6.5 VPN Client Management Command Reference

This section describes all commands that can be called when using vpncmd in VPN Client management mode.

6.5.1 "About": Display the version information

Command Name	**About**
Purpose	Display the version information
Description	This displays the version information of this command line management utility. Included in the version information are the vpncmd version number, build number and build information.
Command-line	*About*
Arguments for "About":	
No arguments are required.	

6.5.2 "VersionGet": Get Version Information of VPN Client Service

Command Name	**VersionGet**
Purpose	Get Version Information of VPN Client Service
Description	Use this to get the version information of the currently managed VPN Client Service program.
Command-line	*VersionGet*
Arguments for "VersionGet":	
No arguments are required.	

6.5.3 "PasswordSet": Set the password to connect to the VPN Client service.

Command Name	**PasswordSet**
Purpose	Set the password to connect to the VPN Client service.
Description	You can make it mandatory to input a password for occasions when the Command Line Management Utility and the VPN Client Manager connect to a VPN Client service to control it. You can use this command to set the password that must be input.

	You can also make it mandatory for this password to be input when doing remote operations (from a computer that is not localhost)
Command-line	*PasswordSet [password] [/REMOTEONLY:yes|no]*
Arguments for "PasswordSet":	
password	Specify the password you wish to set. You can delete the password setting by specifying "none".
/REMOTEONLY	Specify "yes" to only require the password to be input when operation is done remotely (from a computer that is not localhost). This stops the password being required when the connection is from localhost. When this parameter is omitted, it will be regarded as "no".

6.5.4 "PasswordGet": Get Password Setting to Connect to VPN Client Service

Command Name	**PasswordGet**
Purpose	Get Password Setting to Connect to VPN Client Service
Description	Use this to get the setting that determines whether to input a password for occasions when the Command Line Management Utility and the VPN Client Manager connect to a VPN Client service to control it. In the case when a password is requested, it also gets the setting that determines whether this password is only requested when operation is performed remotely (from a computer that is not localhost).
Command-line	*PasswordGet*
Arguments for "PasswordGet":	
No arguments are required.	

6.5.5 "CertList": Get List of Trusted CA Certificates

Command Name	**CertList**
Purpose	Get List of Trusted CA Certificates
Description	Here you can manage the list of certificate authority certificates that are trusted by VPN client. You can use the registered CA certificate list to verify server certificates when connecting to VPN Servers.
Command-line	*CertList*
Arguments for "CertList":	
No arguments are required.	

6.5.6 "CertAdd": Add Trusted CA Certificate

Command Name	**CertAdd**
Purpose	Add Trusted CA Certificate
Description	Use this to add a new certificate to a list of CA certificates trusted by the VPN Client. You can use the registered CA certificate list to verify server certificates when connecting to VPN Servers. To get a list of the current certificates you can use the CertList command. The certificate you add must be saved in the X.509 file format.
Command-line	*CertAdd [path]*
Arguments for "CertAdd":	
path	Specify the file name of the X.509 certificate to register.

6.5.7 "CertDelete": Delete Trusted CA Certificate

Command Name	**CertDelete**
Purpose	Delete Trusted CA Certificate
Description	Use this to delete an existing certificate from a list of CA certificates trusted by the VPN Client. To get a list of the current certificates you can use the CertList command.
Command-line	*CertDelete [id]*
Arguments for "CertDelete":	
id	Specify the ID of the certificate to delete.

6.5.8 "CertGet": Get Trusted CA Certificate

Command Name	**CertGet**
Purpose	Get Trusted CA Certificate
Description	Use this to get an existing certificate from the list of CA certificates trusted by the VPN Client and save it as a file in X.509 format.
Command-line	*CertGet [id] [/SAVECERT:path]*
Arguments for "CertGet":	
id	Specify the ID of the certificate to get.
/SAVECERT	Specify the file name to save the certificate you obtained.

6.5.9 "SecureList": Get List of Usable Smart Card Types

Command Name	**SecureList**
Purpose	Get List of Usable Smart Card Types
Description	Use this to display a list of smart cards that are supported by VPN Client. The types of smart cards listed in this list have had their drivers installed on the current computer and are supported by VPN software. If there is a type of smart card that is currently being used that does not appear in the list, it may be possible to enable use by updating the VPN software to a newer version.
Command-line	*SecureList*
Arguments for "SecureList":	
No arguments are required.	

6.5.10 "SecureSelect": Select the Smart Card Type to Use

Command Name	**SecureSelect**
Purpose	Select the Smart Card Type to Use
Description	Use this to select the type of the smart card to be used by the VPN Client. To get the list of usable smart card types, use the SecureList command.
Command-line	*SecureSelect [id]*
Arguments for "SecureSelect":	
id	Specify the ID of the smart card type.

6.5.11 "SecureGet": Get ID of Smart Card Type to Use

Command Name	**SecureGet**
Purpose	Get ID of Smart Card Type to Use
Description	Use this to get the ID of the smart card type that is set to be used for the current VPN Client. By viewing the results of the SecureList command based on this ID, you can get the type of the currently selected smart card.

	If there is no smart card that is currently selected, 0 will be displayed for the ID.
Command-line	*SecureGet*
Arguments for "SecureGet":	
No arguments are required.	

