# AT&T Global Network Client

Version History

May 2023



# AT&T Global Network Client Version History

## Version 10.8.1 – May 12, 2023

- Add the ability to lock the account in the login dialog
- Update SQLite to 3.41.2
- Address concerns, including all discovered by Veracode scan
- Bug fix: Problem with hard token
- Bug fix: When creating a support log the last part of the net client log is missing
- Bug fix: VNIC is not getting an IP address assigned when using fixed IP and dual access
- Bug fix: Various minor bugs addressed

## Version 10.8.0 – February 28, 2023

- Add DH14 for Cisco Firepower ASA IPSec proposal
- Add the ability to run LPE elevated
- Add the ability to verify the product and the products version for Is Running rule
- Address Veracode Issues
- Prevent the client from installing on Windows 10 1703 and older.
- Replace RSA BSAFE library with Windows Crypto Next Generation API
- Replace the Entrust certificates with OpenSSL certificates
- Update OPSWAT OESIS to version 4.3.3314 - 2023.1.3.29
- Update SQLite to 3.40.1
- Bug fix: Client crashes while trying to create a support package
- Bug fix: Getting an Error using fenced firewall rules
- Bug fix: Select the last used certificate by the user
- Bug fix: Various minor bugs addressed

## Version 10.7.3 – September 8, 2022

- Add capability to allow configuration settings to be applied at the root level, impacting all profiles
- Enhance the authentication information passed to SMx/Service Manager to allow for more flexible AGN Client version control
- Improve Registry updates to display timestamps in an easier to read manner
- Bug fix: Change to use a different Windows time zone function to avoid dependency on a function that was made available with a 2019 Windows update

## Version 10.7.2 – August 8, 2022

- Added the ability for customer to modify setting for all customization profiles (root profile) instead of individually
- Update .NET SQLite to 1.0.116

## Version 10.7.1 – July 28, 2022

- Improved certificate handling when multiple certificates shared the same expiration date
- Update .NET Framework to 4.8
- Bug fix: Add a new user without copying sometimes would copy existing profile data anyhow
- Bug fix: Lightweight Policy Enforcement would not complete the validation steps in certain cases
- Bug fix: Crash occurred when closing and then restarting the application within 5 seconds
- Bug fix: Clean up reporting by removing unnecessary data in the version number field
- Bug fix: Lightweight Policy Enforcement validation was not working correctly in some cases, requiring a change in the logic

## Version 10.7.0 – June 14, 2022

- Added: Improved logging capability
- Added: Logic for more reliable connections to AT&T authentication and reporting servers
- Added: Added customization option to allow a change to the IKE rekey interval
- Added: New option for 5Mb for threshold disconnect logic
- Added: Improved security with HTTPS for the updates of dynamic customization and Wi-Fi access point databases
- Added: Improve the update processing for the dynamic customization and Wi-Fi access point databases
- Added: Updated Lightweight Policy Enforcement
- Added: Upgrade to SQLite 3.38.2
- Added: Improve the update processing for the dynamic customization and Wi-Fi access point databases
- Bug Fix: Activity threshold timeout
- Bug Fix: Item added to auto start section could get stuck at bottom of list
- Bug Fix: Command line connect operation has been fixed
- Bug Fix: Connections through a proxy were not working correctly
- Bug Fix: Corrected the Lightweight Policy Enforcement message for customized clients
- Bug Fix: Create new profile option was not properly saving profile
- Bug Fix: Various minor bugs addressed
- Updated code for increased security as suggested by Veracode source code security analyzer and other AT&T scans
- Removed non used elements of the code

## Version 10.6.0 – December 15, 2021

- Update OPSWAT Lightweight Policy Enforcement (LPE) to provide support for new applications and new versions of existing applications
- Change the file system directory used for OPSWAT LPE for better organization
- Update registry search for Outlook path to allow for emailing of support logs
- Update localization code to allow AGN Client to continue support for Spanish, German, French, and Japanese language
- Disable IPSec DES and MD5 algorithms in the interest of enforcing better security. These algorithms have been previously disabled in the AT&T configuration servers.
- Enhance logs to clearly indicate when Windows 11 is used
- Enhance LPE logging to provide more detail to assist support teams with troubleshooting

- Bug Fix: When an incorrect password was entered followed by entry of a valid password the valid password was still showing as an incorrect password
- Bug Fix: Login Properties did not display correctly when using Secure Desktop (PLAP)
- Bug fix: Update SMRS report data feed to reflect correct service type when using TLS VPN

## Version 10.5.1 – July 29, 2021

- Bug fix: Crash occurred with specific LPE rules

## Version 10.5.0 – June 24, 2021

- Completed moving all remaining databases to SQLite
- Address security and vulnerability concerns, including all discovered by Veracode scan
- Updated OPSWAT Lightweight Policy Enforcement to provide support for new applications and new versions of existing applications
- Update SQLite to version 3.35.5
- Bug fix: Deleting of saved certificate was not working correctly
- Bug fix: Translation to non English languages was not always accurate
- Bug fix: VIG/SIG VPN endpoint selection algorithm logic
- Bug fix: Client was incorrectly creating multiple profiles when using certificates as primary authentication

## Version 10.4.0 – March 31, 2021

- Upgrade LPE Rules, Profiles, Preferences, Auto Start, and Config Settings dbase type database to SQLite.
- Updated the config.xml processing for changes in the database and LPE enhancements.
- Add LPE support for Drive Encryption, Data loss prevention, and Patch Management.
- Removed support for deprecated technologies including Gopher, Socks proxy.
- Fix database error on upgrade from Clients older than 9.9.0.
- Address Veracode Issues.

## Version 10.3.3 – December 30, 2020

- Upgrade Bookmark, SLR, SMRS, and Event dbase type database to SQLite.
- Fixed inconsistent display of login window and update window graphics.
- Address Veracode Issues.
- Updated OPSWAT to support most current list anti-malware and firewall products.
- Check the config.xml version when checking if new install.
- Update SQLite to 3.32.3. due to Security Vulnerability.
- MFA timeout is retransmitting authenticate.
- Disable activity threshold timeout by default.
- Add to the config.xml the ability to select the machine and user certificate to use partial name.
- Improve the error messages for the asset validation checks.
- Fixed application crash.
- Hide service selection panel.
- Add office proxy.

## Version 10.3.0 – March 31, 2020

- Fixed inconsistent display of login window and update window graphics
- Enhanced logging to assist AT&T support team with troubleshooting
- Updated OPSWAT to support most current list anti-malware and firewall products
- Updated AT&T logos to current brand identity
- Removed support for deprecated technologies including VPN Mobility tab, Socks, Hummingbird Socks
- Removed support for Windows 7 (no longer supported by Microsoft)

## Version 10.2.0 – January 27, 2020

- Added SHA2 support and Diffie-Hellman groups 14 and 15 support to provide better security options. Disabled support for SHA-2 DES3 and DES
- Improved display of certificates related to smart card authentication. Certificates are now sorted in order of time remaining before expiration
- Updated OPSWAT version and Lightweight Policy Enforcement database to ensure compatibility with the latest software releases
- Updated cellular connectivity handling to allow Windows to manage the connection instead of the AGN Client
- Logging improvement to capture ipconfig /all and to capture ping results related to certain errors to assist AT&T support teams with troubleshooting
- Ability to add a hyperlink/url to the message window that appears upon connection (if configured)
- Added a capability to easily locate the account and user id to aid customers when contacting the AT&T helpdesk
- Removed logging of certain session information for better security
- Removed password "change" option for RADIUS authentication
- Bug fix - Client crashed in certain cases when using RSA to login two times on consecutive connections
- Bug fix - Session Duration Timeout improvement. Added a notice to the user prior to the disconnect occurring
- Bug fix - VPN capability to Cisco ASA was fixed
- Bug fix - The client will now correctly recognize that RSA Soft Token is installed (i.e. 32 bit RSA software is installed on 64 bit Windows)
- General code cleanup, removal of features that are no longer relevant or available
- Security and vulnerability fixes

