

Administration Guide

ActivClient for Windows 6.2

ACTIVIDENTITY

Table of Contents

Chapter 1: Introduction 12
About ActivClient 12
ActivClient Deployment 13
Deployment and Policy Planning 13
Preparation 13
Deployment 13
Upgrading 14
ActivClient Management 14
Administrative Tools and Samples 14

Chapter 2: Policy Definition 16
ActivClient Customization Methods 16
Using the Advanced Configuration Manager 16
Using Microsoft Windows Registry Editor 18
Using Active Directory Group Policy Objects on Windows 2000 Server and Server 2003 18
Define the ActivClient User Group 19
Add the ActivClient Administrative Template 20
Configure the Policy Settings 21
Using Active Directory Group Policy Objects on Windows Server 2008 22
Configure the Policy Settings 23
ActivClient Policy Settings 25
Card Removal Behavior 26
PIN Management 27
Display New Card window on card insertion 28
Display Unlock Card window when a locked card is inserted 28
Prevent PIN entry shorter than the minimum PIN length 28
Prevent PIN entry longer than the maximum PIN length 29
Prevent change of PIN at first use cancellation 29
Allow PIN verification against the smart card regardless of the PIN length 30
Prevent users from reusing current PIN during PIN change 30
Allow alphabetic characters in PIN code 30
PIN Caching Service 31
Enable PIN caching 32
Always prompt for the PIN code before performing any private key signature operation 32
Always prompt for the PIN code before performing any private key decryption operation 33
Always prompt for the PIN code before performing any other operation 33
Number of minutes before PIN cache is cleared 33
Allow per-process PIN caching 34
Enable “Include” application list 34
Applications “included” in PIN caching 35

Enable “Exclude” application list . . . 36
Applications “excluded” from PIN caching . . . 36
Enable “OpenCard” application list . . . 37
Applications “optimized” for PIN caching . . . 37
Certificate Availability . . . 38
Make certificates available to Windows on card insertion . . . 38
Configure Windows EFS with smart card certificate . . . 39
Remove certificates from Windows on logoff . . . 39
Remove certificates from Windows on smart card removal . . . 40
Display certificate replacement warning . . . 40
Allow certificate enrollment on behalf of another user . . . 40
Outlook Enhancements . . . 41
Setup email certificates in Outlook on card insertion . . . 42
Check CRL for Outlook security profile creation and Publish to GAL . . . 42
Check CRL timeout for Outlook security profile creation and Publish to GAL . . . 43
Automatically publish certificates to the Global Address List . . . 43
Enable audit for Outlook security profile creation and Publish to GAL . . . 43
Encrypt contents and attachments for outgoing messages . . . 44
Add digital signature for outgoing messages . . . 44
Send clear text signed message when sending signed messages . . . 44
Auto-request return receipt for outgoing emails . . . 45
Automatically add sender’s certificate to Outlook contacts . . . 45
Outlook Auto-Contact destination folder . . . 45
Automatically decrypt encrypted emails . . . 46
Add Outlook Security icons in the compose email windows . . . 46
User Console . . . 46
Display Help . . . 48
Display Tree view in Explorer bar . . . 48
Display Tasks view in Explorer bar . . . 48
Allow users to switch between icon and detail views . . . 49
Image displayed on the lower right corner of List view . . . 49
Display user interface/toolbar customization . . . 49
Display reader selection list . . . 50
Display the Smart Card Info icon . . . 50
Display Unlock Card menu . . . 50
Display View Unlock Code menu . . . 51
Display Reset Card menu . . . 51
Display the Change PIN menu . . . 51
Display the New Card menu . . . 52
Display Check for Card Update menu . . . 52
Display My Certificates folder . . . 52
Display CA certificates folder . . . 53
Allow deletion of user certificates . . . 53
Display Import Certificate . . . 53

Automatically register certificates when imported onto the smart card . . . 54
Display Export certificate . . . 54
Display “Make certificates available to Windows” menu . . . 54
Display Publish certificates to GAL menu . . . 55
Allow One-Time Password generation . . . 55
Allow One-Time Password synchronization . . . 55
Display My Personal Info . . . 56
Display the Advanced Configuration Manager . . . 56
Display Advanced Diagnostics . . . 56
Display Troubleshooting . . . 57
ActivClient Agent (Notification Area Icon) . . . 57
Display the “Open” menu item . . . 58
Display the “PIN Initialization Tool” menu item . . . 58
Display the “PIN Change Tool” menu item . . . 58
Display the “Advanced Configuration Manager” menu item . . . 59
Display the “Advanced Diagnostics” menu item . . . 59
Display the “Exit” menu item . . . 59
Display the “Get One-Time Password” menu item . . . 60
Display the One-Time Password window . . . 60
One-Time Password window duration (in seconds) . . . 60
Copy One-Time Password to Clipboard . . . 61
Clipboard One-Time Password expiration (in seconds) . . . 61
Check Point Secure Authentication Agent API . . . 61
Check Point VPN-1 authentication mode . . . 62
Authentication server challenge password . . . 62
Authentication server challenge prompt . . . 62
Notifications Management . . . 63
Display Blocked Card Manager message . . . 63
Card Manager Blocked message . . . 64
Display No Smart Card Reader alert . . . 64
No smart card reader alert message . . . 64
No smart card reader alert duration (in seconds) . . . 65
Display unattended smart card alert . . . 65
Unattended smart card alert message . . . 66
Unattended smart card alert duration (in seconds) . . . 66
Card Auto-Update alert duration (in seconds) . . . 66
Display card expiration notification . . . 67
Display certificate expiration notification . . . 67
Default expiration warning message . . . 67
Default expiration warning period (in days) . . . 68
Default expiration notification period (in days) . . . 68
Expiration Warning Help file . . . 68
Default delay after card insertion for expiration check (in seconds) . . . 69
Logon Window . . . 69

Static Logon Banner—high resolution . . . 70
Moving Logon Banner—high resolution . . . 70
Software Auto-Update Service . . . 70
Software automatic update URL . . . 71
Download path for software updates . . . 71
Number of retries performed when an error occurs . . . 71
Number of minutes between retries . . . 71
Number of days before checking for an update . . . 72
Smart Card Auto-Update . . . 72
Enable Card Auto-Update . . . 73
Frequency of update (in days) . . . 73
Maximum delay for card update check after Windows Logon . . . 73
Maximum delay for card update check after card insertion . . . 74
CMS server URL . . . 74
CMS Synchronization Manager timeout (in seconds) . . . 74
CMS Synchronization Manager retry . . . 75
CMS MDIDC timeout (in seconds) . . . 75
Smart Card . . . 76
Prefer GSC-IS over PIV End Point . . . 76
Enable smart card discovery information caching . . . 76
Devices . . . 77
Authorized smart card readers . . . 77
Terminal Services . . . 78
Enable caching of the selected applet . . . 78
Performance Optimizations . . . 79
Disable certificate caching on card-insertion . . . 79
Disable card auto-registration on card-insertion . . . 79
Advanced Diagnostics . . . 80
Email address where the diagnostics report will be sent . . . 80
Display Email menu in Advanced Diagnostic . . . 80
Perform smart card diagnostics in Advanced Diagnostics . . . 81
Logging . . . 81
Activate the log files . . . 82
Full path to log file . . . 82
Maximum log file size (in MB) . . . 82
Maximum number of file backups . . . 83
Enable performance logging for Windows PKI Smart Card Logon . . . 83
Import/Export ActivClient Configurations . . . 83
Import a Configuration . . . 84
Export a Configuration . . . 85
Configurations for Remote Session Support . . . 85
Remote Sessions in a Citrix Environment . . . 86
Enabling Smart Card Services . . . 86

Configuring Session Disconnection on Smart Card Removal . . . 86
Necessary Adjustments in Microsoft and Citrix Environments . . . 86
EventService ActivClient Settings . . . 87

Chapter 3: Setup Customization . . . 89
Setup Customization Methods . . . 89
Using a Command Line . . . 89
Basic Install Command Line . . . 90
Hide Features . . . 90
Force Features to Display . . . 90
Using Orca . . . 91
Using InstallShield Admin Studio (or Wize Package Studio) . . . 92
ActivClient Setup Customization Options . . . 93
Customize the Feature Installation . . . 93
Customize the Installation Path . . . 94
Customize the Setup Behavior . . . 95
Customize the Setup Restart Behavior . . . 95
Run a Blind Setup . . . 96
Avoid Conflict with Other MSI Products . . . 97
Install Root Certificates Automatically . . . 97
Device Installer Customization Options . . . 98
Customize the Feature Installation . . . 98
Customize the Installation Path . . . 99

Chapter 4: Setup Deployment . . . 100
Deploying Using Standard Methods . . . 100
Deploying Using Active Directory Push . . . 100
Create a Distribution Point . . . 101
Assign a Package . . . 101
Test a Package . . . 102
Redeploy a Package . . . 103
Deploying Using Systems Management Server . . . 103
Configure Client Computers . . . 104
Configure the Server . . . 108
Enable Software Distribution . . . 108
Prepare Collections . . . 109
Create a Package . . . 110
Create a Program . . . 114
Create a Distributed Advertisement . . . 116
About advertisements . . . 117
Advertise the Program to the Targeted Collection . . . 117
Monitor Software Distribution . . . 118

Run an Advertised Program on a Client . . . 118
Deploying using Microsoft System Center Configuration Manager . . . 123

Chapter 5: Upgrading and Updating . . . 124
Upgrading ActivClient . . . 124
Supported ActivClient Upgrades . . . 124
Upgrading Methods . . . 125
Using ActivClient Auto-Update . . . 125
ActivClient Auto-Update Overview . . . 125
Enable ActivClient Auto-Update . . . 127
Configure ActivClient Auto-Update for MSI Updates . . . 127
Configure ActivClient Auto-Update for MSP Updates . . . 128

Chapter 6: Uninstallation . . . 130
ActivClient Uninstallation Methods . . . 130
Managing Remaining Components . . . 130
Components Left Behind by Design . . . 131
Files Left Behind by Design . . . 131
Registries Left Behind by Design . . . 132
Other Components Left Behind by Design . . . 133
Components Left Behind Unexpectedly . . . 134
Files Left Behind Unexpectedly . . . 134
Registries Left Behind Unexpectedly . . . 136
Other Components Left Behind Unexpectedly . . . 138
Components Managed by Windows . . . 138
Files Managed by Windows and Left Behind . . . 138
Registries Managed by Windows and Left Behind . . . 139

Chapter 7: Outlook Usability Enhancements . . . 140
Environment . . . 140
Overview . . . 141
Microsoft Outlook Email Clients . . . 141
Microsoft Exchange Server . . . 142
Emails From and To Any Email Client on Any Platform . . . 142
Outlook Security Profile Configuration . . . 142
Outlook Security Profile Settings . . . 143
Outlook Security Profile Update . . . 145
Profile Selection and Conditions for Security Profile Update . . . 145
Security Profile Updated Values . . . 147
Publish Certificate to GAL . . . 150
Profile Selection and Email Account . . . 150
Configuration . . . 150

Workflow . . . 150
Environment Considerations . . . 151
Interactive Process . . . 151
Audit . . . 152
Auto-Contact . . . 154
Auto-Decrypt . . . 156

Chapter 8: PIN Caching Service . . . 157
Overview . . . 157
PIN Caching Policy - Detailed Description . . . 158
Enabling or Disabling PIN Caching . . . 158
Per Session or Per Process PIN Caching . . . 159
Example 1: Per Process Mode . . . 160
Example 2: Per Session Mode . . . 160
Example 3: Per Session Mode . . . 161
PIN Cache Timeout . . . 161
Example: PIN Cache Timeout of One Hour . . . 162
Force PIN Re-authentication . . . 163
Example: Force PIN Re-authentication in Outlook . . . 164
Application Lists . . . 165
Exclude List . . . 165
Example: Outlook an "Excluded" (Un-trusted) Application . . . 167
Include List . . . 167
Example: Outlook an "Included" (Trusted) Application . . . 169
OpenCard List . . . 169
Example: Winlogon is in the OpenCard List . . . 171

Chapter 9: Auto-Update with ActivID CMS . . . 173
Overview . . . 173
Configuration . . . 174
Card Auto-Update Policies . . . 174
Client Card Auto-Update Configuration . . . 174
CMS Connection Configuration . . . 178
Card Auto-Update Experience . . . 180

Chapter 10: Troubleshooting . . . 181
ActivClient Troubleshooting Tools . . . 181
ActivClient Troubleshooting Tool . . . 181
ActivClient Diagnostics Wizard . . . 181
Advanced Customer Support Logging . . . 182
Troubleshooting Strategies . . . 182
Check Common Issues and Known Problems . . . 182

Analyze Symptoms and Factors . . . 182
Isolate the Error Condition and Reproduce the Error . . . 183
Ask for Technical Support Resources . . . 183

Chapter 11: Customizing the Help File . . . 184
Modify the Existing ActivClient Help . . . 184
Extract the HTML Files . . . 184
Decompile with HTML Help Workshop . . . 185
Decompile from the Command Line . . . 186
Create a New Help Project . . . 187
Configure the Context-Sensitive Controls . . . 187
Add the Header File . . . 193
Configure the Alias Links . . . 194
Integrate Customized Help . . . 194

Appendix A: Packages . . . 195
ActivClient Packages . . . 195
DoD Root Certificates . . . 195

Appendix B: ActivClient Files and Processes . . . 197
Installed Files . . . 197
Core ActivClient Components . . . 209
File Update After Installation . . . 210

Appendix C: Registry Keys . . . 211
Registry Keys Installed by ActivClient 6.2 (32-bit Edition) . . . 211
Registry Keys Installed by ActivClient 6.2 (64-bit Edition) . . . 231
64-bit Registry . . . 231
32-bit Registry . . . 267
Registry Keys Updated After Installation . . . 271

Appendix D: Terms and Acronyms . . . 272
Terms . . . 272
Acronyms . . . 273

List of Tables

Table 2.1: ActivClient Customization Methods 16
Table 3.1: ActivClient Setup Filenames and Editions 89
Table 3.2: Customizable Features and Public Properties 93
Table 3.3: Features Description of the Device Installer Setup 98
Table 7.1: Security Profile Configured Values 147
Table 7.2: Audited Event ID Codes 153
Table 11.1: Context-sensitive identifiers and files 188
Table 11.2: Context-sensitive help call actions 189
Table B.1: ActivClient 6.2 32-bit edition 197
Table B.2: ActivClient 6.2 64-bit edition 203
Table B.3: ActivClient Processes 210

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

List of Figures

Figure 2.1: View of the Advanced Configuration Manager 17
Figure 2.2: Registry Editor Window 18
Figure 5.1: Updating ActivClient 126

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Chapter 1: Introduction

In This Chapter

12 About ActivClient
13 ActivClient Deployment
14 ActivClient Management

This guide explains how to customize, deploy and manage ActivClient™ according to your organization's specific requirements.

ActivIdentity uses industry standards whenever possible so that you can use off-the-shelf products.

ActivClient customization can be performed before deploying the software in order to create a "corporate image". You can also customize ActivClient after it has been deployed, as you update your corporate policies, or as you deploy additional capabilities onto your smart cards and smart card middleware.

This guide applies to all editions of ActivClient:

- ActivClient 32-bit
- ActivClient 64-bit
- ActivClient CAC 32-bit
- ActivClient CAC 64-bit

The differences related to specific editions are indicated where applicable.

Note: ActivClient CAC is an ActivClient edition configured for the US Department of Defense Common Access Card (CAC) deployment.

About ActivClient

ActivClient is the latest smart card and USB token middleware from ActivIdentity that allows enterprise and government customers to easily use smart cards and USB tokens for a wide variety of desktop, network security and productivity applications.

ActivClient enables the use of PKI certificates and keys, one-time password and static password credentials on a smart card or USB token to secure:

- Desktop applications
- Network logon
- Remote access
- Web logon
- E-mail
- Electronic transactions

This document is for:

- System administrators
- System integrators
- People with a good understanding of Microsoft® Windows® registries (for ActivClient product customization) and Windows installer (for ActivClient setup customization)

ActivClient Deployment

The following sections outline the main stages of the deployment process and the decisions to be taken.

Deployment and Policy Planning

- Select ActivClient features to be installed. This defines the functionality available to the end user.

  For further information, see the *ActivClient for Windows Installation Guide.*

- Define the policies to specify ActivClient behavior. The final result should be a combination of security and usability.

  For further information, see Chapter 2, "Policy Definition," on page 16.

Note

ActivIdentity recommends that you test the policy settings with a limited population of users first.

For details on specific ActivClient capabilities and the associated policies, see the following chapters:

- Chapter 7, "Outlook Usability Enhancements," on page 140
- Chapter 8, "PIN Caching Service," on page 157
- Chapter 9, "Auto-Update with ActivID CMS," on page 173

Preparation

- Customize the setup to meet your organization's needs in terms of features and policies.

  For further information, see Chapter 3, "Setup Customization," on page 89.

- Customize the ActivClient Help filed to meet your organization's internal procedures and requirements.

  For further information, see Chapter 11, "Customizing the Help File," on page 184.

Deployment

- Select the deployment method - remote or local - so that either users can perform an interactive setup, or you can automate software installation and configuration using corporate software management technology.

- Deploy the policies.

For further information, see Chapter 4, "Setup Deployment," on page 100.

Upgrading

- Select the upgrade method according to the original installation/deployment method.

  You can also use the ActivClient Auto-Update tool to publish and install the software updates.

For further information, see Chapter 5, "Upgrading and Updating," on page 124.

ActivClient Management

Once ActivClient is successfully deployed and users are using their smart cards for authentication, digital signature or encryption services, the main administrative tasks are to:

- Modify and re-deploy the policies according to organizational needs.
- Monitor ActivClient using the auditing functions (applicable only to specific ActivClient services).
- Troubleshoot any issues (see Chapter 10, "Troubleshooting," on page 181).

Administrative Tools and Samples

The \Admin folder of the ActivClient distribution contains the following utilities and samples, created to facilitate your ActivClient deployment:

- Unsigned setups - unsigned versions of the ActivClient MSI and ActivIdentity Device Installer MSI to use if you want to customize the setup. For further information, see Chapter 3, "Setup Customization," on page 89.
- Configuration - Active Directory administrative template for ActivClient (in ADM and ADMX formats) to use if you want to deploy ActivClient policies in an Active Directory environment. For further information, see Chapter 2, "Policy Definition," on page 16.
- Auto Update - utility to configure ActivClient to download software updates automatically using HTTPS. For further information, see "Using ActivClient Auto-Update" on page 125.
- Update Sample - ActivClient sample hot fix to validate that the ActivClient Auto Update feature is configured as correctly in your environment. For further information, see "Using ActivClient Auto-Update" on page 125.
- Custom Help - header for ActivClient Help, to allow customizing the ActivClient Help and include customer-specific information, such as specific unlock procedures and help desk contact information. For further information, see Chapter 11, "Customizing the Help File," on page 184.

- ActivCard Gold password export utility - tool designed to help customers upgrade from ActivCard Gold to ActivClient 6.2 by accessing passwords that they might have stored on their smart card. For further information, see the `readme.txt` in the folder.

Chapter 2: Policy Definition

This chapter explains how to customize ActivClient. It describes the possible customization methods and details the ActivClient settings. It also explains how to import/export configuration files and configure remote session support.

In This Chapter

16 ActivClient Customization Methods
25 ActivClient Policy Settings
83 Import/Export ActivClient Configurations
85 Configurations for Remote Session Support

ActivClient Customization Methods

Table 2.1 provides an overview of the possible customization methods.

Table 2.1: ActivClient Customization Methods

Product	Description
ActivClient Advanced Configuration Manager, described in "Using the Advanced Configuration Manager" on page 16	Provides a user interface to view and modify the ActivClient registry settings. This tool is accessible from the **Start** menu or from **ActivClient Agent** right-click menu.
Windows Registry Editors (regedit.exe), described in "Using Microsoft Windows Registry Editor" on page 18	Used to view and edit local and remote registries. You also can use the editors to remotely import `.reg` files with the appropriate settings to several computers.
Windows Group Policy, described in: • "Using Active Directory Group Policy Objects on Windows 2000 Server and Server 2003" on page 18 • "Using Active Directory Group Policy Objects on Windows Server 2008" on page 22	Allows you to remotely set the configuration on a group of computers or users.
Enterprise Management product	Use to manage registry settings in a large enterprise (for example, Microsoft SMS or Microsoft System Center Configuration Manager). See the user documentation for your enterprise management product for more information.

Using the Advanced Configuration Manager

Users with administrator privileges can use the Advanced Configuration Manager to configure specific ActivClient policies and standard GSC smart card policies.

The settings that you can modify using the Advanced Configuration Manager are described in "ActivClient Policy Settings" on page 25. Some of these policies are defined and standardized by the United States Government in the *Government Smart Card—Interoperability Specifications*, GSC-IS. For details on this specification, go to http://smartcard.nist.gov/.