6.5.12 "NicCreate": Create New Virtual Network Adapter

Command Name	**NicCreate**
Purpose	Create New Virtual Network Adapter
Description	Use this to add a new Virtual Network Adapter to the system. You can give the virtual network adapter a name of your choice. You can set a name that consists of alphanumeric characters for the virtual network adapter. For Windows 2000 or newer systems, this name can be up to 31 characters, but for Windows 98, 98SE and ME it can be up to 4 characters. If the NicCreate command was called, a new virtual network adapter device driver will be installed on the operating system that the VPN Client is operating on. In this case, depending on the operating system, a dialog box may appear to confirm if it is OK to install the device driver.
Command-line	*NicCreate [name]*
Arguments for "NicCreate":	
name	Specify the name of the virtual network adapter.

6.5.13 "NicDelete": Delete Virtual Network Adapter

Command Name	**NicDelete**
Purpose	Delete Virtual Network Adapter
Description	Use this to delete an existing virtual network adapter from the system. When you delete a virtual network adapter from the system, all the connections which are using that virtual network adapter will be disconnected. Also, the Connection Settings that are set to use a virtual network adapter that has been deleted will have their settings automatically changed to use another virtual network adapter. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.

Command-line	*NicDelete [name]*
Arguments for "NicDelete":	
name	Specify the name of the virtual network adapter.

6.5.14 "NicUpgrade": Upgrade Virtual Network Adapter Device Driver

Command Name	**NicUpgrade**
Purpose	Upgrade Virtual Network Adapter Device Driver
Description	If the device driver version of the existing virtual network adapter is old, then this upgrades to the latest device driver that was bundled with the currently operating VPN client. Even if a upgrade is not performed, the device driver will be reinstalled. In this case, depending on the operating system, a dialog box may appear to confirm if it is OK to install the device driver. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.
Command-line	*NicUpgrade [name]*
Arguments for "NicUpgrade":	
name	Specify the name of the virtual network adapter.

6.5.15 "NicGetSetting": Get Virtual Network Adapter Setting

Command Name	**NicGetSetting**
Purpose	Get Virtual Network Adapter Setting
Description	Use this to get the MAC address setting of the existing virtual network adapter. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.
Command-line	*NicGetSetting [name]*
Arguments for "NicGetSetting":	
name	Specify the name of the virtual network adapter.

6.5.16 "NicSetSetting": Change Virtual Network Adapter Setting

Command Name	**NicSetSetting**
Purpose	Change Virtual Network Adapter Setting

Description	Use this to change the MAC address setting of the existing virtual network adapter. When this command is executed, the currently operating virtual network adapter device drivers will be restarted. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.
Command-line	*NicSetSetting [name] [/MAC:mac]*
Arguments for "NicSetSetting":	
name	Specify the name of the virtual network adapter.
/MAC	Specify the MAC address you wish to set. Specify a 6-byte hexadecimal string for the MAC address. Example: 00:AC:01:23:45:67 or 00-AC-01-23-45-67

6.5.17 "NicEnable": Enable Virtual Network Adapter

Command Name	**NicEnable**
Purpose	Enable Virtual Network Adapter
Description	Use this to enable an existing, disabled virtual network adapter. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.
Command-line	*NicEnable [name]*
Arguments for "NicEnable":	
name	Specify the name of the virtual network adapter.

6.5.18 "NicDisable": Disable Virtual Network Adapter

Command Name	**NicDisable**
Purpose	Disable Virtual Network Adapter
Description	Use this to disable an existing, enabled virtual network adapter. This command can be used when VPN Client is operating on Windows 2000 or newer operating systems.
Command-line	*NicDisable [name]*
Arguments for "NicDisable":	
name	Specify the name of the virtual network adapter.

6.5.19 "NicList": Get List of Virtual Network Adapters

Command Name	**NicList**
Purpose	Get List of Virtual Network Adapters
Description	This allows you to get a list of virtual network adapters registered on the current system.
Command-line	*NicList*
Arguments for "NicList":	
No arguments are required.	

6.5.20 "AccountList": Get List of VPN Connection Settings

Command Name	**AccountList**
Purpose	Get List of VPN Connection Settings
Description	Use this to get a list of VPN Connection Settings registered on the VPN Client.
Command-line	*AccountList*
Arguments for "AccountList":	
No arguments are required.	

6.5.21 "AccountCreate": Create New VPN Connection Setting

Command Name	**AccountCreate**
Purpose	Create New VPN Connection Setting
Description	Use this to create a new VPN Connection Setting on the VPN Client. To create a VPN Connection Setting, in addition to specifying the VPN Connection Setting name and destination server as initial parameters and the destination virtual Hub, and user name, you must also specify the name of the virtual network adapter to use. When a new VPN Connection Setting is created, the type of user authentication is initially set as Anonymous Authentication and the proxy server setting and the verification options of the server certificate is not set. To change these settings and other advanced settings after the VPN Connection Setting has been created, use the other commands that begin with the name "Account".
Command-line	*AccountCreate [name] [/SERVER:hostname:port] [/HUB:hubname] [/USERNAME:username] [/NICNAME:nicname]*
Arguments for "AccountCreate":	

name	Specify the name of the VPN Connection Setting to create.
/SERVER	Specify the host name and port number of the destination VPN Server using the format [host name:port number]. You can also specify by IP address.
/HUB	Specify the Virtual Hub on the destination VPN Server.
/USERNAME	Specify the user name to use for user authentication when connecting to the destination VPN Server.
/NICNAME	Specify the virtual network adapter to use to connect.

6.5.22 "AccountSet": Set the VPN Connection Setting Connection Destination

Command Name	**AccountSet**
Purpose	Set the VPN Connection Setting Connection Destination
Description	Use this to set, for the VPN Connection Setting registered on the VPN Client, the destination VPN Server host name and port number, Virtual Hub name, user name used for connection and virtual network adapter name to use.
Command-line	*AccountSet [name] [/SERVER:hostname:port] [/HUB:hubname]*
Arguments for "AccountSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/SERVER	Specify the host name and port number of the destination VPN Server using the format "host name:port number". You can also specify by IP address.
/HUB	Specify the Virtual Hub on the destination VPN Server.

