Attachmate®

INFOConnect Enterprise Edition

Product Guide

Copyrights and Notices

Attachmate® INFOConnect® Enterprise Edition

Patents

This Attachmate software is protected by U.S. patents 6252607 and 6803914.

Trademarks

Attachmate, the Attachmate logo, CryptoConnect, FileXpress, and PEPgate are either registered trademarks or trademarks of Attachmate Corporation in the USA. INFOConnect is a registered trademark of Unisys Corporation. FIPS 140-1 Validated is a certification mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments. All other trademarks, trade names, or company names referenced in product materials are used for identification only and are the property of their respective owners.

Attachmate Software License Agreement

A copy of the Attachmate software license agreement governing this product can be found in a 'license' file in the root directory of the product.

Licensor

Attachmate Corporation
1500 Dexter Avenue North
Seattle, WA 98109 USA
+1.206.217.7100
http://www.attachmate.com

Third-Party Notices

Third Party Terms and notices are provided in a 'thirdpartynotices' file in the root directory of the product.

Contents

Attachmate INFOConnect Overview

Attachmate INFOConnect Enterprise Edition delivers PC connectivity to mainframes through a suite of terminal emulators, transports, connection tools, print and router services, encryption modules, utilities, APIs, SDKs, and custom installers. Using INFOConnect, users can run host applications, transfer files, and integrate data into other Windows applications. The navigational, scripting, and scheduling tools simplify interaction with host applications and streamline user tasks.

New Features

The following new features are available in this release:

- Windows 7 compatibility and Vista certification. Both INFOConnect and the Print and Transaction Router (PTR) are Windows 7 compatible and certified for Vista.

- Updated SSL/TLS and SSH Security Components. These components are validated against the stringent Federal Information Processing Standards (FIPS 140-2) federal security specification, which enables Attachmate products to adhere to the DoD PKI certification requirements.

- FIPS 140-2 connections. You can now use FIPS mode for both SSH and SSL/TLS connections. FIPS mode enforces the United States government Federal Information Processing Standard (FIPS) 140-2 for the connection. When FIPS mode is enabled, all available settings use security protocols and algorithms that meet this standard.

- PTR Server and PTR Plus (with CUPPS support) options available. For details, contact Attachmate.

- Encryption for CASL and EXTRA! macros. To protect sensitive data in macros, EXTRA! and CASL macros (including source files) are automatically encrypted when they run or when they're saved in their authoring application. Encrypted macros will only run in INFOConnect 9.1 and later. For details on the macro encryption settings, see "Modify Application Settings" on page 36.

- New installation options. During a standard installation, you can change the location of user data and application data on the Data Location tab. In a customized installation, you can assign a new file extension for sessions. For details, see TechNote 2537.

- New display font improves font scalability. INFOConnect installs the Segoe UI Mono TrueType font that includes special emulation characters. To use this font in a session, choose Options > Settings, select Display on the left. From the Fonts tab, choose the font from the menu.

- Print option for screen history. You can print the screen history for 3270, 5250, UTS, ALC, and T27 sessions. To set formatting options, choose Edit > Settings, select Productivity on the left, and click the Screen History tab. To print, from the Screen History tool bar, click the Print icon and specify a printer.

- Size limits for trace files. See "Manage Trace Files" on page 67.

- Ability to prevent sessions from disconnecting when computer goes into standby mode. A new global preference gives the application more control over system standby (or "sleep") mode, which can cause host sessions to disconnect. To specify the Prevent System Sleep preference, choose Options > Global Preferences and click the General tab. How you use this preference depends on your operating system.

  - Windows 7 and Vista enter standby mode without first prompting the user. To prevent host disconnections when the computer is idle, select the Prevent System Sleep check box. All other settings (a colored or cleared check box), allow the computer to enter standby mode.

  - Windows XP enters standby mode only after prompting the user. To keep this behavior, leave Prevent System Sleep at its default setting (a colored box). To prevent the system from entering standby mode, select Prevent System Sleep. To allow the computer to enter standby mode without a prompt, clear the check box.

- Encryption option for Auto Complete dictionary. To enhance security, the Auto Complete dictionary (productivity feature) can now be encrypted. For details, see TechNote 2537.

- New layout option. INFOConnect now includes an option that causes layouts to open sessions sequentially, as in EXTRA! For details, see TechNote 2539.

- Access to EDS Shares via TCP/IP. A new INFOConnect transport library has been added to provide access to the EDS Shares mainframes via TCP/IP. The EDS Shares mainframe must be running software that supports TCP/IP. UDP/IP access remains available.

- Enhanced privacy filters. You can filter sensitive data in more areas of the application, including the Print Screen, Cut, Copy, and Paste commands and the Recent Typing productivity feature. Privacy filters can prevent screen data from being published to Microsoft Word and Outlook. Filters are defined on a per-user basis and apply to all sessions for the given user. To configure privacy filters, in the Accessory Manager, choose Options > Global Productivity Settings, and click Information Privacy settings.

INFOConnect Products

Attachmate INFOConnect Enterprise Edition is available in these product configurations.

- INFOConnect Enterprise Edition for Unisys
  Delivers access to Unisys A-Series mainframes (T27 emulators) and Unisys 2200 mainframes (UTS emulators).

- INFOConnect Enterprise Edition for Unisys, IBM, and Open Systems
  Delivers access to Unisys A-Series mainframes (T27 emulators), Unisys 2200 mainframes (UTS emulators), IBM mainframes (3270 emulators), IBM AS/400s (5250 emulators) and UNIX/Open VMS hosts (VT emulators).

- INFOConnect Enterprise Edition for Airlines
  Delivers access to IBM TPF mainframes and major Global Distribution Systems (ALC emulators), Unisys A-Series mainframes (T27 emulators) and Unisys 2200 mainframes (UTS emulators). A comprehensive set of components and tools developed for the airline/travel industry is also provided.

- INFOConnect Enterprise Edition for Airlines, IBM and Open Systems
  Delivers access to IBM TPF mainframes and major Global Distribution Systems (ALC emulators), Unisys A-Series mainframes (T27 emulators) and Unisys 2200 mainframes (UTS emulators), IBM mainframes (3270 emulators), IBM AS/400s (5250 emulators) and UNIX/Open VMS hosts (VT emulators). A comprehensive set of components and tools developed for the airline/travel industry is also provided.

- INFOConnect Print and Transaction Router (PTR)
  Manages printing and transaction routing by enabling input devices to cooperatively use and share several output devices (queues) through communication links called PTR routes. Three PTR products are available: standard PTR, PTR Plus (includes CUPPs support), and PTR Server. You can install a PTR product with INFOConnect Accessory Manager or as a stand-alone application.

- Attachmate INFOConnect Airlines Gateway
  Manages communication between networked PCs using Attachmate Airlines Client Emulation products and any host that supports Mapping of Airline Traffic over Internet Protocol (MATIP) or any major Global Distribution Systems (GDS) including Sabre, Worldspan, Amadeus, EDS Shares, or Apollo\Galileo. Supports up to 100 terminal addresses per host protocol. For more information, see the *INFOConnect Airlines Gateway Product Guide*.

Major Components and Utilities

Depending on the terms of your INFOConnect license, your INFOConnect product may include some or all of the following components and utilities.

Component	Description
Accessory Manager Frame	Enables PCs using terminal emulators to communicate with hosts such as Unisys mainframes, IBM mainframes, UNIX hosts, or any major Global Distribution System (GDS).
Attachmate Installer Program	Windows Vista Certified MSI Installers created with the Windows Installer XML (WIX) Toolkit and use the standard Attachmate UI component (setup.exe). Includes the Attachmate Customization Tool.
Attachmate Customization Tool	Can be used to customize the installation package using MST files. The Attachmate Customization Tool is a complete replacement for the Custom Installation Wizard, which was used in previous INFOConnect releases to create customized installation images.
Reflection Security Components	Security components that use SSL/TLS or SSH protocols and meet FIPS 140-2 security standards.
DoD-PKI Encryption Module	Provides public key infrastructure (PKI) authentication support certified by Joint Interoperability Test Command (JITC).
Emulators	Provide communication between PCs and mainframes including Global Distribution Systems (GDSs). The INFOConnect terminal emulators include: • ALC (IBM TPF mainframes and GDSs) • T27 (Unisys A-Series mainframes) • UTS (Unisys 2200 mainframes) • 3270, 5250, VT (IBM mainframes, AS/400s, VT hosts)
Split Screen Transports	Enable PCs using Microsoft Windows and INFOConnect Connectivity Services (ICS) to share an INFOConnect path with multiple INFOConnect applications. When used with a Split Screen-enabled Accessory Manager frame, the frame provides additional functionality to the user.
Transports	Enable PCs using INFOConnect Connectivity Services to access hosts and mainframes. For more information, see the following section, Product Features.

EXTRA! for Accessory Manager	Provides a suite of terminal emulators (3270, 5250, and VT) and connection tools that enable PCs to communicate with IBM mainframes, AS/400s, and UNIX\Open VMS hosts.
T27 Print Services and Configuration Utility	Provides a printer pass-through application for T27 connectivity.
	Controls the way T27 Print Services operates. For example, you can specify how Print Services communicates with the host or which printer is used.
Print and Transaction Router (PTR)	Manages printing and transaction routing by enabling several input devices (hosts) to cooperatively use and share several output devices (queues) through communication links called PTR routes. Three PTR products are available: standard PTR; PTR Plus (includes CUPPs support); and PTR Server. You can install a PTR product with Accessory Manager or as a stand-alone application.
Utilities	Export/Import utility: exports data from an INFOConnect database (IC32.cfg) into an .ini or .csv file, as well as imports data from an .ini or .csv file into an INFOConnect database. For more information, open ExpImp32.hlp in the Infocnee\Enu folder.
	Copy ICS Database utility: creates a copy of an INFOConnect database that is identical to the original database except for the location name of the executable files. For more information, open Copics32.hlp in the Infocnee\Enu folder.
	Attachmate Version utility (Atmver.exe): creates a file that displays the version numbers of all INFOConnect products that are installed.
	Getdid.exe: increases the number of sessions allowed by the transports.
	Testgms.exe: for more information, contact Technical Support.

Product Features

The feature groups that are available for the INFOConnect products during installation are described in the following sections.

- INFOConnect Enterprise Edition for Unisys

- INFOConnect Enterprise Edition for Airlines

- INFOConnect Stand-alone Print and Transaction Router (PTR)

See the *INFOConnect Airlines Gateway Product Guide* for information on INFOConnect Airlines Gateway.

INFOConnect Enterprise Edition for Unisys

The feature groups for INFOConnect Enterprise Edition for Unisys are described in the following tables.

- Unisys Transports and Options

- INFOConnect Options Pack

- FTP Client

The feature groups for INFOConnect Enterprise Edition for Unisys, IBM and Open Systems are described in the following tables.

- Unisys Transports and Options

- INFOConnect Options Pack

- FTP Client

- EXTRA! for Accessory Manager

Unisys Transports and Options

Feature	Description
TCPA	Provides access to hosts using the TCP/IP network protocol.
HLCN	Provides NETBIOS connectivity to Unisys A-Series hosts.
INT1	Provides access to Unisys 1100/1200 hosts using the TCP/IP network protocol.
MATIP	Provides access to Unisys hosts using the MATIP network protocol.
FileXpress-XST Client	Enables PCs to connect directly through the XST port and transfer files with a Unisys ClearPath NX/LX series or A-Series mainframe. Requires the host component.
Response Time Monitor Utility	Displays information about communication between one or more PCs running INFOConnect Accessory Manager and a host. You can use this information to identify problems with either your network performance or your host.
CryptoConnect Client ETS	Manages FIPS-140-1 certified encryption between 32-bit INFOConnect UTS or T27 emulators and the CryptoConnect gateway. Resides on a separate PC from the gateway and encrypts and decrypts communication between the client and the gateway.
WinFTP	Transfers files between your PC and any host such as a Unisys ClearPath IX, 2200 Series host, or a UNIX host running FTP server software. The PC must communicate with the host via a WinSock-compatible TCP/IP network.
CCF	Provides CCF protocol over WinSock for migrating NX/View products.

INFOConnect Options Pack

Feature	Description
GraphX32	Enables PCs using Microsoft Windows and INFOConnect Connectivity Services to emulate the graphics capability of the UTS60 terminal by interpreting the UTS60 graphics protocol commands as they are received across an INFOConnect path.
INFOConnect Automation Development Kit	For development of Windows applications that interact with Attachmate terminal emulators. For more information, see the INFOConnect HLLAPI Programmer's Reference.
INFOConnect DataXpress	Enables PCs to transfer files to and from Unisys ClearPath IX or 2200 Series mainframes.
FileXpress–XST API	For Unisys Libra systems only. Integrates FileXpress–XST functions into custom applications. For more information, see the *FileXpress–XST API Programmer's Reference.*
INFOConnect Connectivity Services Development Kit (IDK)	Develop applications and components that use the INFOConnect Connectivity Service (ICS). For more information, see the *INFOConnect Development Kit Basic Programming Reference Manual.*
INFOConnect OLE Custom Control	Develop Windows applications that use INFOConnect paths. For more information, see the *INFOConnect OCX Programmer's Reference.*

FTP Client

Feature	Description
Utilities	Reflection software utilities that provide reliable file transfers with any file server and secure options for users with those requirements.
Kerberos Manager	Manages and configures the Reflection Kerberos client.
Key Agent	Holds multiple private keys that can be used in a Secure Shell (SSH) connection for public key authentication. Also enables agent forwarding for a SSH connection.

EXTRA! for Accessory Manager

Feature	Description
EXTRA! for Accessory Manager	A suite of terminal emulators (3270, 5250, and VT) and connection tools that enables PCs to communicate with IBM mainframes, AS/400s, and UNIX\Open VMS hosts. EXTRA! for Accessory Manager is a stand-alone application that you can run by itself; or you can create and open EXTRA! sessions within Accessory Manager. To use EXTRA! sessions within Accessory Manager, you must keep both applications installed.

INFOConnect Enterprise Edition for Airlines

The tables in the following pages describe the following feature groups for INFOConnect Enterprise Edition for Airlines.

- Airline Transports and Options
- INFOConnect Options Pack
- FTP Client
- EXTRA! for Accessory Manager (for INFOConnect Enterprise Edition for Airlines, IBM and Open System only)

Airline Transports and Options

Feature	Description
INT1	Provides access to Unisys 1100/1200 hosts using the TCP/IP network protocol.
MATIP for ALC	Provides access to airline hosts using the MATIP network protocol.
MATIP for UTS	Provides access to Unisys hosts using the MATIP network protocol.
ATSTCP	Provides access to the Galileo Apollo GDS.
UPDFRAD	Enables PCs to communicate with a SHARES host via UDP.
Sabre	Provides high-speed access to the Sabre GDS.
CryptoConnect Client ETS	Manages FIPS-140-1 certified encryption between INFOConnect UTS or T27 emulators and the CryptoConnect gateway. Resides on a separate PC from the gateway and encrypts and decrypts communication between the client and the gateway.
Airlines Gateway	Provides access to the INFOConnect Airlines Gateway transport.

INFOConnect Options Pack

Feature	Description
GraphX32	Enables PCs using Microsoft Windows and INFOConnect Connectivity Services to emulate the graphics capability of the UTS60 terminal by interpreting the UTS60 graphics protocol commands as they are received across an INFOConnect path.
INFOConnect Automation Development Kit	Develop Windows applications that interact with Attachmate terminal emulators. For more information, see the *INFOConnect HLLAPI Programmer's Reference*.
INFOConnect DataXpress	Enables PCs to transfer files to and from a Unisys ClearPath IX or 2200 Series mainframe.
INFOConnect Connectivity Services Development Kit (IDK)	Develop applications and components that use the INFOConnect Connectivity Service (ICS). For more information, see the *INFOConnect Development Kit Basic Programming Reference Manual*.
INFOConnect OLE Custom Control	Develop Windows applications that use INFOConnect paths. For more information, see the *INFOConnect OCX Programmer's Reference*.

FTP Client

Feature	Description
Utilities	Reflection software utilities that provide reliable file transfers with any file server and secure options for users with those requirements.
Kerberos Manager	Manages and configures the Reflection Kerberos client.
Key Agent	Holds multiple private keys that can be used in a Secure Shell (SSH) connection for public key authentication. Also enables agent forwarding for a SSH connection.

EXTRA! for Accessory Manager

Feature	Description
EXTRA! for Accessory Manager	A suite of terminal emulators (3270, 5250, and VT) and connection tools that let your PCs communicate with IBM mainframes, AS/400s, and UNIX\Open VMS hosts. EXTRA! for Accessory Manager is a stand-alone application that you can run by itself; or you can create and open EXTRA! sessions within Accessory Manager. To use EXTRA! sessions within Accessory Manager, you must keep both applications installed.

INFOConnect Stand-alone Print and Transaction Router

The transports for INFOConnect Stand-alone Print and Transaction Router are described in the following table.

Feature	Description
INT1	Provides access to Unisys 1100/1200 hosts using the TCP/IP network protocol.
MATIP for ALC	Provides access to airline hosts using the MATIP network protocol.
MATIP for UTS	Provides access to Unisys hosts using the MATIP network protocol.
ATSTCP	Provides access to the Galileo Apollo GDS.
UPDFRAD	Enables PCs to communicate with a SHARES host via UDP.
Sabre IP	Provides high-speed access to the Sabre GDS.
Airlines Gateway	Provides access to the INFOConnect Airlines Gateway transport.

System Requirements

For production environments, many users install the various INFOConnect components on separate computers. Specific requirements will vary based on which components are installed, and on other hardware and software components present.

INFOConnect meets the requirements for Windows Vista certification. For Windows Vista platform requirements, follow the Microsoft guidelines.

Note: Attachmate cannot confirm the accuracy of performance, or any other claims related to non Attachmate products.

The minimum system requirements are covered in the following table.

System Component	Description
Operating System	Windows 7 Windows Vista SP1 or greater Windows XP Professional SP2 or greater Windows 2000 Professional with SP4 Terminal Server with Windows 2000 Server or Windows Server 2003 (SP6a) Citrix MetaFrame with Windows 2000 Server or Windows Server 2003

Processor	Intel single processor (or equivalent) Intel multiple processor (or equivalent)
RAM	256 MB

- Windows 2000 Server (latest SP) Windows Terminal Services

- Windows Server 2003 Windows Terminal Services

- Citrix MetaFrame XP Presentation Server, Feature Release 2 or later

APIs and Development Kits

The APIs and development kits that are available for purchase with INFOConnect are documented in the online manuals that can be found in the Pdf_docs_infoconnect directory.

Online Manuals and Guides

Title	Filename/Description
INFOConnect CASL Script Language Guide	Casl_lang_ref.pdf Documents the Common Accessory Script Language (CASL), which is used to create macros that interact with hosts, users, and other macros.
INFOConnect Development Kit Basic Programming Reference Manual	Idk_basic_prog_ref.pdf Provides detailed information about the INFOConnect Connectivity Services (ICS) programming interface, messages, and data types available for ICS Accessory development and for the development of additional data filters (Service Libraries) and connection types (External Interface Libraries).
INFOConnect Development Kit Basic Developer's Guide	Idk_basic_dev_gd.pdf Explains how to install and use the INFOConnect Development Kit.
INFOConnect HLLAPI Programmer's Reference	Ihllapi_prog_ref.pdf Explains how to use HLLAPI to write Windows applications that interact with Attachmate terminal emulators and therefore with host applications.
INFOConnect OCX Programmer's Reference	Ocx_prog_ref.pdf Explains how to use the OLE Custom Control to write Windows applications that use INFOConnect paths.
FileXpress XST–API Programmer's Reference	Filexpress_api_prog_ref.pdf Explains how to integrate FileXpress–XST functions into custom applications.
PTR User API Programmer's Reference	Ptr_uapi_prog_ref.pdf Provides details on creating applications to print vouchers and other specialized tickets from PCs by sending data directly to a printer.
PTR OLE API Programmer's Reference	Ptr_oleapi_prog_ref.pdf Provides details about creating an application that monitors PTR routes.
PTR API Programmer's Reference	Ptr_api_prog_ref.pdf Provides details about using the PTR Development Kit to design a custom host filter.

About This Product Guide and Online Help

Information about INFOConnect is available in this product guide and the component Help systems.