## Version 9.9.1 – January 23, 2019

- Updated Lightweight Policy Enforcement
- Updated WISPr probe URL (changed to eaccess-cdn.att.com) used for hotspot authentication
- Bug Fix to prevent crash when changing password
- Bug fix for "do not allow save password" which allows Administrators to prevent users from saving passwords

## Version 9.9.0 – November 8, 2018

- Added VPN tunnel public IP address to SMRS reports

- Reduced installation size significantly - Wi-Fi hotspot locations are now downloaded during the update process
- Improved centralized management for certificate authentication
- Improved ease of use for certificates used for user authentication
- Updated Lightweight Policy Enforcement
- Improved Wi-Fi hotspot update process
- Improved logging consistency
- Improved logging and status display of TLS1.1 or TLS1.2 connections
- Simplified and cleaned up code by removing components that are no longer required
- Other bug fixes and security improvements

## Version 9.8.3 – April 30, 2018

- Updated Lightweight Policy Enforcement
- Improved hotspot directory update process by replacing a single server accessed by IP address with multiple servers accessed using a URL
- Remove dial options as dial access is being sunset
- Bug Fix: Prevent crash found during some password change scenarios

## Version 9.8.2 – February 28, 2018

- Updated Lightweight Policy Enforcement
- Revised software update logic to remove checks for components that are no longer required

## Version 9.8.1 – November 9, 2017

- Updated to use .Net Framework 4.6 for TLS 1.2 support (for log uploads)
- Updated Log upload function to use TLS 1.2 instead of SSLv3
- Bug Fix: MTU Size
- Bug Fix: Routing of local subnet down VPN tunnel in certain situations

## Version 9.8.0 – September 18, 2017

- Added Multi Factor Authentication support
- Updated Lightweight Policy Enforcement to OPSWAT v4 and update library
- Updated NDIS drivers
- Bug Fix: IPv4 over IPv6 for connections to vVIG
- Bug Fix: Windows 10 DNS issue
- Bug Fix: Probe for Internet access when starting and after disconnecting client
- Bug Fix: Auto Reconnect

## Version 9.7.4 – April 5, 2017

- Updated Lightweight Policy Enforcement library
- Added support for TLSv1.2 for Wi-Fi authentication (WISPRr)

## Version 9.7.3 – February 15, 2017

- Updated Lightweight Policy Enforcement library
- Updated a few English to German translations

## Version 9.7.2 – September 23, 2016

- Support for Windows 10 Anniversary Update (version 1607)
- Updated Lightweight Policy Enforcement library
- Bug fix: Wi-Fi authentication script update
- Bug fix:  Issue with Edge browser launch
- Bug fix:  Issue when Connection history is displayed in Japanese language
- Bug fix:  Crash with region setting/date format change to “Slovakia”

## Version 9.7.1 – April 20, 2016

- Bug Fix: Fix for an issue that was causing the client to crash in French version.

## Version 9.7 – April 8, 2016

- Support for Windows 10.
- Added ability to switch profiles with different authentication types from the Network Logon Windows.
- Added the ability to e-mail the support logs instead of uploading them to AT&T.
- Revised authentication configuration to improve ability to connect to Wi-Fi at certain hotspots.
- Updated Lightweight Policy Enforcement library.

## Version 9.6 – February 2, 2015

- Added Service Manager Reporting (SMRS) support.
- Added Auto Switch Wi-Fi support.
- Renamed Persistent Connections to Auto Reconnect to be consistent with other platforms.
- Auto Reconnect enhancements including new session token for more seamless user experience.
- Wi-Fi authentication updated to v6.

## Version 9.5.1 – June 13, 2014

- Bug Fix: Upload logs issue causing a potential client hang issue.

## Version 9.5 – May 28, 2014

- Support for Windows XP has been removed
- Client will no longer install on Windows XP
- Add support for Gobi 5000 embedded devices
- Remove the splash screen (originally added due to long initial launch times on Windows XP)
- PD logs can now be uploaded to cloud
- Change mobile service selection 3G menu item to 3G/4G (as opposed to LTE)
- When users add Access Point Regions, do not force the user to download all the database files again if they are current
- Include support for latest 3rd party software in LPE
- Consolidate mobility driver installations

- Support program updates from IPv6 FTP server
- Bug Fix: Fix packet loss issue seen with 3DES encryption and heavy outbound, fragmented VPN traffic
- Bug Fix: Fix issue with displaying incorrect encryption method for SSL-T connections
- Bug Fix: Fix mobility driver upgrade installer so it properly installs the current mobility device drivers
- Bug Fix: Ensure the legacy SecureIP service works over an analog dial connection

## Version 9.4.2 – February 27, 2014

- Ensure the client will run even if the machine's .NET config file is invalid
- Correct poor French translations

## Version 9.4.1 – January 20, 2014

- Added support for the Sierra Wireless EM7355
- Enhanced the timeout logic which enables and initializes AGN VNIC Adapter

## Version 9.4 – December 9, 2013

- Require Windows XP SP3
- Require .NET 4.0/4.5
- Consolidate and simplify installation packages
- Remove Save PIN option if soft token software is installed (default behavior)
- Ensure token is installed before prompting user to use software token
- Allow the client to use x64 Authentication providers (software token)
- Turn off AT&T Global Network Firewall by default
- Validate support for EM7700
- Change map preference to use radio button
- Allow program updates from IPv6 FTP server
- Only pin the client icon to the Windows 8 start screen
- Do not require a firewall to be on when using 3rd party hot spots
- Remove legacy mobile device drivers (RIM and Option)
- Consolidate localization files into language subdirectories
- Complete conversion of entire user interface to .NET/WPF
- Customization: Add pre-auth registry check
- Customization: Create a new set of messages for customizing Pre and Post Connect LPE
- Bug Fix: attwifi and partner hotspots are also incorrectly listed as 3rd party hotspots
- Bug Fix: Cellular does not work after NetClient.exe crashes
- Bug Fix: Cellular provider coming back as 'none' in Focus records

## Version 9.3.2 – Oct 10, 2013

- Support for Windows 8.1
- Fix several memory leaks

## Version 9.3.1 – Sep 9, 2013

- Customization: Create a way to prevent closing the client
- Customization: Create a way to hide the Disconnect button

## Version 9.3 – July 5, 2013

- Added support for mobile device GPS features
- Enhanced support for the AT&T Beam (Sierra Wireless 340U)
- Enhancements to the Lightweight Policy Enforcement feature
- Enhancements to the use of digital certificates for authentication
- Enhancements for Wired Ethernet support
- Added the ability to suppress program updates
- Changed ephemeral source ports option to be enabled by default
- Bug Fix: Correct usage of third party authentication providers when do not prompt option is selected

