextRule>                     <!-- next rule 2 -->
                <FailNextRule>0</FailNextRule>                     <!-- done -->
                <FailAction>Disconnect</FailAction>                <!-- Disconnect -->
                <FailMessage>AntimalwareNotRunning</FailMessage>   <!-- Resource message -->
            </rule>
            <rule>                                                 <!-- Firewall -->
                <GroupId>after_connecting</GroupId>                <!-- after connecting -->
                <RuleId>2</RuleId>                                 <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                     <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                <!-- Product Type firewall -->
                <PassNextRule>0</PassNextRule>                     <!-- done -->
                <FailNextRule>0</FailNextRule>                     <!-- done -->
                <FailAction>Disconnect</FailAction>                <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>      <!-- Resource message -->
            </rule>
        </table>
    </tables>
    <lpe_rules>
        <!-- Check every 60 seconds and once a minute after connecting -->
        <rule_group when="before_connecting" poll_frequency="60"/>
        <rule_group when="after_connecting" poll_frequency="60"/>
    </lpe_rules>
```

```
</agnclient>
```

Example 3 Anti-Malware or Firewall not running

Display a warning message for a generic Anti-Virus package and disconnect if not running the Windows Firewall.

```
<?xml version="1.0" encoding="UTF-8"?>
<agnclient>
    <user_interface>
        <module name="NetClientDll" moduleid="2">
            <!-- Modify the message from disconnected to a warning -->
            <resource name="NetClientDll" resourceid="6474" value="Please start your Anti-Malware program
now."/>
        </module>
    </user_interface>

    <tables>
        <table name="lpe_rules">
            <rule>                                                  <!-- Anti-malware -->
                <GroupId>before_connecting</GroupId>                <!-- before connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>              <!-- ProductType Antimalware -->
                <PassNextRule>2</PassNextRule>                      <!-- next rule 2 -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>DisplayWarningMsg</FailAction>          <!-- Warning Msg -->
                <FailMessage>AntimalwareNotRunning</FailMessage>    <!-- Fail message -->
            </rule>
            <rule>                                                  <!-- Firewall -->
                <GroupId>before_connecting</GroupId>                <!-- before connecting -->
                <RuleId>2</RuleId>                                  <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                 <!-- Product Type firewall -->
                <ProductName>Windows Firewall</ProductName>         <!-- Product name Windows Firewall -->
                <PassNextRule>0</PassNextRule>                      <!-- next rule done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>       <!-- Fail message -->
            </rule>
            <rule>                                                  <!-- Anti-malware -->
                <GroupId>after_connecting</GroupId>                 <!-- after connecting -->
                <RuleId>1</RuleId>                                  <!-- rule 1 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Antimalware</ProductType>              <!-- ProductType Antimalware -->
                <PassNextRule>2</PassNextRule>                      <!-- next rule 2 -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>AntimalwareNotRunning</FailMessage>    <!-- Resource message -->
            </rule>
            <rule>                                                  <!-- Firewall -->
                <GroupId>after_connecting</GroupId>                 <!-- after connecting -->
                <RuleId>2</RuleId>                                  <!-- rule 2 -->
                <RuleType>IsRunning</RuleType>                      <!-- Type IsRunning -->
                <ProductType>Firewall</ProductType>                 <!-- Product Type firewall -->
                <ProductName>Windows Firewall</ProductName>         <!-- Product name Windows Firewall -->
                <PassNextRule>0</PassNextRule>                      <!-- done -->
                <FailNextRule>0</FailNextRule>                      <!-- done -->
                <FailAction>Disconnect</FailAction>                 <!-- Disconnect -->
                <FailMessage>FirewallNotRunning</FailMessage>       <!-- Resource message -->
            </rule>
        </table>
    </tables>
    <lpe_rules>
        <!-- Check every 60 seconds and once a minute after connecting -->
        <rule_group when="before_connecting" poll_frequency="60"/>
```

```
        <rule_group when="after_connecting" poll_frequency="60"/>
    </lpe_rules>
</agnclient>
```

Example 4 Anti-Virus and Windows Firewall

AT&T Global Network Client Firewall

The AT&T Global Network Client Firewall is a component of the AT&T Global Network Client which provides basic firewall capabilities. The AT&T Global Network Client Firewall uses the Windows firewall engine for the firewall and fencing.

The AT&T Global Network Client Firewall provides the following:

- Blocks unsolicited traffic when not connected
- Blocks unsolicited Internet traffic while VPN connected

Overview

The AT&T Global Network Client Firewall is designed to protect a computer as a network firewall. The AT&T Global Network Firewall is turned off by default.

If it is turned on, either by the end user while not connected, or through central configuration via the AT&T Service Manager, the AT&T Global Network Client Firewall is active on all network card interfaces and all Microsoft Remote Access Services WAN Networking interfaces whenever the workstation is powered on, regardless of whether there is a current connection to an AT&T network.

The AT&T Global Network Client Firewall monitors IP traffic; if an IP packet received is determined to be unsolicited[4] by the workstation, it is silently discarded. The AT&T Global Network Client Firewall does not perform any user notification of unsolicited traffic. If your computer did not request, negotiate, or grant permission for a connection with another machine, the traffic is silently rejected.

The AT&T Global Network Client Firewall also protects VPN sessions controlled by the AT&T integrated VPN client. Account administrators define their VPN network resources using an Access Control List (ACL) (AKA 'down the tunnel' network resources) in the AT&T Administration Server. Only traffic destined to one of the defined ACL resources is routed through the VPN tunnel. A setting in the AT&T Administration Server controls if non-VPN traffic should route over the Internet or be silently discarded.

Operating Modes

The AT&T Global Network Client Firewall supports three operating modes. Certain modes require configuration in the AT&T administration server. Refer to Appendix A of this guide for more information about configuration options stored in the AT&T administration server. AT&T Global Network Client Firewall values set in the AT&T administration server always take precedence over values set locally using the AT&T Global Network Client.

[4] The AT&T Global Network Client Firewall monitors new solicitation status as well as tracking port and SYNC status for current and expired sessions.

Default

The Default configuration disables the firewall at all times, on all network interfaces.

Trusted Domains

The Trusted Domain configuration is used to control the firewall state for trusted domains. The Trusted Domain configuration enables the firewall at all times on all network interfaces unless it is actively connected and assigned a Connection Specific DNS suffix in a Trusted Domain list defined at installation time. Even in Trusted Domain mode, regardless of the Connection Specific DNS Suffix assigned, if an AT&T Integrated VPN session is established the firewall is enabled on all interfaces. See page 49 for more information on configuration of a Trusted Domain list.

User Controlled

The state of the firewall is controlled using the AT&T Global Network Client Firewall Settings Window described in the section below. This mode will be affected by the values set for **'Enable AT&T Global Network Client Firewall'** and **'User Controlled Firewall'** fields in the AT&T administration server.