INFOConnect Enterprise Edition Product Guide	This guide provides an overall description of INFOConnect, its components, and the solutions you can create with it.
Component Help Systems	General help and context sensitive help is available. The Help systems use WinHlp32.exe, which is not included with Windows 7 or Vista. To open INFOConnect help on Windows 7 and Vista, see Attachmate Technical Note 2294 (http://support.attachmate.com/techdocs/2294.html). Technical Note 2294 also contains information on resolving the following error message that may appear when accessing Help: `There was a problem running the macro.(1037).`

Installation Overview and Considerations

The INFOConnect installers use standard MSI-based deployment technologies. An MSI installation either happens in its entirety or nothing is installed. Any utility that supports the deployment of MSI files can deploy INFOConnect. MSI packages and files also provide a standard way for users to customize the installer.

The INFOConnect installers were built using the Windows Installer XML (WIX) open source toolkit. They're Windows 7 compatible and certified on Windows Vista. The WIX toolkit stores the installer source as XML and allows for standard tools to be used for editing and deployment.

About the Attachmate Installer Program

The user interface for the INFOConnect installers is the standard Attachmate Installer Program — `setup.exe`.

The Attachmate Installer Program provides a standard interface and includes the Attachmate Customization Tool that can be used to customize the installation package using transform (.mst) files.

The installer and INFOConnect are digitally signed and the deliverables are stored as external CAB files. The installer provides for the ability to advertise, publish, and install on demand. INFOConnect also supports the Add/Remove program, including support for a complete uninstall.

The use of patch (.msp) files, using standard MSI mechanisms, is supported with the ability to install a patch with a basic or no user interface along with the ability to uninstall patches.

INFOConnect evaluation software can be converted to a full working version by installing the purchased product, which will upgrade the evaluation software.

User and Application Data Locations

With the Attachmate Installer Program you can customize the locations for the user data and the application data. User data includes files such as macros, schemes, and sessions. Application data includes trace logs and global configuration files such as IC32.cfg and InsMgr32.cfg.

Because of Microsoft logo certification requirements, application data should not be stored under the Program Files directory.

On Windows 7 and Vista, the `Users\Username\Documents` directory is equivalent to the My Documents directory and the `Users\Public\Documents` directory is equivalent to the `All Users\Documents` directory.

User Data Locations

Select this directory	To install products so that
My Documents	Each user has separate user data, including sessions, color schemes, layouts, and the like, and each user may change, create, and delete them without restriction.
All Users\Documents	All users share a single set of sessions and other user data, and all users can add, modify, and delete sessions.
User Defined Directory	Users can to choose where to install the user data files. The user data files location is changed to install to `C:\Documents and Settings\ userid\MyUserFiles`. When the installation is complete, a registry key `HKLM\SOFTWARE\Attachmate\ Accessory Manager\CustomUserDocumentsPath = USERDATALOC_CUSTOM_PATH` contains this path. When the product is run for the first time, it replaces *userid* in this string with the current logged in user's ID, creates the user data location, and copies files to that location.

Application Data Locations

Select this directory	To install products so that
My Documents	Each user has a separate database with separately configurable paths, and each user may change, create, and delete them without restriction. Some transports/options don't support using the `My Documents` directory location.
All Users\Documents	All users share a single database with all sessions and paths, and all users can add, modify, and delete paths. If the end users are "restricted users" under Windows, they will be unable to edit, add, or delete anything from the database. If they are administrators, they can modify, add, and delete without restrictions.

If two or more users share the same PC, the administrator can allow users to create or modify their own INFOConnect paths or restrict users by creating or modifying the paths for them.

Single Users and Multiple Users

The installer correctly handles multiple users per machine and roaming profiles. It also follows Vista user account control (UAC) requirements when storing settings files.

In most customizations, you would choose the `My Documents` directory option for user data (macros, schemes, and sessions). That way, when each user logs on to Windows the first time after INFOConnect is installed, the system automatically creates a set of user data for that user in the specified location.

The `All Users\Documents` directory option is selected to create a single set of application data that all users share.

By default, all users have the same access to all configuration options for the emulators, file transfer products, and transports. However, you can load a different security file to limit access to functions within Accessory Manager, and you can add passwords to the Database Editor.

In this way, an administrator can control how much access the users have to various functions. You can view detailed information about this in the Help after you install the products. For information about Accessory Manager security, click Administrative Help from the Accessory Manager Help menu. For information about Database Editor security, click Database Editor Help Topics from the Database Editor Help menu.

To change a PC from single-user to multiple-user or from multiple-user to single-user after you have installed any INFOConnect product, you must remove all of your current products, then install new ones. You can back up the database using the Export/Import Utility and then import the data into the new database after you install the INFOConnect products. For

information about this utility, go to `Program Files\Attachmate\Infocnee\Enu` and open ExpImp32.hlp.

IPv6 Support

TCPWin32 detects the presence of and uses the new Winsock2 functions which support IPv6. If the new functions are not available, the old calls are used and IPv6 support won't be available. DNS names, IPv6 addresses, or IPv4 addresses may all be specified in the configuration.

This adds IPv6 support to all transports that use TCPWin32, which includes INT-1, TCPA, ATSTCP, MATIP and SABREIP. IPv6 support is not available for CCF, SABRE2 or UDPFRAD.

Although the IPv6 specifications allow for much longer DNS names, this release continues to limit the length of names to 64 characters.

MATIP Service and Network Installation

Because MATIP runs as a service, after a network installation, a user with administrative rights must manually configure and then start the MATIP service.

To configure and start the MATIP service

1. From the Control Panel, open Administrative Tools, and then select Services.

2. Open MATIP Service in the Services list.

3. On the MATIP Service Properties (Local Computer) dialog box, click the Log On tab.

4. Enter the account information of the administrator or user with administrative rights and then click Apply.

5. Click the General tab.

6. Under Service Status, click Start.

Print and Transaction Router (PTR)

Print and Transaction Router (PTR) works with INFOConnect Enterprise Edition for Airlines to manage print and transaction routing. PTR enables several input devices (hosts) to cooperatively use and share several output devices (queues) through communication links called PTR routes. Three PTR products are available: standard PTR; PTR Plus (includes CUPPS support); and PTR Server.

You can install a PTR product as an add-on for Accessory Manager or as a stand-alone product. Stand-alone PTR cannot be installed on a workstation with INFOConnect. If you require INFOConnect and PTR on the same PC, then install PTR with Accessory Manager. Stand-alone PTR uses the Attachmate Installer Program.

For installation instructions, refer to the Read Me file for your PTR product.

Net Stop PTRSERVICE Command

If you get an application error when using the "Net stop ptrservice" command, you can stop the Attachmate PTR service.

To stop the Attachmate PTR service

1. From the Windows Control Panel, open Administrative Tools, and then select Services.

2. Select Attachmate Print and Transaction Router (PTR) and stop or start the service.

Attachmate Installer Program

The Attachmate Installer Program works with common deployment technologies such as GPO or Tivoli. INFOConnect and any prerequisites can be independently deployed. The install can also be deployed using System Management Server (SMS) and can be deployed and/or removed via Group Policies.

Planning Your Installation and Deployment

Your choices for installing and deploying INFOConnect are typically based on a variety of factors, including: your approved business processes, the scale of the deployment, your deployment tools, and whether you want to customize the installation.

For example, a small-scale deployment might consist of using the Setup wizard to install INFOConnect on a few workstations, whereas an enterprise-wide deployment would probably involve extensive customization and testing.

Depending on your requirements, you would most likely use one of the following approaches.

- **Workstation installation**
  With a workstation installation, you install all of the files for INFOConnect to a PC hard drive. You might choose this approach if you are installing INFOConnect on a small number of machines and you do not need to customize the installation. See "Installation Quick Start" on page 23.

- **Basic deployment**
  With a basic deployment, you copy INFOConnect files to an administrative installation point (also called creating an administrative installation image), and then use deployment tools to access these files and create packages that are deployed to workstations. This is a good approach when you need to deploy INFOConnect to a large number of workstations and you do not need to customize the installation. See "Create an Administrative Installation Image" on page 26.

- **Customized deployment**
  With a customized deployment, you copy INFOConnect files to an administrative installation point (the same as in a basic deployment). In addition, you customize the installation to specify the way it installs, looks, and acts on the end users' computers. Customized deployments can be used to deploy to any number of workstations.
  In this scenario, you can provide users with customized workspaces and session documents. See "Customizing Your Installation" on page 29.

Installation Quick Start

Use this quick start to help you install INFOConnect on an individual workstation or from a network location.

Installing on a Workstation

Note: You must log on with administrator privileges to install the product. If you do not have the necessary access rights, ask your system administrator to elevate your privileges.

To install on a workstation

1. Run the Setup wizard.

If you	Do this
Install from a download site	Click the download link and run the download program. Then select a location for the installer files and click **Next**. This extracts the files to the specified location and starts the Setup wizard.
Install from an administrative install image	From the administrative installation point, double-click the setup.exe file.

Note: Install.exe launches the INFOConnect installation splash screen where you can start the installation or exit.

2. From the Setup wizard, click **Continue**, then follow the instructions on the Setup wizard user interface. If there's an existing INFOConnect product installed, it is removed.

3. (Optional) To personalize the installation, click the **User Information** tab and enter the name, organization, and Volume Purchase Agreement (VPA) number (if you have a VPA).

   Note: The purpose of VPA numbers, which are issued by Attachmate, is to allow customer support to expedite service requests.

4. (Optional) To change the default installation folder, click the **File Location** tab, and browse to the folder in which you want to install INFOConnect.

5. (Optional) To change the default user data folder, click the **Data Location** tab, and select the location to which user data is saved.

6. (Optional) To select which features or components are installed, click the **Feature Selection** tab.

7. Click **Install Now**.

Note: Use the Advanced tab of the installer only if you want to create an Administrative installation. The administrative installation does not actually install the product; it places an image of INFOConnect on a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations, and end users can

perform workstation installations by running setup.exe from this
location.

Installing from a Network Location

The following procedure describes one of several methods for installing
INFOConnect to workstations from a network location.

To install INFOConnect from a network location

1. Specify the Share properties of a folder so that users can access it.

2. Create an INFOConnect administrative image in the folder.

3. (Optional) Create a Windows shortcut or command-line link that end
   users can open to install INFOConnect.

4. If you create a shortcut or link, you can add parameters that were not
   included in a customized install, such as making the installation silent.

   Users can install INFOConnect by navigating to the network location of
   the installation file and running the `product.msi` file. Alternately, a user
   can choose Run from the Start menu and enter the following command
   line:

   ```
   msiexec /i path\Product.msi
   ```

   where *path* is the network path to the directory that contains the
   INFOConnect installation files. During this installation, a user can use
   the embedded MSI packages to perform a complete or custom
   installation.

   Note: When installing a file with a customized MSI, the MSI file
   overwrites any existing copies of the file, provided those copies have not
   been modified since they were created. If copies of the file have been
   modified, the MSI file won't overwrite them.

Selecting Features

Use the Feature Selection tab to select product features and determine how
you want to install them. For a list of INFOConnect features, see the
Product Features section.

To select features and components

1. Click the **Feature Selection** tab.

2. For each item, select from the options below.

Choose	To do this
Feature will be installed on local hard drive	Install an item.
Feature will be installed when required	Advertise an item. For example, you can select a component from the Start menu, and it will install at that time.

Feature will be unavailable	Leave an item uninstalled. You will still be able to install the item later using Windows Programs and Features or Add/Remove Programs.

Installer Advanced Tab

Modify the Advanced tab settings only if you want to create an Administrative installation. The administrative installation does not actually install the product; it places an image of INFOConnect on a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations, and end users can perform workstation installations by running setup.exe from this location.

The options are:

Install to this PC	Installs INFOConnect to your computer.
Create an administrative install image on a server	When you create an administrative installation image, an image of INFOConnect is copied to a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations. Also, end users can perform installations by running setup.exe from this location.
Create a log file for this installation	Specifies whether or not a log file is created. The installation log file, which provides details about the installation, is saved in the user's temp directory (%tmp%) with a generated name that begins with atm. To open this folder, launch the Start menu Run command and enter `%tmp%`.

Create an Administrative Installation Image

When you create an administrative installation image, an image of INFOConnect is copied to a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations. Also, end users can perform installations by running setup.exe from this location.

To create an administrative installation image

> **Caution:** For this procedure, use only the Advanced tab and File Location tabs. Configurations made on other tabs will be ignored.

1. Run the Setup wizard (setup.exe).
2. From the **Advanced** tab, click **Create an Administrative install image on a server.**
3. Click **Continue**, and then browse to the folder you want to use for the administrative installation image.
4. Click **Install Now.**

> **Note:** Administrative installation images are typically created in a file server folder. However, you can create administrative installation images in any folder on a local hard disk, which can be useful for testing purposes.

Workstation vs. Administrative Installation

There are two ways to install INFOConnect: a workstation installation, or a customized deployment from an administrative installation.

You can perform these installations from the Setup wizard user interface or from its command line. Or, you can also install INFOConnect directly using MSI.

- **Workstation Installation**
  In addition to accepting the defaults and clicking Install Now, you can customize a workstation install by changing the default location, specifying an organization name, and selecting feature installation states.

- **Administrative Installation**
  The administrative installation does not actually install the product; it places an image of INFOConnect on a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations, and end users can perform workstation installations by running setup.exe from this location.

Install from the Command Line

You can use the Setup wizard command line to install INFOConnect from the distribution (or DVD) image or from an administrative installation image. You can also include command-line options in a batch file to preset installation parameters, and limit user interaction while INFOConnect is installing. You can even suppress installation dialog boxes to provide an unattended installation.

In addition, you can use command-line options to prepare INFOConnect for installation by users. In general, any of the MSI command-line options can be used from the Setup wizard command line.

> **Note:** To view a list of the command-line options for customizing installations, change to the directory in which the setup.exe file resides and enter: setup.exe /?

To install from the command line

At the command prompt or Start menu Run command, change to the directory in which the setup.exe file resides and do one of the following:

- To create an administrative installation image, type:

    ```
    setup.exe /install /admin TARGETDIR=path
    ```

    where *path* is the path to the administrative installation image on the server.

    -or-

- To install to a workstation with typical settings, type:

    ```
    setup.exe /install INSTALLDIR=path
    ```

    where *path* is the path to the installation directory (INSTALLDIR=path is optional).

To install directly with MSI

- At the command prompt or Start menu Run command, change to the directory in which the msi file resides and enter:

    ```
    msiexec.exe /i Installation_file_name.msi
    ```

Enable or Disable Installation Logging

The installation log file, which provides details about the installation, is saved in the user's temp directory (`%tmp%`) with a generated name that begins with atm. To open this folder, launch the Start menu Run command and enter `%tmp%`.

To create or disable an installation log file

1. Run the Setup wizard.

If you	Do this
Install from a download site	Click the download link and run the download program. Select a location for the installer files and click Next. This extracts the files to the specified location and starts the Setup wizard.
Install from an administrative install image	From the administrative installation point, double-click the setup.exe file.

2. On the **Advanced** tab, select or clear **Create a log file for this installation.**
3. Click **Install Now.**

Include Patch Files with the Initial Install

After the Attachmate Installer Program installs the .msi file, it looks in an updates folder for any .msp files to install. You can include service packs and patches with an initial installation by copying the .msp files to an "updates" folder in the same location as setup.exe.

To include Service Packs and Patches with the Initial Install

1. Navigate to the administrative install location for setup.exe.

2. Create a folder named "updates."

3. Copy any .msp files to the updates folder.

4. Any installation that uses setup.exe will apply the .msp files after installing INFOConnect.

Note: If you are not using setup.exe for deployment, any patches in the "updates" folder must applied with your deployment software.

Upgrade Enablers

If there is a folder named "upgrade" included with the product distribution, copy it to the administrative install location. The "upgrade" folder contains files required to perform a successful upgrade from an older product. These "enabler" patches are applied to your system prior to the upgrade.

Note: If you are not using setup.exe for deployment, the patches in the "upgrade"folder must be applied with your deployment software.

Customizing Your Installation

Customize INFOConnect to specify the way you want it to install, look, and act on the end user's computer. Using the tools provided you can:

- Create transforms to customize the installation
  Because multiple transforms can be created for a given install package, you can create customized installations for separate departments or groups of users, each represented in a transform file.

- Create companion install packages and install them
  By creating companion installations, you can install files that configure INFOConnect, or any additional files that are useful to your organization. If you want to install these files with INFOConnect, you can add one or more companion packages to your initial installation. You can also create and install packages at any time after the initial installation. Companion packages show up as independent entries in the Windows list of installed applications, and can be installed or uninstalled independently of INFOConnect. This means that you can upgrade INFOConnect without removing these customized files.

  Because the transforms and companion install packages adhere to MSI standards, these files can be used in conjunction with Active Directory, SMS, or any other Windows Installer-compatible deployment tool.

Attachmate Customization Tool

The Attachmate Customization Tool is a special mode of the Setup wizard that supports custom modifications to the primary install and includes some limited deployment facilities. These are accomplished with a simple user interface and without requiring additional software packages or training.

Use the Attachmate Customization Tool to create transforms or companion installer packages. Each customization has its own set of configuration panels based on your choice on the Select Customization panel.

To open the Attachmate Customization Tool

1. Before you run the Attachmate Customization Tool, create an administrative installation image. See "Create an Administrative Installation Image" on page 26.

2. If another instance of setup.exe is running, close it. You can run only one instance of the setup.exe program at a time.

2. At the command prompt, enter the following command to open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

Create a Shortcut to Start the Attachmate Customization Tool

You can create a shortcut or batch file to start the Attachmate Customization Tool.

To create a shortcut

1. In your administrative install folder, create a Windows shortcut to setup.exe.

2. Rename the shortcut to ACT.

3. Right-click the shortcut and select **Properties**.

4. Append the target path to include /admin as in the following example.

   `[path]\setup.exe /admin`

To create a batch file

- Open Notepad, enter `[path]\setup.exe /admin`, and save the file to your Desktop as a .bat file.

Select a Customization Type

After you start the Attachmate Customization Tool, you can create a transform, a companion install package, or open an existing file of either type.

Caution: If you use the Attachmate Customization Tool to include session documents in a customized deployment, make sure that you create session files with unique names or you may overwrite existing session documents on a user's computer that contain personalized settings or macros.

To select a customization type

- From the Select Customization dialog box, do one of the following, and then click **OK:**
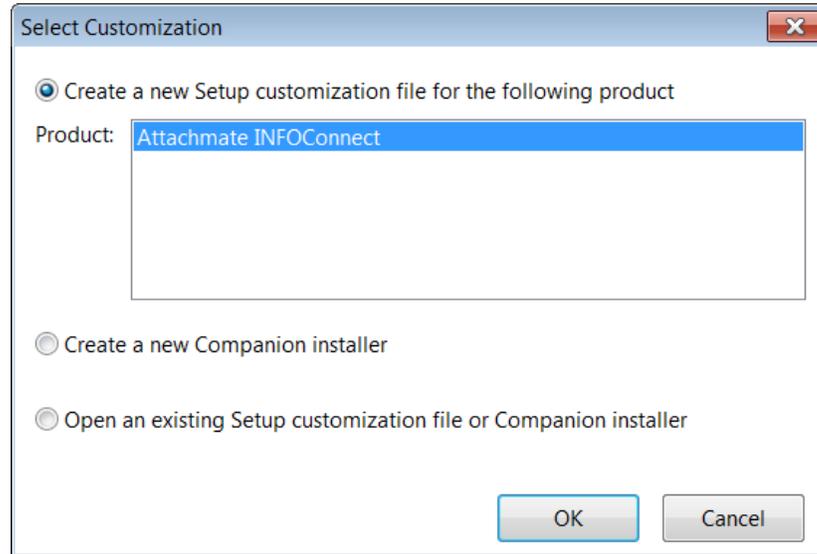
To	Do this
Create a new transform file (.mst)	Select **Create a new Setup customization file for the following product** (the default).
Create a new companion install package (.msi)	Select **Create a new Companion installer.**
Open an existing file of either type	Select **Open an existing Setup customization file or Companion installer.**

Creating and Editing Transforms

Using the Attachmate Customization Tool, you can create standard MSI transforms that modify the primary installer database. You can also open and edit existing .mst files that you have already created for this product using the Attachmate Customization Tool.

After you create the transform, you must include it in the install. Transforms can be used with any install started with setup.exe or with command-line installs (used by many deployment tools). The installer can only apply transforms during an installation.

Note: To install the specified customization, transform files should be saved in the same folder as the package file for INFOConnect and referenced during installation.