## Version 9.2.1 – April 19, 2013

- Corrected issue running client on workstations in some countries

## Version 9.2 – April 15, 2013

- Added support for the Sierra Wireless 340U (Windows 8 not supported)
- Using .Net 4.5 on Windows 8 devices
- Added the ability to clear the message log using Alt-C on the keyboard
- Added ability to customize help desk support countries and numbers in a drop down.
- Re-architected the Access Point databases for fast updating
    - Remove cellular credential information from access points
    - Add new dialog that allows the user to download new AP database files.
    - Added ability to export all access points from the database.
    - Change the Access Point default sorting to show local first, nationwide second when searching by area code or location.
    - Allow the user and administrators to select geographic regions for which to install access point databases for browsing.
    - Add login preference to select between Yahoo maps and Google maps when viewing Access Points
- Added Public Property (LOCK_TO_3G=1) to set Mobility Device to 3G only when using a 3G based Custom APN
- Updated to version 3.5.3633.2 of OPSWAT for Lightweight Policy Enforcement
- Added logging tool for Lightweight Policy Enforcement troubleshooting
- Added reset to LPE compliance when LPE_COMPLIANCE_THRESHOLD is used
- Option Mobility drivers no longer installed by default
- Remove cellular credential information from access point database
- Bug fix for Persistent connections when used with VPN mobility

## Version 9.1.1 – March 5, 2013

- Re-architect Custom APN to handle all user scenarios

- Set NetClient to foreground on Windows 8 after connecting to a preferred hotspot
- Customization: Allow Window Icon customization
- Bug Fix: Fix crash related to Bluetooth adapter ID

## Version 9.1 – November 2, 2012

- Add support for Windows 8 and Windows 8 Pro (see web site for limitations)
- Create Focus records for auto-connected mobility connections
- Add ability to show technical details of the mobility connection
- Add ability to show technical details of VPN connections
- Implement the dynamic update interval value from Service Manager
- PLAP feature is no longer installed by default
- Add the ability for customers to add Custom APN information via the installer's public properties (details found in the Admin Guide)
- Add ability to use a wildcard with Trusted Domains
- Additional customization enhancements (details found in the Admin Guide)
- Simplify implementation of VPN Client adapters for customers implementing Multi-homing prevention
- Update the names of the Mobility (Cellular) technology we're using in our drop-down list of providers
- Add robustness to the installer to ensure none of the client services and components are running
- Focus records can now be uploaded to IPv6 collectors
- Get Focus Collector addresses from Service Manager
- Include support for the latest firewall, anti-virus and anti-malware products in Lightweight Policy Enforcement (3.5.3633)
- Improve the performance of Lightweight Policy Enforcement
- Display a meaningful status when connect button is disabled
- Use a protected config.xml when the zip file has been deployed
- Convert CERT_SHOW, CERT_SHOW_SET, DISABLE_CELLULAR_SDK from config.ini to config.xml
- Bug Fix: Investigate and fix a specific mobility issue with mobile where VPN tunnel doesn't get moved to an existing internet connection
- Bug Fix: Investigate client hung (or) crash during its shutdown after leaving it running for couple of days
- Bug Fix: enter incorrect PIN unlock code on WMB

## Version 9.0.2 – September 12, 2012

- Fixed INTERNET_ONLY=1 public property
- Corrected security flaw

## Version 9.0.1 – August 28, 2012

- Update OPSWAT to latest SDK.
- Correct screen display for usage meter in localization languages
- Make necessary VPN driver change to get the right media disconnect notifications on Vista/Win7
- Make sure Internet Edition writes the default firewall settings to the registry just like managed/laptop connect editions
- Fix the service so the Hotspot list matches WZC when laptops come out of sleep mode

- Correct anatomy in profile names
- Added XML validation for customer driver customizations
- Add package ID to the Help About dialog
- Enable the new LPE feature to show AV/AS products that are detected by the Windows Security Center
- Make the Mobility Information dialog more readable.
- Verify that new firmware for the 313U (Momentum) and the MC7700 (Sierra Gobi 3000) Sierra LTE phone number not showing
- Added ability to not display the Yes/No prompt for soft token use
- Added migrate log to logs menu

## Version 9.0 – July 23, 2012

- New, simplified User Interface to make connecting easier than ever.
- Added latest OPSWAT release for Lightweight Policy Enforcement
- Removed the Client Toolbar as part of User Interface simplification.
- Added ability to show or not show Dial connections.
- Add IPv6 support to Windows XP Firewall.
- Mobility Enhancement: Integrated the new mobility drivers for Huawei devices.
- Mobility Enhancement: Integrate new Sierra Wireless SDK (QMI SDK Build 3416) to address Sierra Wireless GOBI 3000 issues.
- Customization Enhancement: added the ability to lock the UI from changing a custom APN
- Customization Enhancement: added the ability to launch VBScript without a customization request.

## Version 8.11 – April 4, 2012

- Enabled AutoConnect functionality for Windows Mobile Broadband based connection.
- Removed Smith Micro SDK for cellular devices.
- Using the AT Command Set SDK for RIM devices.
- Added generic cellular detection using the AT Command Set for unknown devices.
- Added SMS support for GSM devices using Windows Mobile Broadband.
- Added Windows Mobile Broadband support for CDMA devices.
- Enable override of the bitmap shown on the Windows Vista and Windows 7 PLAP login screen (requires a customization from AT&T.)
- Added the ability to hide the Cellular Usage data menu item (requires a customization.)
- Added public property for minimizing the client to the Task Bar after connecting.
- Added public property for minimizing the System Tray to the task bar after connecting.
- Installation repair function will also run the Sierra Wireless device driver repair.
- Added ability for dynamic customizations to copy ini and xml files
- Bug Fix: the ability for the Option USB velocity to connect with the wwan.css APN.
- Bug Fix: Cisco ASA VPN traffic transmission issue for phase 1 re-key when LZS compression is enabled.
- Bug Fix: signal strength discrepancy for the AT&T USBConnect Momentum card.
- Bug Fix: DNS resolution for the AT&T USBConnect Momentum card when connecting to LTE network.
- Bug Fix: Allow the AT&T USBConnect Momentum card to AutoConnect after a warm reboot.

## Version 8.10.4

- Bug Fix: Ensure connection sequence is not incorrectly removed which was causing the Connect button to remain disabled when it should have been enabled

## Version 8.10.3

- Customization: Allow specification of different IKE re-key time
- Bug Fix: Patch to correct PLAP security issue

## Version 8.10.2

- Bug Fix: Enable overriding PLAP bitmap using a customized installation

## Version 8.10.1

- Bug Fix: Ensure the GINA-less GINA option creates the DUN object when required

## Version 8.10 - December 28, 2011

- Incorporate latest RIM drivers to support the most recent Blackberry devices
- Add support for Windows Mobile Broadband GSM devices
- Add a message to indicate the user does not have MPFW enabled
- Upgrade LPE to support the latest 3rd party anti-virus, anti-spyware, firewall and VPN products (3.4.27.1)
- Added public property to set the behavior for updates over metered connections
- Bug Fix: Use the Correct EA Domain for 3rd party Wi-Fi authentication