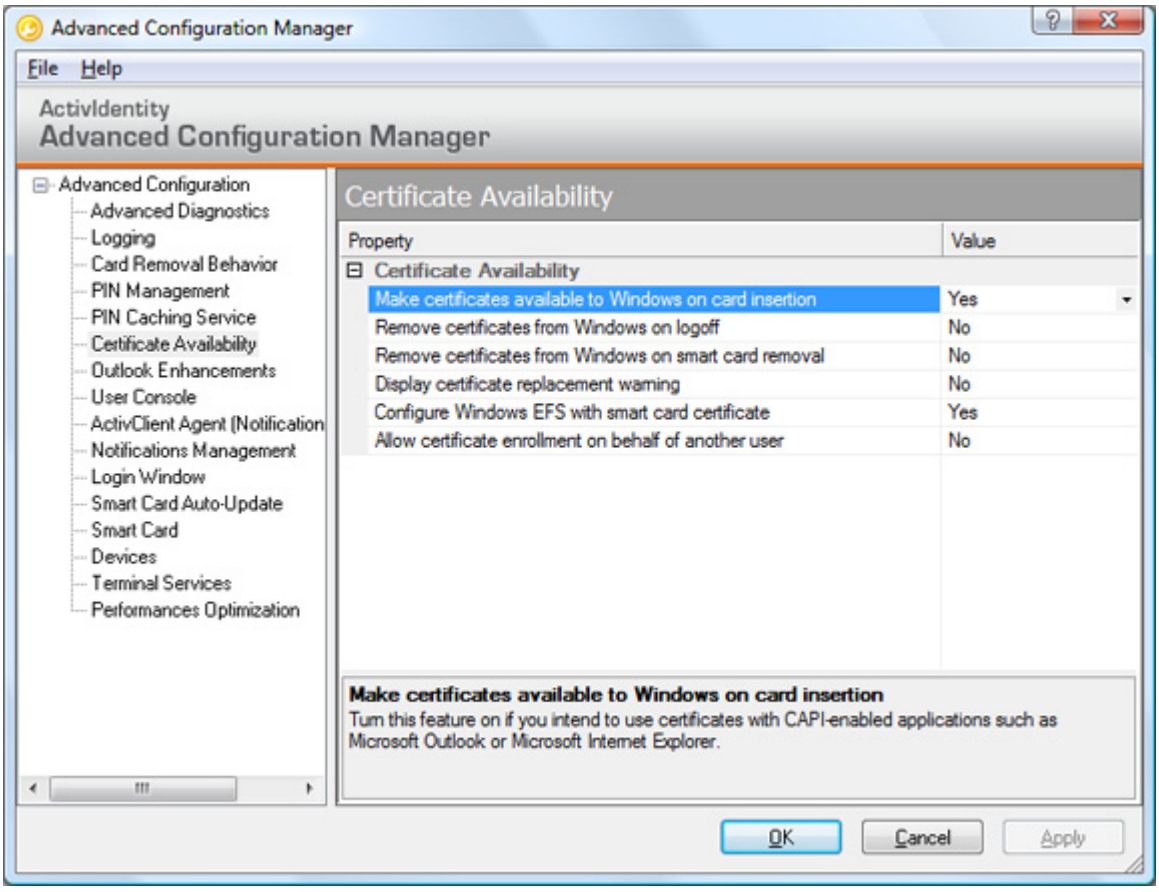
Note

To ensure your changes are taken into account, click Apply before navigating to other configuration categories.

1. To access the **Advanced Configuration Manager, either**:

   – From ActivClient Agent's left or right-click menu, select **Advanced Configuration Manager**.
   – From the ActivClient User Console **Tools** menu, select Advanced, **Configuration**.
   – From the Start menu, go to Programs, ActivIdentity and select **Advanced Configuration Manager**.

Figure 2.1: View of the Advanced Configuration Manager



2. To modify a setting, select the corresponding Value and either enter the value manually or select an option from the drop-down list.

For information on the settings and their values, read the description displayed at the bottom of the window each time you select an option.

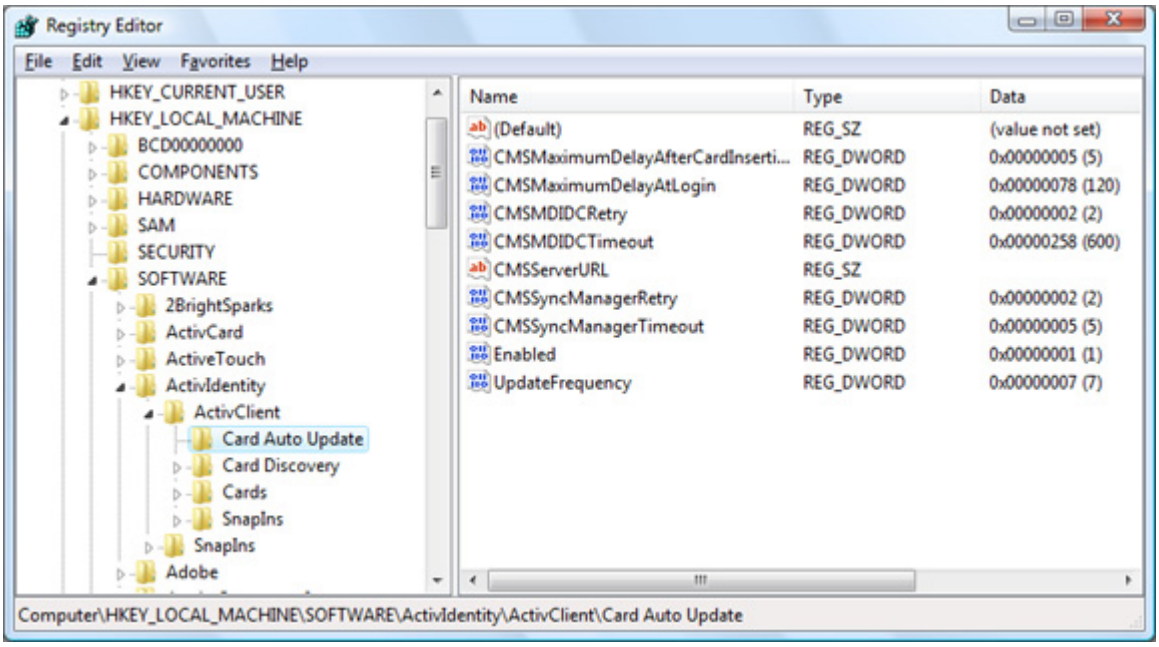
Using Microsoft Windows Registry Editor

In order to store configuration data, ActivClient uses the Windows registry. Administrators can modify the registry settings of a user's machine either locally or remotely by using tools such as Windows Registry Editor to edit key values.

If you intend to customize ActivClient for a large-scale rollout program, prepare the rollout by customizing and testing the product customization for your specific environment. The customization must meet the needs of your user population.

By default, ActivClient creates its configuration with an ACL that allows every user to read those registry keys. Only members of the administrator group can modify the registry keys.

Figure 2.2: Registry Editor Window



Using Active Directory Group Policy Objects on Windows 2000 Server and Server 2003

The Active Directory Group Policy allows you to remotely set the configuration for a group of computers or users. The ActivClient Administrative Template file is delivered in the setup package and you can define the values with the Active Directory Group Policy Editor. You can then push the values to all ActivClient users in the domain.

The ActivClient Administrative Template for Windows 2000 Server and Windows Server 2003 is available in the ADM format.

For Windows Server 2008, it is also available in the ADMX format (see "Using Active Directory Group Policy Objects on Windows Server 2008" on page 22).

The policy deployed using the GPO overwrites the values configured locally.

The policy must be deployed after ActivClient has been installed on all the required machines. If the policy is deployed before installation, the setup will overwrite the customized settings, replacing them with the default settings. You can also customize the setup to install the modified policy settings at installation. For further information, see Chapter 3, "Setup Customization," on page 89.

Setting an Active Directory Group Policy Object (GPO) with default permissions causes the application to deploy for every user or computer within the domain.

To deploy ActivClient policies you must first load ActivClient policies as a new Administrative Template. Then you need to ensure that only specified users receive the application.

Define the ActivClient User Group

1. Either:
   - Start the Microsoft Management Console (MMC) by entering `mmc` in the **Run** window, then select **Active Directory Users and Computers** snap-in.
   - From the Start menu, go to **Programs, Administrative Tools,** and select **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and select **Properties**.
3. Click on the **Group Policy** tab, then click **New**.
4. Enter the name that you want to call this policy (for example, ActivClient 6.2 or ActivClient CAC 6.2), and press **Enter.**
5. Click **Properties** and in the **Security** tab:
   a. From the **Name** list, select the security groups to which you do not want to apply this policy, and then clear the **Allow** option for **Apply Group Policy**.
   b. From the **Name** list, select the security groups to which you want to apply this policy, select the **Allow** option for **Apply Group Policy**, and click **OK.**

   Once the group policy object has been created, you must configure Active Directory to load the ActivClient default template (`ActivClient.adm`) so that the ActivClient settings can be propagated to the newly created group policy object.

Notes

- You must have domain administration access rights to deploy the Group Policy.
- The ActivClient Administrative template defines only ActivClient policies. It does not provided configuration values.
- You can define custom configuration values with the Active Directory Group Policy Editor. The Active Directory Group Policy Editor is an administrative tool of the Windows 2000, 2003 and 2008 servers.

Add the ActivClient Administrative Template

1. Locate the `ActivClient.adm` template file in the **\Admin\Configuration** folder on your ActivClient distribution and make it accessible from the workstation on which you will run the Active Directory management tool. For example, copy this file into `C:\Windows\inf`.

2. From the **Start menu, go to Programs, Administrative Tools, and then select Active Directory Users and Computers**.

3. In the console tree, right-click the domain or Organizational Unit that you want to configure, then select **Properties**.

4. Click the **Group Policy** tab. Drag the pointer to select the group policy setting that you want to edit, then click **Edit**.

5. In the console tree, click the plus sign (**+**) next to **Computer Configuration** in order to expand the list.

6. Right-click **Administrative Templates**, then click **Add/Remove Templates**.

7. Click the **Add** icon, then drag the pointer to select the ActivClient template and click **Open**.

8. Click **Close**.

When you add the ActivClient template file to the group policy, by default only the settings contained in genuine group policy trees are visible in the console. You must change the default user preferences. To do so:

1. From the Group Policy Object Editor's administrative templates, right-click the ActivClient node.

2. From the **View** menu, select filtering.

   – If you are using Windows Server 2003, clear the **Only show policy settings that can be fully managed** option.
   – If you are using Windows 2000 Server, clear the **Show Policies Only** and **Show Configured Policies Only** option.

For more details, go to http://download.microsoft.com/download/0/0/4/0044470e-5f3a-4569-9255-91f932e4da3b/gpintro.doc.

Once the ActivClient Administrative Template is loaded, you can use the Active Directory Group Policy Editor interface to configure specific settings with custom values.

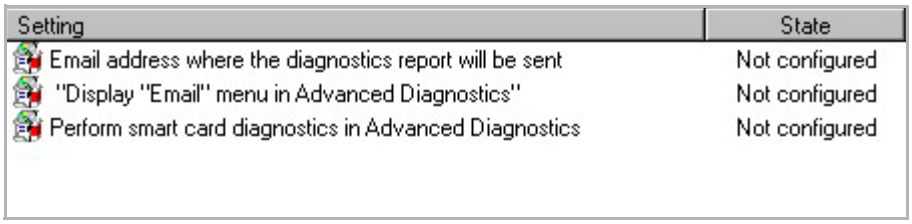
Note

Only configured policies will be propagated. Other policies will keep their current configuration as set at ActivClient installation.

Configure the Policy Settings

1. In the Group Policy Editor, navigate to **Administrative Templates** and select the ActivClient template added in the previous procedure.

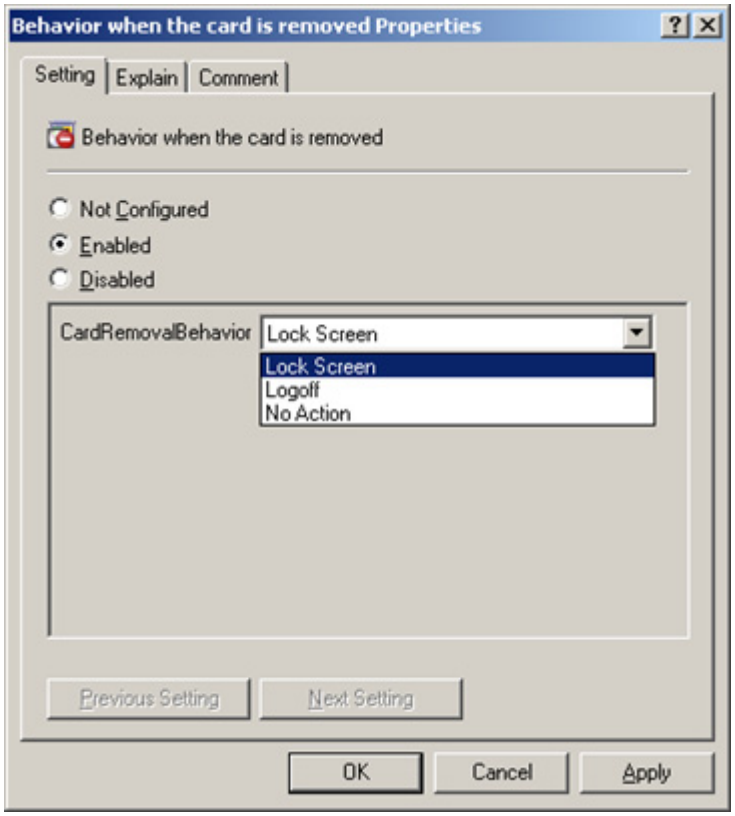
   The Setting and State table is displayed with the Standard tab selected.



2. Either:

   – In the Standard tab, right-click on the required property or setting and click **Properties**.
   – In the Extended tab, select the required property or setting and click **Properties**.

   The setting Properties page is displayed.



3. Configure the settings as detailed in "ActivClient Policy Settings" on page 25.

4. For each setting, you can also set the status with the following options:

Status	Description
Not Configured	When the status is Not Configured and you click Apply, the setting is disabled and any previous values are cleared from the system registry. New values are required when the setting is Enabled.
Enabled	When the status is Enabled and you click Apply, the values you enter are stored in the system registry. If the default value is used, the registry is empty.
Disabled	When the status is Disabled and you click Apply, the setting is disabled. Any values remain in the system registry and are used when the setting is Enabled.

Using Active Directory Group Policy Objects on Windows Server 2008

The Active Directory Group Policy allows you to remotely set the configuration for a group of computers or users. The ActivClient Administrative Template file is delivered in the setup package and you can define the values with the Active Directory Group Policy Editor. You can then push the values to all ActivClient users in the domain.

The ActivClient Administrative Template for Windows Server 2008 is available in the ADMX format.

For Windows 2000 Server and Windows Server 2003, it is also available in the ADM format (see "Using Active Directory Group Policy Objects on Windows 2000 Server and Server 2003" on page 18).

The policy deployed using the GPO overwrites the values configured locally.

The policy must be deployed after ActivClient has been installed on all the required machines. If the policy is deployed before installation, the setup will overwrite the customized settings, replacing them with the default settings. You can also customize the setup to install the modified policy settings at installation. For further information, see Chapter 3, "Setup Customization," on page 89.

Setting an Active Directory Group Policy Object (GPO) with default permissions causes the application to deploy for every user or computer within the domain.

Notes

- You must have domain administration access rights to deploy the Group Policy.
- The ActivClient Administrative template defines only ActivClient policies. It does not provided configuration values.
- You can define custom configuration values with the Active Directory Group Policy Editor. The Active Directory Group Policy Editor is an administrative tool of the Windows 2000, 2003 and 2008 servers.

To deploy ActivClient policies you must first load ActivClient policies as a new Administrative Template. Then you need to ensure that only specified users receive the application.

Add the ActivClient administrative template and create the group policy

1. Locate the `ActivClient.admx` template file in the **\Admin\Configuration** folder on your ActivClient distribution and copy it to `C:\Windows\PolicyDefinitions`.

2. Locate the `ActivClient.adml` template file in the **\Admin\Configuration\EN-US** folder on your ActivClient distribution and copy it to `C:\Windows\PolicyDefinitions\en-US`.

3. From the **Start menu, go to Programs, Administrative Tools, and then select Group Policy Management**.

4. In the console tree, right-click the domain or Organizational Unit that you want to configure, then select **Create a GPO in this domain...**.

5. Create a Group Policy Object (GPO) called, for example, ActivClient, and click **OK**.

Configure the Policy Settings

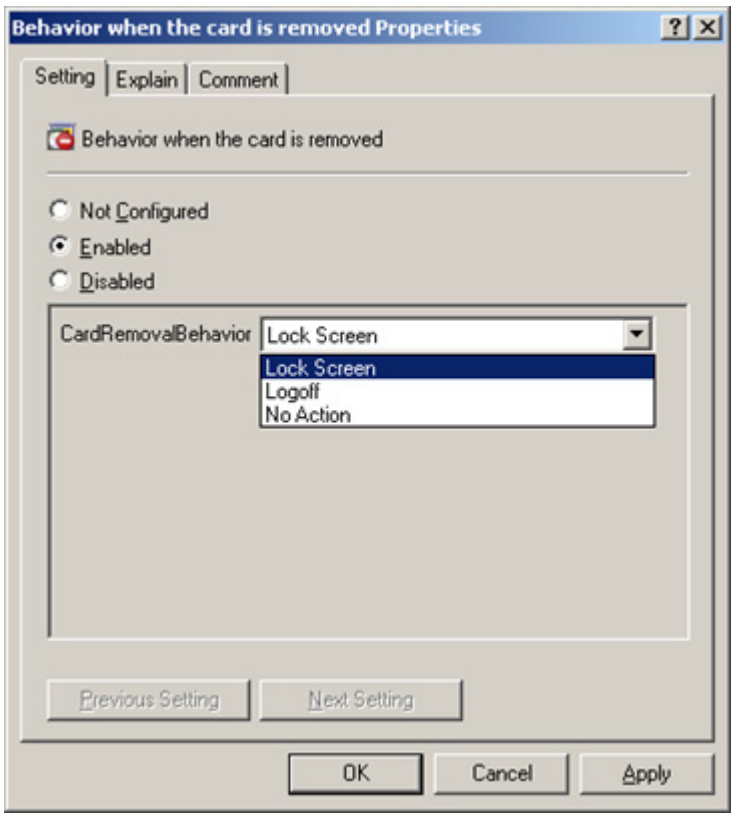
1. To modify the policy settings, right-click on the group policy you just created and select **Edit**.

   The Group Policy Management Editor opens.

2. In the console tree, go to **Computer Configuration**, **Policies**, **Administrative Templates: Policy definitions**.

3. Expand the directory for the **ActivClient** policy to display the available settings.

4. Double-click on a policy setting (for example, Behavior when the card is removed) to display the properties.



5. Configure the settings as detailed in "ActivClient Policy Settings" on page 25.

6. For each setting, you can also set the status with the following options:

Status	Description
Not Configured	When the status is Not Configured and you click Apply, the setting is disabled and any previous values are cleared from the system registry. New values are required when the setting is Enabled.
Enabled	When the status is Enabled and you click Apply, the values you enter are stored in the system registry. If the default value is used, the registry is empty.
Disabled	When the status is Disabled and you click Apply, the setting is disabled. Any values remain in the system registry and are used when the setting is Enabled.

7. To apply the policy to specific users or group of users, return to the Group Policy Management console and select your group policy.

8. In the **Security Filtering** section, add the users and/or groups to which you want to apply this policy.

ActivClient Policy Settings

You can customize the behavior of ActivClient by updating the settings described in this section. Some settings are supported only if you are using ActivClient 32-bit edition.

For details on how to modify these settings at the time of installation, see Chapter 3, "Setup Customization," on page 89.

For details on how to propagate these settings, see "ActivClient Customization Methods" on page 16.

The ActivClient policy settings are divided into the following categories:

Policy category	Action for changes to be applied
"Card Removal Behavior" on page 26	Reboot the workstation
"PIN Management" on page 27	Reboot the workstation
"PIN Caching Service" on page 31	Reboot the workstation
"Certificate Availability" on page 38	Reboot the workstation
"Outlook Enhancements" on page 41	Restart Outlook
"User Console" on page 46	Restart User Console
"ActivClient Agent (Notification Area Icon)" on page 57	Restart ActivClient Agent
"Check Point Secure Authentication Agent API" on page 61	Reboot the workstation
"Notifications Management" on page 63	Reboot the workstation
"Logon Window" on page 69	Reboot the workstation
"Software Auto-Update Service" on page 70	Reboot the workstation
"Smart Card Auto-Update" on page 72	Reboot the workstation
"Smart Card" on page 76	Reboot the workstation
"Devices" on page 77	Reboot the workstation
"Terminal Services" on page 78	Reboot the workstation
"Performance Optimizations" on page 79	Reboot the workstation

Policy category	Action for changes to be applied
"Advanced Diagnostics" on page 80	Restart the Advanced Diagnostics Tool
"Logging" on page 81	Reboot the workstation

The following sections detail the settings in each category and state what action you must take for a policy change to be taken into account.

Card Removal Behavior

Reboot the workstation

For the Card Removal Behavior policy changes to be applied, you must reboot the workstation.

You can specify the behavior of the workstation when the smart card is removed from the reader. For example, you can specify to lock the workstation screen or log off from Windows.

This setting only applies if the smart card was used to log on to Windows, either with a digital certificate or with a static password when using the ActivIdentity Authentication Client Smart Card Password Login feature.