Supported modifications include:

- Install location
- User interface level — silent or interactive (requires setup.exe and setup.ini)
- Feature states, including hidden features
- Modification or removal of shortcuts
- Chaining of other installs, or execution of programs before or after the primary install (requires setup.exe and setup.ini)
- Modifying Windows Installer properties.

Create Transforms

Customize INFOConnect to specify the way you want it to install, look, and act on the end user's computer.

To create an installation transform

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

   An unnamed .mst file opens in the Attachmate Customization Tool.

2. Select items from the list in the left panel to open configuration panels on the right, and then make your customizations.

3. From the **File** menu, choose **Save As**.

   Transform files are saved as .mst files, and it is recommended that you save them in the same folder as the installer package file for INFOConnect.

To modify an existing installation transform

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. Select **Open an existing Setup customization file or Companion installer**, and then click **OK**.

3. In the **Open** dialog box, browse to the location you selected when you created your transform file, and select the *[transform_name]*.mst file.

4. Select items from the list in the left panel to open configuration panels on the right, and then make your customizations.

5. From the **File** menu, choose **Save As**.

6. Transform files are saved as .mst files, and it is recommended that you save them in the same folder as the installer package file for INFOConnect.

Add (Chain) Installations and Run Programs

With INFOConnect you can "chain" installs. You can set up an install to run companion install packages automatically before or after the primary installation. You can also launch other scripts or programs.

To chain installations and programs

1. From a command line, open the Attachmate Customization Tool:

   ```
   [path]\setup.exe /admin
   ```

2. From the Attachmate Customization Tool navigation pane, choose **Add installations and run programs.**

3. Click **Add.**

   The **Add/Modify Program Entry** dialog box opens.

4. In the **Target** list, enter or select the folder where the program .exe file or the .msi file resides, and then enter the executable to run; for example:

   ```
   msiexec.exe
   ```

5. Under **Arguments,** enter the command-line arguments to execute; for example:

   ```
   /i My_installation.msi
   ```

6. Choose one of the following options to specify when to run the program.

   - **Run this program after the base product has been installed**

     -or-

   - **Run this program before the base product has been installed**

   Note: For most cases, select **Run this program after the base product has been installed**. If you select this option before the base product has been installed and the program fails, INFOConnect is not installed.

7. Repeat these steps to add other programs or .msi files.

8. To change the execution sequence, use the arrows next to **Move** (at the bottom left area of the pane. To remove a program from the list, select it in the list and click **Remove.**

Modify Setup Properties

You can modify existing INFOConnect setup properties or add your own properties to the install. An example of an installer property is ARPHELPLINK, which sets the URL used by the support link in Window Programs and Features or Add/Remove Programs.

Caution: Do not overwrite existing properties unless you fully understand how the changes affect your install. Setting properties to improper values can break the install.

To modify installation properties

1. From a command line, open the Attachmate Customization Tool:

   ```
   [path]\setup.exe /admin
   ```

2. From the **Select Customization** dialog box, select the option that best describes the task you are performing.

3. On the Attachmate Customization Tool navigation pane, select **Modify setup properties.**

4. Do one of the following:

To	Do this
Add a property	Click **Add.** On the **Add/Modify Property Value** dialog box, enter the property name in the **Name** box and the property attribute in the **Value** box.
	Note: "Public" properties (those with UPPERCASE names) can be modified, but only those properties as documented in the Windows Installer documentation from Microsoft should be added or changed here. Public properties specific to Attachmate installers should not be changed since changes to these may affect the installation or future updates of those installers.
Modify an attribute for a property that is listed under Property name	Select a property name, and then click **Modify.** In the **Add/Modify Property Value** dialog box, change the attribute in the **Value** box and then click **OK.**
Remove a property that is listed under Property name	Select the property name, and then click **Remove.**

5. From the **File** menu, choose **Save As.**

Select Features and Components

You can select which features and components to install for your end users. Also, you can choose from three options for not installing an item; advertising it, not installing it, and permanently blocking it so that users can not install it later.

To select features and components to install

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. From the Attachmate Customization Tool navigation pane, choose **Set feature installation states.**

3. Select the feature installation states as follows:

Choose	To do this
Feature will be installed on local hard drive	Add a feature to the installation.
Feature will be installed when required	Advertise a feature.
Feature will be unavailable	Leave a feature uninstalled. End users will still be able to select the item and install it from Windows Programs and Features or Add/Remove Programs.
Feature will be hidden from view	Leave a feature uninstalled and hidden. End users will not be able to install the item, and it will not be visible in the Windows Programs and Features or Add/Remove Programs.

Configure Shortcuts

You can change the attributes associated with the pre-defined INFOConnect shortcuts. Also, you can configure shortcuts associated with files you've added to a custom install package.

To configure shortcuts

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. From the **Select Customization** dialog box, select the option that best describes the task you are performing.

3. From the Attachmate Customization Tool navigation pane, choose **Configure shortcuts**.

4. Select the shortcut that you want to configure, and then click **Modify**.

5. In the **Add/Modify Shortcut** dialog box, enter the following settings:

To	Do this
Specify where you want the shortcut to reside	In the **Location** list, enter or select the folder.
	Note: List items that refer to folders (for example, *[ProgramMenuFolder]*) are predefined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, *[ProgramFilesFolder]*\My Folder). Alternatively, you can enter a fully qualified path (for example, C:\Program Files\My Folder), as long as that location is known to exist on the target machine.
Name the shortcut	In the **Name** box, enter a descriptive name.
Add a tooltip to the shortcut	In the **Tooltip** box, enter text to describe the shortcut.
Pass command line arguments to the program	In the **Arguments** box, enter the command-line arguments.
Specify the size of the application window	In the **Run** list, select an initial size for the application window.

Modify Application Settings

The Attachmate Customization Tool allows you to control which features of the application you want to deploy. For example, you can include data files and RUMBA schemes or set productivity and global preference settings in the deployed application. The available features depend on which INFOConnect product you are installing.

To modify application settings

1. From a command line, open the Attachmate Customization Tool:

   ```
   [path]\setup.exe /admin
   ```

2. From the **Select Customization** dialog box, select the option that best describes the task you are performing.

3. From the navigation pane, click **Modify application settings.**
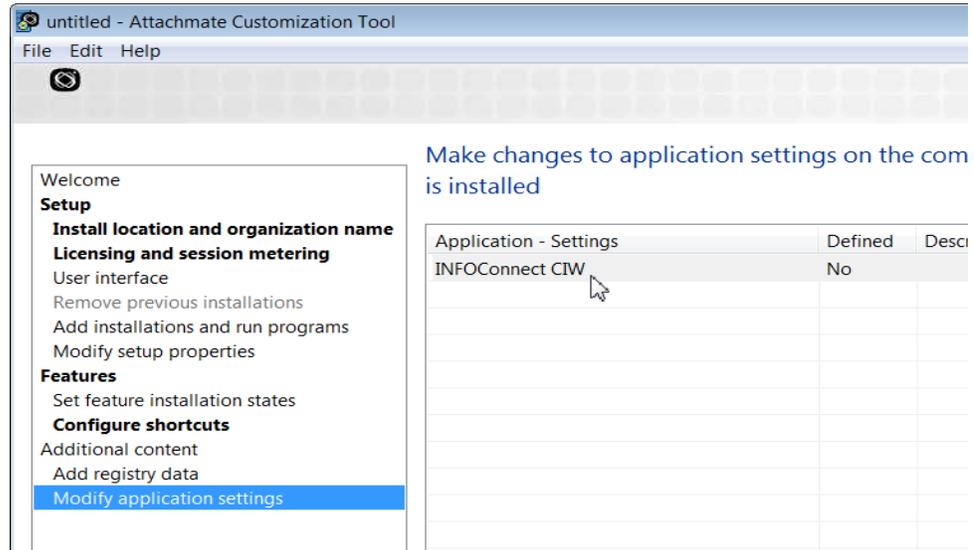
4. From the **Application settings** list, select INFOConnect CIW. The **Modify** button in the lower-right corner of the window becomes active.

   Note: The INFOConnect CIW or Custom Application Wizard was available in earlier versions of INFOConnect as a standalone application. It performs the same functionality in this version but operates only within the context of the Attachmate Customization Tool.

5. Click **Modify.**
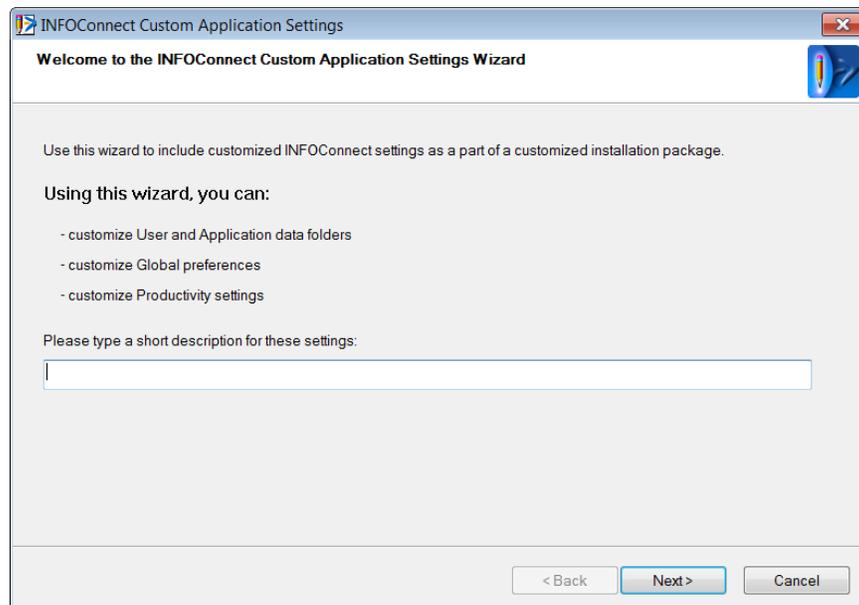
6. On the first panel of the Custom Application Settings wizard, enter a description and press **Next.**

7. Use the following tables to help you select the appropriate options and values for each panel.

Customize User and Application Data Folders

Option or value	Description
User data location	Select the default directories for the schemas, macros and sessions folders.
	My Documents directory: Each user's My Documents folder, from which a user can access his or her own user data.
	All Users\Documents directory: The all-users My Documents folder, from which any user on this system can access all local user data.
	User defined directory: Any user-specified folder.
Application data location	Select the default directories for application data, which includes files such as IC32.cfg, InsMgr32.cfg, Rootcas.cdb, Sabre.cnf, and Stdcfg.atm.
	My Documents directory: Each user's My Documents folder, from which a user can access his or her own application data.
	All Users\Documents directory: The all-users My Documents folder, from which any user on this system can access all local application data.
	Network install directory: When you select **Define users and groups in the INFOConnect database**, the Network install directory option becomes available. Select this option if you want to install INFOConnect in a shared/network manner. When you run the DataBase Editor (DBed32.exe) after a network install, you will see a tree view of users who share the INFOConnect database. The drop-down menu options for "User" and "Group" are available only for a Network install.

Customize Miscellaneous Items

Option or value	Description
Install Attachmate DLC Driver	The DLC driver can only be installed on Windows XP, Windows 2000, or both. It cannot be installed on Windows 7 or Vista.
Install default user data files	Select to install user-defined data files such as demo sessions, schemes, macros, and initial user files.
Install RUMBA Schemes	Select to install RUMBA schemes when migrating RUMBA users to INFOConnect.
Install United (U100) emulation	Select to install the files required for United (U100) emulation.

Customize General Global Preferences

Option or value	Description
Accessory Manager and EXTRA! settings	**Show open session dialog at startup:** When selected, displays the Open Session dialog box to the user at startup (and prevents the user from creating a new session or opening an existing layout on startup). When cleared, displays the Start By dialog box to the user, from which he or she can select a session type or layout. (Default: Cleared.)
	Prompt for disconnection: When selected, prompts the user before each session or layout is disconnected. When cleared, the session or layout automatically disconnects when closed
	Disable event logging: Select to turn off event logging.
	Show Tip of the Day: Clear to prevent the Tip of the Day from displaying. (Default: Selected.)
	Encrypt macros: Select to encrypt macros when they're saved. EXTRA! macros are encrypted when saved in the EXTRA! Basic Editor. The source and output files associated with a CASL macro are encrypted when saved in the CASL Macro Editor. If the source file is newer than the compiled macro, the CASL compiler produces a new encrypted CASL macro file. You can unencrypt a macro by deselecting this option in the Global Preferences dialog box, and then saving the macro in its authoring application.
	Encrypt macros when run: Select to rewrite EXTRA! and CASL macros as encrypted files when they're executed. Both the source and output files associated with a CASL macro are encrypted.
	Note: Encrypted macros will only run in INFOConnect version 9.1 and later.
	Execute only encrypted macros: Select to run only encrypted EXTRA! and CASL macros and to compile only encrypted CASL source files.
	Warning: If the source file associated with a CASL macro is newer than the compiled macro and is unencrypted, the automatic compile will fail and the macro will not be run.

Accessory Manager only settings	**Show Accessory Manager startup dialog:** When selected, displays the Accessory Manager Startup dialog box when Accessory Manager is opened. From this dialog box, the user can choose to create a new session, open an existing session, or open an existing layout. When cleared, Accessory Manager opens a blank workspace. (Default: Cleared.)
	The Startup dialog box will not be displayed if Accessory Manager is started using automation, a portal, or when opening a session from the command line or by double-clicking it.
	Automatically create bookmark files: When selected, creates a bookmark file (.bkm) automatically each time you bookmark a recorded host screen. When cleared, bookmark files must be created manually.
	To create a bookmark file manually, from the Tools menu, choose Page Settings. From the Bookmarks page, click a bookmark, and click Create Bookmark file.
	Show Capture dialog when start capture: When selected, displays the Capture Printer Settings dialog box each time you click Capture from the File menu. When cleared, the capture begins when you click Capture, and the data is handled according to the settings specified in the Capture Printer Settings dialog box. Select this option if you frequently switch the destination or other options for captured data.
On close session	**Auto-save session settings:** When selected, all sessions are automatically saved without user intervention.
	Prompt for session saves: When selected, the user is prompted before sessions are saved.
	Do not Prompt for or Auto save sessions: When selected, the user is not prompted to save sessions, nor are sessions automatically saved. Sessions are saved only if a user initiates a save by selecting a toolbar or menu option.

EXTRA! only settings	**Expand Page Setting dialog box:** From this dialog box, you can edit the navigational path and page identification information for recorded pages.
	Assign ENTER key to left mouse button double click: When selected, double-clicking the left mouse button will function as if the Enter key had been pressed.
	Show Host Name on Taskbar icon when session is minimized: When selected, the name of the host is displayed on the taskbar icon when the session is minimized.
	Open multiple instances of the same session: When selected, multiple sessions of the same connection can be opened simultaneously.
	Set Macro Password box: When selected, prevents macros from recording passwords. A dialog box appears asking the user for the password when the macro is run.
Push update during upgrade install	**Force update of existing current user (HKCU) settings to these General and Advanced Global Preferences settings:** When selected, overwrites all existing HKCU settings in the registry, undoing any personal settings when upgrading.
Set scheme and macro search paths	Choose to set custom scheme and macro search paths prior to deployment from the Search Paths dialog box.
	Macro search path: Use the default path or select Specify search path and Browse to specify the custom path.
	Remote scheme path: Use the default path or select Specify scheme path and Browse to specify the custom path.

Customize Advanced Global Preferences

Option or value	Description
HLLAPI	Shortname association: Select **Shared among all users** or **Unique to each user**
	Transport type: Select **Standard** or **Enhanced.**

Associate Sessions to Shortnames	Opens the Add HLLAPI ShortNames screen where you can add HLLAPI shortnames and associate HLLAPI shortnames with sessions. If you type a full path, it will be included in the installed product in Global preferences. If no path is included, the previously specified path for user data files is used.
	Product: Choose either Accessory Manager or EXTRA!
	Short name: The letter of the short name that your HLLAPI application will use to connect to this session. There are 26 choices, A through Z, for each product type.
	Session name: Enter either an exact path to the session document or browse to the path.
	Host type: Select the host type to which this session connects. The choices are IBM Mainframe (3270), IBM AS400 (5250), or VAX/VMS, UNIX. (Unavailable if Product setting is Accessory Manager.)
	Sub type, Wyse: If you specify VAX/VMS, UNIX as a host type, you can also select Wyse as a sub type. (Unavailable if Product setting is Accessory Manager.)
	Screen size: Based on the host type selected, specify the screen size this for this session. (Unavailable if Product setting is Accessory Manager.)
	IBM Mainframe (3270): 24x80, 32x80, 43x80, or 27x132.
	IBM AS400 (5250): 24x80 or 27x132.
	VAX/VMS, UNIX: 24x80, 25x80,36x80, 48x80, 72x80, 144x80, 72x132 or 144x132.
	Shortname associations: This list displays the shortname and the session file assigned to it. You must assign a HLLAPI shortname before you connect to a session, or if you already have session connections, you must exit all sessions and restart the sessions before the HLLAPI shortname settings will take effect.
Keyboard type	Select the type of keyboard to use.

Customize Global Productivity Settings

Option or value	Description
Productivity features	**Disable all Productivity features:** Select to prevent users from accessing productivity features.
	Enable Productivity pane: Select to allow users to access the Productivity pane, and to set the individual productivity features available from the Productivity pane.
	Show Productivity pane: Select to display the Productivity pane to users by default. This option is unavailable (dimmed) unless the Enable Productivity pane option is selected.
	To set the following individual productivity features, you must first select the Enable Productivity pane. If desired, after making selections, you can hide the Productivity pane and retain the settings to the individual features by clearing the Enable Productivity pane option.
	Enable Scratch Pad: Select to enable by default.
	Enable Macro Bar: Select to enable by default.
	Enable Recent Typing: Select to enable by default.
	Enable History: Select to enable by default.
	Enable Microsoft Office Tools: Select to enable by default.
	The remaining Productivity features can be selected independently of the Productivity pane.
	Enable Spell Checking: Select to enable by default.
	Enable Auto Complete: Select to enable by default.
	Enable Auto Expand: Select to enable by default.
	Enable Keystroke Saving Calculator: Select to allow the Keystroke meter to calculate the number of keystrokes required for each task performed. The Keystroke Saving Calculator calculates the number of keystrokes required for each task, and then displays the actual number of keystrokes saved when those tasks are executed using features such as Auto Complete or Auto Expand. Available in Unisys, 3270, and 5250 sessions only.

Spelling preferences	**Spell check provider:** Wintertree Sentry is the default spell checker.
	Main dictionary path: Click to select a different path.
	Main dictionary list: Click to select a different list.
	Default user dictionary: Click to select a different user dictionary.

Creating a Companion Install Package

Create a companion install package (also called a "companion database") to install any files that are not installed with INFOConnect.

Because companion files are installed independently of INFOConnect, you can upgrade the product without removing these support files. You can also deploy additional support files without re-installing the product. If, for example, you are supporting several business units that require their own customized configuration files, you can create a companion install package for each business unit.

Companion install packages support the following:

- Specification of files and installation directories
- Shortcuts for selected files
- Addition of custom application settings
- Chaining with the primary installer (Chaining must be specified in the .mst file.)
- Removal without affecting the primary installs (The primary install can also be removed without affecting the files added with a companion package.)

Companion install packages can be installed with any mechanism that supports MSI packages. The packages have no built-in user interface other than the standard progress bar.

Create a companion install package (also called a "companion database") to install any files that are not installed with INFOConnect.

To create a companion install package

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. In the **Select Customization** dialog box, select **Create a new companion installer** (or open an existing .msi file) and click **OK.**

3. From the navigation pane, select **Specify package information.**

4. In the **Add/Remove name** box, type the name for the companion installation. (This is the title that is displayed in the **Programs and Features** or **Add/Remove Programs** control panel.)

5. In the **Organization name** box, type the name for your organization.

6. From the navigation pane, select **Specify install locations.**

7. In the **Default installation folder** list, select the folder in which to install the program or files.

8. In the **Default shortcut folder** list, select the folder in which to install program shortcuts.

   Note: List items that refer to folders (for example, [ProgramMenuFolder]) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, [ProgramFilesFolder]\My Folder). Alternatively, you can enter a fully qualified path (for example, C:\Program Files\My Folder), as long as that location is known to exist on the target machine.

9. Under **Installation type**, select one of the following options:

Select	To set up the companion installation to
Installs to all users of a machine	Make files available for every user who logs onto the computer.
Installs only for the user who installs it	Make files available only for the user who installs it.

   Note: Installation Type folder options specify the access for the files (after the installation). These options affect only the folders to which you can install. You cannot change these options after you add a file.