Disabled

The Disabled configuration disables the firewall at all times, on all adapters. The user does not have the ability to turn the firewall on at any time.

When the user selects the **AT&T Global Network Client** from the **Start** menu, and clicks **Firewall Settings Window** the user will receive a message stating **"Your network administrator has chosen not to use the firewall."**

This mode requires a **"NO"** value set for **'Enable AT&T Global Network Client Firewall'** and **'User Controlled Firewall'** fields in the AT&T Administration Server.

Firewall Settings Window

The AT&T Global Network Client Firewall Settings Window allows a user to select the Firewall state (On/Off) when a VPN connection is not active. When the user establishes an active AT&T Global Network Client VPN connection the firewall is automatically enabled on all network interfaces unless the AT&T Global Network Client Firewall is operating in Disabled mode.

Figure 33: Firewall Settings Window

Allowing a user to turn the AT&T Global Network Client Firewall off when not VPN connected may be useful in environments that use enterprise management software to manage computers on a customer LAN since the firewall prevents the management software from having unsolicited access to the target machine.

The AT&T Global Network Client Firewall Settings window can be accessed by clicking the Microsoft Windows **Start** Menu, mouse over **All Programs**, click **AT&T Global Network Client**, and click **Firewall Settings**. The **Firewall Settings** application can only be open when the AT&T Global Network Client application is not running.

Customer Account Administrators can customize their AT&T Global Network Client installation to prevent the **Firewall Settings** window from being installed. Refer to the Customizations Chapter on page 37 of this guide for more information.

Whether users can modify the options on the **Firewall Settings** window can be controlled through the **'User Controlled Firewall'** setting in the AT&T Administration Server. When the **'User Controlled Firewall'** setting is set to **'N'**, the radio buttons on the Firewall Settings Window will be disabled and the user may view, but not change, the current state of the AT&T Global Network Client Firewall. Refer to Appendix A on page 86 of this guide for additional information about settings available in the AT&T administration server.

Managed VPN Access Control Lists

The only exceptions to the static firewall policy of denying all unsolicited traffic exist when there is an active Managed VPN Service connection. When VPN connected, the firewall does not block VPN traffic. With an active VPN connection, users receive all VPN traffic, solicited or unsolicited. Administrators have the ability to define an Access Control List (ACL) identifying the hosts with which a user can communicate

through the VPN. Then the user can only initiate communication to those hosts defined in the Access Control List. If an Access Control List is not defined, all traffic is considered VPN traffic. Administrators can also define an Access Control List for their non-VPN interfaces (aka Internet interface). This is known as the Fenced Internet Access Control List.

Limitations

Beyond the Trusted Domain Customization, the AT&T Global Network Client Firewall policy cannot be customized by the Customer Account Administrator.

AT&T VPN Services

AT&T offers several advanced VPN services. The information in this chapter represents the most common administration and configuration questions.

Using Managed IPSec VPN Services

The security rules of the Managed VPN Services may require additional configuration or specific configuration settings to support your network infrastructure.

Local Resources

Accessing Local Resources

To access local resources (such as printers and other servers) outside the tunnel while a VPN tunnel is established, you must be using a VPN Dual Access capable service. VPN Dual Access allows you to access destinations outside the tunnel either locally or through the Internet in addition to resources down the tunnel.

Customer Account Administrators have the option to allow users that are not configured for Dual Access to access resources on their directly connected subnet by updating the **'Local Subnet Access'** to **'y'** at either the account or client-id level in the AT&T administration server. When the Local Subnet Access flag is set to yes and you are connecting with a non-dual access type service, the AT&T Global Network Client will determine the local subnet and set up the routing/rules to allow access to the local subnet.

Sharing Local Resources

You will not be able to host shared resources on the local LAN (such as printers) when a VPN tunnel is established. This traffic will be viewed as unsolicited IP traffic, and will be silently discarded by AT&T Global Network Client Firewall. The AT&T Global Network Client Firewall must be disabled via the AT&T administration server to support local resource sharing while VPN connected.

Registering VPN IP Address with Dynamic DNS

The AT&T Global Network Client can dynamically register an IP address in DNS when VPN connected regardless of the VPN server type. After VPN connected, the AT&T Global Network Client will gather the domain name, host name, and IP address then send out registration requests to all of the DNS servers in the VPN Adapter interface's DNS server list. To set this option, click **Show the login properties window.** from the **Settings** panel on the main window, click the **Preferences** tab, click **Override Defaults**, scroll down and click **Register VPN connection's address in DNS.** in the **VPN Details** section. If you have opted to turn off DNS registration through the network control panel, then the AT&T Global Network Client will not send the DNS update requests.

If the DNS server is configured for 'Secure Updates Only' and integrated with Active Directory, then the AT&T Network Logon Extensions component is required.

Encryption for IPSec VPN connections

Encryption can be configured in the AT&T administration server at the user account lever or sub account level. If values are specified in the AT&T administration server they will override the AT&T Global Network Client's default proposal behavior. Multiple algorithms can be selected, but the highest supported encryption level will always be proposed first.

Co-existence with Microsoft IPSec

Microsoft IPSec can be used for corporate protection strategies like Domain Isolation, Server Isolation, and IPSec based Network Access Protection (NAP) while VPN connected with the AT&T Global Network Client. Microsoft IPSec traffic travels through an AT&T VPN tunnel. No configuration changes are required when VPN tunneling with SSL-T services using the AT&T Global Network Client. If you are using Version 9.3 or later, no configuration changes are required when using IPSEC either, as the client will now default to use ephemeral source ports.

For IPSec services, the **Use Ephemeral IPSec Ports Login Properties** preference must be enabled. When enabled, the AT&T Global Network Client will NOT stop Microsoft's IPSec service and will use ephemeral source ports (1024+). This enables Microsoft to have sole ownership of IPSec source ports 500 and 4500.

This options is enabled by default. If the end user is having difficulty connecting, and you suspect the use of ephemeral source ports may be causing the issue, you can disable this option. To disable this option, click **Show the login properties window** from the **Settings** panel on the main window, click the **Preferences** tab, click **Override Defaults**, scroll down and deselect **Use ephemeral source ports for IPSec** in the **VPN Details** section.

NAT Traversal

The AT&T Global Network Client IPSec implementation supports NAT traversal through UDP encapsulation of IPSec traffic.

The NAT traversal implementation varies based on tunnel endpoint as listed below:

Cisco®[5] and AT&T Branded Tunnel Endpoints

NAT devices are auto-detected through a series of hashes during IKE negotiations. The AT&T VPN client uses UDP port 4500 as the source port and UDP port 4500 as the destination port in IKE negotiations and ESP IPSec data flows.