6.5.23 "AccountGet": Get Setting of VPN Connection Setting

Command Name	**AccountGet**
Purpose	Get Setting of VPN Connection Setting
Description	Use this to get the VPN Connection Setting contents of a VPN Connection Setting registered on the VPN Client. To change the VPN Connection Setting contents of the VPN Connection Setting, use the other commands that begin with the name "Account" after creating the VPN Connection Setting.
Command-line	*AccountGet [name]*
Arguments for "AccountGet":	

name	Specify the name of the VPN Connection Setting whose setting you want to get.

6.5.24 "AccountDelete": Delete VPN Connection Setting

Command Name	**AccountDelete**
Purpose	Delete VPN Connection Setting
Description	Use this to delete VPN Connection Setting that is registered on the VPN Client. If the specified VPN Connection Setting has a status of online, the connections will be automatically disconnected and then the VPN Connection Setting will be deleted.
Command-line	*AccountDelete [name]*
Arguments for "AccountDelete":	
name	Specify the name of the VPN Connection Setting to delete.

6.5.25 "AccountUsernameSet": Set User Name of User to Use Connection of VPN Connection Setting

Command Name	**AccountUsernameSet**
Purpose	Set User Name of User to Use Connection of VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to the VPN Server, use this to specify the user name required for user authentication. In some cases it is necessary to specify the type of user authentication and specify the required parameters. To change this information you can use commands such as AccountAnonymousSet, AccountPasswordSet, AccountCertSet and AccountSecureCertSet.
Command-line	*AccountUsernameSet [name] [/USERNAME:username]*
Arguments for "AccountUsernameSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/USERNAME	Specify the user name required for user authentication when the VPN Connection Setting connects to the VPN Server.

6.5.26 "AccountAnonymousSet": Set User Authentication Type of VPN Connection Setting to Anonymous Authentication

Command Name	**AccountAnonymousSet**
Purpose	Set User Authentication Type of VPN Connection Setting to Anonymous Authentication
Description	Use this to set the user auth type to [Anonymous Authentication] for when a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to the VPN Server.
Command-line	*AccountAnonymousSet [name]*
Arguments for "AccountAnonymousSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.27 "AccountPasswordSet": Set User Authentication Type of VPN Connection Setting to Password Authentication

Command Name	**AccountPasswordSet**
Purpose	Set User Authentication Type of VPN Connection Setting to Password Authentication
Description	Use this to set the user auth type to Password Authentication for when a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to the VPN Server. Specify Standard Password Authentication and RADIUS or NT Domain Authentication as the password authentication type.
Command-line	*AccountPasswordSet [name] [/PASSWORD:password] [/TYPE:standard|radius]*
Arguments for "AccountPasswordSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/PASSWORD	Specify the password to use for password authentication. If this is not specified, a prompt will appear to input the password.
/TYPE	Specify either "standard" (Standard Password Authentication) or "radius" (RADIUS or NT Domain Authentication) as the password authentication type.

6.5.28 "AccountCertSet": Set User Authentication Type of VPN Connection Setting to Client Certificate Authentication

Command Name	**AccountCertSet**
Purpose	Set User Authentication Type of VPN Connection Setting to Client Certificate Authentication
Description	Use this to set the user auth type to Client Certificate Authentication for when a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to the VPN Server. For this certificate, you must specify a certificate file in the X.509 format and a private key file that is Base 64 encoded.
Command-line	*AccountCertSet [name] [/LOADCERT:cert] [/LOADKEY:key]*
Arguments for "AccountCertSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/LOADCERT	Specify the X.509 format certificate file to provide for certificate authentication.
/LOADKEY	Specify the Base-64-encoded private key file name for the certificate.

6.5.29 "AccountCertGet": Get Client Certificate to Use for Cascade Connection

Command Name	**AccountCertGet**
Purpose	Get Client Certificate to Use for Cascade Connection
Description	When a VPN Connection Setting registered on VPN Client is specified and that VPN Connection Setting uses client certificate authentication, use this to get the certificate that is provided as the client certificate and save the certificate file in X.509 format.
Command-line	*AccountCertGet [name] [/SAVECERT:cert]*
Arguments for "AccountCertGet":	
name	Specify the name of the VPN Connection Setting whose setting you want to get.
/SAVECERT	Specify the file name to save the certificate you obtained in X.509 format.

6.5.30 "AccountEncryptDisable": Disable Encryption when Communicating by VPN Connection Setting

Command Name	**AccountEncryptDisable**
Purpose	Disable Encryption when Communicating by VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers not to be encrypted. Normally communication between VPN Servers is encrypted by SSL to prevent eavesdropping of information and fraud. You can also disable encryption. When encryption is disabled, the communication throughput improves but the communication data flows over the network in plain text.
Command-line	*AccountEncryptDisable [name]*
Arguments for "AccountEncryptDisable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.31 "AccountEncryptEnable": Enable Encryption when Communicating by VPN Connection Setting

Command Name	**AccountEncryptEnable**
Purpose	Enable Encryption when Communicating by VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers to be encrypted by SSL. Normally communication between VPN Servers is encrypted by SSL to prevent eavesdropping of information and fraud. You can also disable encryption. When encryption is disabled, the communication throughput improves but the communication data flows over the network in plain text.
Command-line	*AccountEncryptEnable [name]*
Arguments for "AccountEncryptEnable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.32 "AccountCompressEnable": Enable Data Compression when Communicating by VPN Connection Setting