Description	Defines what happens when the user removes the smart card that was used to log on to Windows. You can configure ActivClient to lock the workstation (default behavior), to log off the user, or not perform any action.
Values	Lock screen: 2 (default) No action: 0 Log off: 1
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\CardRemovalBehavior`
Type	DWORD

ActivIdentity recommends setting the ActivClient “card removal behavior” configuration (by default, enabled and set to “lock screen”) instead of the equivalent Windows configuration option.

The ActivClient feature is especially useful on workstations where several smart cards might be inserted (for example, at a smart card issuance station), in order to guarantee that only the removal of the card used to log on to Windows will trigger the session lock.

To disable the Windows feature:

- On operating systems prior to Windows Vista, use the Microsoft Group Policy MMC snap-in:
  a. Select **Computer Configuration, Windows Settings, Security Settings, Local Policies and then Security Options**.
  b. Set **Smart Card Removal Behavior** to **No action**.
- On operating systems starting with Windows Vista, stop the **Smart Card Removal Policy** service.

The exception to this rule is when ActivClient is installed on a server with Terminal Service or Citrix Presentation Server. In these cases:

- Disable the ActivClient setting.
- Enable the Windows setting and set it to **Lock workstation**.

PIN Management

The following sections detail the PIN Management policy settings to manage the ActivClient PIN options:

- "Display New Card window on card insertion" on page 28
- "Display Unlock Card window when a locked card is inserted" on page 28
- "Prevent PIN entry shorter than the minimum PIN length" on page 28
- "Prevent PIN entry longer than the maximum PIN length" on page 29
- "Prevent change of PIN at first use cancellation" on page 29
- "Allow PIN verification against the smart card regardless of the PIN length" on page 30
- "Prevent users from reusing current PIN during PIN change" on page 30
- "Allow alphabetic characters in PIN code" on page 30

Reboot the workstation

For the PIN Management policy changes to be applied, you must reboot the workstation.

Display New Card window on card insertion

Description	When enabled, users are asked to initialize their smart card as soon as the non-initialized smart card is inserted into the reader. It is advised to disable this setting for deployments with ActivIdentity 4TRESS or ActivID CMS servers, as these products manage the PIN instead of ActivClient.
Values	No = 1 (default) Yes = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\DisableInitCard`
Type	DWORD

Note

Only available if the PIN Initialization Tool is installed.

Display Unlock Card window when a locked card is inserted

Description	If the user inserts a locked smart card, the Unlock Card window is displayed automatically. Disable this feature if it does not match your deployment scenarios (for example, if you do not provide a card unlock service via the telephone).
Values	Yes = 0 (default) No = 1
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\DisableUnlockDlgOnLockedCardInserted`
Type	DWORD

Prevent PIN entry shorter than the minimum PIN length

Description	Defines if ActivClient allows users to perform PIN verification with a PIN that is shorter than the minimal PIN length. **Yes** (default): Prevents entry of PIN code shorter than the minimum PIN length. **No**: Does not prevent entry of PIN code shorter than the minimum PIN length even in the PIN verification dialogs.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\EnableSmallPINEntryPrevention`
Type	DWORD

Prevent PIN entry longer than the maximum PIN length

Description	Defines if ActivClient allows users to perform PIN verification with a PIN that is longer than the maximum PIN length. **No** (default): Does not prevent entry of PIN code longer than the maximum PIN length. **Yes**: Prevents entry of PIN code longer than the maximum PIN length even in the PIN verification dialogs.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\EnableLargePINEntryPrevention`
Type	DWORD

Prevent change of PIN at first use cancellation

Description	Prevents users from canceling the Change PIN process when using their smart card for the first time. **No** (default): Does not prevent end users from cancelling Change PIN dialog that may display at smart card first use. **Yes**: Prevents end users from cancelling Change PIN dialog that may display at smart card first use.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\DisableCancelChangePINatFirstUse`
Type	DWORD

Note

If users cancel the Change PIN prompt, they will see the prompt again at each logon until the PIN change is performed.

Allow PIN verification against the smart card regardless of the PIN length

Description	Defines if, during PIN authentication, ActivClient verifies the entered PIN against the smart card PIN without checking compliance with the PIN length policy first.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\DisablePINPolicyVerificationBeforePINCheck`
Type	DWORD

Prevent users from reusing current PIN during PIN change

Description	Defines if ActivClient allows users to reuse the current PIN as the new PIN during a PIN Change operation.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\EnableSamePINPrevention`
Type	DWORD

Allow alphabetic characters in PIN code

Description	Allows users to enter alphabetic characters in their PIN code.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\AlphaPINAllowed`
Type	DWORD

PIN Caching Service

ActivClient provides advanced Card Authentication Management, which defines how you can use PIN-protected services on the card, such as the RSA private keys.

This involves the use of a PIN Caching Service, that is flexible and that you can configure with a variety of settings, ranging from very easy-to-use to more complex secure settings.

For a full description of the ActivClient PIN Caching Service, see Chapter 8, "PIN Caching Service," on page 157.

The following sections detail the PIN Caching Service policy settings:

- "Enable PIN caching" on page 32
- "Always prompt for the PIN code before performing any private key signature operation" on page 32
- "Always prompt for the PIN code before performing any private key decryption operation" on page 33
- "Always prompt for the PIN code before performing any other operation" on page 33
- "Number of minutes before PIN cache is cleared" on page 33
- "Allow per-process PIN caching" on page 34
- "Enable “Include” application list" on page 34
- "Applications “included” in PIN caching" on page 35
- "Enable “Exclude” application list" on page 36
- "Applications “excluded” from PIN caching" on page 36
- "Enable “OpenCard” application list" on page 37
- "Applications “optimized” for PIN caching" on page 37

Reboot the workstation

For the PIN Caching Service policy changes to be applied, you must reboot the workstation.

Enable PIN caching

ActivIdentity recommends enabling the PIN caching (the default behavior). ActivClient PIN caching is required for most supported configurations. Disable PIN caching only when recommended to do so by ActivIdentity customer support.

Note

All the other PIN Caching Service policies are only available when ActivClient PIN caching is enabled.

Description	Avoids PIN re-authentication requests for every operation by allowing PIN caching. When disabled, PIN caching is handled at the smart card level, PIN re-authentication is needed whenever the smart card requires it.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Allow`
Type	DWORD

Always prompt for the PIN code before performing any private key signature operation

Description	Forces PIN authentication for any private key signature operation.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Sign`
Type	DWORD

Always prompt for the PIN code before performing any private key decryption operation

Description	Forces PIN authentication for any private key decryption operation.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Decrypt`
Type	DWORD

Always prompt for the PIN code before performing any other operation

Description	Forces PIN authentication for any PIN protected operation except for private key signature and private key decryption operations.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Other`
Type	DWORD

Note

ActivIdentity recommends keeping the default setting (Other = 1). If you enable this option (Other = 0), the user experience might not be acceptable, as some functional operations (1 user click) cause several card-level operations (several read commands), which would cause repeated PIN prompts to display.

Number of minutes before PIN cache is cleared

Description	Defines the number of minutes before PIN cache is cleared.
Values	15 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Minutes`
Type	DWORD

Allow per-process PIN caching

Description	Allows users to avoid sharing the PIN cache between Windows processes. When the default (No) setting is applied, all Windows processes running in the same Windows session share the same PIN cache.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\AllowPerProcess`
Type	DWORD

Enable “Include” application list

Description	Grants permanent access to the PIN cache to applications listed in the "Include" list. Select Yes if you want to include applications in PIN caching and follow the steps indicated in the next table.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Include`
Type	DWORD

Applications “included” in PIN caching

Description	Lists the applications that have permanent access to the PIN cache, including in the per-process mode. To include applications in PIN caching: 1. Double click on <application list> in the Value column to open the **Applications “included” in PIN caching** window. 2. Click  and, in the row that displays, click the drop-down list. 3. Locate the application you want to include and click **Open**. 4. Repeat steps 5 and 6 for each application you want to include. 5. When you have finished, click **OK**.
Values	<application list> The following processes are included by default in the “include” application list: • ActivClient User Console (acuscons) • Diagnostics Tool (actswzdg) • ActivClient middleware (accrdsub.exe) • Troubleshooting Wizard (acDiagWz.exe) • Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) Each application is a new STRING, under the Include registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Include\`
Type	REG_SZ

Important

The Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) do not appear in the Advanced Configuration Manager but are included in the registry.

Do NOT remove them from the Include list, or the Windows Logon process will no longer work.

Enable “Exclude” application list

Description	Prevents access to the PIN cache by applications listed in the "Exclude" list. Select **Yes** if you want to exclude applications in PIN caching. Then, follow the steps indicated in the next table.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Exclude`
Type	DWORD

Applications “excluded” from PIN caching

Description	Lists the applications that are not allowed access to the PIN cache. The applications listed behave as if PIN caching was disabled. To exclude applications from PIN caching: 1. Double click on <application list> in the Value column to open the **Applications to be excluded from the PIN caching window.** 2. Click  and, in the row that displays, click the drop-down list. 3. Locate the application you want to exclude and click **Open**. 4. Repeat steps 5 and 6 for each application you want to exclude. 5. When you have finished, click **OK**.
Values	<application list> Each application must be created as a new STRING, under the Exclude registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Exclude\`
Type	REG_SZ

Enable “OpenCard” application list

Description	Allows users to enable OpenCard optimization. Applications listed in the Optimized PIN caching list can perform several card-based operations in a short time (2 seconds) without the need for multiple PIN prompts. Select **Yes** if you want to enable “OpenCard” applications list. Then, follow the steps indicated in Applications “optimized” for PIN caching next table.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\OpenCard`
Type	DWORD

Applications “optimized” for PIN caching

Description	Allows a user to select one or several more applications to be optimized for PIN caching. To enable the “OpenCard” applications list: 1. Double click <Application list> in the **Value** column to open the **Applications “optimized” for PIN caching** window 2. Click  and, in the row that displays, click the drop-down list. 3. Select the application you want to optimize and click **Open**. 4. Repeat for each application you want to optimize. 5. Click **OK**.
Values	<Application list> The following processes are included by default in the “optimized” application list: Microsoft Winlogon processes (lsass, lsass_mount, winlogon, winlogon_mount). Each application is a new STRING, under the OpenCard registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\OpenCard\`
Type	REG_SZ

Important

The Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) do not appear in the Advanced Configuration Manager but are included in the registry.

Do NOT remove them from the OpenCard list, or the Windows Logon process will no longer work.

Certificate Availability

Some applications (for example, Firefox and Thunderbird) are smart card-aware and automatically access smart card-based certificates using ActivClient libraries (in this case, the ActivClient PKCS#11 library).

Other applications (for example, Internet Explorer and Microsoft Outlook) require the certificates to be available in Windows (specifically registered to the Windows CAPI store) prior to using them.

ActivClient provides several features you can customize to make those steps automatic and improve the user experience:

- "Make certificates available to Windows on card insertion" on page 38
- "Configure Windows EFS with smart card certificate" on page 39
- "Remove certificates from Windows on logoff" on page 39
- "Remove certificates from Windows on smart card removal" on page 40
- "Display certificate replacement warning" on page 40
- "Allow certificate enrollment on behalf of another user" on page 40

Reboot the workstation

For the Certificate Availability policy changes to be applied, you must reboot the workstation.

Make certificates available to Windows on card insertion

When Certificate Automatic Registration is enabled, all the certificates present on the smart card are automatically available in the Microsoft Cryptographic API (CAPI) when you insert the smart card. Products such as Internet Explorer and Microsoft Outlook use Microsoft CAPI. This option is turned on (Yes) by default.

The Windows PKI logon works properly even if this option is turned off. If Certificate Registration is turned off, you can enable the certificates with CAPI-enabled applications.

From the User Console **Tools menu**, select **Advanced**, then **Make Certificates Available to Windows**.

Description	Turn this feature on if you intend to use certificates with CAPI-enabled applications such as Microsoft Outlook or Microsoft Internet Explorer.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\AutoReg`
Type	DWORD

Note

ActivIdentity recommends that you disable the equivalent Windows certificate propagation feature.

For some smart card configurations (such as the DOD Common Access Card, the US Government PIV, and cards issued by ActivID CMS), the ActivClient mechanism adds a “friendly name” (compared to the Windows method) which will be useful to identify certificates. To guarantee that the ActivClient mechanism registers the friendly name, the Windows mechanism should be disabled. To do so:

- On operating systems prior to Windows Vista, under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\`, set the `ScCertProp` registry value Name **Enabled** to **0**.
- On operating systems starting with Windows Vista, stop the “Certificate Propagation” service.

Configure Windows EFS with smart card certificate

Description	Enables the automatic configuration of the Encrypting File System feature (Windows Vista and later) with a smart card certificate after Windows smart card PKI login. This feature automatically selects which certificate will be used for EFS.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\AutoConfigEFS`
Type	DWORD

Remove certificates from Windows on logoff

In a deployment, several users can share the same computer (kiosk), and sometimes use the same user account on the kiosk. This functionality for administrators allows to automatically remove the certificates that were registered automatically. This feature requires that the smart card be inserted in the card reader during the log-off operation.

Description	Turn this feature on if you are using a shared Windows account and you do not want to see the certificates from all the users using their smart card on this computer, or if this computer is primarily used to issue smart cards for other users.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\AutoUnRegOnLogoff`
Type	DWORD

Remove certificates from Windows on smart card removal

Description	Turn this feature on if you are using a shared Windows account and you do not want to see the certificates from all the users using their smart card on this computer, or if this computer is primarily used to issue smart cards for other users. By default, this feature is set as No as in the majority of the cases, users use their computer from their own account.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\AutoUnRegOnRemove`
Type	DWORD

Display certificate replacement warning

Description	Allows displaying a warning before replacing the default certificate during certificate download with Internet Explorer.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\CSP\EnableReplaceCertDisplay`
Type	DWORD

Allow certificate enrollment on behalf of another user

Description	Allows users with enrollment agent certificates to download certificates from Microsoft Certificate Authorities, on the "Enrollment on behalf another user" web pages.
Values	No : 0 (default) Yes : 1
Registry Key	`\HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP\DisableDefaultCertSelection`
Type	DWORD

Note

This policy applies to Windows Server 2003; it no longer applies to Windows Server 2008.

Outlook Enhancements

For a full description of Outlook enhancements, see Chapter 7, "Outlook Usability Enhancements," on page 140.

The following sections detail the Outlook enhancements policy settings:

- "Setup email certificates in Outlook on card insertion" on page 42
- "Check CRL for Outlook security profile creation and Publish to GAL" on page 42
- "Check CRL timeout for Outlook security profile creation and Publish to GAL" on page 43
- "Automatically publish certificates to the Global Address List" on page 43
- "Encrypt contents and attachments for outgoing messages" on page 44
- "Add digital signature for outgoing messages" on page 44
- "Send clear text signed message when sending signed messages" on page 44
- "Auto-request return receipt for outgoing emails" on page 45
- "Automatically add sender's certificate to Outlook contacts" on page 45
- "Outlook Auto-Contact destination folder" on page 45
- "Automatically decrypt encrypted emails" on page 46
- "Add Outlook Security icons in the compose email windows" on page 46

Restart Outlook

For the Outlook Enhancements policy changes to be applied, you must restart Outlook.

Setup email certificates in Outlook on card insertion

Description	Enables the automatic configuration of the Outlook security profile on smart card insertion.
Values	Yes : 1 (default) No : 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\AutoRegOutlook`
Type	DWORD

Check CRL for Outlook security profile creation and Publish to GAL

Description	Requires a CRL check in order to automatically configure email certificates in Outlook and to automatically publish certificates to the GAL. If enabled and enforced, the operation is not performed if the CRL is unavailable or if the certificate status is revoked or on hold. If enabled and not enforced, the operation is performed and a Windows event warning is created if the CRL is unavailable or if the certificate status is revoked or on hold. If disabled, the operation is performed regardless of the CRL check status.
Values	0: Disabled 1: Enabled and enforced (default) 2: Enabled and not enforced
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\CRLCheck`
Type	DWORD

Check CRL timeout for Outlook security profile creation and Publish to GAL

Description	Timeout in milliseconds (ms) for each certificate CRL check. Recommended values are between 0 and 50000. 0 is used to represent the system default of 20000 ms
Values	0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\CRLCheckTimeout`
Type	DWORD

Automatically publish certificates to the Global Address List

Description	Enables the automatic publication of the user encryption certificate to the Global Address List (GAL) on smart card insertion.
Values	Yes: 1 No: 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\PublishToGal`
Type	DWORD

Enable audit for Outlook security profile creation and Publish to GAL

Description	Enables auditing of Outlook security profile creation and certificate publication to the Global Address List.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AuditAutoConfiguration`
Type	DWORD

Encrypt contents and attachments for outgoing messages

Description	Turns on the "Encrypt contents and attachments for outgoing messages" option at the next Outlook security profile update.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoRegEncrypt`
Type	DWORD

Add digital signature for outgoing messages

Description	Turns on the "Add digital signature to outgoing messages" option at the next Outlook security profile update.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoRegSignature`
Type	DWORD

Send clear text signed message when sending signed messages

Description	Turns on the "Send clear text signed message when sending signed messages" option at the next Outlook security profile update.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoRegClearTex`
Type	DWORD

Auto-request return receipt for outgoing emails

Description	Turns on the "Request S/MIME receipt for all S/MIME signed messages" option at the next Outlook security profile update (only available with Outlook 2002 and later).
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoRegReceipt`
Type	DWORD

Automatically add sender's certificate to Outlook contacts

Description	Automatically creates and updates contact information with the sender's certificate attached to the opened email.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoContact`
Type	DWORD

Outlook Auto-Contact destination folder

Description	Points to the location where contacts are updated in Microsoft Outlook. This location (folder) must already have been created.
Values	Contacts
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoContactStorage`
Type	REG_SZ

Automatically decrypt encrypted emails

Description	Automatically decrypts opened emails. Allows you to save copies of emails locally in non-encrypted format. Automatically decrypted emails remain decrypted. Consider the security implications before using this option.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AutoDecrypt`
Type	DWORD

Add Outlook Security icons in the compose email windows

Description	Automatically adds Outlook security icons to the **New Mail Message** toolbar on smart card insertion. **Note:** This setting does not apply to Outlook 2003 and later.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\DisplaySecurityIcons`
Type	DWORD

User Console

These policies are available if the User Console is installed.

Some policies are only available if the associated ActivClient components are installed. For example, the policy to access the Advanced Configuration Manager: from the User Console is available only if both the User Console and the Advanced Configuration Manager are installed.

The following sections detail the User Console policy settings:

- "Display Help" on page 48

Restart User Console

For the User Console policy changes to be applied, you must restart the User Console.

- "Display Tree view in Explorer bar" on page 48
- "Display Tasks view in Explorer bar" on page 48
- "Allow users to switch between icon and detail views" on page 49
- "Image displayed on the lower right corner of List view" on page 49
- "Display user interface/toolbar customization" on page 49
- "Display reader selection list" on page 50
- "Display the Smart Card Info icon" on page 50
- "Display Unlock Card menu" on page 50
- "Display View Unlock Code menu" on page 51
- "Display Reset Card menu" on page 51
- "Display the Change PIN menu" on page 51
- "Display the New Card menu" on page 52
- "Display Check for Card Update menu" on page 52
- "Display My Certificates folder" on page 52
- "Display CA certificates folder" on page 53
- "Allow deletion of user certificates" on page 53
- "Display Import Certificate" on page 53
- "Automatically register certificates when imported onto the smart card" on page 54
- "Display Export certificate" on page 54
- "Display “Make certificates available to Windows” menu" on page 54
- "Display Publish certificates to GAL menu" on page 55
- "Allow One-Time Password generation" on page 55
- "Allow One-Time Password synchronization" on page 55
- "Display My Personal Info" on page 56
- "Display the Advanced Configuration Manager" on page 56
- "Display Advanced Diagnostics" on page 56
- "Display Troubleshooting" on page 57

Display Help

Description	Allows displaying the main "Help" standard tool bar button and the "ActivClient Help" command in the "Help" menu in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayHelp`
Type	DWORD

Display Tree view in Explorer bar

Description	Allows displaying the Tree View of the Explorer toolbar in the User Console. If disabled, the Tasks View is the only view available. If both the Tasks and Tree views are disabled, the Explorer toolbar is not displayed.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayTreeViewPane`
Type	DWORD

Display Tasks view in Explorer bar

Description	Allows displaying the Tasks View of the Explorer toolbar in the User Console. If disabled, the Tree View is the only view available. If both the Tasks and Tree views are disabled, the Explorer toolbar is not displayed.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayTaskPanel`
Type	DWORD

Allow users to switch between icon and detail views

Description	Allows users to choose a view type from: • Large Icons • Small Icons • List • Details If this option is disabled, users cannot choose the view type; and the User Console then uses Large Icons.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayViewType`
Type	DWORD

Image displayed on the lower right corner of List view

Description	Allows users to display a customized image as background (lower right corner) for the User Console. Select the path to a 96x143 pixels image in the `.bmp` format.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\BackgroundImage`
Type	REG_SZ

Display user interface/toolbar customization

Description	Allows to customize User Console interface and toolbars.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayUICusto`
Type	DWORD

Display reader selection list

Description	Allows displaying the "Use Reader" menu and the "Reader List" toolbar icon in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayReaderList`
Type	DWORD

Display the Smart Card Info icon

Description	Allows displaying the "Smart Card Info" icon in the right pane of the User Console. The Smart Card Info window displays information such as smart card user name, manufacturer, model and serial number.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayAboutCard`
Type	DWORD

Display Unlock Card menu

Description	Allows to access the Unlock card feature in order to unlock the smart card.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateUnlock`
Type	DWORD

Display View Unlock Code menu

Description	Allows a user to display their unlock code. Only applicable for standalone smart cards.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayUnlockCode`
Type	DWORD

Display Reset Card menu

Description	Allows a user to reset their smart cards. Only applicable for standalone smart cards.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayReset`
Type	DWORD

Display the Change PIN menu

Description	Allows to access and use the Change PIN feature from the User Console Tools menu.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateChangePin`
Type	DWORD

Display the New Card menu

Description	Allows a user to access and use the PIN Initialization Tool feature from the User Console **New Card** menu.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayPinInit`
Type	DWORD

Display Check for Card Update menu

Description	Allows users to access the Check for Card Update feature that checks with ActivID CMS if an update is available for the inserted smart card.
Values	Yes = 1 (default when Auto-Update feature is installed) No = 0 (default when Auto-Update feature is not installed)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ ActivateCheckforCardUpdate`
Type	DWORD

Note

If the Smart Card Update feature is installed, the User Console menu is unavailable until the feature is configured with the ActivID CMS URL.