## Version 8.9 - November 15, 2011

- Add cellular data usage meter
- Ensure the client will correctly display cellular data network type and icon (4G LTE/4G/3G/EDGE)
- IPSec over IPv6 (IKEv1) on Windows XP
- SSL-T over IPv6 direct on Windows XP
- IPv6/IPv4 over IPv6 IPSec/SSL-T VPN to an AT&T VPN server on Windows Vista and later
- Interface to AT&T Service Manager over IPv6
- Integrated stateful firewall support for IPv4/IPv6 on Windows Vista and later
- Focus reporting IPv6 VPN connection information, sent to Focus over an IPv4 network
- IPv6 local subnet access when split tunneling is disabled
- Block IPv6 internet traffic while VPN connected if customer is using AGNC integrated firewall
- Support AT&T initiated SMS messages to customers with Gobi 3000 devices
- Low cellular signal notification
- Show correct marketing names for cellular devices
- Update cellular SDK to support latest 3rd party cellular devices
- Implement native support for Option devices
- Implement native support for devices using the AT command set

- Ensure the AT&T LaptopConnect Momentum is set to full power if the client runs and the device is in a low power state
- Add support for AT&T generated SMS messages for Gobi 3000 devices
- Do not download access point database and software updates over low bandwidth/metered connections by default
- Incorporate T6 client as a feature in the AT&T Global Network Client installation package
- Handle usage data SMS messages from AT&T for metered accounts
- Bug Fix: Persistent connection over auto-connected cellular not always working
- Bug Fix: Client doesn't rollover to the next available SMiX when the internet probe fails
- Bug Fix: Correct Table of Contents for localized help
- Bug Fix: Corrected problem preventing SSL-T from connecting through a proxy
- Bug Fix: In some cases VPN traffic would sporadically cease to pass from the client to the private network
- Bug Fix: 8.7 and 8.8 Vista/Win7 Integrated Firewall blocks IPv6 traffic to on-link hosts
- Bug Fix: Correct issue where network type was incorrectly reported for H+ capable devices supported through the Smartcom SDK
- Bug Fix: The Windows Firewall exception was not added correctly during installation

## Version 8.8 - September 7, 2011

- Incorporate support for Panasonic Gobi 3000 module
- Incorporate support for HP Gobi 3000 module
- When the PC has network connectivity through a device to the internet that is not a Ethernet, Wi-Fi, Cellular, or Dial display an Existing Connection icon in the available networks panel
- Prevent driver installation failure for too many filter drivers error
- Correct excessive CPU usage cause by registry and database access

## Version 8.7.2 - August 11, 2011

- Bug Fix: Upgrades from v6 and v7 do not work
- Handle firmware upgrades for cellular devices to report leading and trailing spaces in the make and model

## Version 8.7.1 - July 25, 2011

- Bug Fix: Client does not use non NIC registered IPv4 DNS values stored in service manager

## Version 8.7 - July 13, 2011

- Support service selection for LTE devices
- Incorporate native Sierra CDMA SDK
- Include cellular phone number in Focus records
- Trusted LAN enhancements for Windows 7 and Windows Vista
- Bug Fix: The toolbar does not work correctly on 64-bit operating systems

- Bug fix: Client doesn't respond when it was minimized to desktop and is then brought back to the desktop

## Version 8.6 - May 27, 2011

- Add ability to connect using a specific network type
- Allow use of menus instead of task panels
- Incorporate native Sierra Wireless GSM SDK
- Provide ability to drop network connection if no VPN exists using OPSWAT
- Add support for Huawei E1815
- Add support for Huawei E368
- Ensure custom APNs work in all scenarios
- When accessing a Free Wi-Fi hotspot, use OPSWAT to check for any Firewall rather than require AT&T firewall
- Implementation of VPN client detection and control using OPSWAT VPN SDK
- Create a means to reorder network adapters
- Add the ability to hide the Ethernet icon for cellular-only kits
- Provide the ability to remove/hide the Dial and Ethernet pops from the access point list for custom clients
- Create DUN object when using GINA-less GINA
- Support IE 9
- Enhance third party VPN Client support
- Add display of support logs in English when using non-English OS
- Bug fix: correct customer issues with CDMA devices in 8.5
- Bug fix: ensure client does not crash when stopping a Free Wi-Fi Hotspot association by selecting a specific Wi-Fi hotspot to get connected
- Bug fix: ensure LDAP checking feature for digital certificate authentications works correctly
- Bug fix: OPSWAT reported Check Point Endpoint Security Antivirus status incorrectly

## Version 8.5 - February 24, 2011

- Add ability to update lightweight policy enforcement components independently of client upgrades
- Add ability to upgrade cellular device drivers (and SDK) independently of client upgrades
- Support for roaming restricted Wi-Fi locations
- For Verizon and Sprint CDMA connections use the RAS interface for establishing the cellular connection
- Add ability to access Program License Agreement after installation
- Correct issue with data usage counters
- Update command line parameter for password
- Integrate Smith Micro WWAN SDK version 3.1205.00.0

## Version 8.4 - January 18, 2011

- Fixed crash that occurred within the new v3 OPSWAT as a result of not handling corrupt registry entries
- Digital Certificate Enhancements
- Update Netmon service to have better interop with IPv6 (when enabled)

- Add ability to centrally define and dynamically update a proxy or autoproxy server for ANY service including cellular internet
- Add ability to centrally define and fence connectivity for ANY service including cellular internet
- Ensure RIG is randomly selected
- Added an option to export the entire access point database
- Integrate Smith Micro WWAN SDK version 3.1105.01.0 into NetClient
- Add ability to specify FTP Server Information for any service including cellular internet
- Fixed problem with using telnet across the internet when VPN connected with dual access and using the AGN firewall
- Update OPSWAT SDK
- Added new Python Wi-Fi script for new 403 authentication method for Aicent
- Add ability to push dynamic customizations for any service including cellular internet
- Change default value for dropdown list for Intranet and Internet options on Advanced Login Options in Connection Wizard

## Version 8.3.2 - December 10, 2010

- Fix for database error on startup due to file permission error
- Fix the e0000001 exception generated by a Windows update published on 11/14/2010 that changed the Win32 IXMLDOMDocument COM API
- Fix for crash in NetCfgSvr.exe after client starts on Japanese XP
- Problem where the client crashes when the Wi-Fi adapter is associating with some hotspots
- Update Smith Micro WWAN SDK to version 3.1105.01.0

## Version 8.3.1 - November 5, 2010

- Add support for Sierra Wireless Crazy Ivan
- Update Smith Micro WWAN SDK to version 3.1105.00.0
- Port Sierra Wireless AutoConnect code to use new Sierra Wireless SDK
- Correct LPE handling of missing/bad data from OPSWAT

## Version 8.3 - October 27, 2010

- Architect cellular interface and move the low-level interfaces into a self-contained module
- Add support for cellular AutoConnect with Gobi devices
- Add Native GOBI 2000 support
- Update Lightweight Policy Enforcement SDK to V3 API
- Update the OPSWAT V3 modules with V3.4.15.1
- Allow switching providers using GOBI
- Integrate cellular device driver merge module 7.2 DR 6
- Remove code that tries to restore the cellular service selection to the original settings when the client exits

- Re-order the drop down list for the My Companies Intranet and Both the Internet and My Companies Intranet selections
- Enhanced client to automatically capture a memory dump in the event of a crash
- Bug Fix: Fixed problem with software updates failing to complete
- Get Microsoft signature for updated LWF and IM drivers
- Show cellular byte counters and icon in NetGM when autoconnected cellular with Internet service
- The client will now alternate connection attempts between different geographies for ANIRA to reduce the time needed to failover when one geography is down