Command Name	**AccountCompressEnable**
Purpose	Enable Data Compression when Communicating by VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers to be compressed. It is possible to achieve a maximum of 80% compression. Compression however places higher loads on the CPU of both the client and server machines. When the line speed is about 10 Mbps or greater, compression can lower throughput, but sometimes it can have the opposite effect.
Command-line	*AccountCompressEnable [name]*
Arguments for "AccountCompressEnable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.33 "AccountCompressDisable": Disable Data Compression when Communicating by VPN Connection Setting

Command Name	**AccountCompressDisable**
Purpose	Disable Data Compression when Communicating by VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers not to be compressed.
Command-line	*AccountCompressDisable [name]*
Arguments for "AccountCompressDisable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.34 "AccountProxyNone": Specify Direct TCP/IP Connection as the Connection Method of VPN Connection Setting

Command Name	**AccountProxyNone**
Purpose	Specify Direct TCP/IP Connection as the Connection Method of VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to set Direct TCP/IP Connection as the connection method to use, in which case the connection route will not be via a proxy server.
Command-line	*AccountProxyNone [name]*
Arguments for "AccountProxyNone":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.35 "AccountProxyHttp": Set Connection Method of VPN Connection Setting to be via an HTTP Proxy Server

Command Name	**AccountProxyHttp**
Purpose	Set Connection Method of VPN Connection Setting to be via an HTTP Proxy Server
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to set Connect via HTTP Proxy Server as the method of connection to use, which requires the specification of the host name and port number of the HTTP Proxy server to communicate via as well as a user name and password (when required). The HTTP proxy server that communication will travel via must be compatible with the CONNECT method to use HTTPS communication.
Command-line	*AccountProxyHttp [name] [/SERVER:hostname:port] [/USERNAME:username] [/PASSWORD:password]*
Arguments for "AccountProxyHttp":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/SERVER	Specify the host name or IP address, and port number of the on-route HTTP proxy server using the format [host name:port number].

/PASSWORD	When user authentication is required to connect to the on-route HTTP proxy server, specify the password. Specify this together with the /USERNAME parameter.

6.5.36 "AccountProxySocks": Set Connection Method of VPN Connection Setting to be via an SOCKS Proxy Server

Command Name	**AccountProxySocks**
Purpose	Set Connection Method of VPN Connection Setting to be via an SOCKS Proxy Server
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to set Connect via SOCKS Proxy Server as the method of connection to use, which requires the specification of the host name and port number of the SOCKS Proxy server to communicate via as well as a user name and password (when required). The on-route SOCKS server must be compatible with SOCKS Version 4.
Command-line	*AccountProxySocks [name] [/SERVER:hostname:port] [/USERNAME:username] [/PASSWORD:password]*
Arguments for "AccountProxySocks":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/SERVER	Specify the host name or IP address, and port number of the on-route SOCKS proxy server using the format [host name:port number].
/PASSWORD	When user authentication is required to connect to the on-route SOCKS proxy server, specify the password. Specify this together with the /USERNAME parameter.

6.5.37 "AccountServerCertEnable": Enable VPN Connection Setting Server Certificate Verification Option

Command Name	**AccountServerCertEnable**
Purpose	Enable VPN Connection Setting Server Certificate Verification Option
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to enable the option to check whether the SSL

	certificate provided by the destination VPN Server can be trusted. If this option is enabled, we recommend that you either use the AccountServerCertSet command to save the connection destination server SSL certificate beforehand in the VPN Connection Setting settings beforehand, or use the CertAdd command etc. to register a root certificate containing the signed server SSL certificate in the list of Virtual Hub trusted CA certificates. If it is not registered, a confirmation message sometimes is displayed on the initial connection. If the certificate of the connected VPN Server cannot be trusted under the condition where the option to verify server certificates was enabled for the VPN Connection Setting, the connection will be promptly cancelled and continual reattempts at connection will be made.
Command-line	*AccountServerCertEnable [name]*
Arguments for "AccountServerCertEnable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.38 "AccountServerCertDisable": Disable VPN Connection Setting Server Certificate Verification Option

Command Name	**AccountServerCertDisable**
Purpose	Disable VPN Connection Setting Server Certificate Verification Option
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to disable the option to check whether the SSL certificate provided by the destination VPN Server can be trusted.
Command-line	*AccountServerCertDisable [name]*
Arguments for "AccountServerCertDisable":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.39 "AccountServerCertSet": Set Server Individual Certificate for VPN Connection Setting

Command Name	**AccountServerCertSet**
Purpose	Set Server Individual Certificate for VPN Connection Setting

Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to a VPN Server, use this to register the same certificate as the SSL certificate provided by the destination VPN Server. If the option to verify server certificates for VPN Connection Settings is enabled, you must either use this command to save the connection destination server SSL certificate beforehand in the VPN Connection Setting settings beforehand, or use the CAAdd command etc. to register a root certificate containing the signed server SSL certificate in the list of Virtual Hub trusted CA certificates. If the certificate of the connected VPN Server cannot be trusted under the condition where the option to verify server certificates was enabled for the VPN Connection Setting, the connection will be promptly cancelled and continual reattempts at connection will be made.
Command-line	*AccountServerCertSet [name] [/LOADCERT:cert]*
Arguments for "AccountServerCertSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/LOADCERT	Specify X.509 format certificate file name that the server individual certificate you wish to set is saved under.