10. To add, update, or remove files or shortcuts, from the navigation pane, select **Add files.** (For details, see the next section.)

   You can also modify setup properties or user settings for the companion installation. When you have finished creating your companion package, you can deploy it by itself or with INFOConnect. The package remains on the end user's computer until it is removed from Windows using **Programs and Features** or **Add/Remove Programs.**

Add Files to a Companion Installer

You can add or remove files and shortcuts to or from a companion install package.

To add a file to the companion installer

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. In the **Select Customization** dialog box, select **Create a new companion installer** (or open an existing .msi file) and click **OK.**

3. From the navigation pane, select **Add files.**

4. In the **Add files to** box, select a folder or type a valid folder path.

5. (Optional) To create a shortcut for the file, select **Include shortcut.**

6. In the **Add files to** box, select a folder or type in a valid folder path to specify the folder to which the file is installed.

Add a Companion Installer to your Installation

You can use this procedure to add one or more custom installer packages to your INFOConnect installation.

To add a companion package to your installation

1. From a command line, open the Attachmate Customization Tool:

    `[path]\setup.exe /admin`

2. Select **Create a new setup customization file for the following product** and click **OK.**

3. From the navigation pane, click **Add installations and run programs.**

4. Click **Add,** browse to select your companion installer (.msi file), then click **Open.** Leave the other settings at their defaults and click **OK.**

5. From the **File** menu, choose **Save As.**

    Note: When you save your transform, the Customization Tool automatically updates the Setup.ini file, adding a [RunPrograms] section with instructions for installing your companion package.

6. Instruct users to install using setup.exe. The companion package is automatically installed after the installation is complete.

Modify User Settings

Use the Modify User Settings pane to add user-specific settings to a companion package. Before you begin, note the following.

*   Modify User Settings is not available for all applications

*   This panel is available only if you are configuring a user-specific package

*   You may be able to install user-specific settings using the Add files pane

To install user settings

1. From a command line, open the Attachmate Customization Tool:

    `[path]\setup.exe /admin`

2. From the navigation pane, click **Specify install locations.** Under **Installation type,** select **Installs only for the user who installs it.**

3. From the navigation pane, click **Modify user settings.**

4. Select the application whose settings you are configuring and click **Define.**

Note: The Define button is available only if the selected application is installed on your workstation.

Deploying INFOConnect

You can choose from several ways to deploy INFOConnect, including the following:

- Microsoft Active Directory
- Microsoft Systems Management Server (SMS)
- Any other Windows Installer-compatible deployment tool

You can also deploy INFOConnect silently from the command line.

Perform a Silent Installation from the Command Line

A silent installation proceeds without the end user being able to intervene or, in some cases, even see that the installation is occurring.

To perform a silent installation

At a command prompt or the Start menu Run command, change to the directory in which the setup.exe file resides, and do one of the following:

- To perform a silent installation with no display, type:

```
setup.exe /install /quiet
```

-or-

- To perform a silent installation that displays a progress bar and disables the Cancel button, type:

```
setup.exe /install /passive
```

Assign and Publish with Active Directory

You can assign and publish your product installation using Microsoft Active Directory. Before you start, ensure that:

- Windows Administrative Tools are installed on your workstation.
- You are a member of Domain Admins and Group Policy Creators and Owners, which is required to publish software.

For more information, see "Active Directory groups" in the Microsoft Management Console help.

To install with Active Directory

1. On the desktop, double-click the Active Directory shortcut.

   The **Active Directory User and Computers Console** opens.

2. Advertise your product installation to members of any organizational units in your Active Directory using appropriate transform modifications.

3. If multiple transforms are specified, make sure the listed order of the transforms is correct, and then click OK. (If you need to change the order for any reason after you click OK, you will have to start over again.)

> **Note:** For more information about assigning and publishing, see "assigning applications" and "publishing applications" in the Microsoft Management Console help.

Deploy with Systems Management Server

Use the Microsoft Systems Management Server (SMS) to deploy to computers running Microsoft Windows. Before you start, ensure that:

- You are using SMS version 1.2 or later. SMS versions earlier than 1.2 are not supported.

- Microsoft Windows Installer software version 2.0 or later is installed on your computer and on all of the computers on which you are installing the product.

To deploy with Systems Management Server

1. Create an administrative install image on your SMS site server.

   This serves as the administrative installation point for deployment.

2. Use the product Package Definition File (.sms) to create the product installation package.

3. Advertise the installation packages to your users.

Maintaining INFOConnect

You can distribute software updates in a standard .msp file format, remove installations, or repair installations.

Once a patch or service pack is installed, a Service Pack tab appears in the Attachmate Installer Program. The Service Pack tab lists the service packs and hotfixes that have been installed and provides an option to remove any of the installed updates.

Distribute Software Updates

Software updates, including service packs and patches, are distributed as .msp files and most deployment software can distribute these files. You can deploy .msp files with the Attachmate Patch utility included with your distribution. Or, after the main installation, you can also apply patches by using an updates folder.

To apply a patch using an "updates" folder

1. Create a folder named "updates" in the same location as `setup.exe.`

2. Copy the .msp files to the "updates" folder.

3. Run the Setup wizard (setup.exe), which will apply the patch.

The Windows Installer technology may require original media when applying a patch. Therefore, the original media should be available to users during this time.

You can use command-line options to deploy patches when INFOConnect is deployed from a network location or via Group Policies.

To apply a patch to an installed administrative image

- At the command prompt or the Start menu Run command, type:

  ```
  msiexec /a [path]\Admin_install.msi /p [path]/Patch.msp
  ```

  INFOConnect is deployed from a network location and the patch is installed to the administrative install point. Each user must repair his or her installation of INFOConnect using the Control Panel to apply the patch.

  - or -

- If INFOConnect is deployed via Group Policies, the group policy is deployed again. (To redeploy the group policy, highlight the policy, right-click, and then choose Re-Deploy. The installation will then be updated the next time the user logs in, or when the computer is rebooted, depending on the type of deployment that was done.)

To distribute updates with the Attachmate Patch utility

1. From the distribution image, open the Attachmate Patch utility by double-clicking the self-extracting executable update file.

2. Follow the instructions given by the utility.

   For detailed instructions on upgrading INFOConnect, refer to the Attachmate Patch Utility Help.

Upgrade or Remove INFOConnect

When you upgrade INFOConnect from a previous release, existing predefined keyboard maps (such as T27.ekm) are not overwritten. This ensures that your changes to those keyboard maps are not lost. However, it also means that you will not receive any new modifications added to them. For instructions on adding new keyboard map features, see the Accessory Manager online help.

Microsoft logo requirements affect the way INFOConnect is uninstalled for multiple users. When INFOConnect is uninstalled, the product is removed completely from the machine and the registry keys are removed from HKEY_CURRENT_USER and HKEY_USER only for the user logged on when the uninstall process was invoked. Therefore, to uninstall INFOConnect from the other users on the same machine, the administrator must manually remove the registry entries and product shortcuts.

In a shared network installation, access to INFOConnect products can be removed at a networked PC. In this case, the products will no longer be accessible at that PC, but they remain installed on the file server and all other users will still be able to share them.

Note: You must log on with administrator privileges to remove the product. If you do not have the necessary access rights, request that your system administrator elevate your privileges.

To uninstall INFOConnect

From the **Programs and Features** or **Add/Remove Programs** control panel, select INFOConnect.

-or-

At the command prompt or the Start menu Run command, change to the directory in which the setup.exe file resides and enter:

```
msiexec /x ProductCodeGUID /qb
```

where `ProductCodeGUID` is the Globally Unique Identifier (GUID) that is the principal identifier for the product. To get the product code, use an MSI editing tool or contact Attachmate Technical Support. `http://support.attachmate.com/contact.`

Repair an Installation

If you are experiencing problems with your installation, you can use the Repair option in the **Programs and Features** or **Add/Remove Programs** control panel. This feature automatically searches for and replaces missing or corrupted files. For more information, see the Windows Help.

Command Line Installation Options

You can use command-line options to install INFOConnect and you can include command-line options in a batch file that can be distributed to your INFOConnect users for their installations.

Installing from the Command Line

Note: You must log on with administrator privileges to install the product. If you do not have the necessary access rights, ask your system administrator to elevate your privileges.

To install INFOConnect from the command line

- From the command line, or from the Start menu Run command, type:

  ```
  msiexec /i path\Product.msi
  ```

  where *path* is the path to the directory that contains the appropriate .msi file, and *Product.msi* is the installation file.

To install a MSI File and Transform file from the command line

- From the command line, or from the Start menu Run command, type:

  ```
  msiexec -i New.msi TRANSFORMS=Filename.mst /qb
  ```

  where the /q option and its parameters n|b|r|f set the user interface level: qn – no UI, qb – basic UI, qr – reduced UI, and qf – full UI.

You can use the installer command line to set the location from which INFOConnect will install various features. You can also change the features available during network installation or selected for installation by default using one of the tools available for editing .msi files.

Setting the Location of INFOConnect Features

You can install all features onto the local drive or you can install all features as run-from-source to install all features from the network.

To set the location of INFOConnect features

From the command prompt, type one of the following:

- For a complete install of all features onto the local drive, type:

  ```
  msiexec /i [path]\[Product].msi ADDLOCAL=ALL /qb
  ```

  where *[path]* is the path to the directory that contains the appropriate .msi file, and *[Product].msi* is the installation file.

- For a complete install where the client installs all features from the network, type:

  ```
  msiexec /i [path]\[Product].msi ADDSOURCE=ALL /qb
  ```

If you share your INFOConnect products on a file server and the networked PCs do not have write privileges to the server, .gid files for the online Help will be created in the Windows\Help folder for each user. If you subsequently install an additional INFOConnect product on the file server,

the user will not see the online Help for that product until he or she deletes the .gid files from his or her Windows\Help folder (these are hidden files).

In a shared network installation, the networked PCs will not have access to the online Help for the INFOConnect transports via the Accessory Manager online Help.

For more information on command line options and parameters, see the Microsoft Windows Installer documentation.

INFOConnect MSI Properties

The following table lists common properties in the INFOConnect .msi file, some of which are used to set default values for installation and global options. They can be specified on the command line or passed in by way of a transform file. If installation values are not specified and the installation dialog boxes are suppressed, the default values are used.

Property	Description
COMPANYNAME=*organization*	Sets the organization name.
INSTALLDIR=*path*	Sets the installation path
USERDATALOC_CUSTOM=*Yes/No*	Default is No. Only works if USERDATALOCATIONMIN and USERDATALOCATIONMINTWO are set to Custom. Set the value to No or Yes based on whether USERDATALOCATIONMIN or USERDATALOCATIONMINTWO is set to Custom. If set to Custom, then set to Yes; for all others, set to No.
USERDATALOC_CUSTOM_PATH=*path*	Only works if USERDATALOCATIONMIN and USERDATALOCATIONMINTWO are set to Custom. Specifies a custom location to store user data. If you replace the user-specific portion of the path with the string *userid*, when the product is run by a user for the first time, the *userid* portion of the path is replaced with the logged-in user's ID.

Windows 7, Vista, XP, and 2000: USERDATALOCATIONMIN=*value*	If you specify a custom user data location, also include the CustomUserDocumentsPath property. You must also set USERDATALOC_CUSTOM_PATH and USERDATALOC_CUSTOM equal to Yes.	
	Sets the location to store user data, where:	
	This value	Saves data under
	MyDocs	My Documents
	AllUsersDoc DataDir	All Users\Documents
	Custom	User-defined directory
	If you specify a custom user data location, also include the CustomUserDocumentsPath property.	

Property	Description		
Windows 7, Vista, XP and 2000: APPDATALOCATION=*value*	Sets the location to store application data, where:		
	This value		Saves data under
	My Documents		My Documents
	AllUsersDocuments		All Users \Documents

Transports and Options — Command Line Properties and Values

You can install transports or options from the command line if you haven't customized your .msi file to install specific transports or options. This is most common for silent or group policy installations. If you do not specify any transports or options, the defaults are installed.

To install transports and options from a command line, use the feature names in the following tables as values for Windows Installer properties such as ADDLOCAL or ADDSOURCE.

You must type the feature name exactly as it appears in the tables below. In previous releases, you would enter <install_value>=1. These values are no longer valid.

Use the MSI feature names with the standard MSI properties and arguments. The ADDLOCAL=<comma delimited list> property would install one or more transports or options locally. For example, to install the Sabre and MATIP for UTS transports locally, you would enter:

```
ADDLOCAL=ICW40_SABRE,MATIP_ AIRLINES
```

Other common properties to set on the command line (but not in a transform) include REMOVE=<comma delimited list>, which uninstalls the feature and ADDSOURCE=<comma delimited list>, which installs the files for that feature to run from a network location.

INFOConnect Unisys Transports and Options

Transport or option	Feature name
TCPA - A Series TCP/IP Transport (default)	ICW40_ATA
HLCN - Host LAN Connection Terminal Services	ICW40_ALA
INT1 Transport (default)	ICW40_OIA
MATIP for UTS Transport	ICW40_MATIP
FileXpress-XST Client	ICW40_XST
Response Time Monitor Utility	ICW40_ARTMS
CryptoConnect Client	ICW40_CRYPTO
WinFTP	ICW40_FTP
CCF	ICW40_CCF

INFOConnect Airlines Transports and Options

Transport or option	Feature name
INT1 Transport (default)	ICW40_OIA_AIRLINES
MATIP for UTS Transport	ICW40_MATIP_AIRLINES
MATIP for ALC Transport (default)	MATIP_ALC_AIRLINES
ATSTCP - Galileo Apollo Travel Services TCP/IP Transport	ICW40_ATS
UDP for TPF Transport	ICW40_FRAD
Sabre IP Transport	ICW40_SABRE
CryptoConnect Client	ICW40_CRYPTO_AIRLINES
Airlines Gateway	ICW40_AIRGATE

PTR Stand-alone Transport and Options

Transport or option	Feature name
INT1 Transport	ICW40_OIA_AIRLINES
MATIP for ALC Transport (default)	MATIP_ALC_AIRLINES
MATIP for UTS Transport	ICW40_MATIP_AIRLINES
ATSTCP - Galileo Apollo Travel Services TCP/IP Transport	ICW40_ATS
UDP for TPF Transport	ICW40_FRAD
Sabre IP Transport	ICW40_SABRE
Airlines Gateway (default)	ICW40_AIRGATE

Administrative Tasks and Tools

This section contains information on the following tasks, tools, and features:

- Working with sessions in Accessory Manager and DataXpress

- Utilities and tools such Response Time Monitor, Export/Import Utility, Security Editor, CnfEdit, and Split Screen Transport

- Productivity pane

- Security and encryption features such as FIPS 140-2, Reflection secure FTP client, Reflection for the Web security proxy server, and Public Key Infrastructure

Starting Your Sessions

All of the terminal emulators and all but one of the file transfer products run within Accessory Manager. DataXpress–ST has its own application window.

The procedure used to start a session varies depending on which product you installed and how the product was installed. The following procedures explain how to start Accessory Manager and DataXpress–ST sessions.

To start Accessory Manager and open a session

1. From the Start menu, open Accessory Manager from the Attachmate INFOConnect Programs group.

2. Do one of the following:

To	Do this
Create a new session	Select New Session from the File menu. The New Session Wizard guides you through creating a session and, if appropriate, an INFOConnect path.
Open an existing session	Select Open Session from the File menu and double-click a session.

3. You can create a shortcut for any existing session and then open that session by double-clicking the shortcut.

To start DataXpress–ST and open a session

1. From the Start menu, open DataXpress–ST from the Attachmate INFOConnect Programs group.

2. Do one of the following:

To	Do this
Create a new session, but not open it	Click Session from the Preferences menu and respond to the subsequent prompts.
Create a session and open it automatically	Click New Session from the Window menu and respond to the subsequent prompts.

Adding Sessions to a Portal or Web Page

You can integrate INFOConnect sessions with portals and other Web pages through an ActiveX control. Then computers that have INFOConnect installed can access the session in a Web-based environment.

If you have an existing portal to which you would like to add a session, you can call this control from the HTML code in your portal. The control opens INFOConnect and displays it in the portal (or, if you choose to do so, opens a new browser window and displays it there). You can define the basic behavior of this ActiveX control by setting its properties in JavaScript added to a Web page.

Scripting Integrated INFOConnect Sessions

By using the Launcher control Session property and scripting, you can access the automation interfaces for INFOConnect. For example, if the Launcher control <OBJECT> name is "launcher," the following JavaScript sets the session connected state to false (disconnects the session):

```
launcher.session.Connected(false);
```

The following JavaScript sends text to the screen:

```
scrn = launcher.session.Screen();
scrn.SendKeys("Hello<Enter>");
```

A full description of the Session object and all of its sub-objects is available in the Help installed with the INFOConnect client application at Infonee\Enu\Epc_ole.hlp. You must have EXTRA! for Accessory Manager installed to get this help file.

Adding a Session to any Web Page

You can add an INFOConnect session to any Web page by calling the INFOConnect Launcher control. The Launcher control has configurable properties that you can set.

To add an INFOConnect session to a Web page

1. In the head section of your target HTML file, use JavaScript to create a function.

2. In the code sample, this is called "mylaunchfunction."

3. In the Body section of your target HTML file, use the onLoad attribute to call the function you created in step 1.

4. In the Body section of your target HTML file, create an object with attributes for id, classid, width, and height.

   The classid must equal "clsid:DE8845A4-B737-4C12-A4DA-B0F0BEED1AC2".

Launcher Control Code Sample

This code sample shows how to call the INFOConnect Launcher control from an HTML page.

```
<HTML><HEAD><TITLE>Sample HTML Page</TITLE>

<SCRIPT LANGUAGE="JavaScript">function mylaunchfunction(){
launcher.launchfile="INT1_1.ADP";
launcher.embedded=true;
launcher.onclose="close";
launcher.launch();}</SCRIPT></HEAD>

<BODY onLoad="mylaunchfunction()">
<H1>INFOConnect Terminal</H1>
<BR>
<OBJECT ID="launcher" CLASSID="clsid:DE8845A4-B737-4C12-A4DA-
B0F0BEED1AC2" HEIGHT="300" WIDTH="500"></OBJECT>
</BODY></HTML>
```

Launcher Control Scripting Code Sample

This code sample shows how to call properties of the session object of the INFOConnect Launcher ActiveX control from an HTML page.

```
<HTML><HEAD><TITLE>Sample HTML Page</TITLE>

<SCRIPT LANGUAGE="JavaScript">function mylaunchfunction(){
launcher.launchfile="INT1_1.ADP";
launcher.embedded=true;
launcher.onclose="close";
launcher.launch();}function connect(){
launcher.session.Connected(true);}function disconnect(){
launcher.session.Connected(false);}</SCRIPT></HEAD>

<BODY ONLOAD="mylaunchfunction()">

<H1>INFOConnect Terminal</H1>
<BR>

<OBJECT ID="launcher" CLASSID="clsid:DE8845A4-B737-4C12-A4DA-
B0F0BEED1AC2" HEIGHT="300" WIDTH="500"></OBJECT>

<BR><BR>
<BUTTON NAME="Test" ONCLICK="connect()">Connect</BUTTON>
<BUTTON NAME="Test" ONCLICK="disconnect()">Disconnect</BUTTON>
```

</BODY></HTML>

Introduction to Response Time Monitor Utility

The INFOConnect Response Time Monitor utility displays information about communication between one or more PCs running INFOConnect Accessory Manager and a host. Specifically, it displays information about transmissions from the PC and responses from the host, calculating both the size of the buffers being sent between the two and the amount of time between each transmission or response. You can use this information to identify problems with either your network performance or your host.

Run Response Time Monitor by choosing RTM Utility from the Attachmate INFOConnect Programs group. Response Time Monitor comes with its own Help.

Introduction to Export/Import Utility

The INFOConnect Export/Import Utility lets you export data from any INFOConnect database into an .ini or .csv file, as well as import data from an .ini or .csv file into an INFOConnect database. You can also create a detail file that provides information about each field in the .ini or .csv file such as the maximum number of bytes allowed in each field or the type of data that each field can contain.

You can use this utility to perform a number of tasks:

- Export path information from an earlier version INFOConnect database and then import it into the current database (IC32.cfg)

- Create a backup copy of your INFOConnect database so that you can restore it if your original database is deleted or becomes corrupted

- Create and edit INFOConnect paths in an .ini or .csv file that you can subsequently import into an INFOConnect database

- Export path information from multiple INFOConnect databases and then import the data into a single master database

- Modify the organization of groups and users in the tree in the shared version of the INFOConnect Database Editor

In previous versions of INFOConnect, 32-bit and 16-bit transport libraries were available. In the current release all transports and databases are 32-bit.