Display My Certificates folder

Description	Allows users to view smart card certificates in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayCertFolder`
Type	DWORD

Display CA certificates folder

Description	Allows users to view the CA certificates stored on their smart card in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayCACertFolder`
Type	DWORD

Allow deletion of user certificates

Description	Allows users to delete user certificates.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\AllowDeleteCert`
Type	DWORD

Display Import Certificate

Description	Allows users to import a certificate onto their smart card from the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayImportCert`
Type	DWORD

Automatically register certificates when imported onto the smart card

Description	Automatically makes certificates available to Windows when imported onto the smart card (using the User Console).
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\AutoRegisterOnImport`
Type	DWORD

Display Export certificate

Description	Allows users to export certificates from their smart card to a file using the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayExportCert`
Type	DWORD

Display “Make certificates available to Windows” menu

Description	Allows users to make available to Windows, from the User Console, the user certificates that are available on their smart card.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateCertificateRegister`
Type	DWORD

Display Publish certificates to GAL menu

Description	Allows users to setup email certificates in Outlook and to publish certificates to the Global Address List.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\DisplayPublishToGal`
Type	DWORD

Allow One-Time Password generation

Description	Allows to generate a smart card-based One-Time Password in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\AllowGenOTP`
Type	DWORD

Allow One-Time Password synchronization

Description	Allows users to resynchronize the smart card-based One-Time Password credentials in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\AllowSynchOTP`
Type	DWORD

Display My Personal Info

Description	Allows users to view the personal information (demographic data) available on their smart card in the User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateTabDemographic`
Type	DWORD

Note

Applicable to CAC and PIV cards issued by the US Government.

Display the Advanced Configuration Manager

Description	Allows users to access and use the Advanced Configuration Manager feature from the User Console "Tools" menu.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateAdminConfig`
Type	DWORD

Display Advanced Diagnostics

Description	Allows to access and use the Advanced Diagnostics tool from the User Console **Standard** toolbar.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateDiagnosticTool`
Type	DWORD

Display Troubleshooting

Description	Allows to access and use the Troubleshooting Wizard from the User Console **Standard** toolbar.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole\ActivateTroubleShooting`
Type	DWORD

ActivClient Agent (Notification Area Icon)

These policies are available if the ActivClient Agent is installed.

Some policies are only available if the associated ActivClient components are installed. For example, the policy about accessing the Advanced Configuration Manager from the Agent is available only if both the Agent and the Advanced Configuration Manager are installed.

The following sections detail the **ActivClient Agent (System tray icon)** policy settings to configure the ActivClient contextual menu by choosing to hide or not some menu items:

- "Display the “Open” menu item" on page 58
- "Display the “PIN Initialization Tool” menu item" on page 58
- "Display the “PIN Change Tool” menu item" on page 58
- "Display the “Advanced Configuration Manager” menu item" on page 59
- "Display the “Advanced Diagnostics” menu item" on page 59
- "Display the “Exit” menu item" on page 59
- "Display the “Get One-Time Password” menu item" on page 60
- "Display the One-Time Password window" on page 60
- "One-Time Password window duration (in seconds)" on page 60
- "Copy One-Time Password to Clipboard" on page 61
- "Clipboard One-Time Password expiration (in seconds)" on page 61

Restart ActivClient Agent

For the ActivClient Agent policy changes to be applied, you must restart the Agent.

You can do this by simply logging off and logging back on again.

Display the “Open” menu item

Description	Allows displaying the "Open" menu item in the ActivClient Agent menu. It opens the ActivClient User Console.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\OpenUserConsole`
Type	DWORD

Display the “PIN Initialization Tool” menu item

Description	Allows displaying the "PIN Initialization Tool" menu item in the ActivClient Agent menu. It starts the PIN Initialization Tool, allowing users to initialize smart cards.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayInitPIN`
Type	DWORD

Display the “PIN Change Tool” menu item

Description	Allows displaying the "PIN Change Tool" menu item in the ActivClient Agent menu. It starts the PIN Change Tool, allowing users to change their smart card PIN.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayChangePIN`
Type	DWORD

Display the “Advanced Configuration Manager” menu item

Description	Allows displaying the "Advanced Configuration Manager" menu item in the ActivClient Agent menu. It starts the Advanced Configuration Manager, allowing users and administrators to update the ActivClient configuration.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayAdvancedConfiguration`
Type	DWORD

Display the “Advanced Diagnostics” menu item

Description	Allows displaying the "Advanced Diagnostics" menu item in the ActivClient Agent menu. It starts the Advanced Diagnostics tool, allowing users and help desk operators to diagnose ActivClient.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayAdvancedDiagnostics`
Type	DWORD

Display the “Exit” menu item

Description	Allows displaying the "Exit" menu item in the ActivClient Agent menu. It closes the ActivClient Agent application.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\ActivateMenuExit`
Type	DWORD

Display the “Get One-Time Password” menu item

Description	Allows users to generate a smart card-based One-Time Password from the ActivClient Agent via the "Get One-Time Password" menu item. This setting is ignored and "Get One-Time Password" option is not available if both "Display the One-Time Password window" and "Copy One-Time Password to clipboard" are disabled.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayGetOTP`
Type	DWORD

Display the One-Time Password window

Description	Allows users to generate a smart card-based One-Time Password from the ActivClient Agent via the "Get One-Time Password" menu item, and to display it in a notification window.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\DisplayOTPWindow`
Type	DWORD

One-Time Password window duration (in seconds)

Description	Defines how long (in seconds) the One-Time Password window is displayed.
Values	10 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\OTPWindowTimeout`
Type	DWORD

Copy One-Time Password to Clipboard

Description	Allows users to generate a smart card-based One-Time Password from the ActivClient Agent via the "Get One-Time Password" menu item, and to copy it to the Clipboard automatically, ready to be pasted into the application of their choice.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\EnableOTPClipboard`
Type	DWORD

Clipboard One-Time Password expiration (in seconds)

Description	Defines how long (in seconds) the One-Time Password is available on the Clipboard.
Values	30 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent\OTPClipboardTimeOut`
Type	DWORD

Check Point Secure Authentication Agent API

The following sections detail the policy settings to configure the ActivClient SAA API behavior:

- "Check Point VPN-1 authentication mode" on page 62
- "Authentication server challenge password" on page 62
- "Authentication server challenge prompt" on page 62

Reboot workstation

For the Check Point SAA API policy changes to be applied, you must reboot the workstation.

Check Point VPN-1 authentication mode

Description	Defines whether the ActivClient One-Time Password authentication for Check Point VPN-1 is synchronous or asynchronous (challenge / response).
Values	Synchronous = 1 (default) Challenge/Response = 2
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SAA\AuthenticationMode`
Type	DWORD

Note

The **Check Point VPN-1 Authentication Mode** feature is available only in 32-bit editions of ActivClient.

Authentication server challenge password

Description	Message to send to the authentication server to get the challenge value (for challenge/response authentication). Use the same value as configured on your authentication server.
Values	Challenge
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SAA\ChallengePassword`
Type	REG_SZ

Authentication server challenge prompt

Description	String prefixing the challenge string received from the authentication server. Use the same value as configured on your authentication server.
Values	Challenge
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SAA\ChallengePrompt`
Type	REG_SZ

Notifications Management

The following sections detail the Notifications Management policy settings to configure a set of information notifications displayed by ActivClient to the end user:

- "Display Blocked Card Manager message" on page 63
- "Card Manager Blocked message" on page 64
- "Display No Smart Card Reader alert" on page 64
- "No smart card reader alert message" on page 64
- "No smart card reader alert duration (in seconds)" on page 65
- "Display unattended smart card alert" on page 65
- "Unattended smart card alert message" on page 66
- "Unattended smart card alert duration (in seconds)" on page 66
- "Display card expiration notification" on page 67
- "Display certificate expiration notification" on page 67
- "Default expiration warning message" on page 67
- "Default expiration warning period (in days)" on page 68
- "Default expiration notification period (in days)" on page 68
- "Expiration Warning Help file" on page 68
- "Default delay after card insertion for expiration check (in seconds)" on page 69

Reboot workstation

For the Notifications Management policy changes to be applied, you must reboot the workstation.

Display Blocked Card Manager message

This message is displayed when a card with a blocked card manager is inserted.

Description	Displays a message when users insert a smart card with the card manager blocked.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\DisplayBlockedCardManager`
Type	DWORD

Card Manager Blocked message

Description	Message displayed when users insert a smart card with the Card Manager blocked.
Values	“Your smart card manager is blocked, please contact the person or organization who gave you this card”
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\ASPH\BlockedCardManagerMessage`
Type	REG_SZ

Display No Smart Card Reader alert

Description	Alerts users if there is no smart card reader connected to the workstation
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\NoReaderWarning\Enable`
Type	DWORD

No smart card reader alert message

Description	Message displayed to users when there is no smart card reader connected to the workstation.
Values	<b>Card Reader Not Detected<\b> \n\nActivClient was unable to detect a smart card reader connected to your computer.\n\nPlease ensure that your smart card reader is properly connected.
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\NoReaderWarning\Message`
Type	REG_SZ

No smart card reader alert duration (in seconds)

Description	Defines how long (in seconds) the No Smart Card Reader Alert is displayed.
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\NoReaderWarning\Duration`
Type	DWORD

Display unattended smart card alert

Description	Warns users if their smart card is still inserted in the smart card reader upon log off or screen lock. You can configure ActivClient to notify the user upon log off and screen lock (default behavior), upon log off only, or never. On Windows 2000, XP, 2003, ActivClient offers visual and audio notifications. On Windows Vista and higher, ActivClient offers audio-only notification (a beep).
Values	“Only at log off” in the drop down = 2 “At log off and screen lock” in the drop down = 1 “Never” in the drop down = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\SmartCardPresenceWarning\Enable`
Type	DWORD

Unattended smart card alert message

Description	Message displayed when the user's smart card is still inserted in the smart card reader upon log off, screen lock, or session disconnect. Not available on Windows Vista and later.
Values	<b>Unattended Smart Card<\b> \n\nActivClient has detected that your smart card was in the reader while your computer was unattended.\n\nPlease remove your smart card prior to leaving your computer.
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\SmartCardPresenceWarning\Message`
Type	REG_SZ

Unattended smart card alert duration (in seconds)

Description	Defines how long (in seconds) the Unattended Smart Card Alert is displayed. Not available on Windows Vista and later.
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\Notification\SmartCardPresenceWarning\Duration`
Type	DWORD

Card Auto-Update alert duration (in seconds)

Description	Defines how long (in seconds) the Smart Card Update Alert is displayed.
Values	5 (default)
Registry Key	`\HKEY_LOCAL_MACHINE\SOFTWARE\CardAutoUpdateWarning\Duration`
Type	DWORD

Display card expiration notification

Description	Notifies users when their smart card has expired or will expire soon
Values	Yes = 1 (default for CAC version) No = 0 (default for non-CAC version)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\EnableCardValidityCheck`
Type	DWORD

Display certificate expiration notification

Description	Notifies users when their certificates have expired or will expire soon.
Values	Yes = 1 (default for CAC version) No = 0 (default for non-CAC version)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\EnableCertificatesValidityCheck`
Type	DWORD

Default expiration warning message

Description	Message displayed when the user's smart card or a user's certificate has expired or will expire soon. Note: To be displayed properly, the message must not exceed 134 characters.
Values	"Contact the person or organization who gave you this smart card."
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\ValidityCheckSentence`
Type	REG_SZ

Default expiration warning period (in days)

Description	Defines how long (in days) before smart card or certificate expiration the warning should display. The default is 60 days before expiration.
Values	60 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlocalConfig\ValidityCheckPeriod`
Type	DWORD

Default expiration notification period (in days)

Description	Defines for how long (in days) the card or certificate expiration warning is displayed once the smart card or certificate has expired.
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\ExpirationNotificationPeriod`
Type	DWORD

Expiration Warning Help file

Description	Defines the full path to the Expiration Warning dialog box. Help file When no value is specified, the ActivClient Help file is used.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\ValidityCheckHelp`
Type	REG_SZ

Default delay after card insertion for expiration check (in seconds)

Description	Defines how long (in seconds) ActivClient should wait after smart card insertion or Windows logon/unlock before ActivClient checks for smart card or certificate expiration.
Values	20 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\GlobalConfig\ValidityCheckDelay`
Type	DWORD

Logon Window

The default static logon banner is:



Size = 413*72.

The default moving logon banner is:

Size = 413*5.

You can use graphics (in bitmap (.BMP) format) of a different size as the logon window will adjust automatically.

The following section detail the Logon Window policy settings that enable you to customize the smart card PIN authentication dialog box defaults and select the banner you want to apply:

- "Static Logon Banner—high resolution" on page 70
- "Moving Logon Banner—high resolution" on page 70

Reboot workstation

For the Logon Window policy changes to be applied, you must reboot the workstation.

Static Logon Banner—high resolution

Description	In the Value column, select a path to a banner (bitmap file) to be displayed in the **Enter PIN** window in high resolution mode.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\AuthenticationDialog\BannerHiRes`
Type	REG_SZ

Moving Logon Banner—high resolution

Description	Thin moving line displayed under the banner in the **Enter** PIN window. In the Value column, select a path to a bitmap file (Moving Logon Banner) displayed in the **Enter PIN** window in high resolution mode.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\AuthenticationDialog\ProgressBarHiRes`
Type	REG_SZ

Software Auto-Update Service

ActivClient provides an Automatic Software Update feature. This section lists the different registry keys related to that feature. No default settings are set for ActivClient auto-update as they are customer dependent.

The following sections detail the ActivClient auto-update policy settings that you can configure:

- "Software automatic update URL" on page 71
- "Download path for software updates" on page 71
- "Number of retries performed when an error occurs" on page 71
- "Number of minutes between retries" on page 71
- "Number of days before checking for an update" on page 72

Reboot workstation

For the Auto-Update Service policy changes to be applied, you must reboot the workstation.

Software automatic update URL

Description	Network location where ActivClient Auto-Update service will look for the software updates.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\AutoUpdate\ActivClient\URL`
Type	REG_SZ

Download path for software updates

Description	Local folder where the software updates are downloaded. The ActivClient Auto-Update service must have read and write permissions for that folder
Values	<Install Dir>\Downloads
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\AutoUpdate\ActivClient\DownloadPath`
Type	REG_SZ

Number of retries performed when an error occurs

Description	Number of times the ActivClient Auto-Update service will attempt to update the software.
Values	3 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\AutoUpdate\ActivClient\NumberOfRetries`
Type	DWORD

Number of minutes between retries

Description	Waiting period (in minutes) before the ActivClient Auto-Update service retries to update the software when a failure occurs.
Values	15 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\AutoUpdate\ActivClient\TimeBetweenRetry`
Type	DWORD

Number of days before checking for an update

Description	Interval (in days) between checks for software updates.
Values	1 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\AutoUpdate\ActivClient\CheckDays`
Type	DWORD

Smart Card Auto-Update

ActivClient provides an Automatic Smart Card Update feature. This section lists the different registry keys related to that feature. No default settings are set for ActivClient auto-update as they are customer dependent.

For a full description of the Smart Card Auto-Update feature, see Chapter 9, "Auto-Update with ActivID CMS," on page 173.

The following sections detail the ActivClient auto-update policy settings that you can configure:

- "Enable Card Auto-Update" on page 73
- "Frequency of update (in days)" on page 73
- "Maximum delay for card update check after Windows Logon" on page 73
- "Maximum delay for card update check after card insertion" on page 74
- "CMS server URL" on page 74
- "CMS Synchronization Manager timeout (in seconds)" on page 74
- "CMS Synchronization Manager retry" on page 75
- "CMS MDIDC timeout (in seconds)" on page 75

Reboot workstation

For the Smart Card Auto-Update policy changes to be applied, you must reboot the workstation.

Prerequisite

The Smart Card Auto-Update is only available if "Enable smart card discovery information caching" on page 76 is enabled.

Enable Card Auto-Update

Description	Enables ActivClient to automatically check if inserted smart cards can be updated with card content updates available in the ActivID Card Management System. Starts the smart card update process if updates are available.
Values	0: Card auto-update is disabled (default) 1: Card auto-update is enabled
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\Enabled`
Type	DWORD

Frequency of update (in days)

Description	Frequency (in days) of smart card update checks.
Values	7 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\UpdateFrequency`
Type	DWORD

Maximum delay for card update check after Windows Logon

Description	ActivClient contacts CMS to determine if smart card updates are available a few minutes after Windows logon. To spread the requests received by CMS, this delay is a random value - between 0 and the maximum delay defined in this policy (in minutes). Recommended values are between 5 and 120.
Values	120 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMaximumDelayAtLogin`
Type	DWORD

Maximum delay for card update check after card insertion

Description	ActivClient contacts CMS to determine if smart card updates are available a few minutes after a smart card is inserted. This delay is a random value - between 0 and the maximum delay defined in this policy (in minutes). Recommended values are between 1 and 10.
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMaximumDelayAfterCardInsertion`
Type	DWORD

CMS server URL

Description	Connection URL for the CMS server (see the ActivIdentity CMS documentation). The port number is included in the URL. Example: http://www.mycompany.com:89898
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerServerURL`
Type	STRING

CMS Synchronization Manager timeout (in seconds)

Description	Maximum time (in seconds) allocated to check with CMS if smart card updates are available
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerTimeout`
Type	DWORD

CMS Synchronization Manager retry

Description	Number of attempts to connect to the CMS Synchronization Manager after timeout.
Values	2 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerRetry`
Type	DWORD

CMS MDIDC timeout (in seconds)

Description	Maximum time (in seconds) allocated to perform a smart card update using CMS My Digital ID Card. When this timeout is reached, the process started to run the browser is terminated.
Values	600 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMDIDCTimeout`
Type	DWORD

Smart Card

The following sections detail the Smart Card middleware policy settings:

- "Prefer GSC-IS over PIV End Point" on page 76
- "Enable smart card discovery information caching" on page 76

Reboot workstation

For the Smart Card policy changes to be applied, you must reboot the workstation.

Prefer GSC-IS over PIV End Point

Description	For smart cards that comply with both the US government GSC-IS and PIV standards, allows specifying which standard takes precedence for the middleware.
Values	No = 1 (PIVEP) (default for non-CAC versions) Yes = 0 (GSC-IS) (default for CAC versions)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\DefaultCardEdge`
Type	DWORD

Enable smart card discovery information caching

ActivIdentity recommends enabling the caching of smart card discovery information (the default behavior) for most deployment configurations. Disabling this functionality is recommended only for issuance workstations where user smart cards are inserted only once - for the card issuance and personalization process.

Note

This policy needs to be enabled if you use the Smart Card Auto-Update with ActivID CMS capability.

Description	Allows performance optimization by caching smart card discovery information. When this option is disabled, the smart card discovery process is repeated at each smart card insertion.
Values	Yes: 1 (default) No: 0
Registry Key	`HKLM\Software\ActivIdentity\ActivClient\Card Discovery\EnableCaching`
Type	DWORD

Devices

The following section details the Devices policy setting that allows you to customize ActivClient behavior regarding hardware devices:

Authorized smart card readers

Description	Configures the list of smart card readers authorized to be used by ActivClient. If the list is empty, ActivClient uses any connected smart card reader. To add a smart card reader: 1. Double-click <reader list> in the **Value** column to open the **Authorized smart card readers** window. 2. Click  and, in the row that is displayed, enter the name of a smart card reader. To select or delete a smart card reader: 1. Follow step 1 above. 2. Either: - Select a smart card reader - Select a smart card reader and click the red cross to remove it from the list.
Values	None
Registry Key	`HKLM\Software\ActivCard\ASPCOM\AuthorizedReadersList`
Type	Multi-string

Reboot workstation

For the Devices policy changes to be applied, you must reboot the workstation.

Terminal Services

The following section details the **Terminal Services** policy setting to configure ActivClient to improve support in remote session environments.