6.5.40 "AccountServerCertDelete": Delete Server Individual Certificate for VPN Connection Setting

Command Name	**AccountServerCertDelete**
Purpose	Delete Server Individual Certificate for VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and a server individual certificate is registered for that VPN Connection Setting, use this to delete that certificate.
Command-line	*AccountServerCertDelete [name]*
Arguments for "AccountServerCertDelete":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.41 "AccountServerCertGet": Get Server Individual Certificate for VPN Connection Setting

Command Name	**AccountServerCertGet**

Purpose	Get Server Individual Certificate for VPN Connection Setting
Description	When a VPN Connection Setting is specified and a server Individual certificate is registered for that VPN Connection Setting, use this to get that certificate and save it as an X.509 format certificate file.
Command-line	*AccountServerCertGet [name] [/SAVECERT:path]*
Arguments for "AccountServerCertGet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/SAVECERT	Specify the certificate file name to save the server individual certificate in X.509 format.

6.5.42 "AccountDetailSet": Set Advanced Settings for VPN Connection Setting

Command Name	**AccountDetailSet**
Purpose	Set Advanced Settings for VPN Connection Setting
Description	Use this to customize the VPN protocol communication settings used when a VPN Connection Setting registered on a VPN Client is specified and that VPN Connection Setting connects to the VPN Server.
Command-line	*AccountDetailSet [name] [/MAXTCP:max_connection] [/INTERVAL:additional_interval] [/TTL:disconnect_span] [/HALF:yes|no] [/BRIDGE:yes|no] [/MONITOR:yes|no] [/NOTRACK:yes|no] [/NOQOS:yes|no]*
Arguments for "AccountDetailSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/MAXTCP	Specify, using an integer in the range 1 to 32, the number of TCP connections to be used for VPN communication. By using data transmission by multiple TCP connections for VPN communication sessions with VPN Servers it is sometimes possible to increase communication speed. Note: We recommend about 8 lines when the connection lines to the server are fast, and 1 line when using a slow connection such as dialup.
/INTERVAL	When communicating by VPN by establishing multiple TCP connections, specify in seconds, the establishing interval for each TCP connection. The standard value is 1 second.
/TTL	When specifying connection life of each TCP connection specify in seconds the keep-alive time from establishing a TCP connection until disconnection. If 0 is specified, keep-alive will not be set.

/HALF	Specify "yes" when enabling half duplex mode. When using two or more TCP connections for VPN communication, it is possible to use Half Duplex Mode. By enabling half duplex mode it is possible to automatically fix data transmission direction as half and half for each TCP connection. In the case where a VPN using 8 TCP connections is established, for example, when half-duplex is enabled, communication can be fixes so that 4 TCP connections are dedicated to the upload direction and the other 4 connections are dedicated to the download direction.
/BRIDGE	Specify "yes" when connecting to the VPN Server using Bridge / Router Mode. When using Bridge / Router Mode to connect, it is possible to provide bridging or routing to another network on the side of the virtual network adapter of the VPN Client. However, if the security policy of the user who is being used for connection denies the use of bridges or routing, then connection will fail.
/MONITOR	Specify "yes" when connecting to the VPN Server using Monitoring Mode. When a connection is made using Monitoring Mode, you can receive all packets that flow through the Virtual Hub. However, if the security policy of the user who is being used for connection does not allow Monitoring Mode, then connection will fail.
/NOTRACK	Specify "yes" will disable the adjustments of routing table. Normally "no" is specified.
/NOQOS	Specify "yes" when disabling VoIP / QoS functions. Normally "no" is specified.

6.5.43 "AccountRename": Change VPN Connection Setting Name

Command Name	**AccountRename**
Purpose	Change VPN Connection Setting Name
Description	Use this to specify a VPN Connection Setting registered on the VPN Client and change its name.
Command-line	*AccountRename [name] [/NEW:new_name]*
Arguments for "AccountRename":	
name	Specify the current name of the VPN Connection Setting whose name you want to change.
/NEW	Specify the new name after the change.

6.5.44 "AccountConnect": Start Connection to VPN Server using VPN Connection Setting

Command Name	**AccountConnect**
Purpose	Start Connection to VPN Server using VPN Connection Setting
Description	Use this to specify a VPN Connection Setting registered on the VPN Client and start a connection to the VPN Server using that VPN Connection Setting. A VPN Connection Setting that has a connecting status or a connected status will continue to be connected to the VPN Server, or continue to attempt to connect to the VPN Server until the AccountDisconnect command is used to disconnect the connection (Note however, if the AccountRetrySet command is used to specify the number of retries, connection attempts will be aborted when the specified value is reached.)
Command-line	*AccountConnect [name]*
Arguments for "AccountConnect":	
name	Specify the name of the VPN Connection Setting whose connection you want to start.

6.5.45 "AccountDisconnect": Disconnect VPN Connection Setting During Connection

Command Name	**AccountDisconnect**
Purpose	Disconnect VPN Connection Setting During Connection
Description	Use this to specify a VPN Connection Setting that is registered on the VPN Client and that is either in the condition of connecting or is connected, and immediately disconnect it.
Command-line	*AccountDisconnect [name]*
Arguments for "AccountDisconnect":	
name	Specify the name of the VPN Connection Setting to disconnect.

6.5.46 "AccountStatusGet": Get Current VPN Connection Setting Status

Command Name	**AccountStatusGet**
Purpose	Get Current VPN Connection Setting Status

Description	When a VPN Connection Setting that is registered on the VPN Client is specified and that VPN Connection Setting is currently connected, use this to get its connection status and other information.
Command-line	*AccountStatusGet [name]*
Arguments for "AccountStatusGet":	
name	Specify the name of the VPN Connection Setting whose information you want to get.