If you are copying your INFOConnect database for use on multiple servers, you might need to use the Copy ICS Database Utility, which lets you change certain directory names within the database. For more information, run Copics32.hlp in the Infocnee\Enu folder.

Export/Import Utility is accessed through the command line only and comes with its own help system. Access the help by running ExpImp32.hlp from the Infocnee\Enu folder.

Viewing Keystroke Savings

From the Productivity pane in Accessory Manager, features such as Auto Expand and Auto Complete reduce the number of keystrokes end users must type to complete tasks.

Keystroke savings are not counted for VT sessions.

The Auto Complete feature saves previous entries you've made when you entered text for Web addresses, forms, or passwords. Then, when you type information in one of these fields again, Auto Complete suggests possible matches.

With Auto Expand feature, you can pre-set acronyms or shortcuts for long words, phrases, and complex repeat commands, reducing the number of keystrokes required to execute tasks and enter host data. Once you have specified the settings for an entry, when you type the corresponding shortcut on the host screen, it automatically expands to the desired word or phrase.

If you prefix an acronym to automatically expand with one or more characters not typically in the first position in a word, such as an equal sign (=), an exclamation point (!), or a caret (^), the word is left "as is."

For example, =ATM won't automatically expand to Attachmate when your intention is to leave it as ATM because you are referring to automatic teller machines (ATMs).

With the Recent Typing feature, you can quickly view and select fields, and automatically populate them with repeat words and commands, eliminating the need to re-enter information manually.

Disabling Client Features with the Security Editor

Using the Security Editor, you can remove commands from the menus, disable buttons on toolbars and QuickPads, and disable keys on keyboard maps. For example, if you want to prevent users from creating a new session, you can remove the New Session option from the File menu. All changes are kept in a Scheme file (.esf). This file can be password protected and then distributed to users on your network. You can configure users with read-only access to the Scheme file.

A default Scheme file (Default.esf), with all client features enabled, is automatically installed in the Schemes directory. You can either edit the default Scheme file or save it under a new name and then modify the new version.

To disable a client feature with the Security Editor

1. Open a session.

2. From the Options menu, select Security.

   The Security dialog box opens.

3. Make sure the Scheme file you want to edit is displayed in the Scheme field. If it isn't, Browse to the correct file.

4. Select the Options tab.

5. If the Scheme file is password protected, you are asked for the password. Enter the password in the Security Password dialog box, then click OK.

6. Select the Category that contains the command(s) you want to set.

7. Clear the check mark from the command(s) you want secured.

8. Repeat steps 6 and 7 for each command that you want secured.

9. To save the Scheme file, choose the File tab and click Save As.

10. Select the file or enter a new file name and click Save.

Using CnfEdit

Some user applications may require a file with the extension .cnf to hold translation tables and other communications data. A .cnf file is in binary format and can only be edited using the CnfEdit program. Several different options can be modified using CnfEdit. Some are not used with current products, but are retained for compatibility with older Gateway products.

Take great care when changing .cnf values. Do not change a value unless you are sure that the new value is valid.

When you update a .cnf file, the changes do not take effect until the product using the file is restarted.

To use CnfEdit

1. From the command line, navigate to Infocnee/Cnf and locate the .cnf file you want to work with.

2. From the command line, type:

    path/CnfEdit

    where *path* is the path to CnfEdit.

3. Press Enter.

    The File Selection screen is displayed.

4. Type the name of the .cnf file you want to edit, then press Enter.

    The Configuration Categories menu is displayed. The column on the left provides a list of six categories. When you move the cursor over a category name, the column on the right provides a list of all the options in that category.

5. Move the cursor over the category containing the options you want to edit, then press Enter. A new screen for editing the options in that category is displayed.

CnfEdit Categories and Options

Category	Option/Description
IA Level Data Entry	**Airline code** The airline code will be set correctly when you receive the .cnf file. Do not change this code unless you are sure that the current code is not correct. **Interchange address** Retained for compatibility with other gateway software. Do not set any values for this parameter. **Host Type** The host type will be set correctly when you receive the .cnf file. Do not change the host type.

Code	Host
00	Any host type not listed here
01	SABRE
02	SABRE (FOS)
03	British Airways (BABS)
04	Continental
05	CPARS
06	JALCOM
07	KLM (CORDA)
08	QANTAS (QANTAM)
09	Worldspan (PARS)
0A	Apollo
0B	Egypt Air
0C	El Al (Israel Airlines)
0D	Thai Airways
0E	Canadian Airlines
0F	Garuda
10	Abacus
11	Amadeus
12	Apollo 2915
14	Shares
15	System One/Amadeus (Unison ALC specification)
16	Turkish

Category	Option/Description
	SITA message TA Retained for compatibility with other gateway software. Do not set any values for this parameter.
	Response Interchange Address Retained for compatibility with other gateway software. Do not set any values for this parameter.
TA Tables	Retained for compatibility with other gateway software. Do not set any values for this parameter.

Screen Translate Tables	Because screen translation is a two-way process, two screen translate tables are supplied with the correct settings for your host. One is used to translate data going to the host; the other is used to translate data coming from the host. Do not change the setting unless you are certain that you are entering correct values.
	Any value may be entered into the tables and very little validation is provided, therefore, you must ensure that the data input is correct.
Communications	This screen displays all the items in the configuration file that are associated with communication between the gateway and the host. Care should be taken when changing these values as it is possible to select combinations of values that will prevent data transmission.
	The Help screen at the bottom right of the screen will display further information about the item situated at the cursor, and also indicate the type of data expected as input.
Printer Translate	Because printer translation is a one-way process from the host to the printer, only one table is required. Do not change the setting unless you are certain that you are entering correct values.
	Most printer character translations will be the same as the display translation. However, some characters will be different. No more than 15 differences are allowed between the display and printer translation tables. If there are more than 15 differences, a warning message is displayed. At this point, it is possible to edit either table until only 15 differences between them are outstanding. The file cannot be saved if there are more than 15 differences.
Printer Escape	These options are not used.

Introduction to the Productivity Pane

Productivity features accelerate data entry and host navigation by reducing keystrokes and mouse clicks. Features such as Spell-check, Auto Complete, Auto Expand, History, Scratch Pad, and Recent Typing enable users to save thousands of keystrokes throughout the day. The Office Tools feature allows you to use Microsoft Word and Outlook application features from your host application. You can create Word documents, send email, schedule appointments, add notes and tasks, and create new contacts.

You use the Productivity Settings pages to enable or disable productivity features and configure individual features. With a session open, choose Settings from the Options menu, then click the Productivity category. Use the following options to define your productivity features:

Productivity Pane Options

Option	Description
General	Select to show or hide each of the buttons in the Productivity pane on the left side of your host session display screen. Spelling: Set criteria for the spelling checker. With Spelling options, you can specify several ways to check spelling as you type, or correct spelling automatically. When the check box for Enable Spell Checking is selected, that feature is activated and ready to use in the host application.
Auto Complete	Select settings enabling you to insert entire items such as dates and entries when you type a few identifying characters. The Auto Complete feature remembers what you type and makes suggestions as it learns commands that are used repeatedly. When the check box for Enable Auto Complete is selected, that feature is activated and ready to use in the host application.
Auto Expand	Add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed, will automatically expand to the full word or phrase. When the check box for Enable Auto Expand is selected, that feature is activated and ready to use in the host application.
History	Set the number of screens to save. You will be able to view and copy information from previous screens, eliminating data entry redundancies. When the check box for Enable History is selected, that feature is activated and ready to use in the host application.
Recent Typing	Set the number of fields to save. You can quickly view, select, and automatically populate fields with repeat words and commands. When the check box for Enable Recent Typing is selected, that feature is activated and ready to use in the host application.
Microsoft Office Tools	Enable or disable each of the settings for the Microsoft Office Tools features. When the check box for Enable Microsoft Office Tools is selected, that feature is activated and ready to use in the host application. When each check box listed under Microsoft Office Tools is enabled, that feature is available for use in the Microsoft Office Tools panel in the Productivity pane on the left side of your host session display screen. From the host, you can quickly access Microsoft Word and Outlook Office features.

For more information about the Productivity pane, see "Changing Productivity Settings" under "Using Sessions" in the Accessory Manager Help.

Introduction to Split Screen Transport

The INFOConnect Split Screen transport enables PCs to communicate with an ALC, ClearPath IX, or 1100/2200 Series host. Using the Split Screen Path template enables you to open multiple terminal emulation sessions using the same path. Once you have the sessions open, you can enter a task or command in one session and direct your output and host responses to display in another open session.

The Split Screen Path template works by specifying a path within a path. From INFOConnect Manager, create a path that uses the Split Screen Path template and then configure the path template by specifying a different path that defines your host connection.

Installing any version of INFOConnect Enterprise Edition that supports ALC will automatically install the Split Screen transport. For more information about using Split Screen transport, see "About Split Screen Access" under "Overviews" in the Accessory Manager Help, or run Split32.hlp from the Infocnee\Enu folder.

Manage Trace Files

Use the following procedure to manage trace files on your system.

1. From the Start menu, start the INFOConnect Manager 32-bit.
2. From the Administer menu, choose Administrator Login.
3. Enter the Administrator password and click OK.
4. From the Administer menu, choose Trace.
5. Select Enable Trace Log.
6. For Custom Trace File Location, specify the path where you want log files to be saved.
7. For Maximum File Size, specify (in MB), the maximum file size before the trace file splits into a new file.
8. For Number of File Cycles, specify the number of files the trace log will split into (for example trace.log.1, trace.log.2), when the maximum file size is reached. When all of these files have reached their maximum file size, the process repeats itself and the first file is overwritten with additional trace data.

Sabre NOFEP Communications Protocol Support

Use the following instructions to connect INFOConnect with the Sabre No Open Front End Processor (NOFEP) system. Customers are required to license CCSAPI from Sabre before they connect via INFOConnect.

Install CCSAPI, the Sabre API, before you install INFOConnect. For information on the API installation, refer to the Sabre documentation.

To verify access to Sabre, test the following connections

- Telnet to access.sabre.com port 30031 (TA access)

- Telnet to access.sabre.com port 30032 (Agency Pooled TA access)

- Telnet to access.sabre.com port 30051 (Printer access)

- Telnet to hsspconfig.sabre.com 389 (LDAP services for NOFEP access)

To configure csapi.cfg

CCSAPI takes its configuration settings from the Csapi.cfg file, which must be placed in the Windows directory.

1. From the Windows directory, open Csapi.cfg in Notepad.

2. Locate the Route names section.

3. In the FIXEDTERMINALHSSP2 entry, (or your own route, if you have created one) replace PUT_YOUR_PROVIDED_VALUE_HERE with (one of) the address(es) provided to you by Sabre (a six digit hex number).

4. Locate the {hssp2terminalfixed} section.

5. Modify SKIPLEADINGCHARS to equal 3.

6. Modify EBCDIC2ASCII to equal "NO".

7. Save and close the file.

To define a new session in INFOConnect Accessory Manager

1. In Attachmate Accessory Manager, from the File menu, select New Session.

2. If asked to select a host type, select ALC Host and click Next.

3. If offered the chance to use an existing path, just click Next to create a new path.

4. Select the SABRE2 connection type and click Next.

5. Enter FIXEDTERMINALHSSP2 or, if you have created one, the name of your own route. Then click Next.

6. Enter (one of) the terminal address(es) provided to you by Sabre (a six digit hex number) and click Next.

7. Enter the path name and description (the path name and description identify the configuration settings in the Accessory Manager database for the workstation). Click Next.

8. Click Finish to use the existing session name or enter another name and click Finish.

    Test the new session. The first time you try to connect to the new terminal address (TA), a standard disconnect NOFEP message may appear. Disregard the message and try again.

FIPS 140-2 Support

Federal Information Processing Standard (FIPS)140-2 is a standard that describes US Federal Government requirements that IT products should

meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST). The standard defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems.

Attachmate received FIPS 140-2 validation from NIST for the Reflection Security Components and the Reflection for the Web Security Components.

Use the following procedures to specify FIPS 140-2 validation for existing and new connections.

Configure FIPS 140-2 for Existing Connections

Existing sessions will continue to use the previously configured connection path unless you deliberately edit the connection properties.

To configure FIPS 140-2 for existing connections

1   In an open session, choose Edit > Settings.

2   On the left, select Connection.

3   Do one of the following:

- For IBM AS/400 sessions, on the General tab, for Security type, choose Attachmate FIPS 140-2 and leave Encryption Strength set to Auto. The appropriate encryption strength will be negotiated for the connection.

- For IBM Mainframe sessions, on the General tab, click the Add button. In the Configure Connection dialog box, for Security type, choose Attachmate FIPS 140-2 and leave Encryption Strength set to Auto. The appropriate encryption strength will be negotiated for the connection.

- For Unisys sessions, on the Connection tab, click the Advanced button. In the Path Wizard, follow the prompts to add your settings. On the page that displays your IP address or host name and port, select the FIPS 140-2 option. Complete the Path Wizard.

- For VMS/UNIX/Asynchronous sessions, on the General tab, click the Advanced button. In the Reflection Secure Shell Settings dialog box, click the Encryption tab and then select Run in FIPS mode.

4   Click OK to exit all dialog boxes.

Configure FIPS 140-2 for New UTS and T27 Connections

When you configure secure UTS and T27 SSL/TLS connections via Reflection for the Web security components, only connections using FIPS 140-2 permitted protocols are allowed.

To configure a FIPS-validated connection

1   In the Accessory Manager, choose File > New to create a new session.

2   In the New Session Wizard, specify Unisys 2200 or Unisys A Series for host type and click Next.

3   Follow the prompts in the Path Wizard.

4   On the page where you enter the IP Address or Host Domain Name and Host Port, select FIPS 140-2.

5   Complete the Path Wizard.

Configure FIPS 140-2 for New TN3270 and TN5250 Connections

FIPS 140-2 is supported in the EXTRA! TN3270 and TN5250 transports as an SSL/TLS connection via Reflection for the Web security components.

To configure a FIPS-validated connection

1   In the Accessory Manager, choose File > New to create a new session.

2   In the New Session Wizard, specify IBM AS/400 or IBM Mainframe for host type and click Next.

3   Follow the prompts in the New Session Wizard.

4   On the tabbed page, on the General tab, do one of the following:

- For IBM AS/400 sessions, from the Security type list, choose Attachmate FIPS 140-2. Leave Encryption Strength set to Auto and click OK. The appropriate encryption strength will be negotiated for the connection. Complete the New Session Wizard.

- For IBM Mainframe sessions, on the General tab, click the Add button. In the Configure Connection dialog box, for Security type, choose Attachmate FIPS 140-2, leave Encryption Strength set to Auto, and click OK. The appropriate encryption strength will be negotiated for the connection.

Configure FIPS 140-2 for New VAX/VMS/UNIX or Asynchronous Connections

FIPS 140-2 is supported via SSH connections in VT Telnet connections. In these connections, FIPS 140-2 is provided by Reflection Security Components.

To configure a FIPS-validated connection

1   In the Accessory Manager, choose File > New to create a new session.

2   In the New Session Wizard, specify VAX/VMS/UNIX, or asynchronous hosts for host type and click Next.

3   Follow the prompts in the New Session Wizard.

4   On the General tab, do one of the following:

- For Telnet connections, enter the host name. Then, click the Security tab, and for Type of security, choose Attachmate FIPS 140-2.

- For SSH connections, for Host, enter the host name, and then click the Advanced button. In the Reflection Secure Shell Settings dialog box, click the Encryption tab and select Run in FIPS mode.

Reflection Secure FTP Client

The Reflection Secure FTP client provides FIPS 140-2 compliant support for a wide variety of FTP servers, including Unix, NetWare, Unisys, HP

3000, IBM mainframe, AS/400 and OpenVMS. It allows you to encrypt file transfers using industry-standard SSL/TLS or SSH protocols, export and import settings in XML format, and perform site-to-site transfer between FTP servers.

The Reflection Secure FTP client is a feature in the INFOConnect Enterprise Edition installation along with the following utilities:

- Kerberos Manager: Manages and configures the Reflection Kerberos client.

- Key Agent: An application that holds multiple private keys that can be used in Secure Shell connections for public key authentication. It also enables agent forwarding for a Secure Shell connection.

Reflection for the Web Security Proxy Server

The Reflection for the Web security proxy server is a component of Attachmate Reflection for the Web, remote host access software that securely connects browsers to applications on hosts such as IBM, OpenVMS, and Unisys. Using SSL v3.0 or TLS v1.0 protocols, the security proxy provides secure connections to hosts even if they are not running an SSL/TLS server. The Reflection for the Web security proxy server can run on any server with Java Runtime Environment 1.3 or higher, 95 MB of disk space and a minimum of 512 MB of RAM.

Reflection for the Web security proxy server features and capabilities include the following:

- FIPS 140-2 validated cryptographic code

- Encryption strengths up to 256-bit AES

- Clients can connect to multiple hosts through a single listening port

- End-to-end SSL connections where the client completes an SSL handshake directly with the host

- Centrally managed access control where authentication and authorization are verified by the proxy

Configuring Reflection for the Web Security Proxy Server for INFOConnect

To configure the Reflection for the Web security proxy server, you will need the Reflection for the Web installation image and an INFOConnect (Unisys or Airlines) installation image.

Configuring the security proxy server can be divided into these general tasks:

- Install the security proxy server.

- Configure the security proxy server.

- Start the security proxy server.

- Generate the server certificate.

- Configure the emulation client session.

To install the security proxy server.

1. Install Reflection for the Web. The security proxy is the minimum feature set to install.

2. Note the server name and the network ports used.

3. When asked for the common name for the server, note the following:

   - Must be all ASCII characters

   - May be a full DNS name such as hostname.domain.com

   - May be a NETBIOS name such as hostname

   - May be the IP address of the server

4. The Organizational Unit field can be a department name.

5. The Organization field can be the company name.

6. The suggested name for the Certificate Friendly Name field is "Management Server."

7. Fill in the other fields as needed to complete the installation.

8. Note the URL for the server.

To configure the security proxy server

1. Select the Security Proxy Wizard from the Windows Start menu.

2. On the Advanced Settings tab, uncheck Client Authorization.

3. SSL 3.0 may need to be unchecked.

   Note: Since SSL 3.0 cannot used for FIPS-140-2 connections, TLS must be enabled on the Reflection for the Web security proxy server for FIPS-140-2 connections.

4. On the Proxies tab, define the proxy connections.

   The Export Proxy window appears, trying to update the RWeb Manager. If the RWeb Manager is not present, the update will fail. This is normal. Restart the Reflection Security Service so that the configuration is read.

To start the security proxy server

1. From the Windows Start menu, select Start Security Proxy.

2. Click Next on each screen.

   The Terminal windows appear briefly and close.

To generate the server certificate

1. From the Security Proxy Wizard, select the Security Proxy Certificates tab.

2. Select Export and save the file as RWEBproxy.cer.

   The .cer file type happens with a normal export. If you need Base64, import by selecting Certificates from the Content tab of the Internet Options window (Control Panel or Internet Explorer). On Windows 7 or Vista, ensure that you force the import to use a trusted store.

To configure the emulation client session

- Configure the emulation client session (INFOConnect or EXTRA!) to connect to the IP address and port for the host type on the security proxy server.

Port Numbers for Emulation Clients

The following table lists the default port numbers emulation clients can use to access hosts.

Terminal	Port
UTS	Port 102
UTS secure	Port 3782
T27	Port 23
UDPFRAD	Port 3020
ATSTCP	Port 2748
MATIP	Port 350

SABRE	Port 12001
SABRE2	Port 30031
TN3270	Port 23
TN5250	Port 23
Telnet	Port 23

Introduction to Public Key Infrastructure

A Public Key Infrastructure (PKI) is a system that helps facilitate secure communications using digital certificates. INFOConnect supports the use of a PKI for host (server) and user (client) authentication during FIPS 140-2 validated SSL/TLS sessions.

Authentication

Authentication is the process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), or something you have (such as a private key or token). In a typical session to a remote host, the client authenticates with a password, but the host is not authenticated. More secure protocols (including FIPS 140-2 validated SSL/TLS) require host authentication. Host authentication is accomplished using public key cryptography. In addition, SSL/TLS can also be configured to use public key cryptography for user authentication.