## Version 8.2 - September 10, 2010

- Added IPv6 over IPv4 IPSec tunneling to an AT&T VPN server(SIG/VIG)
- Improved Integration with Checkpoint Integrity for Endpoint Security offering
- Update the OPSWAT V2 code to the 3.4.14.1 level
- Corrected issue where Connect button is disabled when Private-line connection sequence is selected
- Set proxy on DUN object when connecting via tethered cellular device
- Integrate Smith Micro WWAN SDK version 3.1005.00.0 into NetClient
- Fix accessibility Problem: Tab sequence gets lost on "not connected" screen
- Fix accessibility Problem: JAWS cannot read popup dialog windows
- Fix accessibility Problem: JAWS cannot read the contact phone numbers in the support dialog
- Fix accessibility Problem: black and white high contrast modes are not honoring screen colors
- Bug Fix: Properly configure subnet mask on the VPN adapter when handed out by VPN server on Vista/Windows 7
- Bug Fix: Fixed crash occurring when a PC is configured with a large DNS suffix list
- Bug Fix: Do not prompt if the user wants to use RSA Soft Token if current profile is Internet only

## Version 8.1.2 - July 22, 2010

- Fixed performance issue seen when uploading files over the local network on Windows Vista/7
- Fixed issue where overriding the firewall state with the UI on Windows Vista/7 was not persisting across boots
- Ensure upgrade will complete with Windows Firewall disabled
- Fixed crash that was occurring when PC is shutdown while IPSec VPN connected after a re-key has occurred and no VPN traffic is being passed through the VPN tunnel
- Fixed issue that was preventing the VPN from working on Windows Vista/7 when another product installed an intermediate driver (i.e. Cisco IPSec client, VirtualBox, etc.)

## Version 8.1.1 - June 16, 2010

- Add support for broadband APN
- Enhance Software Updates
- Add ability to rename profiles
- Cellular only users are never made aware of client software updates

- Update display of connection status information to display both the remote access and the VPN information
- Enhance logging - use logging service in the client
- Add the ability to customize the client install so that the DNS/WINS values from service manager will be set directly on the cellular adapter
- Ensure users are prompted for credentials when using LaptopConnect Wi-Fi when necessary
- Make connected cellular details dialog look more like the not-connected dialog
- Update OPSWAT SDK to version 2 level 3.4.9.1
- Integrate version 3.0905.00.0 of Smith Micro WWAN SDK into NetClient
- Show Wi-Fi access as N/A if service manager denies the user Wi-Fi access
- Fixed blue screen when using SSL-T on Windows XP and internet interface MTU size is lower than the default
- Allow the user to skip prompts to install upgrades at each startup
- bug fix - Ensure that a dial operation is not started when dial connections are hidden

## Version 8.1 - April 15, 2010

- Added VPN, fencing, and firewall support for Windows 7 Mobile Broadband devices
- Limited the occurrence of ''Sorting Access Points''
- Added Windows Firewall exception for AT&T client for all networks (Vista/7)
- Integrated support for latest LaptopConnect cellular device drivers
- Integrated support for latest 3rd party cellular devices
- Updated support for the Lightweight Policy Enforcement
- Refined third party Wi-Fi authentication logic flow
- Deny access to the private network until the user has acknowledged the corporate banner text
- Correct defect causing a crash when enumerating Machine Certificates on Windows Vista and Windows 7 for Restricted Users
- Reverted Windows XP intermediate driver back to v7 driver architecture
- Block all IPv6 traffic when an "everything down the tunnel" IPv4 connection is established
- Modified status.htm to allow for dynamic length content such as IPv6 addresses
- Ensure Cisco and Nortel ISAKMP ports are not aged from PC firewalls
- Increase size of integrated firewall state table to reduce session aging
- Added ability to configure the integrated firewall with specific application state tables to prevent sessions from aging
- Prevent the installation from downgrading an installed client
- Fixed inactivity timeout issue when using VPN mobility with an unsupported cellular device that appears to be a dial adapter
- Ensured skin files are removed during rollback
- Fixed problem where VPN private line was being corrupted during a VPN roam event
- Bug Fix: Connection speed is not cleared from status bar after resume
- Bug Fix: Unlock SIM Feature dialog does not close
- Bug Fix: Close Event Handles in NetVPN calls

## Version 8.0.4 - February 26, 2010

- Update to address system vulnerability with GINA and PLAP implementations

## Version 8.0.3 - February 11, 2010

- Once connected cellular phone number should be listed when clicking on the cellular icon under the disconnect button
- Displayed the wireless number in additional locations in the client
- Added support for RSA SoftID Version 4
- Do not show an error for the access point database being too old for cellular connections
- Ensure the client can be restored using the desktop icon when minimized to the system tray
- Integrate latest version of Smith Micro cellular SDK (3.0800.01.0) into NetClient
- Fix various issues when connecting with different cellular providers on the same computer
- Fixed routing problem with local subnet feature when used with dual access VPN connections
- Add setting to allow user to disable cellular AutoConnect support so CDMA devices work
- Reduce frequency of "sorting access points"
- Fix FTP code in software updates service so it does not make unnecessary connections when retrieving files
- Do not re-download the same AP update if the user does back-to-back manual updates
- Don't show dial records in browser if dial is hidden

## Version 8.0.2 - December 11, 2009

- Integrate support for latest LaptopConnect cellular device drivers
- Integrate Smith Micro WWAN SDK v3.0715.01.0
- Update OPSWAT SDK to version 2 level 3.4.6.1
- Repair corrupted database files
- The local subnet feature is now supported with dual access VPN connections
- Bug fix: Do not keep repeating connection sequence errors when using persistent connections
- Bug fix: Customer with no preferred Wi-Fi access is seeing preferred sites
- Bug fix: Blob cache can grow to many hundreds of megabytes

## Version 8.0.1 - November 30, 2009

- Correct erroneous "the connection sequence has completed without establishing a connection" error
- FIX: Eliminate crash in NetMsg
- FIX: LaptopConnect Wi-Fi can show as N/A sometimes

## Version 8.0 - October 8, 2009

- Incorporate multiple languages into a single client build
- Initial IPv6 Remote Access Support over SSL-T
- Make sure the domain and DNS suffix search list are left intact if no value is received from Service Manager

- Comply with Section 508 requirements
- Get VPN Driver signed for new Windows 7 Logo Program
- Allow administrators to suppress the upgrade reboot
- Simplified Typical installation path by moving FastPath dialog into Custom Setup Path
- Always generate installation log for executable installers
- Bug Fix: NetUpdates GUI appears to hang during automatic update of AP directory on a slow connection
- Update Python Wi-Fi scripts to reflect renaming of NetClient.dll
- Upgraded application support for lightweight policy enforcement to version 3.4.2
- Integrate latest version (3.0602.00.0) of Smith Micro cellular SDK into NetClient
- Bug Fix: User incorrectly told they entered wrong password when connecting WIG
- Support AutoConnect functionality of select cellular devices
- Restore the default service selection (2G or 3G) to the default value when the client starts
- Improve hotspot analysis state machine so the state that asks the user to turn on the firewall is only displayed if hotspot probing really needs to be done
- Added support for jumbo frame local traffic
- Improved error handling when IPSec logon timeout to all VPN servers is exceeded
- Fixed SSL-T vulnerability