6.5.47 "AccountNicSet": Set Virtual Network Adapter for VPN Connection Setting to Use

Command Name	**AccountNicSet**
Purpose	Set Virtual Network Adapter for VPN Connection Setting to Use
Description	Use this to change the Virtual Network Adapter name that the existing VPN Connection Settings registered on the VPN Client will use for the connection to a VPN Server.
Command-line	*AccountNicSet [name] [/NICNAME:nicname]*
Arguments for "AccountNicSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/NICNAME	Specify the Virtual Network Adapter name to use when connecting to the VPN Server.

6.5.48 "AccountStatusShow": Set Connection Status and Error Screen to Display when Connecting to VPN Server

Command Name	**AccountStatusShow**
Purpose	Set Connection Status and Error Screen to Display when Connecting to VPN Server
Description	When a communication setting is registered on the VPN Client and that communication setting is being used to connect to the VPN Server, use this to set the connection status and error screen to be displayed on the computer display.
Command-line	*AccountStatusShow [name]*
Arguments for "AccountStatusShow":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.49 "AccountStatusHide": Set Connection Status and Error Screen to be Hidden when Connecting to VPN Server

Command Name	**AccountStatusHide**
Purpose	Set Connection Status and Error Screen to be Hidden when Connecting to VPN Server
Description	When a communication setting is registered on the VPN Client and that communication setting is being used to connect to the VPN Server, use this to set the connection status and error screen to not be displayed on the computer display.
Command-line	*AccountStatusHide [name]*
Arguments for "AccountStatusHide":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.50 "AccountSecureCertSet": Set User Authentication Type of VPN Connection Setting to Smart Card Authentication

Command Name	**AccountSecureCertSet**
Purpose	Set User Authentication Type of VPN Connection Setting to Smart Card Authentication
Description	Use this to set the user auth type to Smart Card Authentication for when a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting connects to the VPN Server. Also, you must specify the names of the certificate object and the private key object stored on the smart card.
Command-line	*AccountSecureCertSet [name] [/CERTNAME:cert] [/KEYNAME:key]*
Arguments for "AccountSecureCertSet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/CERTNAME	Specify the name of the certificate object stored on the smart card.
/KEYNAME	Specify the name of the private key object stored on the smart card. The private key must be compatible with the certificate specified by /CERTNAME.

6.5.51 "AccountRetrySet": Set Interval between Connection Retries for Connection Failures or Disconnections of VPN Connection Setting

Command Name	**AccountRetrySet**
Purpose	Set Interval between Connection Retries for Connection Failures or Disconnections of VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting attempts to connect to a VPN Server, use this to specify the interval to wait between connection attempts and the limit of how many times to retry connecting when communication with the VPN Server was disconnected or when the connection process failed. If the user authentication type is Smart Card Authentication, no connection retry will be performed regardless of the Number of Connection Attempts setting.
Command-line	*AccountRetrySet [name] [/NUM:num_retry] [/INTERVAL:retry_interval]*
Arguments for "AccountRetrySet":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.
/NUM	Specify the number of times to make consecutive retries. By specifying "999", there will be limitless attempts to reconection (always connect). By specifying "0", not attempt at reconnection will be made.
/INTERVAL	When attempting a reconnection, this sets how many seconds to wait after the previous disconnection or connection failure before starting the reconnection process.

6.5.52 "AccountStartupSet": Set VPN Connection Setting as Startup Connection

Command Name	**AccountStartupSet**
Purpose	Set VPN Connection Setting as Startup Connection
Description	Use this to specify a VPN Connection Setting registered on the VPN Client and set it as the startup connection. The VPN Connection Setting that is set as the startup connection will automatically start the connection process when the VPN Client service starts.
Command-line	*AccountStartupSet [name]*
Arguments for "AccountStartupSet":	

name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.53 "AccountStartupRemove": Remove Startup Connection of VPN Connection Setting

Command Name	**AccountStartupRemove**
Purpose	Remove Startup Connection of VPN Connection Setting
Description	When a VPN Connection Setting registered on the VPN Client is specified and that VPN Connection Setting is currently set as a startup connection, use this to delete the startup connection.
Command-line	*AccountStartupRemove [name]*
Arguments for "AccountStartupRemove":	
name	Specify the name of the VPN Connection Setting whose setting you want to change.

6.5.54 "AccountExport": Export VPN Connection Setting

Command Name	**AccountExport**
Purpose	Export VPN Connection Setting
Description	Use this to specify a VPN Connection Setting registered on the VPN Client and export its contents as a text file. By exporting a VPN Connection Setting file, and then later, importing it, you can duplicate the contents of a VPN Connection Setting. Also, because it gets saved as a text file, you can edit the contents using a conventional text editor. The export destination file is saved as a UTF-8 format text file. Also, it is convenient to save the file name with the file extension .vpn as this file extension is associated to the Windows Edition VPN Client Manager.
Command-line	*AccountExport [name] [/SAVEPATH:savepath]*
Arguments for "AccountExport":	
name	Specify the name of the VPN Connection Setting to export.
/SAVEPATH	Specify a file name for the save destination.

6.5.55 "AccountImport": Import VPN Connection Setting

Command Name	**AccountImport**
Purpose	Import VPN Connection Setting
Description	Use this to import the VPN Connection Setting file that was exported by the AccountExport command and add it to the VPN Client.
Command-line	*AccountImport [path]*
Arguments for "AccountImport":	
path	Specify the file name of the import source.