Public Key Cryptography

Public key cryptography uses a mathematical algorithm, or key, to scramble (encrypt) data, and a related key to unscramble (decrypt) it. One of the keys is a public key, which can be freely distributed to communicating parties, and the other is a private key, which should be kept securely by the owner of the key. Data encrypted with the private key can only be decrypted with the public key; and data encrypted with the public key can only be decrypted with the private key, allowing digital signatures to be verified.

When keys are used for authentication, the party being authenticated creates a digital signature using the private key of a public/private key pair. The recipient must use the corresponding public key to verify the authenticity of the digital signature. This means that the recipient must have a copy of the other party's public key and trust in the authenticity of that key.

Digital Certificates

Digital certificates provide a secure way to distribute public keys. Certificates are provided by a trusted third party, called a certification authority (CA). Each certificate includes a public key and identifying information about the owner of that key. In addition, the certificate is digitally signed by the CA. Anyone with a copy of the CA's public key can ensure that the contents of any certificate issued by that CA have not been altered. Because you trust the CA, you can be confident that the key owner is who or what he claims to be, and that the public key has not been tampered with.

All SSL/TLS sessions require certificates for host authentication; without the necessary certificate, you cannot make a host connection. Depending on the host configuration, you may also need to install certificates (configure a private key) for client authentication.

Digital Certificate Stores

Digital certificates are maintained on your computer in certificate stores. A certificate store contains the certificates you use to confirm the identity of remote parties, and may also contain personal certificates, which you use to identify yourself to remote parties. Personal certificates are associated with a private key on your computer.

The Reflection Certificate Manager can be configured to use digital certificates located in either or both of the following stores. However, for use with the DoD PKI, you must use the Reflection certificate store and disable the use of the Windows certificate store by the Reflection Certificate Manager.

- **Windows Certificate Store:** This store can be used by a number of applications, including Web browsers and Email clients. Some certificates in this store are included when you install the Windows operating system. Others may be added when you connect to Internet sites and establish trust, when you install software, or when you receive an encrypted or digitally signed email. You can also import certificates manually into your Windows store. Manage the certificates in this store using the Windows Certificate Manager.

- **Reflection Certificate Store:** This store is used only by Reflection applications, and this is the certificate you must use for DoD PKI purposes. To add certificates to this store, you must import them manually. You can import certificates from files and also use certificates on hardware tokens such as smart cards. Manage the certificates in this store using the Reflection Certificate Manager.

  When you configure the Reflection Certificate Manager to use only the Reflection certificate store (when use of the Windows store is disabled), only those certificates you have imported into the Reflection store are used for host authentication.

Additional Private Key (Certificate) Information and Safeguards

Depending on the host configuration, you may also need to install personal certificates (configure a private key) for client authentication.

77

DoD PKI Configuration Overview

This section provides a summary of the main steps required for INFOConnect to operate within the Department of Defense (DoD) Public Key Infrastructure (PKI) environment. To configure INFOConnect to use the required FIPS 140-2 validated SSL/TLS connections, you must complete the tasks outlined below, in INFOConnect and the Reflection Certificate Manager.

INFOConnect Tasks

Use the Path wizard to create a new INFOConnect path or configure an existing INFOConnect path to use the following options:

- FIPS 140-2 encryption

- CRL or OCSP certificate revocation checking

- Verify host name against host certificate name

Reflection Certificate Manager Tasks

Use Reflection Certificate Manager to complete the following tasks and configurations:

- Disable the use of the Windows certificate store for SSL connections.

- Configure the appropriate server for certificate revocation checking.

- Install the appropriate trust points (referred to as Trusted certification authorities or Certification authorities in Reflection Certificate Manager).

To enable FIPS 140-2 validated SSL/TLS for an existing configuration

Note: This procedure is required for DoD PKI users.

1. Run the Database Editor.

2. From the Connection Type list box, do one of the following:

To	Do this
Configure a TCPA connection type	a. Select TCPA.
	b. From the Paths and their descriptions list, click the name of the path that you want to modify.
	c. Click the Path tab.
	d. Click Advanced.
Configure an INT1 connection type	a. Select INT1.
	b. Click the Connection tab.
	c. Click Advanced.

3. Select FIPS 140-2 in the Encryption group box.

4. Type the IP address or domain name of the security proxy in the IP address or domain name text box, and then click Configure PKI in the Encryption group.

5. From the PKI Settings dialog box, select Verify host name against certificate name, select at least one of the options from the Certification revocation group box, and then click Reflection Certificate Manager.

   The Certificate Manager opens.

6. Configure the Certificate Manager for use in your situation.

7. Close the Reflection Certificate Manager and then click OK on the PKI Settings dialog box.

8. Click Configure in the Socket group.

   The TCP Path Options dialog box opens.

9. Make sure the appropriate port on the proxy server is specified.

10. (Optional) Type an alternate IP address or domain name in the IP address or domain name text box in the Alternate path group, and then select the appropriate encryption setting.

    INFOConnect automatically reuses the PKI settings you configured for the security proxy.

11. Click OK from the TCP Path Options dialog box and any subsequent dialog boxes.

12. Save the record.

When the new session connects to the security proxy, a Padlock symbol appears on the status bar to indicate a secure connection. If you have multiple active sessions, the status bar shows the state of the session that has focus within Accessory Manager.

CryptoConnect

The CryptoConnect Encrypted Transport System (ETS) consists of a gateway and one or more clients that fully encrypt communication between INFOConnect emulators and a host. To do so, the CryptoConnect TCP/IP Gateway runs on a Windows server and fully encrypts communication sent from the host to the client. The client (CryptoConnect ETS) resides on a separate PC from the gateway and encrypts and decrypts communication between the client and the gateway.

CryptoConnect encryption is FIPS 140-1. The Reflection for the Web security components, which provide FIPS 140-2 encryption, will replace CryptoConnect in future releases.

Encrypting EXTRA! for Accessory Manager Sessions

Encrypt existing or new EXTRA! for Accessory Manager sessions by editing the connection settings.

SSL v3.0 provides a secure TN3270 session that implements standard SSL support as provided directly by some IBM mainframes and products such as the Attachmate SNA Gateway. It allows the use of Smartcard and client certificate pass through, but will not connect to the CryptoConnect Gateway.

To edit the connection settings

1. Create a new session or open an existing session.

2. Select Settings from the Options menu.

3. From the Settings screen, click Connection and then Add or Edit.

   The Configure Connection dialog box appears.

4. On the General tab of the Configure Connection dialog box, specify the following:

To use	Set this
Standard SSL v3.0 encryption with Smartcard and client certificate pass through features with TN3270 sessions	The host alias or IP address of the SSL-enabled host or TN3270 gateway SSL V3.0 as the level of encryption. If you select Use Microsoft Security Implementation, you will need a Cryptographic Security Provider application provided by a third party, usually the Smartcard vendor or Microsoft.

The new settings take effect the next time you open the session. A Padlock symbol appears on the session status bar when you run a session that has a secure connection. If you have multiple active sessions, the status bar shows the state of the session that has focus within Accessory Manager.

If you specify encryption for a host or gateway that does not support encryption, or if you fail to select encryption for a host or gateway that supports encryption, the session terminates with an error.

Unencrypting EXTRA! for Accessory Manager Sessions

- You can turn off encryption by selecting None for the encryption level and for FIPS-140 sessions, by replacing the CryptoConnect Gateway IP address with the host IP address or host alias, host name, or DNS host name.

Encrypting OTS Sessions

When you encrypt existing or new OTS sessions, all sessions to be encrypted must use encrypted channel and connection configurations, and those configurations must specify the gateway IP address or domain name rather than the host IP address or domain name.

You can use the INFOConnect Accessory Manager or Database Editor to enable or disable encryption for individual client connections. If you have numerous existing OTS sessions to encrypt, you can also encrypt each client's OTS sessions all at once through the INFOConnect Manager by configuring the ICW40-TCP package at each client PC as explained below.

Notes

UTS Users: Once you encrypt particular channel or connection configurations, all sessions that use those configurations are encrypted. Unencrypted sessions must use unencrypted channel and connection configurations. If you specify encryption for a host or gateway that does not support encryption, or if you fail to select encryption for a host or gateway that supports encryption, the session terminates with a Session path closed error.

T27 Users: If you specify encryption for a host or gateway that does not support encryption, the session terminates in an Encryption/ negotiation failure error; if you fail to select encryption for a host or gateway that supports encryption, the session fails to respond.

To create new encrypted sessions

Use the session and path wizard screens in Accessory Manager.

To encrypt a single existing OTS session

1. In the Database Editor, go to the TCP/UDP Path Options dialog box.

2. Select Encrypted Connection.

3. Type the IP address or domain name of the CryptoConnect TCP/IP Gateway in the IP address or domain name text box.

4. Click Configure to open the TCP path options dialog box.

5. Verify that the correct information is specified for the Remote port and value options as follows:

For this connection	Specify these options	Value
Any T27 connection	Remote Port: TELNET	23
Any UTS connection with a DCP-Gateway mode connection type	Remote Port: TELCON	256

Any UTS connection with a DCP-IP Router mode or HLC connection type	Remote Port: TP0	102

6. (Optional) Type an alternate IP address or domain name in the Alternate IP address or domain name text box.

7. If you want the alternate IP address to be encrypted, you must type the name of an alternate CryptoConnect TCP/IP Gateway and select Encrypted connection.

8. Click OK on the TCP/UDP path options dialog box and any subsequent dialog boxes.

9. Click the Save icon on the toolbar.

When the new session connects to the CryptoConnect TCP/IP Gateway, a Padlock symbol appears on the status bar to indicate a secure connection. If you have multiple active sessions, the status bar shows the state of the session that has focus within Accessory Manager.

Encrypting Several Existing OTS Sessions at One Time

The ICW40-TCP page allows you to configure several existing OTS sessions at one time. When you configure the ICW40-TCP package, the INFOConnect Manager reads the cryptocn.ini file to obtain the IP addresses of the host and gateway to encrypt all of the sessions connecting to each host IP specified. A sample cryptocn.ini is included in the Infocnee directory.

If you do not modify the cryptocn.ini, or if you have existing sessions that connect to an IP address that you do not specify in the cryptocn.ini file, the Convert existing paths to use encryption dialog box appears when you configure the ICW40-TCP package. Complete that dialog box to encrypt the remaining sessions, or, if you do not want to encrypt those sessions, indicate that no change is necessary.

To modify the cryptocn.ini file

1. In line 1, enter the IP address or DNS name of the host your clients access as follows. You must include the square brackets around the host IP or DNS name.

   ```
   [123.456.78.901]
   ```

2. In line 2, do one of the following:

To	Do this
Provide the IP address of the CryptoConnect TCP/IP Gateway that you direct the clients to for encryption	Enter Gateway=*234.567.89.012* where *234.567.89.012* is the IP address
Not use a gateway for a particular host or to not encrypt communication with a particular host	Enter Gateway= Communication to that host will not be encrypted

3. To set the Fallback option do one of the following:

To	Do this
Enable the client to access the host directly (without encryption) in the event of a problem accessing the gateway	Set Fallback to True: [123.456.78.901] Gateway=234.567.89.012 Fallback=TRUE
Enable the client to access the host without encryption	Set Fallback to False: [123.456.78.901] Gateway=234.567.89.012 Fallback=FALSE If you do not set the Fallback option, the default FALSE will be used.

4. Complete steps 1 - 3 for each host in your network that you want to connect to with encrypted sessions.

   If the various client configurations sometimes reference the host by the DNS name and sometimes by the IP address, include an entry for each kind of configuration in the file.

5. Save the modified Cryptocn.ini file in the Windows directory on the client PC.

6. (Optional) If you have several clients that access the same hosts, you can copy this file to the Windows directory on additional client PCs.

To configure the ICW40-TCP package through the INFOConnect Manager

1. Start INFOConnect Manager 32-bit.

2. From the Configure menu, select Packages.

3. Select the ICW40-TCP line and click Quick Config.

4. If the Convert existing paths to use encryption dialog box appears, do one of the following each time you are prompted:

If you want	Do this
The sessions connecting to that host to remain unencrypted	Click No change.
The sessions connecting to that host to be encrypted	Complete the configuration as follows: a. Enter the IP address of the CryptoConnect TCP/IP Gateway in the Name or IP address field. b. Select Retain old address as unencrypted fallback to have the client access the host without encryption in the event of a problem accessing the gateway. c. Click OK to encrypt all sessions associated with that IP address.

5. Repeat step 4 until you are no longer prompted to complete the Convert existing paths to use encryption dialog box.

6. When the Convert existing paths to use encryption dialog box no longer appears, your existing sessions are configured and ready to be used and you can exit INFOConnect Manager.

Unencrypting OTS Sessions

When you unencrypt a UTS session, all sessions associated with the connection name are then unencrypted.

To unencrypt an OTS session

1. Open the session.

2. On the TCP/UDP path options dialog box, make these changes:

    *   Replace the name of the CryptoConnect TCP/IP Gateway with the name of the host in the IP address or domain name text box.

    *   Clear the Encrypted connection check box.

3. If you specified a CryptoConnect TCP/IP Gateway as the alternate IP address, make these changes on the TCP path options dialog box:

    *   Replace the name of the CryptoConnect TCP/IP Gateway with the name of the host in the IP address or domain name text box.

    *   Clear the Encrypted connection check box.

Unencrypted UTS Sessions

When you unencrypt a UTS session, all sessions associated with the connection name are then unencrypted. If you need to run both encrypted and unencrypted UTS sessions from the same client, the terminal ID (TID), channel, environment, and connection configurations for each kind of session (encrypted or unencrypted) must be unique.

Because it is easy to inadvertently mix and match the named channel, environment, and connection configurations, it is recommended that you give similar descriptive names to all the named configurations that are related to one kind of session. For example, an encrypted channel to a DCP in a demand mode could use dcp_enc and dcp_dem_enc as the channel and environment configurations names.

To create a UTS session that uses an encrypted channel/connection without affecting existing unencrypted sessions

1. Create a new UTS session in Accessory Manager, completing the dialog boxes as prompted. Ensure that you do the following:

   - Assign a unique TID to the session.

   - Enter a new name for the channel. (If you do not enter a new channel name, you will not be able to use the original channel for an unencrypted session.)

   - Enter a new environment name.

   - Enter a new connection name.

   - Enter the IP address or domain name of the CryptoConnect Gateway and select the Encrypted connection box.

2. Click Finish to establish the session.

   When the new session connects to the CryptoConnect TCP/IP Gateway, a Padlock symbol appears on the status bar to indicate a secure connection.

   When you configure additional encrypted sessions, you can use the same channel and environment names as long as you use a new TID and path name. You will not be prompted to enter a connection, check the encryption option, or enter the gateway IP address if you re-use the channel and environment. The new session gathers that information from the channel and environment configurations.

Using EXTRA! for Accessory Manager

EXTRA! for Accessory Manager is a suite of terminal emulators (3270, 5250, and VT) and connection tools that let your PC communicate with an IBM mainframe, AS/400, or DEC host. EXTRA! for Accessory Manager is a stand-alone application that exists in a separate folder. You can run this application by itself, or you can create and open EXTRA! sessions within Accessory Manager.

To use EXTRA! sessions within Accessory Manager, you must keep both applications installed. When you open an EXTRA! session within Accessory Manager, the session still requires files from the Infocnee\Extra folder to run.

Limitations of EXTRA! for Accessory Manager

Although you can create and open EXTRA! sessions within Accessory Manager and perform most of the functions that you can with any other emulator, there are some limitations:

- Any keyboard maps, QuickPads, toolbars, or schemes located in the remote folder (as specified on the Global Preferences dialog box) are not copied. To use any of these files, you must copy them manually to the Infocnee\Accmgr32 folder or whatever folder is specified as the local or remote folder on the Global Preferences dialog box.

- When you display the Open Session dialog box using Accessory Manager, only .adp files are displayed by default. To view all files in the Sessions folder, select All Files from the Files of Type list box. (Any 3270, 5250, or VT sessions that you create using Accessory Manager automatically use the .adp file extension, and will be immediately visible in the Open Session dialog box.)

- Edit settings and File transfer settings do not appear in the Apply settings category on the Action dialog box, so you cannot apply edit schemes or file transfer schemes using keyboard maps, QuickPads, toolbars, or HotSpots. However, you can create these schemes and use them in your session using the Settings dialog box.

- You cannot associate file transfer schemes with recorded host screens. File Transfer Schemes does not appear in the Available Settings list box on the Settings tab on the Page Settings dialog box.

- Any data about the session that was typed on the Properties dialog box using EXTRA! for Accessory Manager is not available from the Accessory Manager application window.

- Accessory Manager does not support EXTRA! layout files (.ewl).

    Although context-sensitive Help is available for all dialog boxes, no other online Help for EXTRA! is accessible from within Accessory Manager. To access additional online Help for this product, you must run EXTRA! for Accessory Manager as a stand-alone application and click the desired item from its Help menu.

EXTRA! Administrative Tools

In addition to the utilities included with INFOConnect, EXTRA! for Accessory Manager provides a few utilities that are installed into the same program group under Windows.

Scheduling Events with NiteApps

NiteApps automatically starts an application or executes a batch command file on your personal computer at the time and day you specify. NiteApps operates whether or not EXTRA! is running. Consequently, you can use NiteApps to start personal computer applications independent of your work on the host.

For NiteApps to run a program or batch command file, the NiteApps application must be loaded and in Run mode. To ensure that your scheduled programs run daily, you can create a Windows shortcut to NiteApps and then place this shortcut in your Windows Startup directory. This will cause the NiteApps program to load in the Run mode each time you start your personal computer.

To load NiteApps

1. From the Start menu, choose INFOConnect Enterprise Edition and select NiteApps.

2. From the NiteApps File menu, choose Open.

3. From the Open dialog box, select the NiteApps configuration file (.nap) that contains the list of programs you want to execute and click Open.

   The existing events are displayed in the Events dialog box.

4. Choose Run to start the NiteApps file.

5. The first time you start NiteApps, the Events dialog box is empty. You can begin scheduling events by choosing the Add button. If you have previously created a NiteApps file, NiteApps displays a list of scheduled events for the last NiteApp created. To create a new NiteApps file, select New from the File menu and click the Add button. The Schedule Event dialog box opens.

   For detailed information on the Schedule Event dialog box, select the Help option on the NiteApps dialog box and choose the Help Topics option.

To schedule an event

1. On the NiteApps dialog box, click Edit to edit an existing NiteApps file or Add to create a new NiteApps file.

2. Enter the event name.

3. Enter the full path and filename of the program file or batch file you want NiteApps to start, or select the filename by using the Browse function. Include any necessary command parameters. If the parameter is a data filename, include its path as well as its filename.

4. If the event occurs on a continual basis, select Recurring Event. If you select Hourly, be sure to choose the proper timing.

5. When you are finished scheduling events, click OK.

6. To save the NiteApps file, select Save or Save As from the File menu and assign a filename to the file.

Editing Host Code Pages

With the Attachmate Host Code Page Editor, you can create custom code pages that:

- Can be used for display, printer and file translations

- Change how a character is translated between the host and the PC

Use the Host Code Page Editor to change host values if characters print or display incorrectly, or if a department wants different characters to appear. For example, if an asterisk (*) prints incorrectly on a laser printer, you can change the host value to print a dollar sign ($) instead. Or, you can easily meet the request of a department to print a space instead of a pipe sign (¦). You can also create a new host page to make temporary printing changes to a host document.

The Host Code Page Editor makes it easy for you to determine which host value should display. For example, if you are having trouble with file transfer and would like to learn which value should display a copyright symbol (©), you can open Host Code Page Editor and identify the value.

To edit a host code page

1. Run the following file to open the Host Code Page Editor:

   [install_directory]\Attachmate\Infocnee\AtmCpEdt.exe

2. From the File menu, choose New. The Select Base Host Code Page appears.

3. Select the Host Code Page that you want to modify, and click OK. The selected Host Code Page is displayed in the Editor.

4. Double-click the value you want to modify, enter the new value, then press the Enter key. You must use the Enter key to establish the new value.

5. Save your new custom code page with a unique name.

Sending Commands to an AS/400 Host without a Display Session

Using the Remote Command utility, you can start and control non-interactive programs on an AS/400 host without opening an AS/400 display session. Commands can be sent individually or in combination, and can be saved as an ASCII file for resubmission. Return codes are received, but program data cannot be returned from the host.

The Remote Command utility provides:

- An interface to automate sending one command or a batch of commands.

- An API set for Remote Command and Distributed Program Call. This includes header files, an .lib file, and sample code.