## Version 7.7.2 - October 13, 2009

- Improved network monitoring to better screen out adapters that are not physical devices (i.e. McAfee's Intermediate driver virtual miniport interface)
- Improve connection experience when at a private line location by no longer performing internet probes
- Improve GOBI support on Dell laptops
- Fixed SSL-T vulnerability
- Bug Fix: software update service not retrieving the correct proxy settings from Internet Explorer
- Fixed issue when the first connection is made from a private line location and the client is configured to normally connect with single sign-on but the private line server is configured for CDA
- Wi-Fi profiles being deleted when they shouldn’t' be
- Bug Fix: Fixed issue where the 2nd or greater SSID in the list of private limited access (aka private line) was not being identified as private when creating a Wi-Fi connection sequence attempt
- Bug Fix: The correct connection type is now passed to AT&T VPN servers
- Bug Fix: Client unable to start if SLR database table gets corrupted
- Bug Fix: Allow client to connect to preferred hotspot when already associated

## Version 7.7.1 - June 11, 209

- Reduce installation time for cellular device drivers by integrating merge module 6.12
- Software Updates: do not download program update if it was previously downloaded but not installed

## Version 7.7 - May 8, 2009

- Added ability to capture and analyze VPN packets using WireShark (Ethereal) and Microsoft Network Monitor
- Added support for browser based logons

- Changed AT&T Global Network Client program icon
- Install access point database to CommonAppData folder
- Added ability to automatically login to Windows when connected from WinLogon Desktop (GINA)
- Improved ability to remove DNS, WINS, domain name and DNS suffix search list values
- Improved initial experience by removing display of Windows location / area code window when location is unknown
- Improved accuracy of roaming warning when using a non-roaming cellular providers in the US
- Replaced consumer orange 3G fireball graphic with enterprise blue 3G fireball graphic
- Improved ability to hide specific connection types through customization
- Upgraded to use WWAN SDK version 3.0500.10.0
- Upgraded application support for lightweight policy enforcement to version 2.5.19.1
- Improved the persistence of the options on the Windows login (GINA) by saving and restoring them when the computer is restarted
- Propagate installation UI option to chained installation packages
- Available Networks Task Panel is now expanded by default
- Changed to only show the "Change" button in Add/Remove programs
- Changed to prompt to disconnect prior to minimizing the client when configured with the "prompt to disconnect" and "minimize" network awareness options
- Updated the help to correctly reflect the current Change Password steps
- Enabled specification of the selected connection sequence at installation time
- Updated Python Interpreter To 2.6
- Removed prompt for hotspot requirement of VPN
- Improved logging and user experience for 802.11 analysis
- Set the timeout to be used when no cellular service is detected before the cellular card causes a unexpected disconnect
- Updated Authentication method values being sent to FOCUS

## Version 7.6.2 - March 20, 2009

- Improved handling of suspend/resume when the client is running
- Incorporated latest cellular device drivers into the installation package (merge module 6.10.100)
- Ensured threshold timeout does not incorrectly trigger during connections with very high data transfers
- Improved detection of new existing internet connection after the client has been disconnected for a period of time
- Fixed problem with best VIG selection algorithm
- Improved persistence of IPSec connections when using VPN mobility
- Fixed problem with cleaning up VPN network configuration during a Windows Logoff event(a problem introduced in 7.6.0)

## Version 7.6.1 – January 22, 2009

- Monitor the process for the latest version of the Nortel Extranet Client
- Incorporated latest cellular device drivers into the installation package
- Added command line parameters to enable/disable the firewall while not connected

- support for PLAP for 64 bit Windows Vista Added
- Integrated latest Smith Micro cellular SDK (3.0400.10.0)
- Improve responsiveness of NetUpdates progress bar during AP directory updates
- Corrected the "Use Same Credentials as AGNS" function of the "Hook Gina"
- Corrected restoration of Domain Suffix List

## Version 7.6 - December 8, 2008

- Added ability to download software updates (including Access Point database updates) in the background (even when the main program is not running)
- Added ability to prevent multi-homing while connected
- Added ability to centrally-manage and dynamically update all customizations
- Added ability to select preferred cellular service type (3G or 2G)
- Added ability to configure warnings for cellular roaming connections
- Added ability to display centrally-configured password rules
- Added support for monitoring the NetMotion VPN client
- Added ability to manually disable local subnet access
- Added ability to configure a compliance threshold for Lightweight Policy Enforcement (LPE)
- Added client type and version in flow to Cisco VPN servers for client access-rule configuration
- Added installation properties to enable persistent connections
- Added user's admin status to the top of the support log
- Added Wi-Fi encryption type to connection status window
- Added a warning message that is displayed if the access-point directory is too old
- Ensure we do not prevent installation on Windows 7
- Added the ability to force the GINA to operate in Hook Mode even if a non-standard GINA is present
- Added description of command-line parameter status code to help file and Admin Guide
- Improved IPSec to SSL-T failover from Cisco/Nortel to an AT&T Labs VPN server
- Improved organization of encryption code (in preparation for FIPS certification)
- Increased the size of the migrate log written to the support log
- Improved organization of Lightweight Policy Enforcement (in preparation for future LPE component dynamic updates)
- Improved tooltip messages for LaptopConnect Wi-Fi in connection sequence window
- Improved problem diagnostics tool
- Improved integration with Lenovo Access Connections
- Upgraded Integrity Client to version 6.5.063.222 in Managed Endpoint Security editions
- Upgraded application support for lightweight policy enforcement to version 2.5.12
- Changed to reduce health-check timeout for ANIRA VPN connections
- Changed to properly clean-up IPSec SA delete payloads for each session when connecting to a GSR from behind a NAT device
- Removed idle timeout setting and enabled threshold timeout by default
- Changed service-level reporting to refresh "last upload date" in case the program is left running for multiple days
- Fixed the size of the page file written in message log
- Fixed the warning displayed if Windows Zero Config is not running
- Fixed contents of connection status window when connected over LaptopConnect Wi-Fi
- Fixed migration of Trusted LAN settings during upgrades
- Obtain Microsoft WHQL certification for filter driver
- Fixed some scenarios where a hang or crash was occurring when suspending/resuming a PC

- Fixed problem with changing an expired password for Cisco CDA connections
- Fixed throughput meter when using VPN mobility to move from cellular to Wi-Fi

## Version 7.5 - October 6, 2008

- Force client to wait longer for cellular service
- Added support for tethering Blackberry 9000 [Bold] on 32-bit Vista
- Add additional cellular device drivers to LaptopConnect Edition
- Upgraded the cellular SDK to the latest version (3.0301.04.0)
- Changed to trim leading and trailing spaces from user IDs
- Changed to prevent install on Windows 2000
- Removed Microsoft Visual C run-time version 7.1 from installation
- Fixed problem preventing display of No Default Network warning
- Fixed display of error 460 during challenge-response authentication
- Fixed problem with network awareness when connected to both the corporate LAN and another network(i.e. Wi-Fi)

## Version 7.4.1 - September 2, 2008

- Changed to allow firewall state to be toggled while disconnected with Endpoint Security installed
- Fixed 'connection sequence is empty' issue observed after certain customizations
- Fixed problem with VPN connections for Windows 2000 users running without admin rights