[5] Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

This implementation is based off the following Internet drafts:
http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-02.tx

Configuring UDP Encapsulation

A preference labeled **Negotiate UDP Encapsulation with VPN server for NAT Traversal** is available in the Login Properties/Preferences panel to allow an end user to alter the use of NAT Traversal. The default value for this preference can be centrally configured in the AT&T administration server, but can be overridden by a user. To utilize NAT Traversal, this preference must be selected along with configuring the NAT Traversal settings on the VPN endpoint.

The AT&T Global Network Client client supports most NAT devices. There are known difficulties when tunneling IPSec traffic through NAT/firewalls which are documented in the following RFC http://www.ietf.org/rfc/rfc3715.txt.

AT&T is committed to supporting all NAT device vendors that are aware of the known IPSec compatibility issues and comply with the industry standards.

Cisco Passwords

If your network logon password has expired as determined by the authentication flows between the Cisco tunnel server and the Windows Primary Domain Controller, the AT&T Global Network Client will display a prompt for you to enter a new password. The VPN negotiation code will complete the change password exchange.

Using Managed SSL VPN Services

Managed SSL VPN is a client based tunneling solution. Managed SSL VPN traverses customer site proxies and firewalls without requiring network configuration changes. Fenced Internet hosts can be specified when tunneling with SSL-T dual access from a private line location.

Managed SSL VPN Services use TCP port 443 for authentication and tunneling. Alternatively, TCP port 80 can be used by unchecking the **Authenticate with HTTPS** preference in the AT&T Global Network Client **Login Properties**. Managed SSL VPN is successful because unlike IPSec, TCP port 443 can be passed through a proxy. The AT&T Global Network Client can be configured for proxy settings specific to connections using the AT&T Global Network Client using **Setup Wizard** or **Login Properties**, or the AT&T Global Network Client can use Microsoft Windows Internet Options proxy settings.

Network Layer Solution

Unlike some SSL solutions, Managed SSL VPN is a network layer solution. Therefore, all IP based applications (File Sharing/Outlook Exchange/VOIP/etc) are supported. Additionally, customer account administrators can access end user systems for software pushes, ad hoc message, etc. just as if their end users were residing on the Company's private local LAN.

Being VPN connected from behind a customer site proxy presents an extra layer of complexity for web-based applications such as a browser. By default, web-based applications will send all traffic directly to the proxy. However, Private LAN (VPN) and Local LAN traffic need to be routed differently. The AT&T Global Network Client enables a user to configure Internet Options for each specific proxy location to handle web-based applications correctly.

Security/Authentication

The Managed SSL VPN service use AT&T authentication server based authentication. The AT&T SSL VPN Server dictates the encryption method and currently enforces 3 DES and SHA-1. The AT&T SSL VPN Server is configured with an Entrust Server Certificate, and the AT&T Global Network Client utilizes Microsoft Internet Explorer's root certificate. When a TCP disconnect is detected, the AT&T Global Network Client will reestablish the session without user interaction.

Configuring the AT&T Global Network Client to Establish a VPN Connection through a Proxy

The AT&T Global Network Client performs these steps in the following order when establishing a VPN connection during the initial authentication request:

1. Attempt to connect directly across the existing network connection.
2. Attempt to connect using the user specified proxy information for this location, if specified.
3. Attempt to connect using the Microsoft Operating System (Internet Explorer) supplied proxy information.

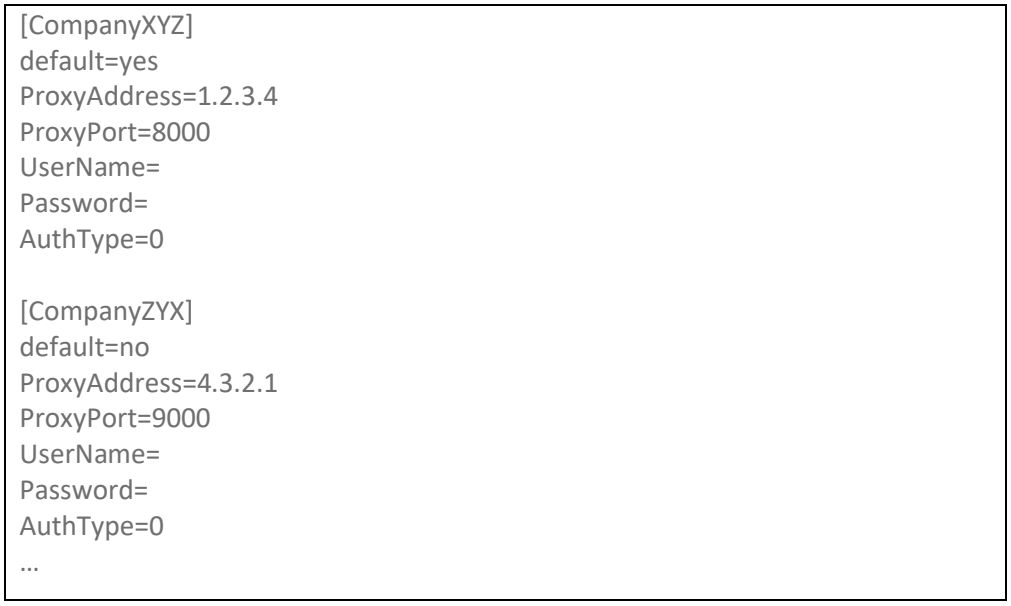
The AT&T Global Network Client User's Guide contains detail instructions on configuring the proxy in the AT&T Client, through the Microsoft operating system, and the browser.

Importing a Proxy File for SSL connections

You have the option of using a proxy.ini file to configure browser settings specific to the proxy location you are visiting so you can access your corporate network through your SSL connection. The proxy settings are used by the AT&T Global Network Client to authenticate and establish the connection to your private network.

Proxy.ini File

You will need to provide your users with the proxy.ini file. Proxy information entries are configurable in the "proxy.ini" file located in the \Program Files\AT&T Global Network Client directory. One or more proxy information entries can be configured in the "proxy.ini" file. Below is a sample proxy.ini file.



```
[CompanyXYZ]
default=yes
ProxyAddress=1.2.3.4
ProxyPort=8000
UserName=
Password=
AuthType=0

[CompanyZYX]
default=no
ProxyAddress=4.3.2.1
ProxyPort=9000
UserName=
Password=
AuthType=0
…
```

Figure 34: Proxy.INI File Example

proxy.ini Field Information:

default - If yes, and the AT&T Global Network Client could not connect through a direct network connection, an attempt to connect will automatically be made by the AT&T Global Network Client to establish a VPN connection with this Proxy Information. Only one entry should be specified as the default entry if multiple entries exist in the proxy.ini file.

ProxyAddress – IP Address of the proxy. This cannot be an auto proxy url.

ProxyPort – Port used to connect to the proxy.

UserName – Used for Proxies that require authentication. (this can be left blank and the user will be prompted later)

Password – Used for Proxies that require authentication. (this can be left blank and the user will be prompted later)

AuthType – 0 indicates the proxy does not require authentication.