Enable caching of the selected applet

ActivIdentity recommends enabling the caching of the selected applet (the default behavior). Disable caching only when recommended to do so by ActivIdentity customer support.

Description	Allows improving performance by enabling caching of the applet selected on the smart card. Caution is required when using Terminal Services or Remote Desktop with more than one instance of ActivClient accessing the smart card: this option must then be disabled (No) to prevent risks of smart card data corruption.
Values	Yes = 1 (default in most configurations) No = 0 (default when you install ActivClient on a server with Terminal Services)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\EnableSelectedAppletCaching`
Type	DWORD

Reboot workstation

For the Terminal Services policy changes to be applied, you must reboot the workstation.

Note

For read-only smart cards (such as the DOD Common Access Card or PIV cards for the US Government), this policy has no effect.

Performance Optimizations

The following sections detail the **Performance Optimizations** policy setting to disable certificate caching and card auto registration at card insertion:

- "Disable certificate caching on card-insertion" on page 79
- "Disable card auto-registration on card-insertion" on page 79

Reboot workstation

For the Performance Optimizations policy changes to be applied, you must reboot the workstation.

Disable certificate caching on card-insertion

ActivIdentity recommends enabling the certificate caching on card insertion (the default behavior). Certificate caching is required for most supported configurations. Disable certificate caching only when recommended to do so by ActivIdentity customer support.

Description	By default, ActivClient caches certificates on smart card insertion to improve performance in further card operations. When selected, this option prevents ActivClient from reading and caching smart card certificates on card insertion to improve immediate performance.
Values	Yes: 1 No: 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\EventService\DisableCertificateCaching`
Type	DWORD

Disable card auto-registration on card-insertion

Description	By default, ActivClient attempts to recognize and register cards from an unknown type (unsupported cards) on smart card insertion, to allow supporting new card types without any software update. When selected, this option disables this ActivClient feature to improve immediate performance.
Values	Yes: 1 No: 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\DisableCardAutoRegistration`
Type	DWORD

Note

If ActivClient is installed along with another card middleware on the same workstation, you might need to disable ActivClient card auto-registration (that is, set the policy to 1).

This will allow each smart card middleware to connect only to the smart card they respectively support.

Advanced Diagnostics

The Advanced Diagnostics tool is designed to help diagnose issues with ActivIdentity software installed on your computer.

You can configure the Advanced Diagnostics tool to send troubleshooting results by email. This decreases the risk that information is lost or modified once it is generated.

The following sections detail the Advanced Diagnostics policy settings:

- "Email address where the diagnostics report will be sent" on page 80
- "Display Email menu in Advanced Diagnostic" on page 80
- "Perform smart card diagnostics in Advanced Diagnostics" on page 81

Restart Advanced Diagnostics Tool

For the Advanced Diagnostics policy changes to be applied, you must restart the tool.

Email address where the diagnostics report will be sent

Description	Allows specifying an email address where the diagnostics report will be sent.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic\Mail`
Type	REG_SZ

Display Email menu in Advanced Diagnostic

Description	Allows users to access the "Email" menu in the Advanced Diagnostics interface, in order to send the diagnostics report by email.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic\DisplayMail`
Type	DWORD

Perform smart card diagnostics in Advanced Diagnostics

Description	Allows to perform smart card diagnostics on inserted smart cards.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic\SmartCardDiagnostic`
Type	DWORD

Logging

ActivClient can be configured to generate log files that contain detailed information for every action performed by ActivClient. The information contained in these files might be useful to your technical support when trying to solve problems.

The ActivClient User Console provides users an interface to enable / disable logging and configure a couple of policies. Additional policies are available and presented in this chapter.

The following sections detail the Logging policy settings:

- "Activate the log files" on page 82
- "Full path to log file" on page 82
- "Maximum log file size (in MB)" on page 82
- "Maximum number of file backups" on page 83
- "Enable performance logging for Windows PKI Smart Card Logon" on page 83

Reboot workstation

For the Logging policy changes to be applied, you must reboot the workstation.

Note

ActivClient allows you to configure log files without necessarily having administrator rights (other ActivClient policies can only be updated with administrative rights).

Activate the log files

Description	Allows users to create log files for every action performed by the product. No security sensitive information is logged. This may affect performance and should be activated only when required by Technical Support for troubleshooting purposes.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Logging\Activated`
Type	DWORD

Full path to log file

Description	Configures the full path to the generated log file.
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Logging\LogFile`
Type	REG_SZ

Maximum log file size (in MB)

Description	Specifies the maximum size (in megabytes) of the log file. The default size is 5 MB..
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Logging\MaxFileSize`
Type	DWORD

Maximum number of file backups

Description	Specifies the maximum number of log file backups. The default number is 1.
Values	1 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Logging\MaxFileBackups`
Type	DWORD

Enable performance logging for Windows PKI Smart Card Logon

Description	Enables the creation of entries in the Windows Event Viewer when a Windows PKI Smart Card Logon starts and ends. This is used to troubleshoot Windows PKI Smart Card Logon performance. Caution is needed when the smart card is used for other operations such as email signing or SSL authentication, as incorrect entries might be added in the Windows Event Viewer.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\ActivCard\ActivClient\CSP\EnableWindowsPKILoginProfiling`
Type	DWORD

Import/Export ActivClient Configurations

To allow you to easily revert to a default configuration or switch between two corporate configurations, the Advanced Configuration Manager provides import and export functions.

ActivClient configuration files are either registry (.reg) or text (.txt) files and are independent of the operating system and processor type.

The configuration files are stored in the Configuration folder in the Advanced Configuration Manager installation directory.

The setup also installs a `default.reg` file that contains the default values for the ActivClient settings.

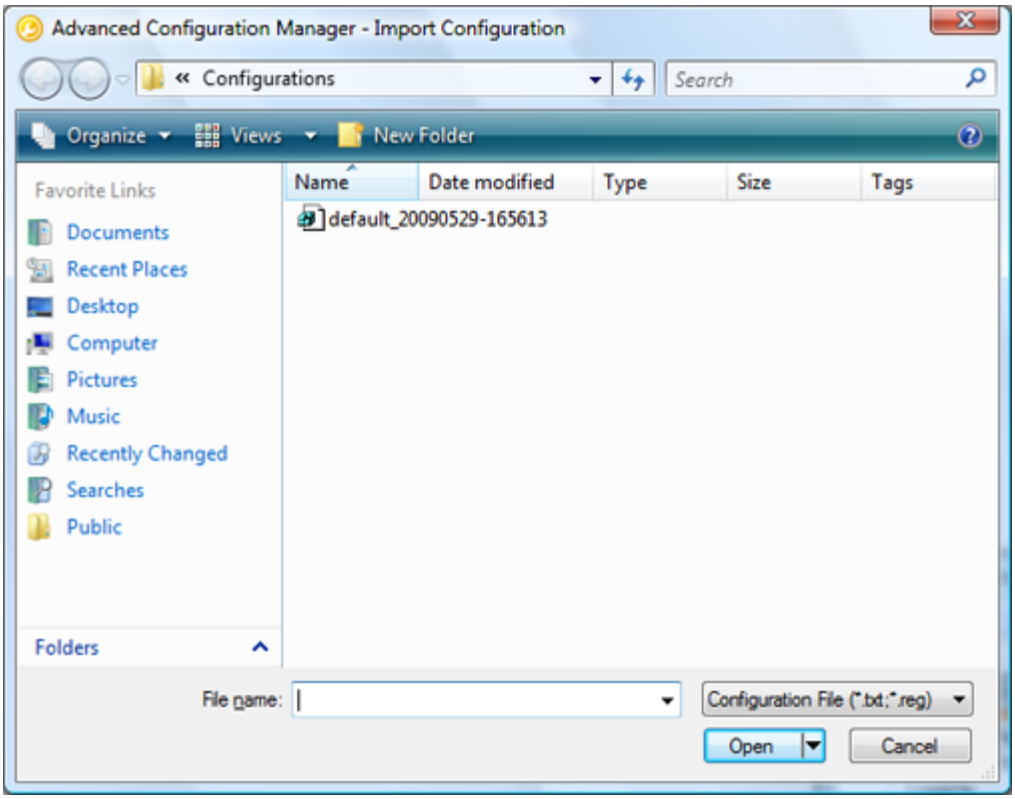
Note

You must have local administrator rights to access, create and delete files in the Configuration folder.

Import a Configuration

By importing a configuration file, you can update several or all of the local configuration settings in a single operation.

1. From the Advanced Configuration Manager's File menu, select **Import..**.



2. Select the configuration file to import and click **Open**.

   As importing the specified configuration file will overwrite your current settings, you are prompted to confirm your selection.

3. Click **Yes** to continue or **No** to cancel.

   The Advanced Configuration Manager checks that the file:

   – Is in one of the supported formats (either .reg or .txt)
   – Conforms to the security and consistency checks (same as those applied during a manual update)

Note

None of the keys are updated until the entire configuration file is validated.

If there is an consistency error, the original configuration is safe and unchanged.

When the file is validated:

- Only already installed settings are imported
- Keys that are not related to a feature already installed are ignored.

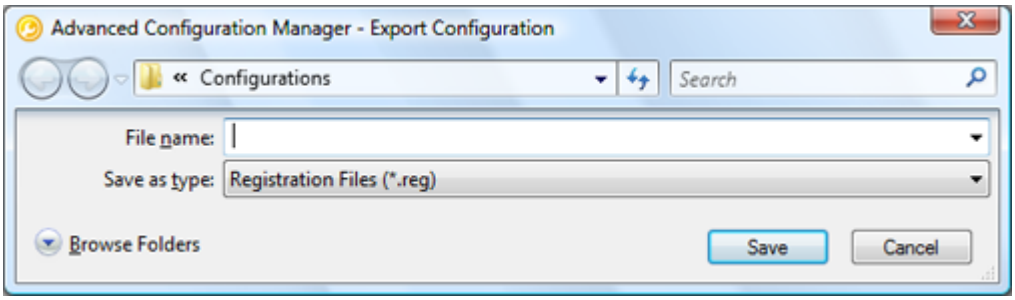
  This enables you to use the same configuration file regardless of the ActivClient features installed. Only the keys corresponding to settings already displayed in Advanced Configuration Manager are installed in the local registry.
- If a registry key has been deleted by mistake on the local machine, it is updated in the registry by the import operation.
- All the keys that are not listed in the configuration file remain unchanged.

4. Once the import operation is successful, the registry is updated with the new settings values. The Advanced Configuration Manager refreshes the properties display to reflect the recent updates and prompts you to reboot the workstation.

Export a Configuration

By exporting a configuration file, you can save the local Advanced Configuration Manager settings.

1. From the Advanced Configuration Manager's File menu, select **Export...**.



2. Select a configuration file to overwrite an existing configuration file or define a file name to create a new one and click **Save**.

   All the settings displayed in the Advanced Configuration Manager can be saved the registry (.reg) file format or text file (.txt) format.

   The generated configuration file can be safely installed using the Windows Registry Editor or by double-clicking the file.

Note

Installation using the Registry Editor or double-clicking overwrites the existing keys. If if a sub-key is not listed in the file, it will be erased. As a result, all the keys exported are either:

- Keys without sub-keys (values)
- Keys for which all the sub-keys are exported as well

Configurations for Remote Session Support

In this section you learn about these topics:

- "Remote Sessions in a Citrix Environment" on page 86.

- "Necessary Adjustments in Microsoft and Citrix Environments" on page 86

Remote Sessions in a Citrix Environment

Enabling Smart Card Services

To enable the smart card services, you must create or modify the following registry entries on the Citrix server:

Note

This section only applies to Citrix Presentation Server 4.0. It does not apply to Presentation Server 4.5, XenApp 5.0 and later.

1. Open the **Windows Registry Editor** and use the following registry key path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Smart Card Hook
```

2. From the **Edit** menu, select **Add Value** and enter the following:

Value Name	Flag
Data Type:	REG_DWORD
Data:	80000000

3. From the **Edit** menu, select **Add Value** and enter the following:

Value Name	FilePathName
Data Type:	REG_SZ
Data:	scardhook.dll

Configuring Session Disconnection on Smart Card Removal

You must have a specific configuration for ActivClient and for Windows to obtain a Citrix disconnection on smart card removal.

The ActivClient setting "Behavior at card removal" must be set to "No action" and the Microsoft setting "Behavior at card removal" must be set to “Lock workstation.”

Necessary Adjustments in Microsoft and Citrix Environments

Depending on the hardware and software computer configuration on which ActivClient and Citrix/RDP client are running, you might have to customize ActivClient in order to provide the desired behavior.

EventService ActivClient Settings

The following table lists the EventService ActivClient settings.

Registry Key	Default value	Description
`RDPWaitTime`	8000	The DWORD value indicating the delay for first notification of the new reader list after RDP connection. When ActivClient runs on a slow computer, increase this value to make sure that card operations are properly redirected on the client side. Set this value in milliseconds. Default value is 8000 milliseconds.
`RunEventServiceAsSystem`	Yes 1 (Default) No: 0	This setting is automatically set by the setup. If the operating system is later than Windows 2000 Server and TSE is enabled, the key is set to 1. In this case, a system service acevents is configured in order to improve performance to read the certificates before the PIN code entry in the Windows GINA. Run the ActivClient EventService as a system resource. Associated key: HKLM\SOFTWARE\ActivCard_ ActivClient\ EventService_ RunEventServiceAsSystem

Note

You can also list the default ActivClient setting by using the following registry key path: `HKLM\Software\ActivCard\ActivClient\EventService`.

Registry Key	Default value	Description
`ReaderListPollingPeriod`	30000 (Default)	The DWORD value indicates how often ActivClient checks for reader plugging/ unplugging in a RDP or Citrix session using calls to Microsoft Smart Card Service (SCardSvr). For slow networks (such as UMTS, satellite connection) where calls to such call may take several hundred milliseconds, you may want to increase ReaderListPollingPeriod to higher values. Set this value in milliseconds. **Note:** This key is necessary only on the RDP/Citrix servers. When ActivClient is installed on a user workstations, ActivClient uses specific Windows device APIs to manage detection of reader plugging/unplugging.

Chapter 3: Setup Customization

This chapter explains how to customize the ActivClient setup. It describes the possible customization methods and details the ActivClient setup options. It also explains how to customize the Device Installer.

In This Chapter

89 Setup Customization Methods

93 ActivClient Setup Customization Options

98 Device Installer Customization Options

Setup Customization Methods

Using a Command Line

This section describes how to use a command line.

To...	See...
Use the basic command line to install a product.	"Basic Install Command Line" on page 90
Start the ActivClient setup program with a pre-defined list of features to install, to not install, or to hide from the setup-installation option tree.	"Hide Features" on page 90
Start ActivClient setup program in blind mode i.e. default features installation without any user interface displayed	"Run a Blind Setup" on page 96

You must be logged on as a local administrator in order to execute these commands.

ActivClient Setup applications are MSI files. ActivClient Setup file names depend on the ActivClient edition, as listed in Table 3.1.

Table 3.1: ActivClient Setup Filenames and Editions

ActivClient edition	ActivClient Setup file name
ActivClient 6.2 (32-bit)	ActivClient x86 6.2.msi
ActivClient 6.2 (64-bit)	ActivClient x64 6.2.msi
ActivClient CAC 6.2 (32-bit)	ActivClient CAC x86 6.2.msi
ActivClient CAC 6.2 (64-bit)	ActivClient CAC x64 6.2.msi

In all command line examples provided in the following sections, the ActivClient setup file name is referenced as `<ActivClient setup>.msi`, where `<ActivClient setup>` is the appropriate name for the ActivClient edition in use, as listed in Table 3.1.

Basic Install Command Line

The basic command line used to install a product (with Microsoft Installer) is:

```
Msiexec.exe  /i "<path>\<ActivClient setup>.msi"
```

where:

- *<path>* is the ActivClient setup path.
- *<ActivClient setup>* is the ActivClient setup .msi file name.

This command allows installation of the default ActivClient setup, just as when double-clicking **ActivClient setup file**.

Note

The quotation marks shown in the above command line are necessary when there are spaces in the file name.

Hide Features

To hide one or several features in the setup program, use the following command:

```
msiexec.exe /i "<path>\<ActivClient setup>.msi <feature1>=-1
<feature2>=-1"
```

where:

- *<path>* is the ActivClient setup path.
- *<ActivClient setup>* is the ActivClient setup .msi file name.
- *<feature n>* is the public property of the feature to hide. See "Customize the Feature Installation" on page 98 for more information.

The quotation marks shown in the above command line are necessary when there are spaces in the file name.

Note

Once ActivClient is installed, you can modify the installed components using the “Add or Remove Programs” applet in the Windows Control Panel.

Features hidden during initial installation (that is, the features that are not installed) will display in the **ActivClient Custom Setup** screen, where you can select them for installation.

Examples

To hide the ActivClient Agent feature in ActivClient 32-bit edition 6.2, use the following command:

```
msiexec.exe /i "<path>\ActivClient x86 6.2.msi" ACSAGENTREQ =-1
```

Force Features to Display

To force installation of one or several features from the setup program, use the following command:

```
msiexec.exe /i "<path>\<ActivClient setup>.msi <feature1>=1 <feature2>=1"
```

where:

- *<path>* is the ActivClient setup path.

- *<ActivClient setup>* is the ActivClient setup `.msi` file name.
- *<feature n>* is the public property of the feature to hide. See "Customize the Feature Installation" on page 98 for more information.

Using Orca

This section describes how to edit the `.msi` file in order to customize the setup by changing the appropriate Public Property values. This can be done with Orca, a free resource editor program distributed by Microsoft. Orca is part of the Windows Installer SDK. The default values can be updated directly in the MSI.

The first two steps in this procedure are Orca tool retrieval and installation.

1. Go to the following Web site:

   http://www.microsoft.com/downloads/details.aspx?familyid=e96f8abc-62c3-4cc3-93ad-bfc98e3ae4a3&displaylang=en

2. Install the Windows Installer SDK from the Web site, and then install Orca by double-clicking the `Orca.msi` file from the \Program Files\Microsoft SDK\Bin directory.

   After the Orca installation completes, a shortcut is available in your **Start** menu.

3. Start the Orca tool and open one of the following ActivClient setup files, depending on edition:

   ```
   ActivClient x86 6.2.msi