6.5.56 "RemoteEnable": Allow Remote Management of VPN Client Service

Command Name	**RemoteEnable**
Purpose	Allow Remote Management of VPN Client Service
Description	Use this to allow management of a VPN Client service from a remote computer that is not localhost, via a remote connection by Command Line Management Utility or VPN Client Manager.
Command-line	*RemoteEnable*
Arguments for "RemoteEnable":	
No arguments are required.	

6.5.57 "RemoteDisable": Deny Remote Management of VPN Client Service

Command Name	**RemoteDisable**
Purpose	Deny Remote Management of VPN Client Service
Description	Use this to deny management of a VPN Client service from a remote computer that is not localhost, via a remote connection by Command Line Management Utility or VPN Client Manager.
Command-line	*RemoteDisable*
Arguments for "RemoteDisable":	
No arguments are required.	

6.5.58 "KeepEnable": Enable the Keep Alive Internet Connection Function

Command Name	**KeepEnable**
Purpose	Enable the Keep Alive Internet Connection Function
Description	This allows you to enable the Keep Alive Internet Connection Function. By using the Keep Alive Internet Connection Function for network connection environments where connections will automatically be disconnected when there are periods of no communication that are longer than a set period, it is possible to keep alive the Internet connection by sending packets to a nominated server on the Internet at set intervals. You can set a destination host name etc, by using the KeepSet command. To execute this command on a VPN Server or VPN Bridge, you must have administrator privileges.
Command-line	*KeepEnable*
Arguments for "KeepEnable":	
No arguments are required.	

6.5.59 "KeepDisable": Disable the Keep Alive Internet Connection Function

Command Name	**KeepDisable**
Purpose	Disable the Keep Alive Internet Connection Function
Description	This allows you to disable the Keep Alive Internet Connection Function. To execute this command on a VPN Server or VPN Bridge, you must have administrator privileges.
Command-line	*KeepDisable*
Arguments for "KeepDisable":	
No arguments are required.	

6.5.60 "KeepSet": Set the Keep Alive Internet Connection Function

Command Name	**KeepSet**
Purpose	Set the Keep Alive Internet Connection Function

Description	Use this to set the destination host name etc. of the Keep Alive Internet Connection Function. For network connection environments where connections will automatically be disconnected where there are periods of no communication that are longer than a set period, by using the Keep Alive Internet Connection Function, it is possible to keep alive the Internet connection by sending packets to a nominated server on the Internet at set intervals. When using this command, you can specify the following: Host Name, Port Number, Packet Send Interval, and Protocol. Packets sent to keep alive the Internet connection will have random content and personal information that could identify a computer or user is not sent. You can use the KeepEnable command or KeepDisable command to enable/disable the Keep Alive Internet Connection Function. KeepSet does not change the enabled/disabled status. To execute this command on a VPN Server or VPN Bridge, you must have administrator privileges.
Command-line	*KeepSet [/HOST:host:port] [/PROTOCOL:tcp|udp] [/INTERVAL:interval]*
Arguments for "KeepSet":	
/HOST	Specify the host name or IP address, and port number of the destination using the format "host name:port number".
/PROTOCOL	Specify either tcp or udp.
/INTERVAL	Specify, in seconds, the interval between the sending of packets.

6.5.61 "KeepGet": Get the Keep Alive Internet Connection Function

Command Name	**KeepGet**
Purpose	Get the Keep Alive Internet Connection Function
Description	Use this to get the current setting contents of the Keep Alive Internet Connection Function. In addition to the destination's Host Name, Port Number, Packet Send Interval and Protocol, you can obtain the current enabled/disabled status of the Keep Alive Internet Connection Function.
Command-line	*KeepGet*
Arguments for "KeepGet":	
No arguments are required.	

6.5.62 "MakeCert": Create New X.509 Certificate and Private Key

Command Name	**MakeCert**
Purpose	Create New X.509 Certificate and Private Key
Description	Use this to create a new X.509 certificate and private key and save it as a file. The algorithm used to create the public key and private key of the certificate is RSA 1024 bit. You can choose to create a root certificate (self-signed certificate) or a certificate signed by another certificate. To create a certificate that is signed by another certificate, you require a private key file (base 64 encoded) that is compatible with the certificate that uses the signature (X.509 format file). When creating a certificate, you can specify the following: Name (CN), Organization (O), Organization Unit (OU), Country (C), State (ST), Locale (L), Serial Number, and Expiration Date. The created certificate will be saved as an X.509 format file and the private key file will be saved in a Base 64 encoded RSA 1024 bit format file. The MakeCert command is a tool that provides the most rudimentary function for creating certificates. If you want to create a more substantial certificate, we recommend that you use either free software such as OpenSSL, or commercial CA (certificate authority) software. Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually performs the RSA computation, generates the certificate data and saves it to file is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*MakeCert [/CN:cn] [/O:o] [/OU:ou] [/C:c] [/ST:st] [/L:l] [/SERIAL:serial] [/EXPIRES:expires] [/SIGNCERT:signcert] [/SIGNKEY:signkey] [/SAVECERT:savecert] [/SAVEKEY:savekey]*
Arguments for "MakeCert":	
/CN	Specify the Name (CN) item of the certificate to create. You can specify "none".
/O	Specify the Organization (O) item of the certificate to create. You can specify "none".