1 indicates the proxy requires authentication

Importing the Proxy.ini file

To import your proxy.ini file, use the Settings and Proxy Settings menu.

Figure 35: Proxy Settings Menu

Dynamically VPN Connect

For companies who want users to VPN connect behind a proxy server, the AT&T Global Network Client can dynamically detect a proxy server in the network path and VPN connect using Transparent Tunneling (SSL-T). With this feature you can roam from a non-proxy site to a proxy site and not have to manually change any settings on the AT&T Global Network Client. This option only works with AT&T VPN Servers (VIG/SIG/Gateway) terminating the connection.

This option requires central configuration and configuration in the AT&T Global Network Client. You must be authorized for both SSL and IPSec services in the AT&T Administration Server and the **SSL AT&T Global Network Client Allow Proxy** setting must be set to **Y** in the AT&T administration server. To configure this option in the AT&T Client, click **Settings** menu; then **Login Properties**. Click the **Preferences** tab; click **Override Defaults**; scroll down and click **Use SSL Tunneling when a proxy server is detected** in the **VPN Details** section.

If your company prefers to use IPSec but would like a failover service that will traverse more network paths, the AT&T Global Network Client can dynamically failover to Transparent Tunneling (SSL-T) service if the IPSec connection fails for any reason. In the AT&T administration server, set the **AT&T Global Network Client IPSec Failover** setting to **Y**. To configure this option in the AT&T Global Network Client, click **Settings** menu; then **Login Properties**. Click the **Preferences** tab; scroll down and click **Use SSL Tunneling when an IPSec connection cannot be established** in the **VPN Details** section.

Best VIG Selection

The **AT&T Global Network Client** uses both **IPSec** and **SSL** for secure, encrypted tunneling. During session establishment time the Client learns which VIGs it is provisioned to by sending a query to Service Manager. The Client then selects which specific VIG it will connect to at this time based on a "health check" algorithm. The algorithm takes into account both the latency to the VIGs and the "busy-ness" of the VIGs.

A standard way that user profiles are configured is for the Client to first attempt to establish a VPN tunnel to the best VIG based on results of a health check. If the client fails to connect to the first VIG in the list using IPSec then SSL, an attempt will be made using IPSec then SSL to the other VIG. The AGN Client will continue alternating between both VIGs for the entire connection attempt, for example:

vig 1 – blade/ip address 13 - IPSec

vig 1 – blade/ip address 13 - SSL

vig 2 – blade/ip address 4 - IPSEC

vig 2 – blade/ip address 4 - SSL

vig 1 – blade/ip address 9 - IPSec

vig 1 – blade/ip address 9 - SSL

...

The operating theory here is that the IPSec tunnel likely failed due to a firewall/filter issue at the client-side and 'falling back' to SSL will likely resolve the issue as SSL has a much easier time of traversing firewalls. This connection activity is automatic and transparent to the user.

VIGs are deployed in specific pairs and there is at least one pair of VIGs in each geographic region. For ANIRA, customers are typically provisioned to a single pair of VIGs. One does not pick any two VIGs to use but rather a specific VIG pairing. For example, in the US there are multiple VIGs deployed in 10 cities and users are normally provisioned to one pair. Some customers may be provisioned to multiple pairs in unique situations to address an issue such as capacity.

IPv6 Support

Support for the following IP version tunneling scenarios is available when using IPSec or SSL-T VPN terminating to an AT&T VPN Server (SIG or VIG):

- IPv6 over IPv4
- IPv6 and IPv4 over IPv4
- IPv4 over IPv6
- IPv4 and IPv6 over IPv6

Tunneling is automatic and transparent to the user. IP Address configuration occurs during tunnel setup when the VPN server assigns the VPN Client address(s).

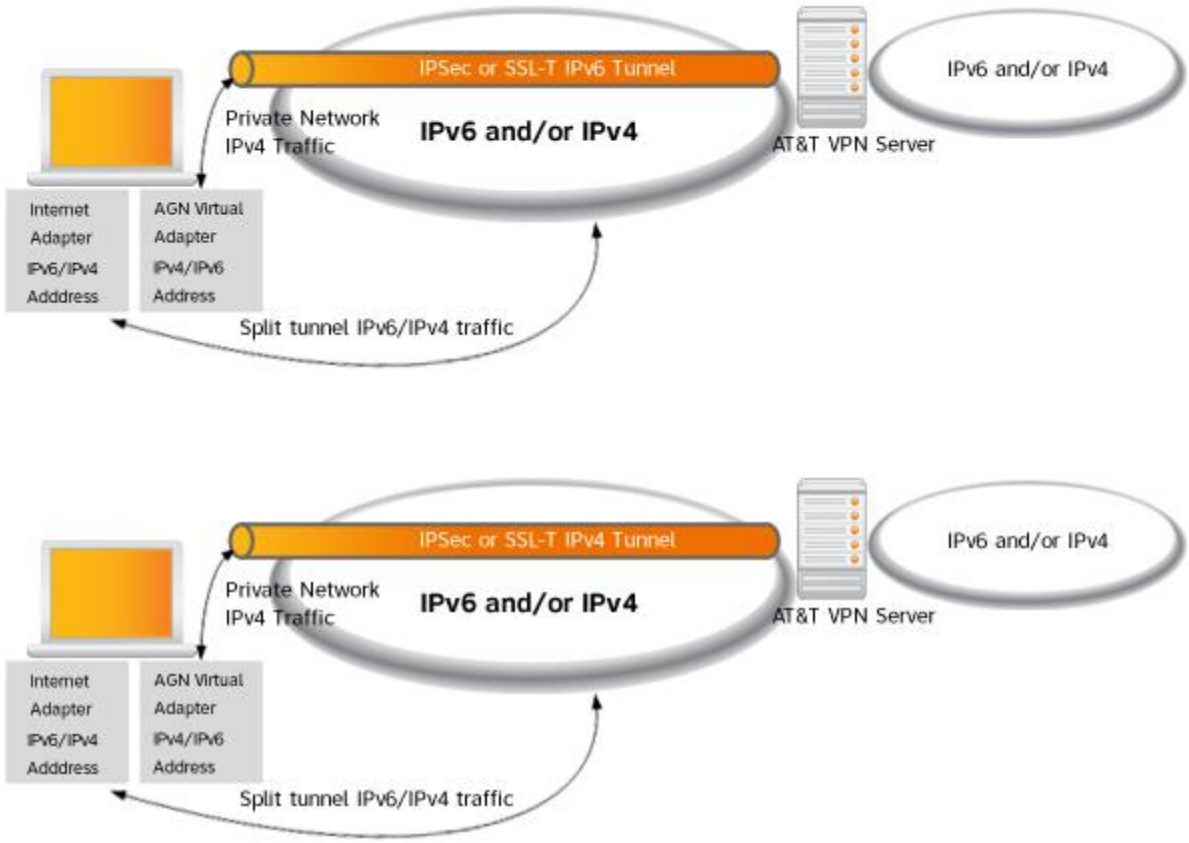


Figure 36: IPv6 Support

IP version preference

The AT&T Global Network Client can be configured to prefer an IP version for establishing a VPN connection when connected to an IPv4/IPv6 dual stacked network. The default preference is currently IPv4. This setting is centrally configured through the AT&T administration server.