The API set and sample code is installed to the following location:

```
install_directory\Attachmate\Infocnee\Samples\Rcsample.*
```

To send commands to an AS/400 host without a display session

1. Determine the non-interactive programs on the AS/400 host that you want to start and control from your personal computer. For example, to send an immediate message to one or more message queues, you would use the SNDMSG command.

2. From the display session, test the command to make sure that it is a legitimate command.

3. Write down or copy the command lines that you are entering from the display session.

4. Open the Remote Command utility.

5. From the File menu, choose Open.

6. If you are creating a new command script (.RCS), choose New.

     -or-

   If you are editing an existing command script, select the filename of the command script that you want to edit, and then choose **Open.**

7. Enter the command lines.

To send	Do this
One command line	Move the cursor to the command line to be sent, then choose the Send Command button.
All commands listed in the box	Choose the Send All Commands button.

When commands are sent, the actual messages that were sent are displayed in the Command Output Messages box.

8. Choose Save to save the command script (.rcs).

You can also choose Save As to save an edited command script to be resubmitted, or Exit to close the Remote Command dialog box without saving your changes.

APPN End Node Support

The INFOConnect APPN End Node implementation makes it possible for workstations to participate in an APPN network. Information can be exchanged with any APPN Network Node, which results in improved performance and easier configuration in the network.

Many different APIs in the APPC/APPN environment are supported, including:

- APPC
- CPI-C
- WOSA APPC
- WOSA CPI-C

APPN Node supports Dependent LU Requester (DLUR/DLUS) conversations with your 3270 applications. This allows you to route full 3270 traffic across your APPN network. The Dynamic Definition of Dependent LU (DDDLU) feature enables simpler configuration of VTAM physical units (PU). You can assign pools of LUs on the host instead of listing each LU on a PU definition.

Using the APPN Node Manager application, users and administrators can monitor, activate and deactivate items in the APPN Node, and the INFOConnect Status App utility supports all types of APPC and CPI-C tracing.

These highlights are a subset of the features available in the INFOConnect APPN End Node implementation. Context-sensitive Help is available throughout the APPN Configurator and APPN Node Manager applications to provide more assistance.

The recommended configuration procedure is to use the New Session wizard to create new sessions and specify connectivity prior to using the APPN Configurator to add peer connectivity.

Appendix A: INFOConnect Configuration File Reference

In addition to host session configuration files, there are many other configuration files that you may want to deploy to your users. These include macros, toolbars, QuickPads, hotspots, keyboard maps, and color schemes. INFOConnect installs a selection of configuration files that you can use or modify.

For more information about creating these types of configuration file, open a session and select INFOConnect Help Topics from the Help menu.

With the Attachmate Customization Tool, you can provide additional files with your custom installation. For example, you may want to include a preconfigured session file, or a macro. Following is a list of the type of files that can be added to an INFOConnect installation:

File Type	Description
.adp	INFOConnect session file
.app	Print session file
.atb	PTR Device initialization files
.atm	T27 Print config file
.aww	INFOConnect layout file
.bgr	PTR device initialization file
.bkm	Bookmark file
.btp	PTR device initialization file
.cfg	INFOConnect database file
.cmu	Menu scheme file
.cnf	ALC configuration file
.ctt	Custom translation table file
.dic	Custom dictionary file
.dll	PTR direct link libraries
.e3c	3270 color scheme file
.e3e	3270 edit scheme file
.e5c	5250 color scheme file
.e5e	5250 edit scheme file
.e5t	5250 file transfer file
.eac	Auto complete dictionary file

`.ead`	Auto expand dictionary file
`.ebd`	Dialog file
`.ebh`	Macro header file
`.ebm`	Macro file
`.edc`	DEC color scheme file
`.ede`	DEC edit scheme file
`.edp`	EXTRA! display session file
`.edt`	DEC transfer scheme file
`.ehs`	HotSpot scheme file
`.eil`	IND$file transfer list file, PTR external interface libraries
`.eis`	IND$file scheme file
`.ekm`	Keyboard map file
`.elf`	EXTRA! layout file
`.env`	Navigation action file
`.epp`	EXTRA! printer session file
`.eqp`	QuickPad file
`.esf`	Security editor file
`.etb`	Toolbar file
`.etl`	Batch transfer list file
`.exs`	EXS file
`.flt`	Aomdemon filter file
`.ftb`	AS400 batch file transfer list file
`.hff`	PTR host file filter
`.his`	VT history file
`.hst`	History file
`.inf`	INFOConnect setup file
`.lsr`	PTR device initialization file
`.msr`	PTR device initialization file
`.mtr`	Session monitor file
`.nap`	NiteApps file
`.ocr`	PTR device initialization file

`.qpr`	QuickApp file
`.sdb`	Demo doc file
`.set`	Profs print settings
`.sl`	PTR service libraries
`.tbl`	Translate table file
`.tem`	Migrate wizard file
`.tlx`	Wintertree spellchecker dictionary configuration file
`.txt`	Text file
`.xcp`	APPN node file
`.xml`	Privacy file
`.xwc`	CASL macro executable file
`.xws`	CASL macro source file
`privacy.xml`	Privacy filtering file

Appendix B: Launcher Control Property Descriptions

You can add an INFOConnect session to any Web page by calling the INFOConnect ActiveX control. This control is called by the `launch` method, and uses several properties, described below.

Method name	Syntax	Description
launch	BOOL launch()	Creates and opens the INFOConnect session specified in the `launchfile` property.

Property name	Type	Description
launchFile	String	Required. The filename of session to open.
		This can be any of the following formats:
		SessionName.adp
		Drive:\DirectoryName\SessionName.adp
		http://ServerName/DirectoryName/SessionName.adp
		scripting requires double back-slash characters in strings such as: "C:\\Accounting\\SessionName.adp"
userid	String	Optional. A user ID that can access this session configuration.
password	String	Optional, write-only. A valid password for this session configuration.
embedded	Boolean	Optional. If true, the session opens embedded in a browser window. If false, the session opens in the standard INFOConnect window.
		The default setting for this property is true.

session	IDispatch	Read-only. This property returns a pointer to the session object. This allows programmatic access to the session object and all of its sub-objects.
		A full description of the properties and methods of the session object and all of its sub-objects is available in the Help installed with the INFOConnect client application here:
		install directory\Attachmate\Infconnect\Enu \Epc_ole.hlp
onclose	String	Optional. Determines what happens to the session when the Web page containing the ActiveX control closes (such as when moving to a different Web page, or closing the browser). The behavior resulting from this property depends upon whether the control is embedded or not. See the table below for details.

onclose Property

Unless an embedded session is using the `detached` value for the `onclose` property, when the session window closes, the session disconnects.

possible `onclose` **values**	if embedded	if not embedded
close	The session window will close when the Web page containing the ActiveX control closes.	The session window will close when the associated browser closes. The associated browser is the one that opened the Web page containing the ActiveX control.
detach	The session window opens as a stand-alone INFOConnect window, and loses any association with the browser that initially opened it.	The session window doesn't make an association with the browser that opened it, and so remains independent whether the browser is closed or not. This is the default setting for a non-embedded session.

cached	The session window will close when the Web page containing the ActiveX control closes; however, the session remains connected. The session's state is cached by the browser, allowing the user to visit other Web pages, and then return to the Web page that calls the session, without losing her place in the host application. If the user closes the browser, the session is dis-connected and the state is lost. This is the default setting for an embedded session.	Do not use this property if the session is not embedded.

Appendix C: Attachmate Customization Tool Reference

Use the Attachmate Customization Tool to create transforms or companion installer packages. Each type of customization has its own set of configuration panels that display depending on your choice on the Select Customization panel.

Transform Files

To create or edit transform files

1. From a command line, open the Attachmate Customization Tool.

   `[path]\setup.exe /admin`

2. From the Select Customization dialog box, do one of the following:

   - Select Create a new setup customization file for the following product.

     -or-

   - Select Open an existing setup customization file or companion installer and, in the Open dialog box, select a .mst file.

Refer to the following panels and values when creating and/or editing transform files.

Navigation pane	Panel / Description	
Welcome	Welcome to the Attachmate Customization Tool	
	Provides a description of the tool and how to use it.	
Install location and organization name	Specify the default installation folder on the user's computer	
	Specifies the installation folder and the value for the MSI standard COMPANYNAME property.	
	This setting	**Does this**
	Default installation folder	Specifies where to install the product files. (Install location changes are disabled if the primary product installer does not support changing the install location.)

	Note: List items that refer to folders (for example, [ProgramMenuFolder]) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, [ProgramFilesFolder] \My Folder). Alternatively, you can enter a fully qualified path (for example, `C:\Program Files \My Folder`), as long as that location is known to exist on the target machine.	
	Organization name	Specifies the MSI standard COMPANYNAME value.
Licensing and user interface	Accept license agreement and choose user interface level for installation	
	To configure a transform, you must accept the product license on behalf of your users.	
	If the transform is used along with setup.exe, you can also specify the user interface level for the Setup wizard GUI during the install. These settings are available when Use this customization with interactive installs using setup.exe is selected.	
	This setting	**Does this**
	None	Displays no interface.
	Basic	Displays only a progress bar.
	Full	Displays the full Setup wizard interface.
	No cancel	Sets up the install so that it cannot be cancelled after it begins.
	For some products you can enter a Volume Purchase Agreement (VPA) number.	
	Note: The purpose of VPA numbers, which are issued by Attachmate, is to allow customer support to expedite service requests.	
Add installations and run programs	Add, modify, or remove additional product installations and run programs	
	Specifies MSI packages to install and/or additional programs to run before or after the primary install. You can also specify a companion package generated by this tool.	
	This setting	**Does this**

	Add	Opens the Add/Modify Program Entry dialog box from which you can add programs along with their command line arguments.
	Modify	Opens the Add Files to Package dialog box from which you can browse to the files you want to add.
	Remove	Removes a selected program from the table. (Active only when a program is selected in the table.)
	Move arrows	Moves programs up or down in the action sequence.
Modify setup properties	Set properties for setup to apply during the installation	
	Defines public Windows Installer properties.	
	This setting	**Does this**
	Add	Opens the Add/Modify Property Value dialog box from which you can define or redefine public properties. You can modify properties in the installer database or you can create your own.
	Caution: Do not overwrite existing properties unless you fully understand how the changes affect your install. Setting properties to improper values can break the install.	
	Modify	Opens the Add/Modify Property Value dialog box so that you can change the values for the selected property. (Active only when a property is selected in the table.)
	Remove	Removes a selected property from the table. (Active only when a program is selected in the table.)
Set feature installation states	For each feature, click to select the installation state	
	Specifies feature installation states using the standard MSI feature options.	

Configure shortcuts	Modify or remove existing shortcuts for this product
	Specifies the details for shortcuts associated with added files.
	Note: Clearing a Shortcut Name check box only blocks the installation of the shortcut. The shortcut remains and can be enabled by editing the transform.

	This setting	**Does this**
	Modify	Opens the Add/Modify Shortcut dialog box from which you can change the location, name, tooltips, arguments, and initial window size of the program for which the shortcut is configured.

Modify Application Settings	Use this pane to modify settings that affect the product you are installing. Modifications you make here affect all users of the computer on which the product is installed. The features available on this pane (if any) depend on which product you are installing.

Companion Installations

To create or edit companion files

1. From a command line, open the Attachmate Customization Tool.

   ```
   [path]\setup.exe /admin
   ```

2. From the Select Customization dialog box, do one of the following:

   - Select Create a new companion installer.

     -or-

   - Select Open an existing setup customization file or companion installer and, in the Open dialog box, select an .msi file.

Refer to the following panels and values when creating and/or editing companion install packages.

Navigation pane	Panel / Description
Welcome	Welcome to the Attachmate Customization Tool
	Provides a description of the tool and how to use it.

Specify package information	Specify companion package information	
	Specifies the name displayed in the Add/Remove control panel and the value for the MSI standard COMPANYNAME property.	
	This setting	**Does this**
	Add/Remove name	Specifies the name shown in the Add /Remove control panel.
	Organization name	Specifies the value for the COMPANYNAME and Manufacturer properties.

Specify install locations	Specify the default installation folders on the user's computer	
	Specifies locations for files and shortcuts.	
	This setting	**Does this**
	Default installation folder	Specifies where to install the files.
	Note: List items that refer to folders (for example, *[ProgramMenuFolder]*) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, `[ProgramFilesFolder] \My Folder`). Alternatively, you can enter a fully qualified path, provided it exists on the target machine.	
	Default shortcut folder	Specifies where to install the shortcuts.
	Installation type folder	
	Specifies the access for files (after the installation). These options affect only the folders to which you can install. You cannot change these options after you add a file.	
	Installs to all users of a machine	
	Sets up the companion installation so that files are available for every user who logs on to the machine.	
	Installs only for the user who installs it	
	Sets up the companion installation so that the files are available only for the user who installs it.	
Add files	Specify files to add to the user's computer during installation, their location, and whether shortcuts are associated with the files.	

Navigation pane	Panel / Description	
	This setting	**Does this**
	Add files to	Specifies the folder in which to install the file selected in the table.
	Note: List items that refer to folders (for example, [ProgramMenuFolder]) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, `[ProgramFilesFolder] \My Folder`). Alternatively, you can enter a fully qualified path (for example, `C:\Program Files \My Folder`), as long as that location is known to exist on the target machine.	
	Include shortcut	Specifies creation of a shortcut for the file selected in the table.
	Add	Opens the Add files to Package dialog box from which you can browse to files you want to add.
	Update	Sets selection of the install location or whether to add or remove a shortcut. (This allows you to change these selections after the file is added to the table.)
	Remove	Removes the file selected in the table.
Configure shortcuts	Modify or remove existing shortcuts for this product Specifies details for shortcuts associated with added files.	
	Note: Clearing a Shortcut Name check box only blocks the installation of the shortcut. The shortcut remains and can be enabled by editing the transform.	
	This setting	**Does this**
	Modify	Opens the Add/Modify Shortcut dialog box from which you can change the location, name, tooltips, arguments, and initial window size of the program for which the shortcut is configured.

Navigation pane	Panel / Description	
Modify setup properties	Set properties for setup to apply during the installation	
	Defines public Windows.	
	This setting	**Does this**
	Add	Opens the Add/Modify Property Value dialog box from which you can define or redefine public properties. You can modify properties in the installer database or you can create your own.
	Caution: Do not overwrite existing properties unless you fully understand how the changes affect your install. Setting properties to improper values can break the install..	
	Modify	Opens the Add/Modify Property Value dialog box from which you can change the values for the select property (Active only when a property is selected in the table.)
	Remove	Removes a selected property from the table. (Active only when a program is selected in the table.)
Modify user settings	Make changes to user settings on the computer where the customization file is installed	
	Note: You can modify user settings only if the Installs only for the user who installs it option in the Specify install locations panel is selected.	
	This setting	**Does this**
	Application Settings	This button is available for some products. It specifies application settings to include with the primary product install package.
	Define	Opens a tool for the selected application, with which you can set user access to INFOConnect features.

	Defaults	Resets the setting to its default value.
	Remove	Removes a selected property from the table. (Active only when a program is selected in the table.)

Program Entries

To create or edit program entries

1. From a command line, open the Attachmate Customization Tool:

   `[path]\setup.exe /admin`

2. From the navigation pane, click Add installations and run programs.

3. To add a new program, click Add.

   -or-

   To modify settings for a program in the table, select the program, and then click Modify.

4. Specify how to run a program included in an installation.

For this item	Do this
Target	Specify the folder in which the program resides.
Arguments	Specify command-line arguments for the executable.
Run this program after the base product has been installed	Select to run the program executable after the base installation is complete.
Run this program before the base product has been installed	Select to run the program executable before the base installation starts.

Note: List items that refer to folders (for example, *[ProgramMenuFolder]*) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, *[ProgramFilesFolder]*\My Folder). Alternatively, you can enter a fully qualified path (for example, C:\Program Files\My Folder), as long as that location is known to exist on the target machine.

Property Values

To create or edit property values

1. From a command line, open the Attachmate Customization Tool:

    [path]\setup.exe /admin

2. From the Select Customization dialog box, select the option that best describes the task you are performing.

3. From the navigation pane, click Modify setup properties.

4. To add a new property, click Add.

    -or-

    To modify a property in the table, select the property, and then click Modify.

5. Set the property names and values to create new properties or to modify properties in the installer database.

Shortcuts

To create or edit shortcuts

1. From a command line, open the Attachmate Customization Tool:

    [path]\setup.exe /admin

2. From the Select Customization dialog box, select the option that best describes the task you are performing.

3. From the navigation pane, click Configure shortcuts.

4. Under Shortcut name, select a shortcut, and then click Modify.

5. Set the following values to configure a shortcut in a INFOConnect install.

For this item	Do this
Location	Specify where you want the shortcut to reside.
Name	Enter a name for the shortcut.
Tooltip	Enter text that describes the shortcut.
Argument	Enter command-line arguments to pass to the program.
Run	Specify an initial size for the application window.

Note: List items that refer to folders (for example, [ProgramMenuFolder]) are pre-defined folder keywords. You can create customized directories by adding new folder names with typical directory syntax (such as, [ProgramFilesFolder]\My Folder). Alternatively, you can enter a fully qualified path (for example,

C:\Program Files\My Folder), as long as that location is known to exist on the target machine.

Registry Data

Caution: Adding or modifying registry data incorrectly can cause problems that may require you to reinstall the Windows operating system.

To add or modify registry data

1. From a command line, open the Attachmate Customization Tool:

    `[path]\setup.exe /admin`

2. From the Select Customization dialog box, select the option that best describes the task you are performing.

3. From the navigation pane, click Add registry data.

4. To add a new registry value, click Add.

    -or-

    To modify a registry value in the table, select the value, and then click Modify.

5. Specify registry keys and values to add or modify during the installation process. By modifying registry values, you can change the way the application operates. (For example, for certain Attachmate applications, you can add a value that specifies to never save settings on exit.)

For this item	Do this
Key	Enter the complete Registry path from the root.
Name	Enter the registry value name. If the value name is Null, the data entered into the Value column are written to the default registry key.
Type	Select the data type of the value. Types include strings, integers (DWORD), or binary values.
Value	Enter the value.

Glossary

acquisition phase

> Windows Installer phase of installation during which the installer determines procedure. Acquisition phase begins when an application or user instructs the Windows Installer to install an application or feature. The installer then queries the database for information as it generates the execution script for the installation.

> *See also* execution phase and Installation Mechanism.

advertising

> Windows Installer capability to make the interfaces required for loading and to make an application available without installing the application. When a user or application activates an advertised interface, the installer then proceeds to install the necessary components.

> *See also* assigning, publishing and install-on-demand.

AID keys

> Keys that send commands to the host, such as ATTN, Enter, and SYS RQ. To make it possible for you to invoke these same host functions from a PC keyboard, the functions are assigned to PC keys or key combinations.

application server

> A program that manages operations between an organization's back-end systems and a user's computer. Typically used for transaction-based applications.

assigning

> During a Windows Installer installation, makes an application available, and makes it appear as if it has been installed to a user, without actually installing it. Assigning adds shortcuts and icons to the Start menu, associates appropriate files, and writes registry entries for the application. When a user tries to open an assigned application, then the installer installs the application. Assigning and publishing are two methods of advertising.

attribute

> 1. In the markup languages XML and HTML, a name-value pair within a tagged element that modifies certain features of that element. 2. In screen displays, an element of additional information that controls such characteristics as the background and foreground colors of the character, underlining, and blinking. 3. In a database record, the name or structure of a field. For example, the files Lastname, Firstname, and Phone would be attributes of each record in a Phonelist database. The size of a field or the type of information it contains would also be attributes of a database record.

> *See also* element, property.

autofield

> An automatically created user field.

bean

Reusable piece of Java code, also called a Java bean. Beans can be generated from tasks and combined to create an application.

See also JavaBeans, task, task bean.

cabinet file

In a Windows Installer installation, a single file, usually with a .cab extension, that stores compressed files in a file library. The cabinet format is an efficient way to package multiple files because compression is performed across file boundaries, significantly improving compression ratio.

cache

1. A special memory subsystem in which frequently used data values are duplicated for quick access. A disk cache refers to a portion of RAM that temporarily stores information read from disk. A memory cache stores the contents of frequently accessed RAM locations and the addresses where these data items are stored. 2. A reserved portion of a computer's RAM or hard disk set aside to temporarily hold information, for example, a Web browser cache.

See also Java caching.