/OU	Specify the Organization Unit (OU) item of the certificate to create. You can specify "none".
/C	Specify the Country (C) item of the certificate to create. You can specify "none".
/ST	Specify the State (ST) item of the certificate to create. You can specify "none".
/L	Specify the Locale (L) item of the certificate to create. You can specify "none".
/SERIAL	Specify the Serial Number item of the certificate to create. Specify using hexadecimal values. You can specify "none".
/EXPIRES	Specify the Expiration Date item of the certificate to create. If you specify "none" or "0", 3650 days (approx. 10 years) will be used. You can specify a maximum of 10950 days (about 30 years).
/SIGNCERT	For cases when the certificate to be created is signed by an existing certificate, specify the X.509 format certificate file name to be used to sign the signature. When this parameter is omitted, such signature signing is not performed and the new certificate is created as a root certificate.
/SIGNKEY	Specify a private key (RSA, base-64 encoded) that is compatible with the certificate specified by /SIGNCERT.
/SAVECERT	Specify the file name to save the certificate you created. The certificate is saved as an X.509 file that includes a public key that is RSA format 1024 bit.
/SAVEKEY	Specify the file name to save private key that is compatible with the certificate you created. The private key will be saved as an RSA-format 1024-bit private key file.

6.5.63 "TrafficClient": Run Network Traffic Speed Test Tool in Client Mode

Command Name	**TrafficClient**
Purpose	Run Network Traffic Speed Test Tool in Client Mode
Description	Use this to execute the communication throughput measurement tool's client program. Two commands, TrafficClient and TrafficServer, are used for the communication throughput measurement tool to enable the measurement of communication throughput that can be transferred between two computers connected by IP network. The TrafficServer command is used first on another computer which puts the communication throughput measurement tool server in a listening condition. Then the TrafficClient command is used to connect to that

	server by specifying its host name or IP address and port number, which makes it possible to measure the communication speed. Measurement of the communication speed is carried out by concurrently establishing multiple TCP connections and calculating the actual number of bits of data that can be transferred within a specified time based on the respective results of transferring the maximum stream data on each connection and then using that to calculate the average value (bps) of communication throughput. Normally when there is one TCP connection, it is common to only be able to achieve communication speeds slower than the actual net throughput because of limitations related to the TCP algorithm. We therefore recommend the establishment of multiple concurrent TCP connections when measuring communication results. Because the throughput that is measured using this measurement method is calculated from the bit length of the data that arrives on the receiver side as a stream by TCP, the packet loss that occurs during transfer and the packets with corrupted data are not included in the packets that actually arrive, which means it is possible to calculate a genuine value that is close to the maximum possible communication bandwidth of the network. Using the measurement results, i.e. the stream size transferred by TCP, the approximate value of data volume that actually passed through the network is calculated and this is divided by time to calculate the bits per sec (bps). The calculation assumes the type of the physical network is Ethernet (IEEE802.3) and the MAC frame payload size is 1,500 bytes (TCP MSS is 1,460 bytes). By specifying the /RAW option, the calculation will not make corrections for the TCP/IP header and MAC header data volume. Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually conducts communication and measures the throughput is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*TrafficClient [host:port] [/NUMTCP:numtcp] [/TYPE:download|upload|full] [/SPAN:span] [/DOUBLE:yes|no] [/RAW:yes|no]*
Arguments for "TrafficClient":	
host:port	Specify the host name or IP address and port number that the communication throughput measurement tool server (TrafficServer) is listening for. If the port number is omitted, 9821 will be used.

/NUMTCP	Specify the number of TCP connections to be concurrently established between the client and the server for data transfer. If omitted, 32 will be used.
/TYPE	Specify the direction of data flow when throughput measurement is performed. Specify one of the following options: "download", "upload" or "full". By specifying "download" the data will be transmitted from the server side to the client side. By specifying "upload" the data will be transmitted from the client side to the server side. By specifying "full", the data will be transferred in both directions. When "full" is specified, the NUMTCP value must be an even number of two or more (half the number will be used for concurrent TCP connections in the download direction and the other half will be used in the upload direction). If this parameter is omitted, "full" will be used.
/SPAN	Specify, using seconds, the time span to conduct data transfer for the measurement of throughput. If this parameter is omitted, "15" will be used.
/DOUBLE	When "yes" is specified, the throughput of the measured result will be doubled and then displayed. This option is used for cases when a network device etc. is somewhere on the data route and the total throughput capability that is input and output by this network device is being measured.
/RAW	By specifying "yes", the calculation will not make corrections for the TCP/IP header and MAC header data volume.

6.5.64 "TrafficServer": Run Network Traffic Speed Test Tool in Server Mode

Command Name	**TrafficServer**
Purpose	Run Network Traffic Speed Test Tool in Server Mode
Description	Use this to execute the communication throughput measurement tool's server program. Two commands, TrafficClient and TrafficServer, are used for the communication throughput measurement tool to enable the measurement of communication throughput that can be transferred between two computers connected by IP network. To set the TCP port of this computer to the Listen status to listen for the connection from the TrafficClient of another computer, specify the port number and start the server program using the TrafficServer command. You can display more detailed information on the communication

	throughput measurement tool by inputting "TrafficClient /?". Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually conducts communication and measures the throughput is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*TrafficServer [port]*
Arguments for "TrafficServer":	
port	Specify, using an integer, the port number at which to listen for the connection. If the specified port is already being used by another program, or if the port cannot be opened, an error will occur.

6.5.65 "Check": Check whether SoftEther VPN Operation is Possible

Command Name	**Check**
Purpose	Check whether SoftEther VPN Operation is Possible
Description	Use this to check if the current computer that is running vpncmd is a suitable operation platform for SoftEther VPN Server / Bridge. If this check passes on a system, it is highly likely that SoftEther VPN software will operate correctly on that system. Also, if this check does not pass on a system, then this indicates that some type of trouble may arise if SoftEther VPN software is used on that system.
Command-line	*Check*
Arguments for "Check":	
No arguments are required.	