IP version failover

Granular control over the number of VPN connection attempts to make with the preferred IP version is supported. This setting is only pertinent on IPv4/IPv6 dual stack networks. The default number of VPN connection attempts per IP version is defaulted to 2. This setting is centrally configured through the AT&T administration server.

For example, if there are 3 VPN servers and IPv6 is preferred. The AT&T Global Network Client's connection attempt list would be ordered as follows:

1. Attempt VPN server 1 using IPv6.
2. Attempt VPN server 2 using IPv6.
3. Attempt VPN server 1 using IPv4.
4. Attempt VPN server 3 using IPv6.
5. Attempt VPN server 2 using IPv4.
6. Attempt VPN server 3 using IPv4.

Integrating with Third Party Software

Although the AT&T Global Network Client contains an integrated VPN client that supports multiple tunnel endpoints, some customers prefer to use a third-party VPN client and use the AT&T Global Network Client to establish an underlying Internet connection. Examples of third party software VPN clients that the AT&T Global Network Client integrates well with are Cisco AnyConnect®[6] and Nortel VPN client.

In other cases, the AT&T Global Network Client is used to establish the VPN connection and third party software is used as the underlying Internet connection. This section describes how the AT&T Global Network Client interacts with some third party software clients.

ThinkVantage® Access Connections™[7]

ThinkVantage® Access Connections™ is a connectivity assistant program for your ThinkPad computer. When a Wi-Fi or mobile connection is made, there can be contention between the ThinkVantage Access Connections client and the AT&T Global Network Client.

The user can specify which software client is in control of the connection by clicking on **Login Properties**, **Preferences** tab, and checking the box next to **Disable Lenovo Access Connections** under the **When this program starts** section. This checkbox is only visible when the Access Connections software is detected on the user's computer.

If this checkbox is checked (default), the AT&T Global Network Client will assume control of both Wi-Fi and mobile access on startup and will disable the Access Connections software if running. If the AT&T Global Network Client does disable Access Connections on start up, it will re-enable it before exiting.

If this checkbox is *not* checked, the AT&T Global Network Client will disable its own Wi-Fi and mobile control and allow Access Connections to control the network access.

WireShark® and Microsoft Network Monitor

Network traffic analysis tools, WireShark®[8] and Microsoft Network Monitor are supported with AT&T Global Network Client 9.1 and later. The network traffic will be logged to the dynamic VPN IP address of the AT&T Global Network Client VPN session being monitored. The MAC address of the VPN adapter is statically defined in the AT&T Global Network Client and will be the same across all instances of the AT&T Global Network Client on the network, the IP address must be used to identify individual machine activity.

[6] Cisco AnyConnect® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.
[7] ThinkVanatage® and Access Connections™ are trademarks of Lenovo in the United States, other countries, or both.
[8] Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation

Help/Customer Support

Support Forum

AT&T offers an on-line support forum for topics related to the AT&T Global Network Client. Access the forum via your web browser at:

http://bizcommunity.att.com

You must register as a user to access all features of the support forum. You can post questions for AT&T development and support personnel as well as access support documents and presentations via the forum.

Contact AT&T

In the **Help** panel on the main window, click **Contact customer support** to open the **Customer Support** window containing your AT&T help desk phone numbers.

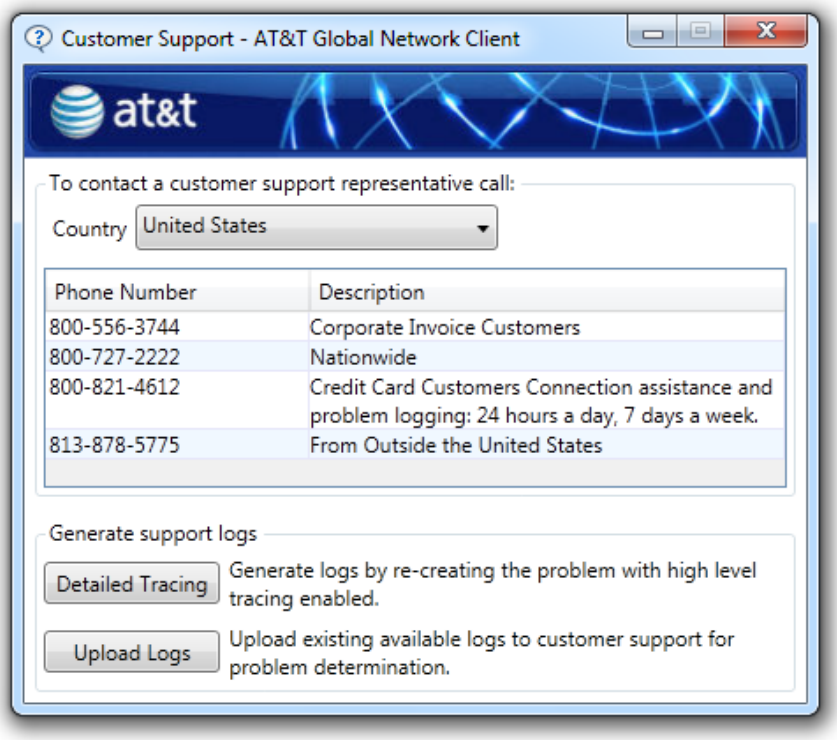


Figure 37: Customer Support Window

In addition to calling for support you can click **View support log…** to open a web page with useful information about your installation of the AT&T Client.

Click **Close** to return to the AT&T Client.

Frequently Asked Administration Topics

Using Digital Certificates for Authentication

AT&T offers the use of x.509v3 Entrust and Microsoft digital certificates to authenticate users for Internet and Managed VPN services.

Use of certificates may require custom software development at a cost to our customers. Contact your AT&T account team to engage product management for assistance.

AT&T does not create, distribute or maintain user digital certificates. You must support your own digital certificate infrastructure. AT&T uses the common name as the user ID / unique identifier; therefore you must enforce uniqueness on this attribute. The custom client development team can work with you to use a limited list of other attributes as well. Contact your AT&T account team for further assistance with Digital Certificate Authentication.

When using Digital Certificates for authentication you must use Public Properties to set them correctly for use. See the Customizations Chapter on page 37 of this guide for additional information about Public Properties.

Additionally, the use of Digital Certificates must be configured centrally in the AT&T administration server.

If your company is using more than one certificate, the user will be prompted to select which signature certificate to use for their connection (encrypted certificates are not displayed).