   ActivClient x64 6.2.msi

   ActivClient CAC x86 6.2.msi

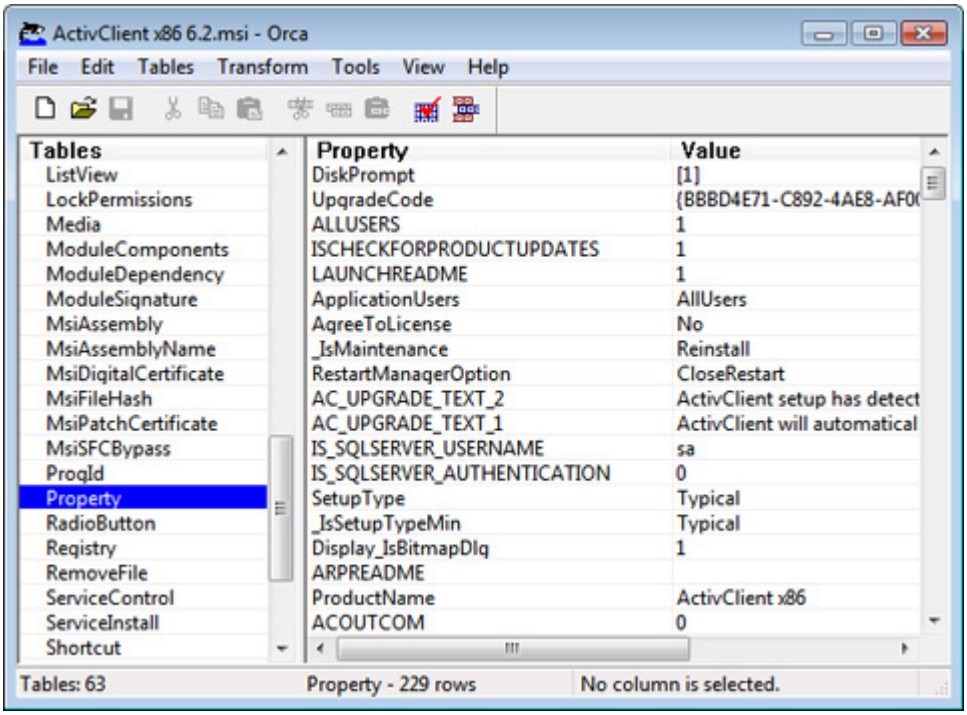
   ActivClient CAC x64 6.2.msi
   ```

Note

The quotation marks shown in the above command line are necessary when there are spaces in the file name.

Note

This must be applied to the unsigned MSI. Otherwise, it will invalidate the digital signature.



4. Select **Property** in the **Tables** column.
5. Locate and select the property you want to change.

   You can refer to the Public Properties list in "Customize the Feature Installation" on page 93.
6. Change the property's value to -1 (to hide it) or 1 (to force it to display).
7. Repeat the procedure for all other properties you want to edit.
8. Save the file.

You can then place this setup program on the network for use by all end users.

Important

- Public Properties names might be very similar. Only those without underscores will be taken into consideration.
- When a property value is changed to -1, the feature is hidden. That is, it does not display at ActivClient installation, nor does it display if you try to modify the installed components using the “Add/Remove Programs” applet in the Windows Control Panel.

Using InstallShield Admin Studio (or Wize Package Studio)

Depending of your deployment configuration, the deployment of a customized setup can be done using either:

- A customized MSI file, see "ActivClient Setup Customization Options" on page 93
- ActivClient MSI file together with an MST file

You can use either InstallShield Admin Studio or Wize Package Studio to customize the ActivClient msi setup and to generate Transforms files (MST files).

InstallShield Admin studio and Wize Package Studio allow setup customization (MSI and MST management) and packages integrity validation.

InstallShield Admin studio and Wize Package Studio user interfaces hide typical setup complexity for the following customization operations:

- Removing or relocating shortcuts
- Changing registry settings
- Adding files

For further information, see InstallShield Admin studio and Wize Package Studio documentation.

Note

If MSI customization is applied to the signed MSI, the update will invalidate the MSI digital signature.

ActivClient Setup Customization Options

Customize the Feature Installation

ActivClient Setup allows you to customize the behavior of different features one at a time. That is, it is possible to disable or hide a feature during the installation, or force it to be installed.

The registry keys default values defined in the MSI can also be customized. MSI customization must be done on the unsigned MSI file (located in the \Admin\Unsigned setups folder on the ActivClient CDROM). If it is done on the signed MSI, the update will invalidate the MSI digital signature.

The following table lists the features and their associated public property that you use to customize the setup program. Their installation values are:

- No installation value = -1
- Default installation value = 0
- Forced installation value = 1

Note

The ActivClient base services node and feature are a mandatory part of ActivClient installation and cannot be removed from it; thus, they do not have a public property.

Table 3.2: Customizable Features and Public Properties

Feature name	Feature description	Public property	ActivClient edition
`Digital`	Digital Certificate Services	`DIGITALREQ`	32-bit and 64-bit
`CAPI`	Microsoft CAPI Support	`CSPREQ`	32-bit and 64-bit
`Outlook`	Microsoft Outlook Usability Enhancements	`OUTLOOKREQ`	32-bit and 64-bit
`Netscape`	Firefox and Thunderbird support	`NETSCAPEREQ`	32-bit only

Table 3.2: Customizable Features and Public Properties (Continued)

Feature name	Feature description	Public property	ActivClient edition
PKCS	PKCS#11 Support	PKCSREQ	32-bit and 64-bit
Entrust	Entrust Entelligence Desktop Solution Support	ENTRUSTREQ	32-bit only
OTP	One-Time Password Services	OTPREQ	32-bit and 64-bit
CheckPoint	Check Point VPN-1 support	CHECKPOINTREQ	32-bit only
GSCIS	N/A	GSCISREQ	32-bit and 64-bit
PIVSupport	N/A	PIVAPIREQ	32-bit and 64-bit
ACOMX	N/A	ACOMXREQ	32-bit and 64-bit
UserConsole	User Console	USERCONSREQ	32-bit and 64-bit
PINInitTool	PIN Initialization Tool	PININITTOOLREQ	32-bit and 64-bit
PINChangeTool	PIN Change Tool	PINCHANGETOOLREQ	32-bit and 64-bit
Acsagent	ActivClient Agent	ACSAGENTREQ	32-bit and 64-bit
AdvConfMan	Advanced Configuration Manager	ADVCONFMANREQ	32-bit and 64-bit
AdvDiag	Advanced Diagnostics	ADVDIAGREQ	32-bit and 64-bit
AutoUp	Auto-Update Service	AUTOUPDATEREQ	32-bit and 64-bit
CMS_MDIDC	Card auto-update service with ActivID CMS	CMSMDIDCREQ	32-bit and 64-bit
Help	Online Help	HELPREQ	32-bit and 64-bit
Troubleshooting	N/A	TRBLSHTREQ	32-bit and 64-bit

The name of the CSP is customizable using the Public Property CSPNAME. By default its value is “ActivClient Cryptographic Service Provider.” For example, you can update this name to take into account product re-branding.

Customize the Installation Path

To set the installation directory, use the property INSTALLDIR in the following command:

```
msiexec.exe  /i "<path>\<ActivClient setup>.msi" INSTALLDIR="<InstallationDIR>"
```

where:

- *<path>* is the ActivClient setup path.

- *<ActivClient setup>* is the ActivClient setup `.msi` file name.
- *<InstallationDIR>* is the desired installation directory; for example, `D:\Program Files`.

Note

The quotation marks shown in the above command line are necessary when there are spaces in the file name.

Customize the Setup Behavior

Customize the Setup Restart Behavior

In some installation cases the ActivClient setup program must restart at the end of the installation process. In order to skip the restart at that point (for example, if another program is to be installed after ActivClient) or to force it, use the `REBOOT` property.

Note

If the setup determines that a restart is required and you suppress the restart, some features might not be available until the next restart.

`REBOOT` value	Description
`Force`	Forces the restart, but stops if an error occurs.
`ForceAlways`	Forces the restart without checking the errors.
`Suppress`	Suppresses prompts for a restart at the end of the installation, but still prompts the user with an option to restart whenever the `ForceReboot` action is present. If there is no user interface (that is, a blind setup), then the system automatically restarts at each `ForceReboot`. Restarts at the end of the installation (for example, caused by an attempt to install a file already in use) are suppressed.
`ReallySuppress`	Suppresses all restarts and restart prompts initiated by a `ForceReboot` action. Suppresses all restarts and restart prompts at the end of the installation. Both the restart prompt and the restart itself are suppressed. For example, the restart at the end of the installation caused by an attempt to install a file in use are suppressed.

You can use the `REBOOT` property as follows:

To force the restart	`msiexec.exe /i "<path>\<ActivClient setup>.msi" REBOOT=Force` where: • *<path>* is the ActivClient setup path. • *<ActivClient setup>* is ActivClient setup MSI file.
To disable the restart	`msiexec.exe /i "<path>\<ActivClient setup>.msi" REBOOT=ReallySuppress` where: • *<path>* is the ActivClient setup path. • *<ActivClient setup>* is ActivClient setup MSI file.

Run a Blind Setup

To run a blind setup (that is, one where no user interface is displayed), use the following command:

```
msiexec.exe /i "<path>\<ActivClient setup>.msi" /q
```

where:

- *<path>* is the ActivClient setup path.
- *<ActivClient setup>* is ActivClient setup MSI file.

These options can be combined with other Windows Installer command line options as described in the table below. This table is available in the Windows Installer documentation (http://msdn2.microsoft.com/EN-US/library/aa367988.aspx).

Note

The quotation marks in the command line are necessary when there are spaces in the file name.

/q	n|b|r|f	Set the user interface level.	
		q , qn	No UI.
		qb	Basic UI. Use **qb!** to hide the Wizard **Cancel** button.
		qr	Reduced UI with no modal dialog box displayed at the end of the installation.
		qf	Full UI and any authored FatalError, UserExit, or Exit modal dialog boxes at the end.
		qn+	No UI except for a modal dialog box displayed at the end.
		qb+	Basic UI with a modal dialog box displayed at the end. The modal box is not displayed if the user cancels the installation. Use **qb+!** or **qb!+** to hide the **Cancel** button.
		qb-	Basic UI with no modal dialog boxes. **Note:** **/qb+** is not a supported UI level. Use **qb-!** or **qb!-** to hide the **Cancel** button.

Avoid Conflict with Other MSI Products

You might want to avoid installing ActivClient with some incompatible MSI products. To do this, you must add the ProductCode of the incompatible product into the Property table of ActivClient setup:

`AC_PRODUCT_UNSUPPORTED_X` must contain the ProductCode GUID of the incompatible product to detect. (By default, this list is empty).

`AC_PRODUCT_UNSUPPORTED_TABLE_LENGTH` is the number of products to detect.

Install Root Certificates Automatically

During ActivClient installation, ActivClient checks a folder named **Certificates** and automatically installs the root certificates found in it. To set this up:

1. Copy the ActivClient `.msi` file from the CD to the location from which you will perform the installation.
2. In the folder to which you copy the ActivClient `.msi` file, create a folder named **Certificates**.

Certificate formats

These certificate files (with .cer file extensions) must be "DER encoded binary X.509".

"Base-64 encoded binary X.509" files are not supported.

Note

You need domain administrative access rights during setup to properly install root certificates.

3. Copy all root certificate files that must be installed into the **Certificates** folder.

Device Installer Customization Options

Customize the Feature Installation

The ActivIdentity Device Installer setup customization method is identical to the customization method of ActivClient setup.

MSI customization must be done on the unsigned MSI file (located in the \Admin\Unsigned setups\ActivIdentity Device Installer folder on the ActivClient CDROM). If it is done on the signed MSI, the update will invalidate the MSI digital signature.

See the previous section "ActivClient Setup Customization Options," starting on page 93 for further information.

The following table lists the features and their associated public property that you use to customize the setup program. Their installation values are as followed:

- No installation value = -1
- Default installation value = 0
- Forced installation value = 1

Table 3.3: Features Description of the Device Installer Setup

Feature Name	Feature description	Public Property	Edition
`Serial(*)`	ActivIdentity Serial Smart Card Reader	`SERIALREQ`	32bit
`PCMCIAV1(*)`	ActivIdentity PCMCIA reader V1	`PCMCIAV1REQ`	32bit
`PCMCIAV2`	ActivIdentity PCMCIA reader V2	`PCMCIAV2REQ`	32bit and 64bit
`USBKeyV2`	ActivIdentity USB Key V2	`USBKEYV2REQ`	32bit and 64bit
`USBKeySim(*)`	ActivIdentity USB Key Sim	`USBKEYSIMREQ`	32bit
`USBV2(*)`	ActivIdentity USB reader V2	`USBV2REQ`	32bit
`USBV3(*)`	ActivIdentity USB reader V3	`USBV3REQ`	32bit
`ActivDiag`	ActivDiag	`ACTIVDIAGREQ`	32bit

* This command is not supported on Windows Vista or later.

To properly install the ActivIdentity Serial Smart Card Reader, the COM port on which the ActivIdentity Serial Smart Card Reader is connected must be specified if it is different from COM1 (the default value). You can do this either by updating the public property PORTCOM in the `.msi` file with the Orca tool or by specifying the COM port in the command, as in this example:

```
msiexec.exe /i "<path>\ActivIdentity Device Installer x86 2.2.msi"
SERIALREQ=1  PORTCOM=COM2
```

Customize the Installation Path

To set the installation directory, use the property INSTALLDIR in the following command line