## Version 7.4 – August 3, 2008

- Add ability to connect to Wi-Fi access points using credentials stored on the AT&T LaptopConnect cellular SIM
- Added support for connecting to third-party wired Ethernet locations that require a browser login
- Added support for CryptoCard soft-token customer-direct authentication
- Added installation option to Custom path to enable Internet as the default service (does not prompt for credentials for cellular Internet connections)
- Added retrieval of network settings when connecting over an existing Internet connection
- Upgraded cellular SDK to latest version -- 3.0203.01.0
- Upgraded application support for lightweight policy enforcement to version 2.5.9.1
- Improved third-party authentication with new extendable architecture
- Improved start-up and shutdown performance
- Improved connection history by increasing the number of prior connections retained
- Improved logging of Wi-Fi authentication flows
- Changed to disable third-party Wi-Fi connections when running on the Windows logon desktop
- Changed to not categorize unencrypted Wi-Fi access points as preferred private
- Changed to sustain VPN connection when a secondary, not in use, network adapter is disabled
- Changed to remove (and later restore) auto-proxy settings during third-party browser-based logins
- Changed to include program name in title of software updates progress window
- Changed to use new AT&T Wi-Fi logo
- Changed to use Cisco's IPSec phase 1 rekeying (NAT-T floated UDP port)

- Removed support for Cisco proprietary IPSec UDP encapsulation algorithm
- Removed ability to use version 5 or 6 skins
- Fixed display of cellular info when there are cellular network changes
- Fixed display of command-line parameter help when using ''-help''
- NOTE: This is the final release for Windows 2000

## Version 7.3.2 – July 18, 2008

- Upgraded cellular device support for ACM 6.8.100 compatibility
- Upgraded application support for lightweight policy enforcement to version 2.5.9
- Fixed migration of user settings left behind after uninstalling version 6
- Reset invalid GlobalMaxTcpWindowSize if necessary
- Fixed potential memory leak in NetCfgSvr.exe for some users that turn off their Wi-Fi antenna
- Fixed ability to connect when using version 5 or 6 skins
- Fixed a potential crash (Windows error report event ID 799894910)

## Version 7.3.1 - June 12, 2008

- Fixed VPN Mobility problem when moving IPSec connections to another network interface when 2 networks are available and the RIG address is 15 characters (US impact primarily)
- Fixed cellular connections when the phone book is missing or empty on Windows 2000
- Fixed invalid password issue on initial connect attempt after switching from a profile that uses secure id to a profile that uses a static password for authentication
- Fixed issue where the month was wrong on the timestamp in the netvpn.txt and netssl.txt support files
- Fixed problem where a crash could occur, in some circumstances, when cloning a profile that is configured with an expiration interval for saved passwords
- Fixed problem where persistent connections mode is disabled if user selects Show Login Properties while connected
- Fixed problem with Windows system sounds after disconnecting
- Updated application support for Lightweight Policy Enforcement

## Version 7.3 - April 30, 2008

- Added support for VPN mobility, persistent connections, and network awareness to improve mobile PC user experience
- Added ability to connect without requiring AT&T Global Network credentials to certain types of networks (like cellular, private Wi-Fi, and free Wi-Fi)
- Added ability to configure local LAN settings from the main window
- Added ability to configure a private-line connection from the main window.
- Added automatic sizing to main window
- Added ability to display special AT&T alert messages (received via SMS) while connected over cellular
- Add user preference to enable/disable cellular device monitoring

- Added support for detecting and using locked BlackBerry devices
- Added ability to restrict which cellular devices can be used to connect
- Added ability to expire saved passwords
- Added ability to configure the client (at install time) to use settings returned from the VPN server for CDA
- Added listing of installed files to support log
- Added warning to install of Premium editions to warn that Managed Endpoint Security service is not available on Windows Vista
- Added cellular SDK version number to support log
- Added support for using HTTPS (port 443) for Internet probing
- Improved support for VPN connecting through an authenticating proxy with the v7 interface
- Improved VPN tracing by saving netvpn.txt and netssl.txt for the last three VPN connections
- Improved IPSec SA delete message to only contain the sender's SPI
- Improved cellular device detection
- Improve reliability of automatic Internet detection
- Improved support for embedded cellular devices in HP notebooks
- Improved localization of Windows logon (GINA) components
- Improved (reduced) memory usage after connecting
- Updated LaptopConnect device driver support to version 6.8
- Updated lightweight policy enforcement to version 2.5.5.1
- Changed to not display Network Login window if all credentials are saved
- Changed to use HTTPS for authentication when connecting over cellular with custom APNs
- Changed to enter new password on login window (instead of separate new-password window)
- Changed to display name of Windows Vista edition in support files
- Changed default window frame to use Vista theme
- Changed to show the Windows logon (GINA) feature during the custom installation path
- Removed ''change password'' link from connected window
- Fixed a problem that caused custom password label text to be duplicated
- Fixed a problem in the Login Properties window when deleting empty browser settings on the Program page
- Fixed selection of digital certificates on Network Login window
- Fixed background color of ''save password'' checkbox when running Windows classic theme
- Fixed problem with outbound traffic being reported incorrectly on the histogram for SSL-T connections on Vista
- Fixed problem when disconnecting dial during Windows logoff
- Obtain Microsoft digital signature for filter driver

## Version 7.2 - January 21, 2008

- Added support for 64-bit Windows Vista.
- Added ability to install device drivers for AT&T LaptopConnect devices
- Added a self-help feature that allows a user to reset their cellular configuration settings.
- Attempt to force Integrity to use the correct license key during installation
- Added ability to display "advanced login properties" when accessing setup through the Login Properties window.
- Added support for RSA EAP - Protected OTP (SecurID over Wi-Fi).
- Added ability for support personnel to export access-point list.
- Improved the prompt displayed when connecting over a previously established Wi-Fi connection.
- Improved performance of free Wi-Fi detection by caching previous detection results.
- Improved method of retrieving current status from Integrity Client for Managed Endpoint Security users.
- Improved handling of cellular error scenarios (SIM problems and others).
- Improved error message for invalid current password while changing password.
- Improved phone number selection window to always select top 2 numbers when appropriate.
- Enhanced the Wi-Fi toll warning for automatic connections.
- Enhanced logging of network events (Netmon) to retain multiple connection attempts.
- Enhanced the display of the AT&T 3G indicator and added a cellular roaming warning.
- Updated application support for lightweight policy enforcement.
- Changed to log signal strength of Wi-Fi and cellular connections prior to disconnecting.
- Changed to not show hyperlinks in pop-up messages when in running on Windows logon desktop.
- Changed initial focus on Network Login window to be on OK button if password saved.
- Changed to allow new passwords greater than 8 characters.
- Changed to better handle DHCP flow while VPN connected with IPSec. On some computers, DHCP renew requests were being routed through the wrong interface resulting in 908 error (a heartbeat timeout).
- Changed to display skin change message when reverting back to default.
- Changed the registration web page to be non-modal.
- Changed position of main window when connecting from the Windows logon desktop so that the Windows login window is not obscured.
- Changed Managed Endpoint Security policy enforcement to not require a rule to trust the VPN servers.
- Fixed DNS issue for unregistered users using RADIUS filter IDs.
- Fixed problem when initial window is empty and program does not function on Windows Vista Home Premium with UAC enabled.
- Fixed a problem that prevented the program from running with any Windows theme (other than "classic"). Upgraded to Xtreme Toolkit 11.2.
- Fixed problem with the centrally-managed setting to allow user control of firewall.
- Fixed a problem connecting to certain partner Wi-Fi access points that use a modified "chunked encoding" for the HTTP responses.
- Fixed unnecessary VPN prompt when connecting over broadband in some situations.

- Removed orphaned pages from the help file.