Troubleshooting Installation

The AT&T Global Network Client *executable* (not MSI file) installation package automatically generates an installation log file and places it in the %temp% folder. The log file name will mimic the installation file name, with .log replacing the installation file extension.

Appendix A: Central Configuration

The AT&T administration server stores the configuration information for all users, including service type and service options. The AT&T Global Network Client interfaces with the AT&T administration server to retrieve values set by you, the Customer Account Administrator. The AT&T administration server supports a tiered architecture. You can set values at three levels: Model, Account, or UserID. Models are thr highest level and can apply to multiple accounts. Accounts are the second level and typically have many userids assigned to an account. User IDs are the lowest level and typically are assigned to a single end user.

Configuration of the values can be done by your AT&T representative or by you, via an AT&T provided administration tool, AT&T Global Network Services Customer Support Tools and Reports, located at http://globalnetwork.support.att.com. Click the link for **Encrypted access to web tools and reports** under the AT&T Managed Network Services (MNS) Tools/Reports section located on the main page. Enter your **Account**, **User ID** and **Password** to login. After login select **Administration Tools for AT&T Service Manager** from the drop down list on the top of the screen. Click **Guide** on the **Navigation Menu** on the left hand side of the screen to access the "Administration Tools for AT&T Service Manager Guide". All AT&T Accounts/User IDs are not authorized to use the tools; and access requires configuration by AT&T. Contact your AT&T representative for additional assistance using AT&T Global Network Services Customer Support Tools and Reports.

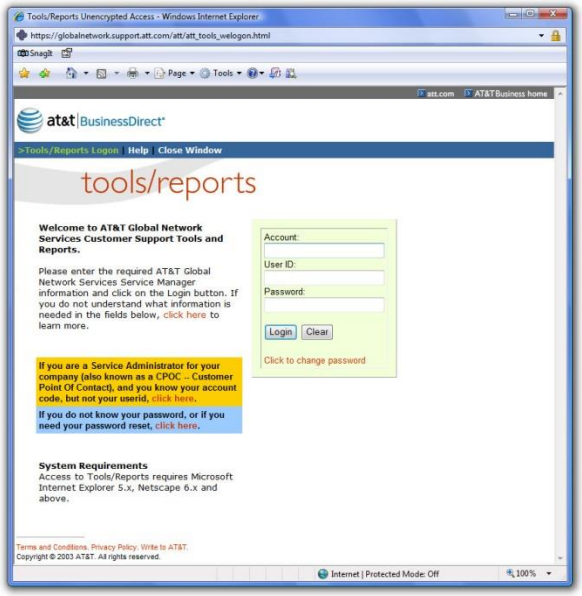


Figure 38: AT&T Administration Server Configuration Tool

The AT&T Global Network Client configuration values in the AT&T administration server are shown in the table in the next section. Inaccurate configuration of central values can produce unexpected results and errors for your users, questions about any of the individual fields should be directed to your AT&T account representative prior to making changes.

Central Configuration Values

Retrieval of Network Settings Over an Existing Internet Connection

For Internet over broadband connections the AT&T Global Network Client will query the user to retrieve the network settings. After connecting, if a profile containing an account and user id is active, the default service will be "Internet" and the connection will take place over an existing Internet connection.

The AT&T Global Network Client will retrieve the following fields from the Service Manager and save to the user profile:

- Default Service
- Wi-Fi bitmask
- Dynamic Customization info (ftp server and ftp path)

AT&T Administration Server Client Configuration Values

Field	Info	Default	Value/Behavior
General Service Options			
Activity Threshold Timeout	Optional Will inherit from model	Blank	Set to number in range: 1-60 Specifies a numeric value in minutes which defines the maximum time which can transpire before the AT&T Global Network Client will timeout the user.
Activity threshold Bytes	Optional Will inherit from model	Blank	Set to number in range: 50-50,000 Specifies a numeric value in bytes defining the minimum size of an IP packet which would indicate user activity (minimizes chatty applications such as IM retaining a connection after actual user activity has stopped)
Authentication Method	Required	R	D – Radius L – LDAP R – RACF S – SecurID W – SafeWord

Field	Info	Default	Value/Behavior
Default Service Type[9]	Required		03 = LAN Dial 06 = Internet 07 = Async Terminal Services (ATS) 08 = Async Pass Through 0A = VPEF (VCOM, XPC) 0C = Fixed IP 0F = TCP Clear 10 = Managed Tunneling Service using IPSec (MTS/IPSec) 12 = Managed Tunneling Services using IPSec with Dual Access
DNS	Recommended	Blank	Specifies Primary & Secondary DNS for your account Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.
Domain Name	Recommended	Blank	The domain name to be active for the session. Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.

[9] See Additional Service Information Section of this guide for descriptions.

Field	Info	Default	Value/Behavior
Domain Search Suffix 1-5 –	Optional	Blank	Up to 5 domain suffixes may be entered to aid in web address searching (for example, att.com). Beginning with Version 8.0, setting this value to Blank will remove any previously cached customized value from the AT&T Global Network Client.
Help Desk Number	Optional	Blank	xxx-xxx-xxxx - Defines the Help Desk Phone number that will appear in the AT&T Global Network Client
Local Subnet Access	Allows users that are not configured for Dual Access or split tunneling to access resources on their directly connected subnet	N	Y = Allow local subnet access N = Do not allow local subnet access
Network Awareness	Optional	N	When set the AT&T Global Network Client will use values in the NetworkAwareness.xml file to define actions for networks. (see Network Awareness Customization) Y=Enable Network Awareness and use values in xml file N=Disable Network Awareness, ignore xml file.

Field	Info	Default	Value/Behavior
Persistent Connection	Optional	Y	Enables the Persistent Connection feature Y=Allow Persistent Connections N=Do Not Allow Persistent Connections
Save Password Expiration Interval	Optional	0	Defines the number of hours after which a user is forced to reenter their password, even if the "Save Password" option is enabled in the AT&T Client. 0=Never #=Number of hours until the user is forced to enter their password
Time For Password to Expire			Can only be updated by AT&T. support personnel
WINS	Recommended	Blank	Specifies the primary and secondary WINS values for your account.
AT&T Global Network Client Firewall			
Enable AT&T Global Network Client Firewall	Optional Will inherit from Model	Blank	Y – AT&T Global Network Client Firewall is enabled N – AT&T Global Network Client Firewall is disabled
User Controlled Firewall	Optional Will inherit from Model	Blank	Y – User has modify access to Firewall Settings Window. N – User can not modify settings on Firewall Settings Window.