```
msiexec.exe  /i "<path>\ActivIdentity Device Installer x86 2.2.msi"
INSTALLDIR="<InstallationDIR>"
```

where:

- *<path>* is the ActivClient setup path.
- *<InstallationDIR>* is the desired installation directory; for example, `D:\Program Files`.

Device Installer editions

- ActivIdentity Device Installer x86 2.2.msi
- ActivIdentity Device Installer x64 2.2.msi

Note

The quotation marks in the command line are necessary when there are spaces in the file name.

Chapter 4: Setup Deployment

This chapter explains how to deploy ActivClient once you have customized the options and setup.

In This Chapter

100 Deploying Using Standard Methods
100 Deploying Using Active Directory Push
103 Deploying Using Systems Management Server
123 Deploying using Microsoft System Center Configuration Manager

Deploying Using Standard Methods

The standard deployment method consists in running either one of the following:

- `ActivClient x86 6.2.msi`
- `ActivClient x64 6.2.msi`
- `ActivClient CAC x86 6.2.msi`
- `ActivClient CAC x64 6.2.msi`

The ActivClient setup uses MSI, the current standard in Windows. Most Enterprise Management products support MSI technology. Therefore, if you are using or planning to use a product that is MSI compatible (such as Tivoli or Novadigm), this product will likely work with ActivClient.

Before using an MSI-compatible product on your production network, ActivIdentity strongly recommends that you perform a test with ActivClient in a separate test environment.

Deploying Using Active Directory Push

This section describes how to deploy ActivClient using the automated software push capabilities in

- Windows Server 2000 Active Directory
- Windows Server 2003 Active Directory
- Windows Server 2008 Active Directory

As an administrator you can remotely install ActivClient to a set of users or computers. This dramatically reduces the total cost of ownership of ActivClient because administrators are not required to perform installation in person at every workstation. Users do not require information on how to install the product, thereby eliminating on-site installation support and associated help desk calls.

You can use Active Directory push to do the following actions in the order given below:

- "Create a Distribution Point" on page 101
- "Assign a Package" on page 101

- "Test a Package" on page 102
- "Redeploy a Package" on page 103

See Chapter 3, "Setup Customization," on page 89 for instructions on how to create the appropriate MSI package for users before you attempt to deploy ActivClient.

The following table lists the tasks associated with distributing ActivClient in the order they are to be performed and where to find information about each task:

Task No.	Task Description	See
1.	Create a shared network folder	"Create a Distribution Point" on page 101
2.	Limit deployment to a predefined user population	"Using Active Directory Group Policy Objects on Windows 2000 Server and Server 2003" on page 18
3.	Distribute a package containing ActivClient to computers.	• "Create a Package" on page 110 • "Assign a Package" on page 101
4.	Test the package	"Test a Package" on page 102
5.	Redeploy a package	"Redeploy a Package" on page 103

Create a Distribution Point

1. Log onto the server computer as an administrator.
2. Create a shared network folder in which to place an ActivClient msi file for each ActivClient edition to be deployed.
3. Set permissions on the shared network folder to allow access to the distribution point.
4. Copy each ActivClient edition msi file (`ActivClient x86 6.2.msi`, `ActivClient x64 6.2.msi`, or both) to the distribution point.

Assign a Package

The package to be deployed must be assigned to a group of computers (an Active Directory Organizational Unit, or OU) on which the package is to be installed. Computers with 32-bit operating systems and those with 64-bit operating systems must be separated on two different units, one with ActivClient 6.2 32-bit and one with ActivClient 6.2 64-bit. For these two deployments, follow these steps:

1. Start the Active Directory Users and Computers snap-in**.**
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and select **Active Directory Users and Computers.**
3. In the console tree, right-click your domain, and select **Properties.**
4. Click the **Group Policy** tab, drag the pointer to select the group policy object to which you want to assign this package, and click **Edit.**
5. In the console tree, click the plus sign (+) to expand **Computer Configuration**, and then click on the plus sign (+) to expand **Software Settings.**
6. Right-click on **Software Installation**, select **New**, and point to **Package.**
7. In the **Open** dialog box under **File Name**, enter the full **Universal Naming Convention** (UNC) path to the shared folder that contains the MSI package you want. For example:\\ file server \ share \ file name.msi

   Note

   Do not browse to the location. Make sure that you use the UNC path to the shared folder.
8. Click **Open**, click **Assign**, and click **OK.**

   Note

   It is mandatory that the package is assigned to a computer, as opposed to assigning it to a user.

The package is listed in the right pane of the **Group Policy** window.

9. Close the **Group Policy** window, click **OK**, and then close the **Active Directory Users and Computers** window.

   When the client computer starts, the managed software package is automatically installed.

Test a Package

To validate the package, you can force package installation on a computer from the target Organizational Unit (OU) and verify that the installation has completed successfully. To do so:

1. Log onto a computer that is part of the target OU.
2. Click the **Start** button, point to **Settings**, and select **Control Panel**.
3. Select **Start**, then **Settings**. From the **Control Panel** menu, go to the **Add/ Remove Programs** window, then click **Add New Program**.
4. In the **Add programs from your network** list, select the ActivClient edition that you published, then click **Add**.

   The package is validated as ActivClient is installed.

5. Click **OK**, and then click **Close.**

Redeploy a Package

In some cases, you might want to redeploy a package. For example, you can use the redeploy function to upgrade to a more recent version.

Use the following procedure to redeploy a package:

1. Start the Active Directory Users and Computers snap-in.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and point to **Active Directory Users and Computers**.
3. In the console tree, right-click your domain, and select **Properties**.
4. Click the **Group Policy** tab, drag the pointer to select the group policy object with which you deployed the package, and click **Edit**.
5. Click the plus sign (+) to expand the **Software Settings** item that contains the **Software Installation** container with the package you used to deploy ActivClient.
6. Drag the pointer to select the **Software Installation** container.
7. In the right pane of the **Group Policy** window, right-click the package, select **All Tasks**, and point to **Redeploy Application**.
8. When the following message displays, click **Yes**.

   “Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?”
9. Close the **Group Policy** window, click **OK**, and close the **Active Directory Users and Computers** window.

Deploying Using Systems Management Server

This section describes how to deploy ActivClient with Microsoft Systems Management Server (SMS).

As an administrator you can remotely install ActivClient for a set of users or computers. This reduces the total cost of ownership of ActivClient because administrators are not required to perform installation in person at every workstation. Also, users do not require instruction on how to install the product, thereby eliminating on-site installation support and associated help desk calls.

Note

The information in this section applies to both the 32-bit and 64-bit versions of ActivClient. To deploy both you must perform the procedure twice, remotely installing the two ActivClient versions to different set of computers.

Here are the tasks to follow in order deploy a program using SMS:

Task	Description
Create an SMS package	1. Configure the clients, see "Configure Client Computers" on page 104 2. Configure the server, see "Configure the Server" on page 108
Run the advertised program on the client	See "Run an Advertised Program on a Client" on page 118

An SMS package contains files and instructions that direct the software distribution process. Each package contains a program, an **msiexec command line** that runs on each targeted computer, as well as the package source files that are used by the program when it runs (that is, software installation files).

Programs within a package are broadcast to client computers using an **advertisement.**

An advertisement defines the collection of client computers that will receive the advertisement, the programs they will receive, and the schedule.

You must configure the client computers and the server to create an SMS package.

Prerequisites

- Microsoft SMS 2003 (with the latest service pack) is installed on the distribution server.
- All client computers are connected in the same domain.
- The product (CD image) is stored on the server in a shared folder.

Configure Client Computers

Before configuring the clients computers, you must first initialize client discovery.

You can initialize the client discovery process in two ways:

- Modify the logon scripts to start the discovery process when the users log on.
- Run the System Management Installation Wizard on the computer that you want to discover or to install as a SMS client (`SMSman.exe`).

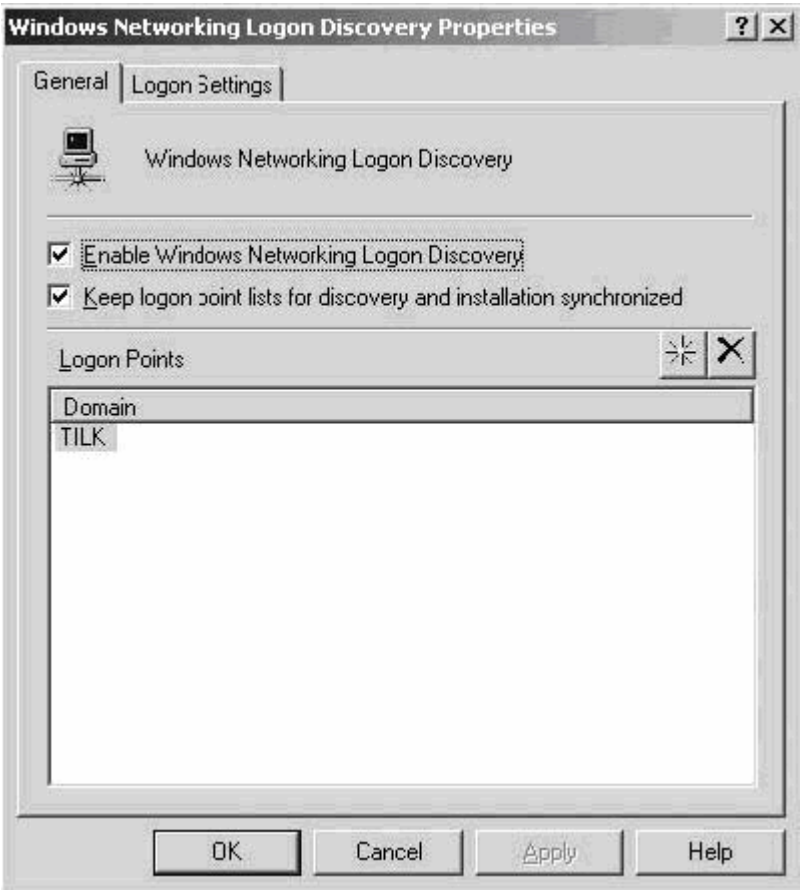
1. Start the **SMS Administration Console**, click the **Start** button, point to **Programs**, point to **System Management Server**, point to **SMS**, and point to **Administration Console.**

   The **SMS Administration Console** is displayed.

2. In the console tree, click the plus sign (+) to expand **Site Settings**, and drag the pointer to select **Discovery Methods**.

3. Select the discovery method you want to use from the **Name** list.

The General tab of the Windows Networking Logon Discovery Properties window is displayed.

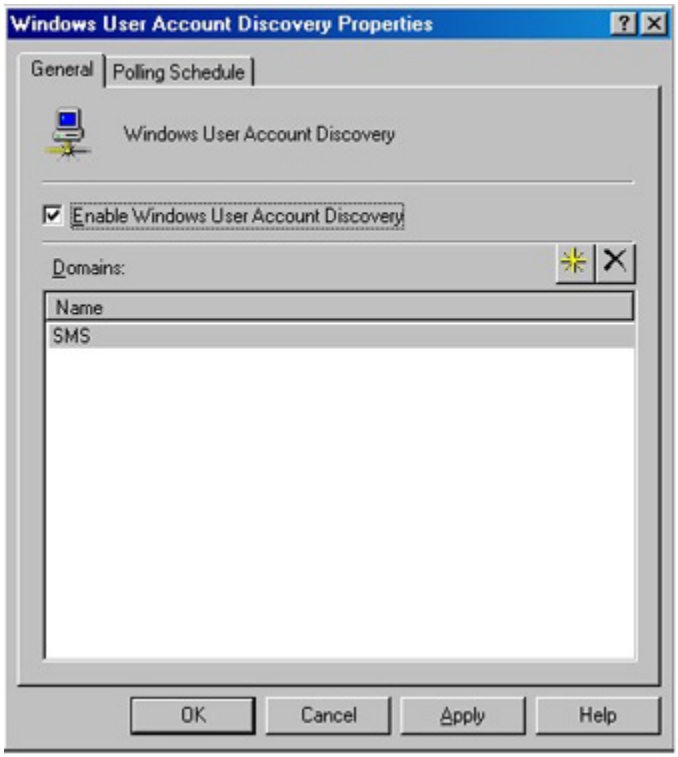


4. If not already selected, click the **General** tab and select both:
   - **Enable Windows Networking Logon Discovery**
   - **Keep logon point lists for discovery and installation synchronized**
5. From the **Domain** list, select the domain you want to discover.
6. Click the **Logon Settings** tab.

   The **Logon Settings** tab of the **Active Directory System Discovery Properties** window is displayed.
7. Perform the following:
   a. Check the **Modify user login scripts** option.
   b. Select the **Bottom of existing script** option.

c. At the **Logon point update schedule** section, click on the up and down arrows to select the number of hours you want to pass before the next update.

8. Click on the **OK** button. The General tab of the Windows User Account Discovery Properties window is displayed.



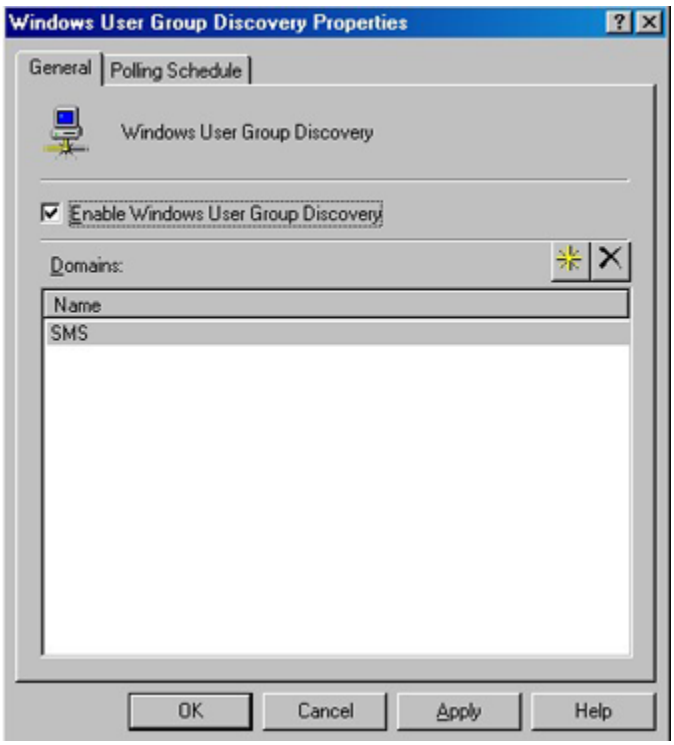
9. If not already selected, click on the **General** tab and:

   a. Select the **Enable Windows NT User Account Discovery** option.

   b. From the **Domain** list, highlight the domain you want to target.

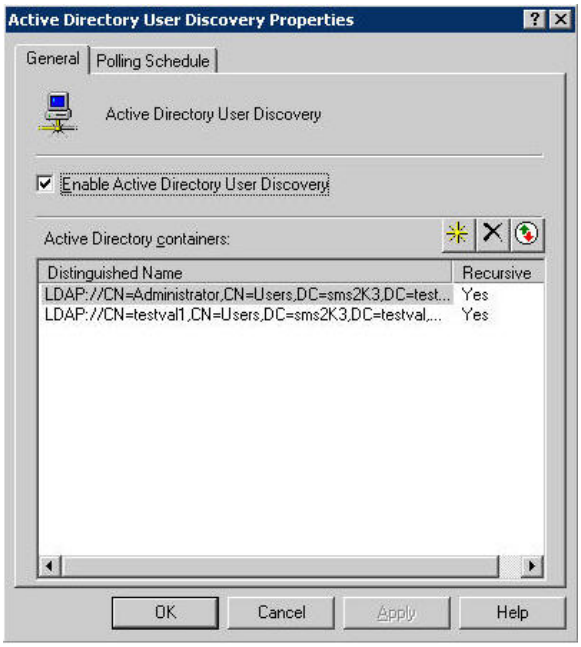
10. Click **OK**.

    The General tab of the Windows User Group Discovery Properties window is displayed.



11. Repeat step 9 in the **General** tab of the Windows NT User Group Discovery Properties.

12. Click **OK.** The General tab of the Active Directory User Discovery Properties window is displayed.



13. Select the **Enable Active Directory User Discover** option.

14. Manage (add, delete or move) your container in the **Active Directory Containers section**.

15. Click **OK.**

Note

Your container can be a selection of specific users of the domain or just the whole domain itself.

Once the SMS client software is installed, the SMS client service is available on the client computer. The Control Panel contains the following files:

- System Management Control Panel applet
- Advertised Programs Control Panel applet
- Advertised Programs Monitor Control Panel applet

See the SMS documentation from Microsoft for further details.

Configure the Server

The following table lists the tasks that you must complete when configuring the server. It also lists where to find more information about each task.

Task #	Task Description‘	For more information, see