CASL Macro Editor

An Accessory Manager program that you can use to create and edit CASL macros. The CASL Macro Editor is similar to a text editor, but also provides menu items for compiling and running CASL macros.

CASL macro

A series of instructions for performing specified tasks automatically. These instructions use a special script language called the Common Accessory Script Language (CASL).

character attribute

Determines how characters in text fields are treated. Mainframe character attributes determine whether fields are protected or unprotected, alphanumeric or numeric-only, and modified or unmodified.

See also extended attribute bytes.

child

1. A process initiated by another process (the parent). The parent process often sleeps (is suspended) until the child process stops executing. 2. In a tree structure, child refers to the relationship of a node to its immediate predecessor.

class

In the Java programming language, a type that defines the implementation of a particular kind of object.

class path

An environment variable that tells Java-based applications where to find Java class libraries.

client (adj)

> Pertaining to a networked computer. For example, a client application is an application that either runs directly on a client or is downloaded from a server to a client.

client (n)

> 1. On a local area network or the Internet, a computer that accesses shared network resources provided by another computer (called a server). 2. In object-oriented programming, a member of a class (group) that uses the services of another class to which it is not related. 3. A process, such as a program or task, that requests a service provided by another program — for example, a word processor that calls on a sort routine built into another program. The client process uses the requested service without having to "know" any working details about the other program or the service itself.

code page

> A table of numeric codes used to represent language-specific characters. Code pages are a way of providing support for character sets and keyboard layouts used in different countries. To display characters correctly, you must select the code page used by your host.

COMMAREA

> An area of memory on the host used to transfer inputs and outputs between COBOL programs. A particular COBOL program may use only some of the fields in the COMMAREA. There can be a single COMMAREA used for both inputs and outputs, or there can be separate COMMAREAs for each.

Common Accessory Script Language (CASL)

> A special script language used in all CASL macros.

> You can view or print a copy of the *CASL Script Language Guide* by installing the Adobe Acrobat Reader, running the Acrobat Reader, and opening the Casl_lag_ref.pdf file.

components and features

> The Windows Installer organizes an installation around the concepts of components and features. A feature is a part of the application's total functionality that a user may decide to install independently. A component is a piece of the application or product to be installed. The installer always installs or removes a component from a user's computer as a coherent piece. Components are usually hidden from the user. When a user selects a feature for installation, the installer determines which components must be installed to provide that feature.

configuration

> 1. A set of parameters that define and control the behavior of sessions and applets, which may be for terminal emulation, host printer emulation, or file transfer. 2. A set of parameters for connecting to a UTS or T27 host.

connection

> The communication link between a client and a host that allows users to interact with the host from the client computer.connection type

> The communication mechanism used by the client to establish a connection with a host.

context

> Information that adds meaning to something else. For example, a task's context could be the host connection or session with which it is associated. If the task's context is maintained, or preserved, the session remains connected after the task has completed, and the session is available to run the next task.

> *See also* stateful task.

copybook

> A file containing COBOL data declarations that was included when the COBOL program on the host was compiled. A particular copybook may be included in more than one COBOL program; a program can include several copybooks.

> A COBOL copybook declares the names and data types of variables that associated COBOL programs use to exchange information in the COMMAREA. Typically, programs that exchange data in this way are compiled with the same copybook file.

> *See also* COMMAREA.

correlation ID

> An identifier assigned to an individual transaction, used in end-to-end tracing to track the transaction across multiple components.

daemon

> A program that runs on a host to provide network services. A daemon in UNIX is similar to a TSR (Terminate and Stay Resident) program in DOS.

data source

> A host, database, or other application or repository from which information is retrieved.

decision branch

> An action that executes other actions depending on current conditions. A decision branch action consists of at least one rule and at least one condition test. If the condition test meets the rule, the branch evaluates to "true," and the event continues by executing the subsequent action.

dedicated session

> A session that is associated with a specific logical unit (LU) or terminal or station ID. Using dedicated sessions ensure that specific sessions are assigned to specific clients at run-time.

deploy

> 1. To install software onto multiple computers, either one-at-a-time or across a network. 2. To make software available on a network so that multiple users can access or install it.
>
> *See also* activate, publish.

detail table

> A table made up of detail screens, which present very long records in more than one level. The first level of the table displays only the first level of fields for each record. When a record is selected, more fields can be shown in a separate screen.
>
> *See also* table.

directory service

> A repository of information used to manage people and resources within an organization.

discovery

> In peer-to-peer computing, a mechanism used by computers on a network to locate and interact with one another.

download

> To transfer programs or data from a host or Web server to your local computer.

element

> In an XML document, an element is made up of a start-tag, an end-tag, and data in between. The start- and end-tags describe the data within the tags, which is considered the value of the element. The element may contain text, comments, or other elements.

environment

> A named set of configuration options used with Unisys ClearPath IX or 2200 Series hosts.

execution phase

> When the Windows Installer executes a script of installer actions.
>
> *See also* acquisition phase and installation mechanism.

export

> To extract data and make it available in another file or format.
>
> *See also* deploy, publish.

extended attribute bytes (EABs)

> Codes used by many mainframe applications to display highlighting, reverse image, blinking, and seven colors.
>
> *See also* character attributes.

failover

> A backup operation in which the functions of a primary resource (such as a server) are automatically assumed by a secondary resource, should

the primary resource fail or be shut down. Used to make systems more fault-tolerant, failover is typically an integral part of mission-critical systems that must be constantly available.

free ID

An ID that has been assigned to a name but that has not yet been allocated to any client.

global screen

A screen sent by the host that is not the result of a user action, for example, a message sent by the host, but not a transient screen.

See also unrecognized screen.

HLLAPI (High Level Language Application Programming Interface)

An IBM API that makes communication between a PC and a mainframe computer possible. The PC must run 3270 emulation software, and then define an interface between the PC application and the emulation software. This API type is also referred to as "screen-scraping," because the characters used would otherwise be displayed on a terminal screen.

host

A mainframe, mini-computer, or information hub with which the PC communicates.

host access ID

Connection data that is unique for an individual session with a host. The type of connection data and available properties for an ID depend on the host type with which it will be used.

host code page

See code page.

host field

A fixed region of the host screen with associated text and attributes.

host-initiated screen

See global screen.

HotGUI

A terminal applet that is just like the regular terminal session, except that it uses a GUI-style interface, as opposed to the traditional "green screen" interface.

IConnectorAccess

The interface implemented in Verastream (formerly Synapta Services Builder) to pass data using XML.

instance document

An individual XML document that conforms to a particular schema.

See also XML Schema.

installation-on-demand

> Windows Installer service that installs applications or features as requested by the user or another application. Advertising makes a feature or application available for install-on-demand installation.

installation mechanism

> In a Windows installation, there are two phases to a successful installation process: acquisition and execution. If the installation is unsuccessful, a rollback phase may occur. At the beginning of the acquisition phase, an application or a user instructs the installer to install a feature or an application. The installer then progresses through the actions specified in the sequence tables of the installation database. These actions query the installation database and generate a script that gives a step-by-step procedure for performing the installation. During the execution phase, the installer passes the information to a process with elevated privileges and runs the script. If an installation is unsuccessful, the installer restores the original state of the computer. When the installer processes the installation script it simultaneously generates a rollback script. In addition to the rollback script, the installer saves a copy of every file it deletes during the installation. These files are kept in a hidden, system directory. Once the installation is complete, the rollback script and the saved files are deleted.

installation-on-demand

> Windows Installer service that installs applications or features as requested by the user or another application. Advertising makes a feature or application available for install-on-demand installation.

interface object

> *See* task interface object.

ITask

> The interface implemented in Verastream (formerly Synapta Services Builder) to pass data using task beans.

JavaBeans

> A component architecture for the Java programming language developed initially by Sun Microsystems. JavaBeans components are called "beans."

> JavaBeans allows developers to create reusable software components that can then be assembled together using visual application builder tools. A builder tool can analyze how a bean works, developers can customize the appearance and behavior of a bean, and customized beans can be stored and reused.

> *See also* bean.

Java caching

> The process of installing Java applets or other software on a client so that the files can be run locally rather than from the server. Java caching is controlled by settings on the server rather than by the browser's cache settings. Clearing the browser's cache (either the memory cache or the disk cache) does not remove files installed via Java

caching. The location of the files and the procedure for removing them varies, depending on the browser and the applet.

Javadocs

API documentation in HTML format, generated from Java source code.

keyboard map

A file that defines the function that each key on a computer keyboard performs to communicate with a host. For example, the Ctrl + e key combination might be mapped to perform the TRANSMIT function.

layout

An arrangement of session windows, their positions on the desktop, and their host connections.

layout file

A file that defines an arrangement of session windows, including all windows in their specified sizes and positions. By opening the file, you can restart all the sessions in the layout at a later time.

legacy data

Proprietary host data, such as data on an IBM mainframe.

login task

A task that is used to log in to the host.

loop action

A decision branch action that, once completed, re-evalutes the condition and re-executes as long as the branch condition remains true.

See also decision branch.

macro

A series of instructions for performing specified tasks automatically. CASL macros are written using the CASL Script Language.

migrate

To convert existing files for use with a newer version of an existing product or competitive product.

MSI file

Windows Installer installation file (.msi) is a COM-structured storage file containing the instructions and data required to install an application. Every package contains at least one .msi file. The .msi file contains the installer database, a summary information stream, and possibly one or more transforms and internal source files. An .msi file can be either compressed or non-compressed. A compressed .msi file can hold files, but cannot be changed. An uncompressed .msi file is smaller and files can be added to it, but the additional files must be copied to the location of the .msi file. During a custom installation, if a new compressed .msi file is required (as the case would be when files are added) you will be prompted for a new .msi filename.

MSM file

Windows Installer merge modules (.msm files) provide a standard method by which developers deliver shared Windows Installer components and setup logic to their applications. Merge modules are used to deliver shared code, files, resources, registry entries, and setup logic to applications as a single compound file. Developers authoring new merge modules or using existing merge modules should follow the standard outlined in this section.

A merge module cannot be installed alone; it must be merged into an installation package using a merge tool. Developers wanting to use merge modules must obtain one of the freely distributed merge tools, such as Mergemod.dll, or purchase a merge tool from an independent software vendor. Developers can create new merge modules by using many of the same software tools used to create a Windows Installer installation package, such as the database table editor Orca provided with the Windows Installer SDK.

MSP file

A Windows Installer patch (.msp file) is a file used to deliver updates to Windows Installer applications. The patch is a self-contained package that generally contains all the information required to update the application. Patches contain at minimum two database transforms. One transform updates the information in the installation database of the application. The other transform adds information that the installer uses for patching files. The installer uses the information provided by the transforms to apply patch files that are stored in the cabinet file stream of the patch package. A patch package does not have a database like an installation package (.msi file.)

MST file

A Windows Installer transform (.mst) file adds or replaces elements in the original database. For example, a transform can add a feature or set of features for a specific set of users or a specific group of users. A common use for transforms is the customization of base installation packages for particular groups of users. Multiple transforms can be applied to a base package and then applied on-the-fly during installation. This extends the capabilities of the installer to create custom packages and provides a mechanism for efficiently assigning the most appropriate installations to different groups of users. Transforms can also be used to apply a minor fix to an application that does not warrant a major upgrade.

multiple users

An installation where the product files are installed on a single PC that multiple users share. Each user who wants to run the products runs a separate installation utility. Product configuration and management is normally handled by the PC administrator.

NavMap

A file that contains the navigation information required to access screens within a host application. This information can include screens, fields, keystrokes, and paths between screens.

node

1. In tree structures, a location (set of information) on the tree that can have links to one or more nodes below it (child nodes). The topmost node is called the "root." The root can have zero or more child nodes; the root is the parent node to its children. Each child node can in turn have zero or more children of its own. Every node in a tree has exactly one parent node (except for the root, which has none), and all nodes in the tree are descendants of the root node. 2. In an XML document that is modeled after a tree, each element in the tree is considered a node. An XML-based application can store data in all the different types of nodes and in all the fields of each node. XML states that there must be at least one element in each document: the root node. All nodes are one of four types: character, processing instruction (PI), comment, or element. Character, PI, and comment nodes have no children, so they are always leaf nodes in an XML document tree.

package

1. An .msi file and any external source files that may be pointed to by this file. A package therefore contains all the information the Windows Installer needs to run the UI and to install or uninstall the application.

2. A group of related Java classes and interfaces that provides access protection and namespace management. Bundling groups of related Java classes and interfaces into a package builds in control access between classes (both inside and outside the package), and makes it possible to quickly determine the relationship between the classes and the interfaces. Also, by creating a new namespace, it prevents the names of classes from conflicting with those in other packages.

parent

1. The first of two or more connected objects in a hierarchical data structure system, a parent structure invokes its child structure, which inherits the parent's attributes. 2. A process from which a child process is started.

parent/child

1. The relationship between processes in a multitasking environment in which the parent process calls the child process and most often suspends its own operation until the child process aborts or is completed. 2. The relationship between nodes in a tree data structure in which the parent is one step closer to the root (that is, one level higher) than the child.

See also child.

pinpoint customization

To provide custom logic for a targeted aspect of implementation.

See also scripted.

preference

A setting for an application or tool, typically set by users.

See also property.

primary server

Within each server cluster, there is one primary server and one or more secondary servers. All configuration changes take place through the cluster's primary server. Configuration data, event log files, and trace log files are dynamically replicated across all servers in the cluster, ensuring that all active servers have access to the latest data. Although you can access the console from another server in the cluster just as you do from the primary server, the console request is automatically redirected to the primary server. If the primary server ever goes off-line, the server with next highest priority in the cluster takes over primary server responsibilities.

product

A single, stand-alone application sold separately (such as EXTRA! X-treme) or a single, stand-alone set of closely related applications or a larger system of applications (EXTRA! Mainframe Server) that are sold and marketed together.

See also component.

property

1. A characteristic of an object. Depending on the object, the user might set its properties. 2. In Windows, a characteristic or parameter of an object or device. Properties of a file, for example, include type, size, and creation date and can be identified by accessing the file's property sheet.

See also attribute, preference.

protected field

A field in which a user cannot enter, modify, or erase data.

publishing

Windows Installer method of advertising a feature or application. Publishing does not populate the UI. However, if another application attempts to open a published application, there is enough information present for the installer to assign the published application.

See also, advertising.

QuickPad

An onscreen keypad that provides a convenient way to send commands to the host.

recipient

A user or group of users on the system.

relative field

A user field for which the size varies, depending on the data contained in the field.

See also user field.

remotable object

An object that can be controlled from a different computer than the computer to which it has been deployed.

resource adapter

A system-level software driver used by an application server or client to connect to an enterprise system. A resource adapter is typically specific to an enterprise system. It is available as a library and is used within the address space of the server or client using it.

A resource adapter plays a central role in the integration and connectivity between your enterprise system and an application server. It is the point of contact between application components, application servers, and enterprise information systems. The Attachmate J2EE Connector is a resource adapter.

See also application server.

resource adapter module

A package of information needed to deploy and run your task file from an application server.

See also application server, resource adapter.

runtime service

A program that handles the transmission of information between a data source and a deployed application.

scheme

A collection of configuration options.

For example, a color scheme might reflect certain colors for certain types of characters. A HotSpot scheme might include a specific combination of text and region HotSpots.

If you do not save a scheme as its own file, the configuration options become part of the session profile.

screen bindings

Associations between custom application forms and the data processed by your host application. For example, you could bind user input from a text field to specify where to send the data, or you could bind host output data to specify where to get the data to populate a control.

screen recognition rule

See recognition rule.

Screen Native Access

See Native Access.

scriptable

An element within the design-time task configuration for which the user can provide custom logic using script.

scripted

An element of the design-time task configuration that the user has overridden with script.

server

> 1. On a local area network (LAN), a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network. 2. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client.

> *See also* client.

service

> A program, routine, or process that performs a specific function.

> *See also* runtime service, Windows service.

service bean

> A Java bean that includes multiple tasks in a single bean. Service beans have a method for each task. Task inputs and outputs are arguments to the method. Service beans can be used to create applications in any Java application development environment.

> *See also* bean, task interface object, Web service.

session

> 1. A configured communication connection with a host. A session can be in either a connected or a disconnected state. 2. The GUI representation of a connection to a host through which users interact with a host. The GUI components can include representations of host screens and file lists, as well as various tools such as toolbars, QuickPads, Macro Recorders/Editors, and keyboard mappers. Sessions can also be specific to host screens, file transfer, or printing.

session file

> The file that contains the configuration information for a session.

session pool

> A group of host sessions that share a common configuration and NavMap.

session profile

> A file that contains all the configuration information associated with a session, including the INFOConnect path, terminal type, file transfer protocol, and other settings.

session template

> In EXTRA! X-treme, a session configuration on which you can base a new session.

standalone installation

> An installation mode in which the product files are installed in a location (usually a PC hard disk) that one or more users will access.

stateful task

A task that maintains context, keeping track of your configuration settings and what you were doing the last time you ran an application. A stateful task can start where a previous task ended.

Compare stateless task. *See also* context task.

stateless task

A task that does not maintain context information about previous actions.

Compare stateful task.

task

A sequence of transactions that perform a particular job. A task can be a simple data transfer, such as updating a database record, or it can be more complex, such as logging onto a host application, navigating to a particular screen, and sending and retrieving data. It could even be a combination of tasks that make up a business application. A task consists of one or more transactions.

transcoding

A process that reformats a single source of Web content to suit the needs of different display devices, such as both hand-held and desktop displays. Transcoding eliminates the need to rewrite content to meet the requirements of each device separately.

transform (.mst) file

A file that holds all customized changes made to the MSI's database, including additional file information. Existing .mst files can be overwritten, or the filename can be changed to retain an existing .mst file, thereby writing all changes to a new transform file.

transient step

One or more transitional screens sent by the host without the user sending an AID key to the host.

translation table

A file that modifies the data sent between the host and a client to ensure that the client can display characters that are not part of the U.S. English character set.

transport

The communication software that enables a PC to communicate with a host via a specific type of network. For example, the INFOConnect TCP/IP Transport enables communication via a TCP/IP network.

tree

A data structure containing zero or more nodes that are linked together in a hierarchical fashion. The topmost node is called the root. The root can have zero or more child nodes, connected by edges (links); the root is the parent node to its children. Each child node can in turn have zero or more children of its own. Nodes sharing the same parent are called siblings. Every node in a tree has exactly one parent node (except for the

root, which has none), and all nodes in the tree are descendants of the root node. These relationships ensure that there is always one — and only one — path from the root node to any other node in the tree.

unattended installation

An installation performed without user interaction, in which installation dialog boxes are suppressed. Also known as a silent installation.

unexpected screen

A screen that does not match a destination screen for the current step in a task. An unexpected screen may be recorded in the NavMap but occurs out of the order expected.

unformatted screen

A screen that does not contain fields defined by the host application.

unrecorded screen

A screen that has not been recorded as part of the current task.

upload

To transfer programs or data from your local computer to a central host or Web server.

user field

An area of the host screen that you define as a field. A user field does not alter the actual host screen.

URL (Universal Resource Locator)

An Internet site address that typically starts with a protocol name followed by the organization that maintains the site. The suffix identifies the kind of organization. For example, http://www.attachmate.com identifies the Web server at Attachmate Corporation. The http://www indicates that it is a Web server that uses the http protocol, and the .com suffix identifies Attachmate as a commercial site. Generally, commercial URLs end with .com, educational URLs end with .edu, military URLs end with .mil, and government URLs end with .gov.

If the URL points to a specific page, additional information, such as a port name, the directory in which the page is located, and the name of the page file, is included. Web pages authored using HTML (Hypertext Markup Language) often end with an .htm or .html extension.

viewer

An applet or control that loads within a Web browser to provide host access capability.

Web service

Software that dynamically interacts with other software using Internet protocols and formats such as HTML, XML, TCP/IP, and SOAP, and handles the transmission of information between a data source and a deployed application.

See also task interface object.

Web Services Description Language (WSDL)

The Web Services Description Language (WSDL) is an XML format published for describing Web services.

Windows Installer

Microsoft client-side installer service for managing the installation of applications. The application must be encapsulated in a package, consisting of an .msi file and optional external source files.

See also, package, .msi file.

Windows service

A program, routine, or process that typically begins running as soon as the computer starts. Windows services are started, stopped, and configured from Services in the Windows control panel.

XML Schema

A file that defines the structure, content, and semantics of XML documents. A single schema defines a class of XML documents. An individual XML document that conforms to a particular schema is called an instance document. The metadata files for Attachmate products are written using XML Schema format.

See also metadata.