AT&T VPN			

Field	Info	Default	Value/Behavior
AT&T Global Network Client IPSec Failover	Optional	Blank	Y– Dynamically failover to Transparent Tunneling (SSL-T) service if the IPSec connection fails for any reason. N – Do not failover to Transparent Tunneling
Allow Access List Exceptions	Optional	Blank/N	Y = Allow users to define exceptions to VPN access list N = Do not allow users to define exceptions to VPN access list
Allow User Switches[10]	Optional	Blank	Y = Allow computer to remain VPN connected under current Windows user account when performing Fast User Switch (client remains running) or User Logoff (client will exit but connection persists) on local PC. N = Exits client and terminates VPN session when performing Fast User Switch or User Logoff on local PC.

[10] Keeping a VPN connection active after a Fast User Switch or User Logoff can produce unexpected results and is a potential security risk; therefore it is recommended this value only be set to Y for short term troubleshooting purposes.

Field	Info	Default	Value/Behavior
IPSec VPN Tunnel Settings			Set Encryption to: DES Triple DES AES 128 AES 192 AES 256 Set Authentication to: HMAC – SHA1 HMAC – MD5 Set Compression: LZS
Negotiate UDP	Optional	Blank	Y = Negotiate UDP Encapsulation N = Do not negotiate

Field	Info	Default	Value/Behavior
SSL AT&T Global Network Client Allow Proxy –	This option only works on AT&T VPN Servers (SIG/GIG - MTS-IPSec and MTS-IPSec DA) connections. You must profile your users for AT&T VPN Tunneling Services SSL, AT&T VPN Tunneling Services IPSec, and Transparent Tunneling (SSL-T).		Y = Dynamically failover to SSL-T service if a proxy is detected. N = Do not dynamically failover to SSL-T if a proxy is detected.
Tunnel Dual Access	Optional	Blank	Y = Managed Tunneling Service Dual Access is enabled and the user is allowed to access Internet locations. N = Managed Tunneling Service Dual Access is disabled and the user can not access Internet locations.

Figure 39: Central Configuration Values Table

Additional Service Information

FixedIP

The FixedIP service provides remote access to your company's private Intranet via a network-based VPN to a VPN server on your Intranet. The assigned IP address can be static or assigned from a customer-specific address pool on your VPN server. The service supports multiple protocols and provides centrally managed network-based subnet filtering and network-based firewall security. This is a network based VPN service and no VPN software is required on the workstation.

FixedIP DualAccess

The FixedIP DualAccess service is the same as the FixedIP service with the addition of being able to access to the Internet using the same network connection.

Managed IPSec VPN

Managed IPSec VPN provides remote access to a company's private network via an end to end IPSec VPN from the AT&T Global Network Client to a VPN server (AT&T SIG or Cisco) on your company's private Intranet. The service provides centrally managed subnet filtering on the workstation and local firewall security as well as centrally managed network-based subnet filtering and network-based firewall security.

Managed IPSec DualAccess VPN

The Managed IPSec DualAccess VPN is the same as Managed IPSec VPN with the addition of being able to access the Internet using the same network connection.

Managed IPSec Authentication Method

The authentication for the VPN is provided by the AT&T Global Network authentication server. The authentication can be performed directly by the Central Authentication Server or the Central Authentication Server can proxy to/verify the request with a customer managed authentication server.

Managed SSL VPN

The SSL VPN service, also known as Transparent Tunneling, traverses customer site proxies and firewalls using SSL to minimize network configuration changes normally required for IPSec VPN tunneling. SSL VPN is useful for connecting from locations that block IPSec or only allow Internet access through a proxy server. AT&T SSL VPN is terminated by an AT&T SIG VPN Server.

Managed SSL Dual Access VPN

The Managed VPN SSL DualAccess VPN is the same as SSL VPN with the addition of being able to access the Internet using the same network connection

Appendix B: Third-Party Firewall Support

Network Firewalls

You may need to alter your network firewall configuration to allow AT&T Global Network Client management and VPN traffic to route properly. The table below lists the required changes.

Source	Destination	Protocol Port Source	Protocol Port Destination	Action	Reason for opening
ALL SERVICES					
Local PC	144.160.245.70	TCP:1024 +	HTTP:80	Allow	SLA Data collector
Local PC	144.160.245.71	TCP:1024 +	HTTP:80	Allow	SLA Data collector
Local PC	12.120.7.222 12.120.7.223 12.120.23.222 12.120.23.223	TCP:1024 +	HTTP:80	Allow	Hotspot Directory Updates
Local PC	SMX List	TCP:1024 +	HTTP:80 (443)	Allow	Authentication
Local PC	165.87.194.246	TCP:1024 +	TCP:21	Allow	Passive FTP for AGNC, Certificate and Firmware updates
Local PC	12.154.55.131	TCP:1024 +	HTTP:80 (443)	Allow	Log upload server
IPSec					
Local PC	VPN Tunnel Server IP Addresses	ESP (50)	ESP (50)	Allow	IPSec
VPN Tunnel Server IP Addresses	Local PC	ESP (50)	ESP (50)	Allow	IPSec
Local PC	VPN Tunnel Server IP Addresses	UDP:500	UDP:500,	Allow	IPSec (IKE)
VPN Tunnel Server IP Addresses	Local PC	UDP:500	UDP:500,	Allow	IPSec (IKE)
Local PC	VPN Tunnel Server IP Addresses	UDP:1024+	UDP 4500	Allow	IPSec with NAT Traversal

VPN Tunnel Server IP Addresses	Local PC	UDP 4500	UDP:1024+	Allow	IPSec with NAT Traversal
AT&T Network-Based IP VPN Remote Access service					
Local PC	VPN Tunnel Server IP Addresses	UDP:1024+	UDP:5080	Allow	AT&T VIG Server Health Check
SSLT					
Local PC	VPN Tunnel Server IP Addresses	TCP:1024 +	TCP:443	Allow	SSL

Figure 40: Network Firewall Configuration Table

SMX List

Last Updated 4/6/2020

Name	Region	Location	Internet Address
US21R	US	Allen, Tx	204.146.172.230
US22R	US	Redwood City, CA	204.146.166.107
US25R	US	Ashburn, VA	12.67.9.15
GB03R	EMEA	London	32.112.51.115
DE03R	EMEA	Frankfurt	32.112.50.131
NL03R	EMEA	Amsterdam	195.212.144.21
HK02R	AP	Hong Kong	122.248.141.245
JP03R	AP	Tokyo	210.88.1.199
JP04R	AP	Osaka	210.88.144.43

Figure 41: SMiX Address Table

Personal/Client Firewalls

The AT&T Global Network Client program uses IP to communicate with other computers on the network just like other network programs (such as web browsers and e-mail programs). Third-party personal firewalls can prohibit certain types of network communication. Running multiple firewalls on users' PCs can cause difficulties and is not supported by AT&T.

Some firewalls must be configured to allow the AT&T Global Network Client to communicate with the network in order for client features to function properly. The table below lists the required changes. More information about the features is found in the list below the table.