## Version 7.1.1 - October 30, 2007

- Ensured profiles for all users are migrated when upgrading from prior releases
- Some WPAPSK hotspots cannot be configured through NetClient
- Fixed C++ runtime error that was seen on PCs running certain endpoint security software.

## Version 7.1 - September 12, 2007

- Added ability to centrally configure keep alive intervals for Cisco VPN connections.
- Added support for VPN client load balancing for Cisco VPN connections.
- Added ability to connect prior to logging onto Windows Vista. (Added support for the Credential Provider architecture - GINA replacement on Windows Vista.)
- Added ability to periodically update cellular card firmware.
- Added display of dBm (decibels with respect to one milliwatt) signal strength for cellular connections.
- Added data traffic counts and monthly connection summaries to the connection history window.
- Added ability to shrink window to floating or docked "minibar."
- Added 3G fireball to cellular icon when AT&T wireless 3G service is detected.
- Added connect and disconnect options to the system menu.
- Added ability to configure private, limited-access Wi-Fi (private line over Wi-Fi) during installation.
- Added new FastPath code for defaulting login window to use pin and token.
- Added ability for administrator to specify out of compliance disconnect time for Endpoint Security
- Added ability to display web links (URLs) in pop-up message windows.
- Updated application support for lightweight policy enforcement.
- Updated CheckPoint Integrity Client to version 6.5.063.175 (in Premium editions) for Managed Endpoint Security service.
- Improved VPN IPSec connections on Vista to allow fall back to native (non-NAT traversal) IPSec.
- Improved private-line VPN connections to utilize DNS, WINS, and Domain name returned from the VPN server.
- Improved the number of proxy exceptions that can be used.
- Improved lightweight policy enforcement when running multiple antivirus and anti-spyware applications.
- Improved performance on multiprocessor and multi-core computers.
- Improved display of Wi-Fi details and private Wi-Fi error messages.
- Improved future migration of custom skins by providing defaults for all entries in branding file.
- Improved the appearance of the windows visible on user desktop after connecting from Windows logon desktop (GINA).
- Improved reliability and plug-and-play support for cellular devices.
- Improved detection of Wi-Fi access points that go out of service or out of range.
- Improved certificate authentication to allow user IDs up to 100 characters.
- Improved support for Sierra Wireless AirCard 595.
- Changed virus definition file age default threshold from 30 days to 5 days for lightweight policy enforcement.

- Changed cellular banner for "Wireless by AT&T" name change.
- Changed Available Networks window to show Wi-Fi status whenever it is available (even if not authorized to access preferred Wi-Fi).
- Changed text of premium Wi-Fi warning.
- Changed to prevent unsolicited local traffic when allowing access to the local network during VPN connections.
- Changed to include unencrypted preferred private Wi-Fi access points in free Wi-Fi detection.
- Changed trace window to ensure it comes to foreground.
- Fixed a problem when searching through a large list of access points in the Browse Directory window.
- Fixed problem when dialing the Singapore 800 number with an ID that has 250 or more access list entries.
- Fixed problem where GINA window disappears under certain conditions.
- Fixed several command-line parameters to work with the v7 skin.
- Refreshed digital certificates used for authenticating with AT&T VPN servers.
- Added ability to configure the client, at install time, to use DNS, WINS, and Domain name settings returned from the VPN server.

## Version 7.0.3 - August 30, 2007

- Increased of polling Integrity Status from 15 seconds to 60 seconds
- Used alternate function to query the workstations compliance state from the Integrity Client
- Allowed administrator to specify number of server lost retries using Windows Installer public property MPFW_SERVERLOST_RETRIES
- Allowed administrator to specify minutes to allow workstation to be out of compliance prior to disconnection using Windows Installer public property MPFW_OOC_DISCONNECT_MINUTES

## Version 7.0.2 – June 27, 2007

- Fixed a problem when importing trusted LAN configurations
- Fixed a "server busy" message that could appear when CPU is temporarily overloaded
- Fixed an issue where an Internet Option checkbox was inadvertently set
- Fixed a problem when entering multi-byte passwords

## Version 7.0.1 – May 24, 2007

- Added ability for administrator to control disabling of Windows Firewall for Endpoint Security installations
- Added new version of Endpoint Security component (Check Point's Integrity Agent)
- Added ability to install without the Firewall Settings application (Firewall_GUI feature)
- Added third-party Wi-Fi to default automatic connection sequences which contained Wi-Fi
- Improved display of lengthy, customized VPN Client ID instructions
- Improved performance of Wi-Fi discovery and connections on Vista and XP (with native Wi-Fi fix installed)
- Improved error handling during access-point directory downloads
- Improved display of SSID in event history

- Updated application support for lightweight policy enforcement
- Fixed threshold inactivity timeouts when using the version 7 skin

## Version 7.0 – April 30, 2007

- Added new v7 user interface
- Added ability to configure and connect to user-defined, private, encrypted Wi-Fi access points
- Added limited support for Windows Vista
- Added ability to centrally manage and configure default VPN Client IDs
- Added an event history window for easier viewing of prior connections and to assist problem determination
- Added periodic automatic updating of VPN encryption certificates
- Added custom support for 3 policies (VPN, LAN, Other) to Managed Personal Firewall Service
- Added ability to encrypt data sent to an AT&T VPN server using AES
- Added the ability to connect through a proxy via an automatic-connection sequence
- Added ability to monitor third-party firewall, antivirus, and anti-spyware programs (through lightweight policy enforcement) while not connected
- Added ability to disable cellular card monitoring when client is running
- Added ability to choose between version 6 or version 7 user interface
- Added ability for dynamic DNS registration to be initiated from an AT&T VPN Server
- Added ability to dynamically detect preferred Ethernet connections in hotels for automatic connections
- Added ability to maintain VPN connection while switching to a different Windows user
- Added diagnostic output from Network Configuration Service to support log files
- Added support for connecting to a VPN from a network that uses the Classless Static Route Option (DHCP)
- Improved third-party Wi-Fi connection process
- Improved support for cellular cards and tethered modems for automatic connections
- Improved Wi-Fi authentication with new data-driven scripting engine that is automatically updated as part of access-point list updates
- Improved ability to connect to third-party Wi-Fi and Ethernet access points when a proxy is configured in Internet Explorer
- Improved device-driver installation to not require a reboot under certain reinstall scenarios
- Improved error handling for the rare case when the VPN and Internet IP addresses are the same
- Improved ability to localize the Network Logon Extensions (GINA)
- Updated application support for light-weight policy enforcement
- Updated the Program License Agreement
- Changed to share settings across Windows users instead of keeping separate for each Windows user ID
- Changed integrated firewall policy to allow NetBIOS name resolution via broadcast requests for file and printer sharing
- Changed to restore firewall state after completing free Wi-Fi discovery
- Changed to use native Windows Wi-Fi API when available
- Changed to not start the VPN for a customer-direct authentication (CDA) connection in Internet-only countries

- Changed to not display "Warn if Primary DNS is not available" login property
- Changed to allow the installation directory (INSTALLDIR) to be customized during a major upgrade
- Changed to prevent user from modifying the proxy location description field
- Removed 'Accept-GZIP' from Wi-Fi authentication HTTP requests
- Removed display of Vista's 'Network Awareness' pop-up during Wi-Fi connections
- Refresh digital certificates used for authenticating with AT&T VPN servers
- Fixed erroneous 'cellular' traveling recall popup