Feature	Protocol: Port
Disconnect Warning	UDP:7000
SLA Data Collection, Hotspot Directory Updates, and Dynamic Customization Updates	HTTP/TCP:80

Figure 42: Client Firewall Configuration Table

Hotspot Directory and Dynamic Customization Updates

The AT&T Global Network Client periodically checks for and downloads updates to the software using HTTP (TCP port 80).

SLA data collection

The AT&T Global Network Client uploads data about all connection attempts using HTTP (TCP port 80) to a server after connecting. This data is used for measuring SLAs (Service Level Agreements). If the SLA data is not collected, AT&T will not provide service-level guarantees.

AT&T requires companies to add policy rules to their firewalls to allow SLA data to be sent to those servers.

Appendix C: Using the Command Line Program

The AT&T Global Network Client can be started using the command line program. This program accepts the following command-line parameters:

AT&T Client

netclient.exe [-connect] [-login=LoginProfile] [-password=Password]

netclient.exe [-login=LoginProfile] [-password=Password]

netclient.exe [-exit | -exitnow]

netclient.exe [-disconnect | -disconnectnow]

netclient.exe [-help]

netclient.exe [-password=Password]

netclient.exe [-timeout=[IdleTime] [,[DurationTime] [,[ThresholdTime] [,[ThresholdBytes] [,WarnTime]]]]]

Parameters[11]:

-connect

Displays the Login window and starts a connection if the password is saved or if the password is entered as a command-line parameter (-password).

-disconnect

Disconnects after prompting for confirmation if necessary.

-disconnectnow

Disconnects with no confirmation.

[11] Note: Some of these parameters can be combined on the same command-line (for example 'netclient.exe -connect -login="my Internet login"'.

-exit

Closes this program and prompts for confirmation before disconnecting if necessary.

-exitnow

Closes this program with no confirmation before disconnecting.

-getstatus

Returns a code to indicate the state of this program. This parameter is only useful when invoked from a program that can interpret the return code.

Status codes returned by –getstatus:

NotRunning	0
Initializing	100
NotConnected	200
BeforeConnecting	300
BeforeConnectAttempt	350
VerifyExistingInternetConnection	370
VerifyExistingProxyConnection	375
BeforeWiFiConnect	720
ConnectingWiFi	730
AuthenticatingWiFi	740
AfterWiFiConnect	750
BeforeEthernetConnect	756
AuthenticatingEthernet	758
AfterEthernetConnect	760
PauseWhileConnectingForTesting	765
Phase1Authenticate	770
NoPhase1OrPhase2Needed	780
BeforeTunneling	800
Tunneling	900
AuthenticatingTunnel	1000
AfterTunneling	1100
AfterConnecting	1200
ConnectedNoVPN	1250
ReattachingToVPNServer	1270
AfterReattachingToVPNServer	1275
Connected	1300
BeforeDisconnecting	1400
Disconnecting	1500

AfterDisconnecting	1600
Disconnected	1700
Exiting	1800

-help

Displays this help window.

-login=LoginProfile

The specified LoginProfile is made the current login profile. If LoginProfile contains spaces it should be enclosed in double-quotes (for example: -login="my Internet login").

-password=Password

Sets the password for the current login profile, as if Password was entered on the Login window.

-timeout

Changes the timeout properties. Five separate parameters may be included an idle time, a duration time, a threshold time, threshold bytes and a timeout warning time. All of the times are in seconds. See Timeout Options for a description of these options. Any of the five parameters can be left empty to indicate no change or set to zero to disable the timeout. Invalid values will be ignored.

NOTE: The idle-timeout parameter has become obsolete and is ignored in version 7.6 and higher. The idle-timeout parameter was left in place to remain compatible with other programs that previously passed that parameter.

Examples:

netclient.exe -timeout=,,,,0

Leave the timeouts unchanged but disable the timeout warning.

netclient.exe -timeout=,3600,,,60

Set a duration timeout of 1 hour and display a warning 1 minute before disconnecting.

AT&T Global Network Client Firewall

netfw.exe[-firewall=on|off]

Parameters:

-firewall=on|off

Turns AT&T Global Network Client Firewall on or off.

Index

A

Access Control List, 70
Accessibility Features, 60
AT&T Administration Server, 84
AT&T Authentication Server, 11
AT&T Client Installation Package, 16
AT&T Global Network Client Firewall, 10, 68
  Disabling, 69
  FIREWALL_STATE public property, 54
  Operating Modes, 68
  Settings Window, 69
AT&T Managed Services, 10
AT&T Service Manager. *See* AT&T Authentication Server
Authentication, 10
AutoConnect, 29
Automatic Connection, 18
Automatic Updates, 31, 95
  Other programs, 25
Autostart, 23

C

Central Configuration. *See* Configuration
Command Line Options, 44
Configuration, 18, 84
  Advanced, 20
  Central, 20
  Login Properties, 20
Connection Sequence, 18
Customizations, 37

D

Default Service, 22
Digital Certificates, 11, 83
Distribution, 16
  MSI, 16
DNS, 22
Domain Suffix, 22
Dynamic DNS, 72

E

Editions, 15

F

Fenced Internet, 71
Firewall Settings, 93
FixedIP, 92
FixedIP Dual Access, 92

H

Help, 82

I

Installation, 15
  Checklist, 14
  Editions. *See* Editions
  Requirements, 13
Installation Log, 83
InstallShield, 15, 37
Internet Explorer Proxy Settings, 26
IPSec, 72
IPSec Encryption, *73*

L

LDAP. *See* Digital Certificates
Lightweight Policy Enforcement, 10, 62, 64
  Threshold, 63
Login Properties. *See* Configuration
LPE. *See* Lightweight Policy Enforcement

M

Managed IPSec Dual Access VPN, 92
Managed IPSec VPN, 92
Managed SSL Dual Access VPN, 92
Managed SSL VPN, 92
Managed VPN IPsec, 72
Managed VPN Services, 10
Microsoft IPSec, *73*
Multi-Homing
  Preventing, 29

N

NAT Traversal, *73*
Network Firewall Configuration, 93
Network Service

Default. *See* Default Service

P

Persistent Connections, 27
Preferences, 23
Profile Manager, 21
Profiles, 20
Program Control, 62
Proxy, *74*

R

RADIUS, 11
Remove, 33

S

SafeWord, 11
SecurID, 11, 19
Sharing Local Resources, 72
SoftToken, 11
Software Updates. *See* Automatic Updates
SSL, *74*
System Requirements. *See* Installation

T

Timeouts, 26
Token, 19
Trusted Domain Customization, 49

U

UDP Encapsulation, *74*
Uninstall, 33
Upgrading Client Software, 17

W

Windows Installer, 16, 37
  Features, 37
  Public Properties, 39
  Shortcuts, 44
  Transform, 45
WINS, 22

X

x.509, 83