1.	Enable software distribution.	"Enable Software Distribution" on page 108.
2.	Prepare collections.	"Prepare Collections" on page 109.
3.	Create a package.	"Create a Package" on page 110.
4.	Create the programs.	"Create a Program" on page 114
5.	Create the distributing advertisements.	"Create a Distributed Advertisement" on page 116.
6.	Monitor software distribution.	"Monitor Software Distribution" on page 118.

Enable Software Distribution

Use the following procedure to enable software distribution:

1. Start the **SMS Administrator Console**, click the **Start** button, point to **Programs**, point to **System Management Server**, point to **SMS**, and point to **Administration Console**.

2. In the console tree, click the plus sign (+) to expand **Site Settings**, and drag the pointer to select **Client Agents**.

3. Right-click **Advertised Program Client Agent** and select **Properties**.

4. Click the **General** tab and select the **Enable software distribution to clients** option.

Prepare Collections

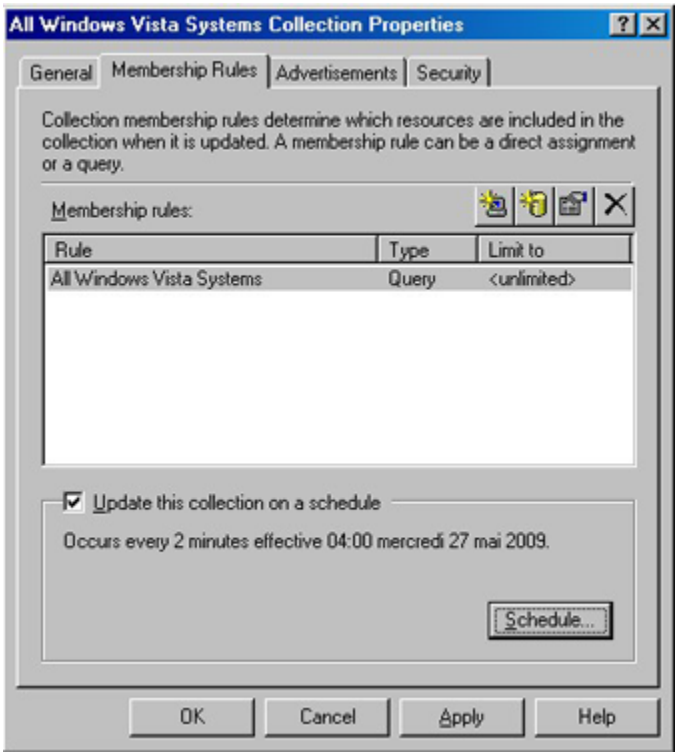
Use the following procedure to prepare collections:

1. Start the **SMS Administrator Console**, click the **Start** button, point to **Programs**, point to **System Management Server**, point to **SMS**, and point to **Administration Console.**

2. In the console tree, click the plus sign (+) to expand **Site Settings**, and drag the pointer to select **Select Collections.**

3. Right click to create a new collection that contains the clients where you want to remotely install the package, and click **OK or use the default collection.**

   The **Collection Properties** window for the collection you created is displayed.



4. Click the **Membership Rules** tab and enter the membership rules.

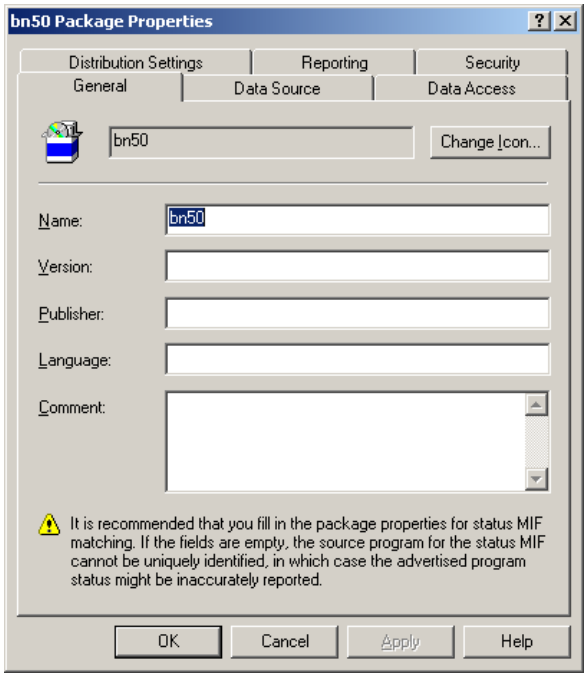
5. Click **Schedule** and set the duration of your choice.

This allows SMS to begin the discovery process immediately.

Create a Package

1. Start the **SMS Administrator Console**, click the **Start** button, point to **Programs**, point to **System Management Server**, point to **SMS,** and point to **Administration Console.**

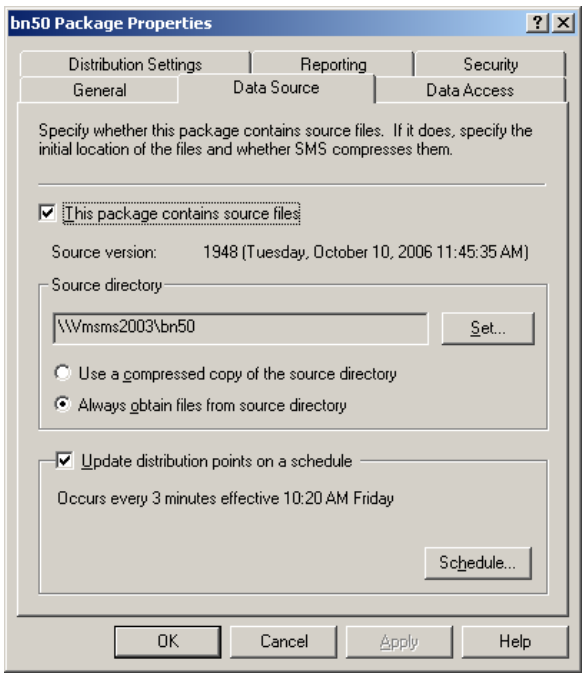
2. In the console tree, click the plus sign (+) to expand **Site Database**, and drag the pointer to select **Packages**. The Package Properties window is displayed.



3. Create a new package by performing the following: Click the **General** tab if not already selected.

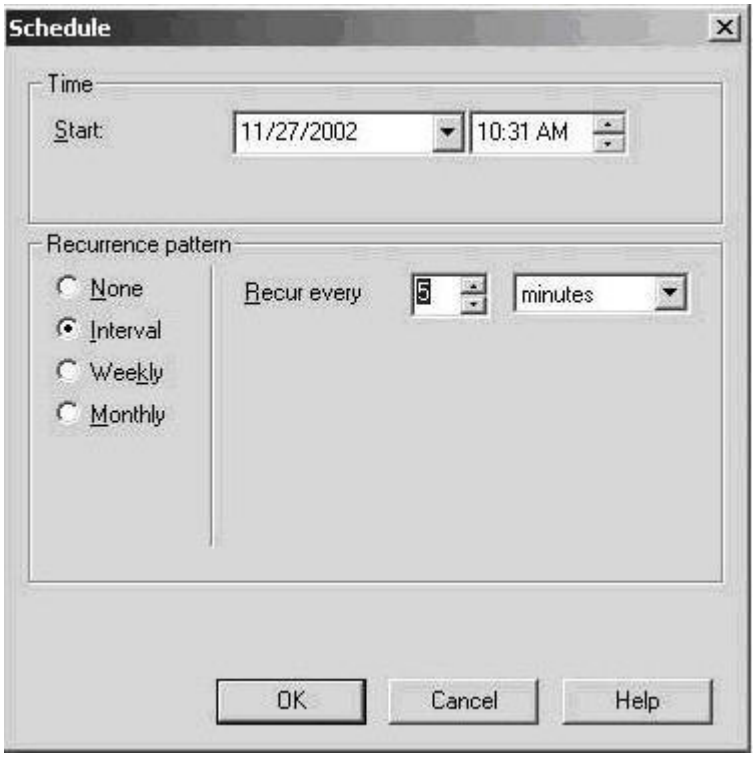
4. Fill in the package properties.

5. Click on the **Data source** tab, then specify the directory containing the source files.



6. Select **Update distribution points on a schedule**, and click **Schedule**.

   The **Schedule** window is displayed.



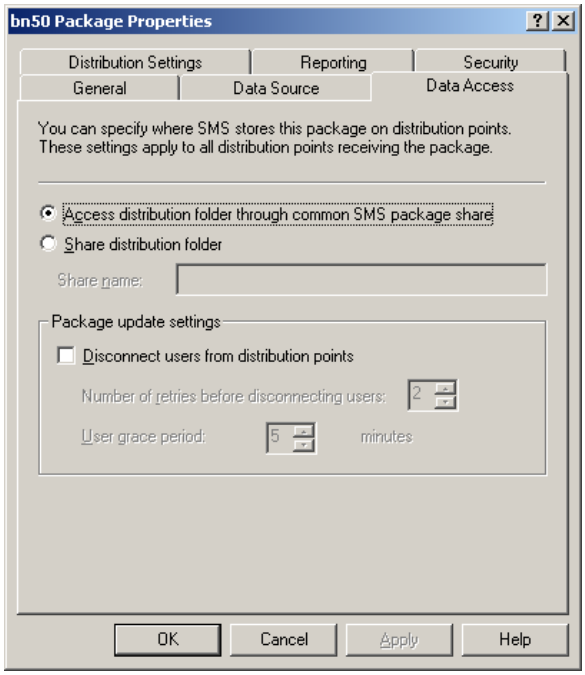
7. To configure a schedule:

   a. In the **Start** box, click the drop-down arrow and select a date and time that you want to start the distribution points update.

   b. In the **Recurrence** pattern section, select a pattern.

   c. In the **Recur every** section, click the up-down arrows to select a number and unit of time for the updates to recur, and click **OK**.

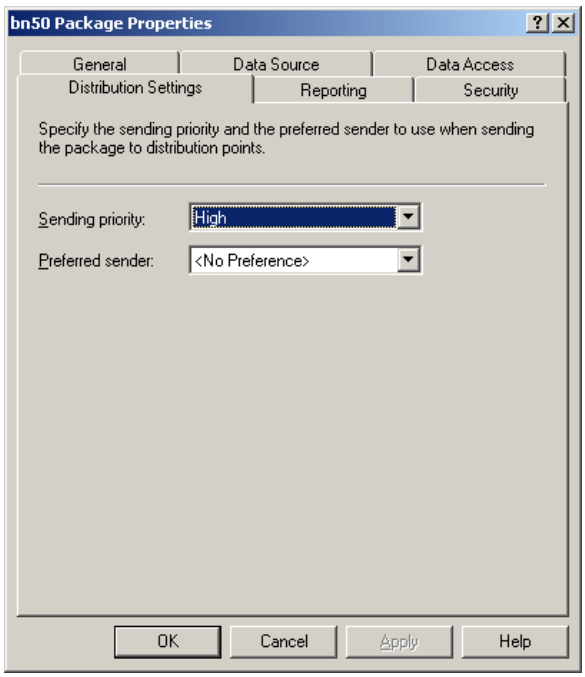
8. Go to the **Data Access** tab.



9. Select the **Access distribution folder through common SMS package share** option.

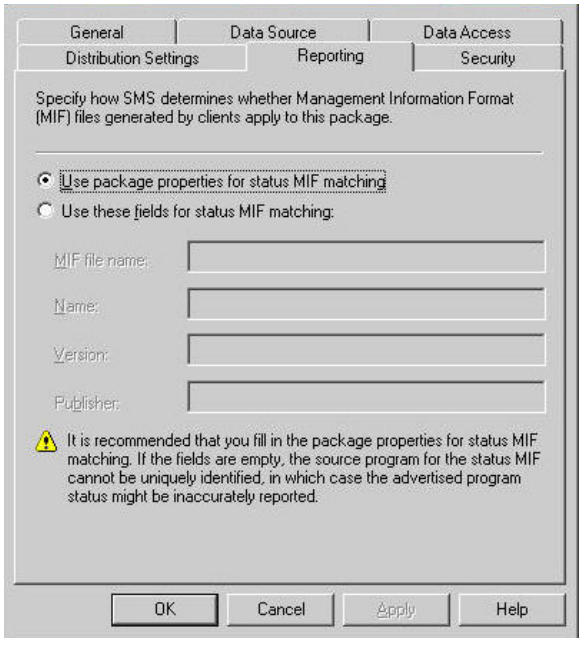
10. Click **OK**.

11. Go to the **Distribution Settings** tab.



12. From the drop-down lists, select the **Sending priority** (medium by default) and **Preferred sender** settings.

13. Go to the **Reporting** tab.



14. Select **Use package properties for status MIF matching** option.

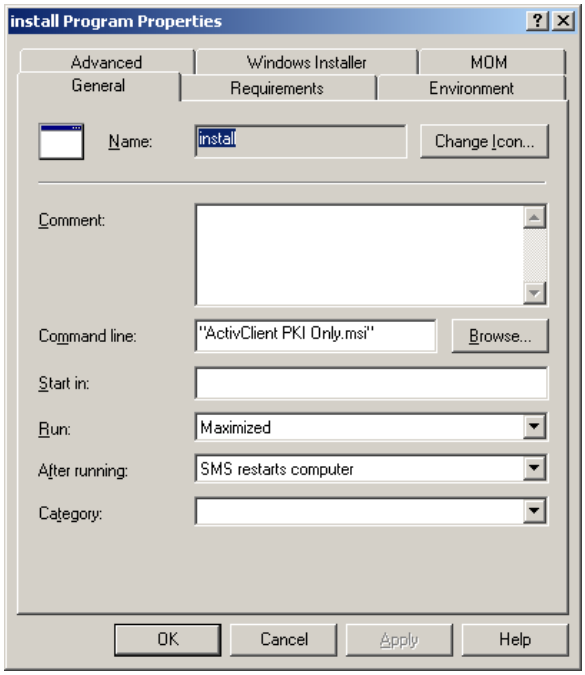
15. Click **OK**.

Create a Program

Use the following procedure to create a program.

1. For this package, select **Programs**, and create a new program.

   The **Install Program Properties** window is displayed.



2. Go to the **General** tab and:

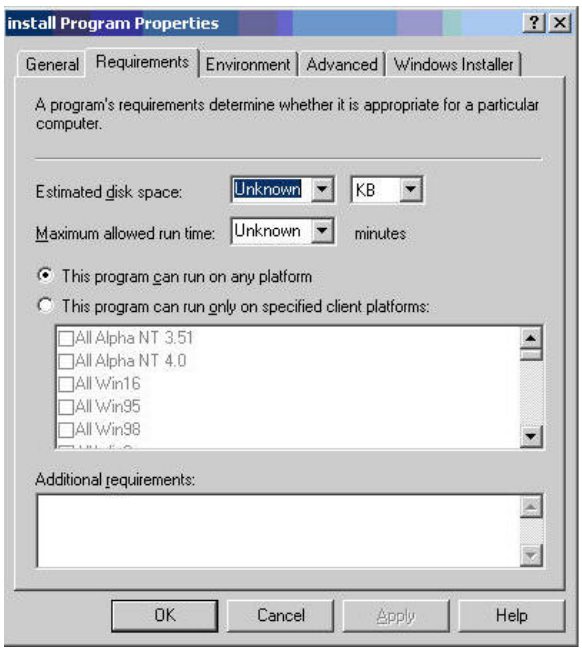
   a. In the **Name** field, enter a name for the program, for example Install ActivClient.

   b. In the **Command line** field, enter the command line. This is the Windows Installer line that you want to be executed on the client.

   c. In the **Run** field, select **Maximized** from the drop-down list.

   d. In the **After running** field, select **SMS restarts computer** from the drop-down list.

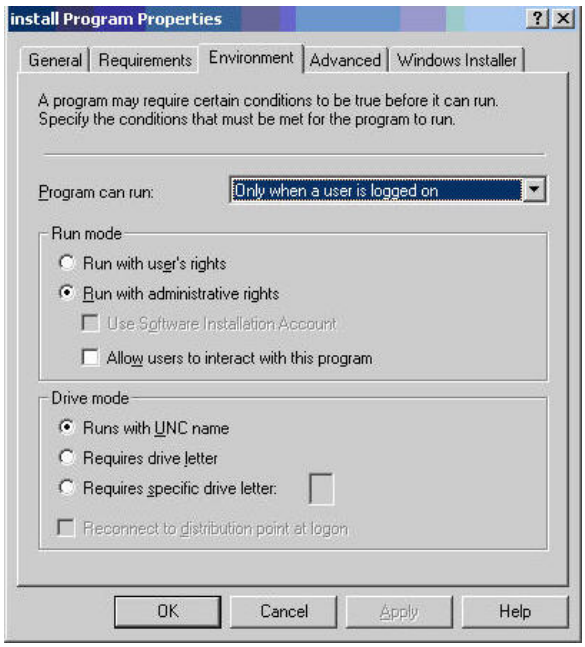
3. Go to the **Requirements** tab and:



a. Click the **Estimated disk space** drop-down to set the number and unit of measurement for the disk space you estimate is required to store this program.

b. Click the drop-down arrow next to **Estimated run time** to set the run time you estimate is required to run this program.

4. Go to the **Environment** tab and do the following:



a. Click the **Program can run** drop-down arrow to select when the program can run.

b. Update the check box **Allow users to interact with this program** according to your company software deployment policy.

c. Select the **Run with administrative rights** and **Runs with UNC name** options.

5. Go to the **Advanced** tab and do the following:

a. If this is an update, check the **Run another program first** check box and click the drop-down arrows for **Package** and **Program** to select the package and program that must be run before running the current program. For example, the uninstall program.

The following are the programs available in the ActivClient package:

To...	Then...

Install ActivClient	Use one of following command lines depending of your operating system:
	
	`msiexec /i "ActivClient x86 6.2.msi/q`
	`msiexec /i "ActivClient x64 6.2.msi/q`
	
	-or-
	
	`msiexec /i "ActivClient CAC x86 6.2.msi" /q`
	`msiexec /i "ActivClient CAC x64 6.2.msi" /q`
	
	Note: When the command line is run by SMS in hidden mode the \q parameter is mandatory.

Uninstall ActivClient	Use the command lines provided in Chapter 6, "Uninstallation," on page 130 to uninstall either ActivClient or ActivClient CAC.

b. Click the drop-down arrow for **When program is assigned** to select when the program will run.

c. If you want to remove software when it is no longer advertised, or disable the program on computers where it is advertised, select the appropriate check boxes.

Create a Distributed Advertisement

To make a program in a package available to a client, you must advertise the program to the targeted collection.

About advertisements

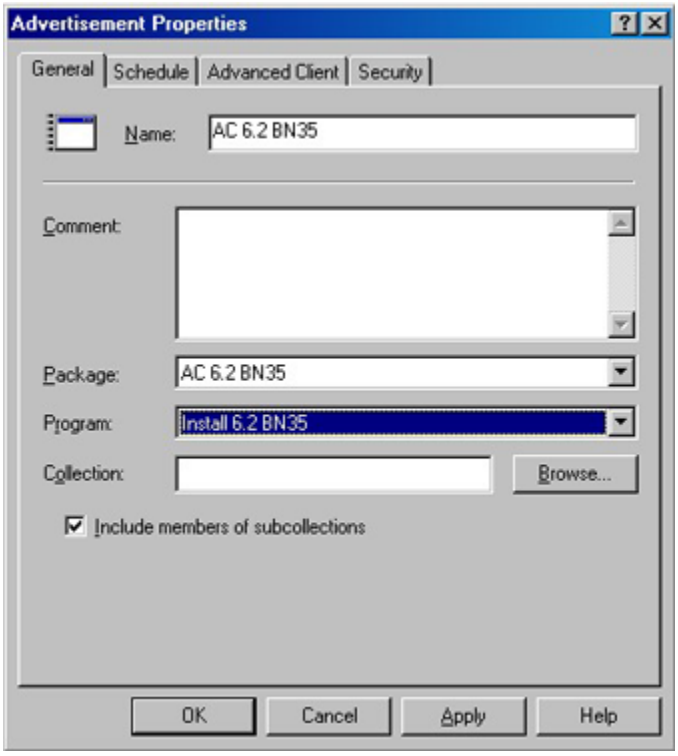
An advertisement defines the:

- Package and the program to run on the client
- Target collection
- Schedule for the program's advertisement to the clients

Advertise the Program to the Targeted Collection

1. Select **Advertisement** and click **New**.

   The General tab of the Advertisement Properties window is displayed.



2. If not already selected, click the **General** tab, and enter the name, package, program, and collection

3. To remove a program from the list of available programs after a specified period of time, click the **Schedule** tab, and click **Select Advertisement will expire** and specify the date.

Monitor Software Distribution

Monitoring packages allows you to check package status and monitor software distribution.

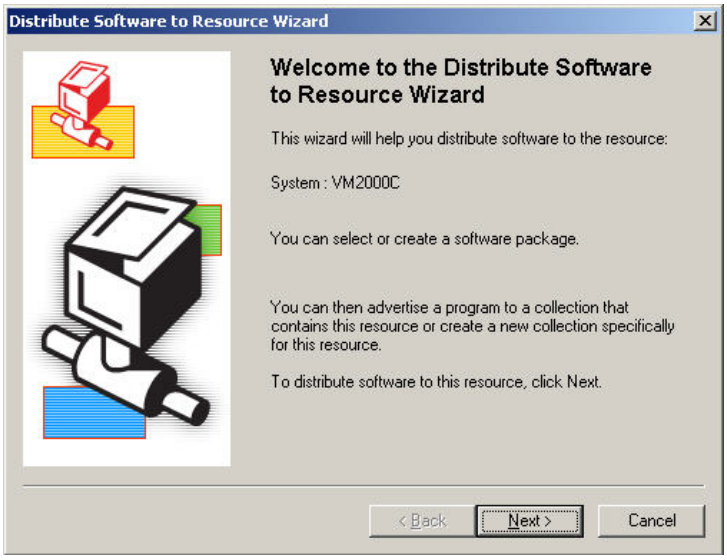
Monitoring advertisements allows you to check advertisement status.

Run an Advertised Program on a Client

When a new program is advertised, a warning message displays on the client. You must then run the advertised program on the client.

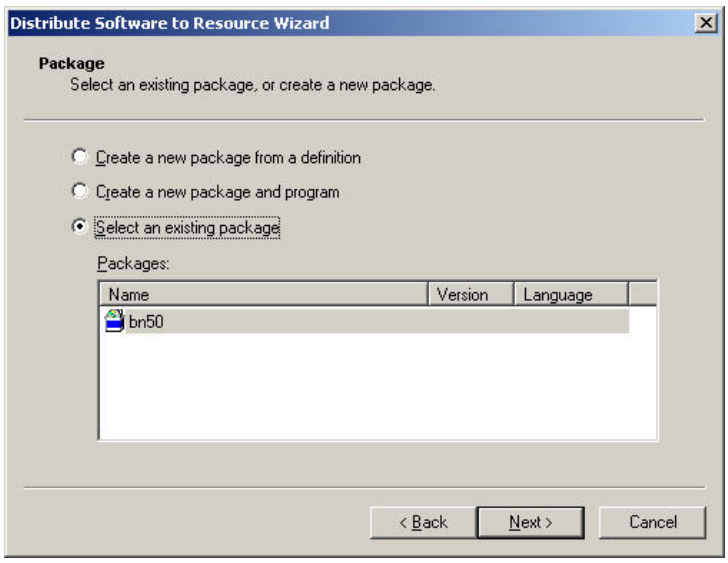
1. Select **Advertised Program** from the **Control Panel** to determine which advertised programs are available.

2. You can use the **Advertised Programs Wizard** to select the how and where the desired programs are installed.



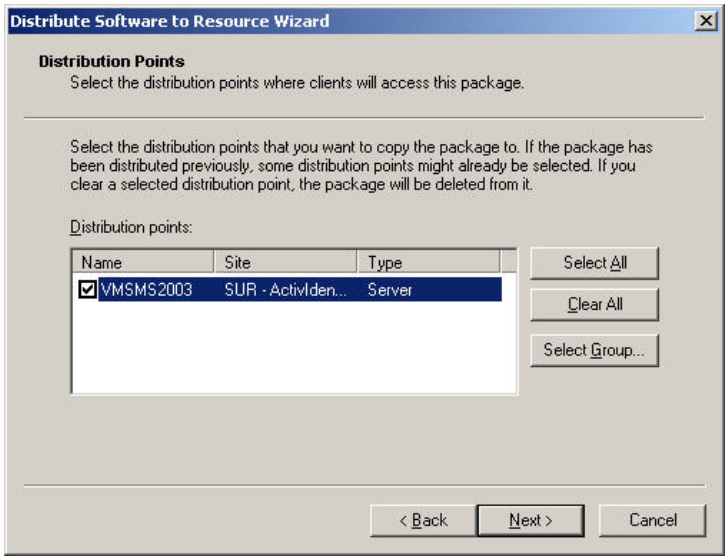
3. Click **Next** to display the **Package** page, choose the package you want to push, and click **Next**.

   The Distribution Points dialog is displayed.



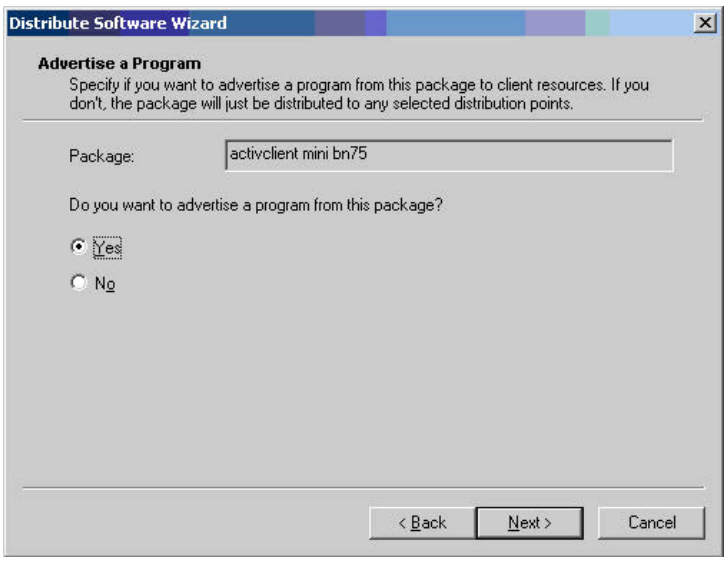
4. Select an existing package, or create a new package, and then click **Next**.

   The Distribution Points dialog is displayed.



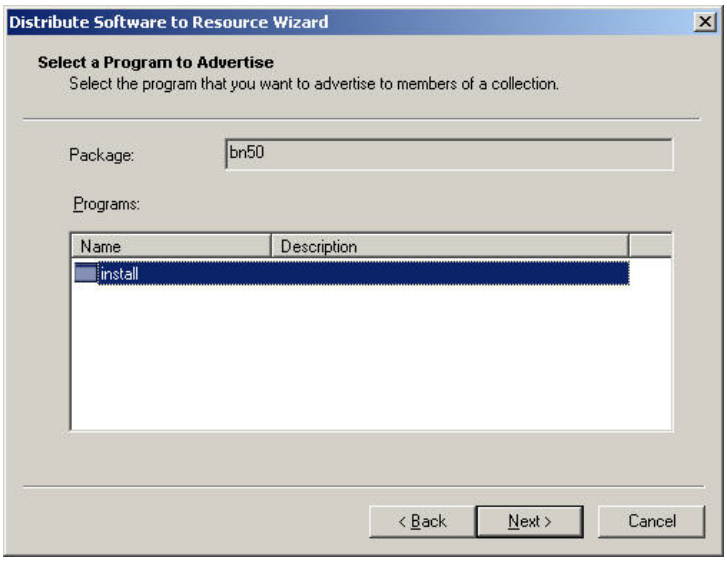
5. Select the distribution point, and click **Next**.

   The Advertise a Program page is displayed.



6. Click **Yes** to advertise the program, and click **Next**.

   The Select a Program to Advertise page is displayed.



7. Select the program to advertise, and click **Next.**

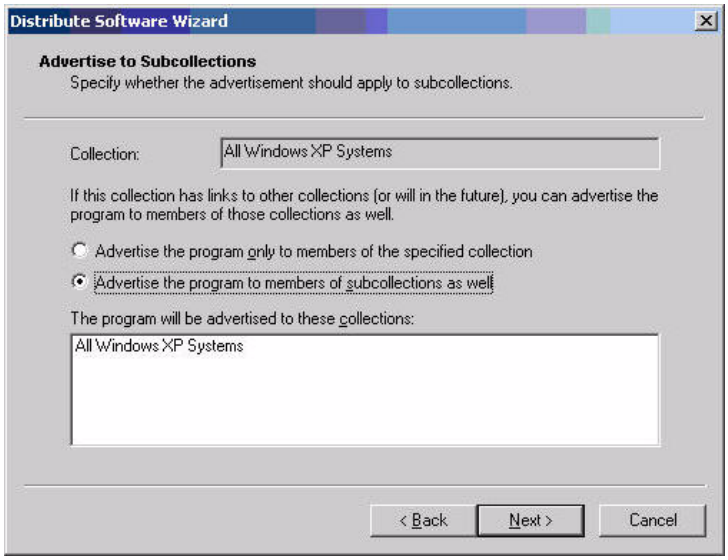
   The Current Advertisements page is displayed.

8. Choose **Create a new advertisement**, and click **Next**.

   The Advertisement Target page is displayed.

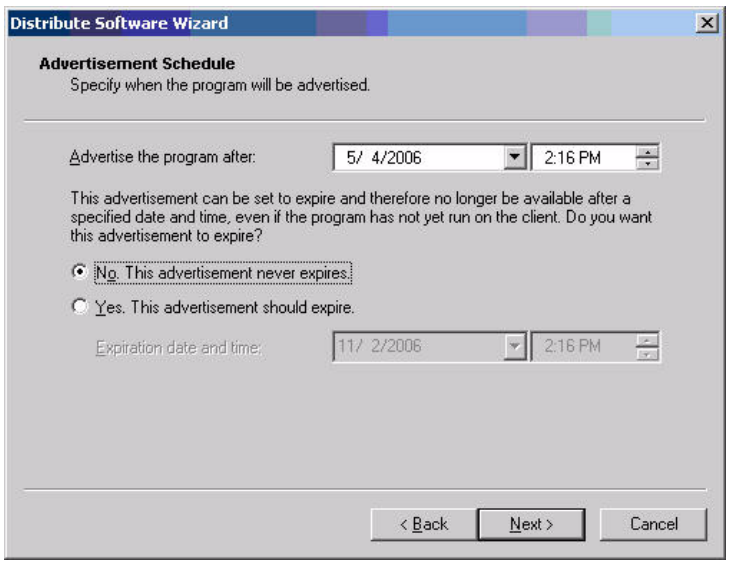
9. Select the collection you want to distribute the package, for example All Windows XP System, and click **Next**.

   The Advertise to Subcollections page is displayed.



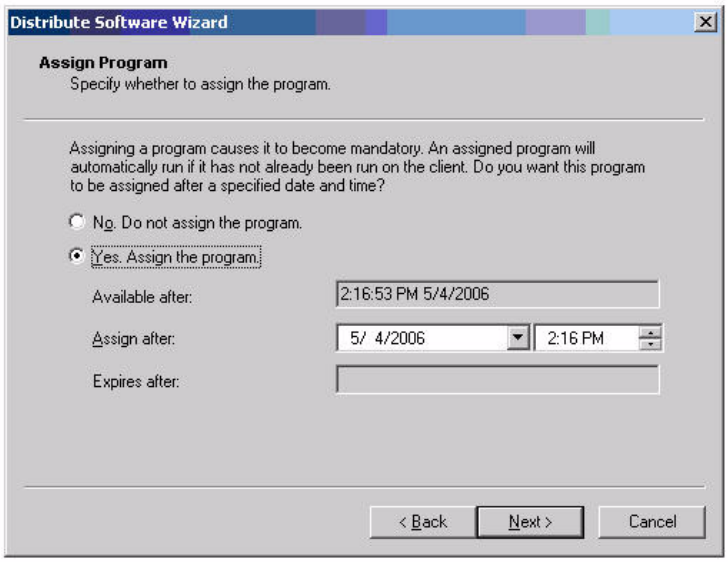
10. Select if you want to distribute software to only the specified collection or the subcollection, and click **Next**.

    The Advertisement Schedule is displayed.



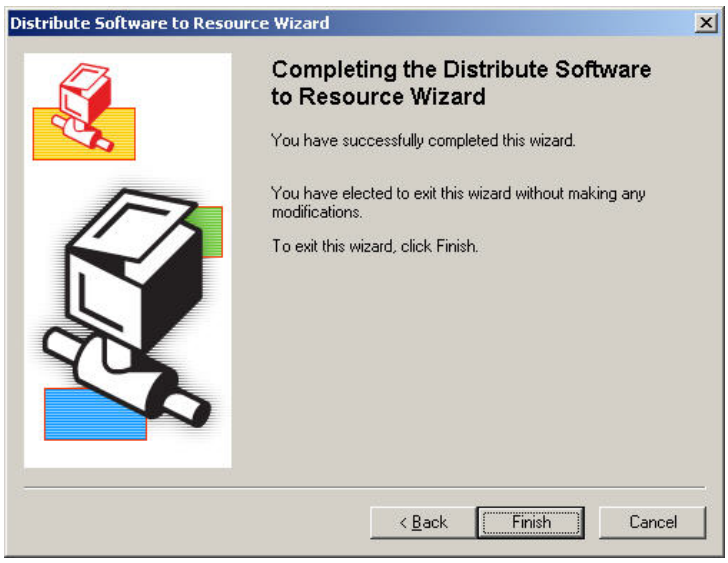
– If you do not want to make a schedule, click **Next**.
– If you want to set an advertisement schedule, click **Yes** and select an expiration date and time. The default is “No. This advertisement never expires.”

The Assign Program page is displayed.



The Completing the Distribute Software Wizard page is displayed.

11. Select **Yes, assign the program**, and click **Next**.



12. Click **Finish**.

Deploying using Microsoft System Center Configuration Manager

You can deploy ActivClient with Microsoft System Center Configuration Manager (SCCM). As an administrator, you can remotely install ActivClient for a set of users or computers. This reduces the total cost of ownership of ActivClient because administrators are not required to perform installation in person at every workstation. Also, users do not require instructions on how to install the product, thereby eliminating on-site installation support and associated help desk calls.

Note

For complete details on SCCM installation, configuration, and usage, see the Microsoft documentation.

The steps to deploy ActivClient using SCCM are similar to those of the SMS deployment procedure (see "Deploying Using Systems Management Server" on page 103). The deployment process involves a new wizard-based user interface specific to SCCM with the following steps:

1. Create a package.
2. Create a program for the package.
3. Advertise the package.
4. Create and update distribution point.

Chapter 5: Upgrading and Updating

This chapter explains how yo upgrade ActivClient and to use the Auto-Update feature.

In This Chapter

124 Supported ActivClient Upgrades
125 Upgrading Methods
125 ActivClient Auto-Update Overview
127 Enable ActivClient Auto-Update
127 Configure ActivClient Auto-Update for MSI Updates
128 Configure ActivClient Auto-Update for MSP Updates

Upgrading ActivClient

Supported ActivClient Upgrades

ActivClient 6.2 setup allows you to upgrade automatically from previous versions. The upgrade paths depend on the ActivClient editions.

ActivClient 6.2 and ActivClient CAC 6.2 (32-bit editions) support upgrade from:

- ActivCard Gold 2.2 CAC (and any SP)
- ActivCard Gold 2.3.1 (any SP)
- ActivCard Gold for CAC - PKI Only 3.0 (any Feature Pack)
- ActivClient 5.3.1 PKI Only
- ActivClient 5.4 PKI Only
- ActivClient Mini 5.5
- ActivClient PKI 6.0
- ActivClient CAC 6.0
- ActivClient 6.1 (and any service pack) (32-bit edition)
- ActivClient CAC 6.1 (and any service pack) (32-bit edition)

ActivClient 6.2 and ActivClient CAC 6.2 (64-bit editions) support upgrade from:

- ActivClient 6.1 (and any service pack) (64-bit edition)
- ActivClient CAC 6.1 (and any service pack) (64-bit edition)

ActivClient setup automatically detects the previous version and upgrades it during installation. You do not have to uninstall the previous version.

If you had customized the previous ActivClient version (by specifying which components to install, or by updating some configuration options), relevant settings will be preserved after the upgrade. However, this is not applicable to upgrades from ActivCard Gold.

For all other versions not mentioned in the above list, you need to uninstall them prior to installing ActivClient 6.2.

Upgrading Methods

There are several ways to upgrade ActivClient, depending on how you initially installed the product:

- If you used the interactive setup, see the *ActivClient for Windows Installation Guide.*
- If you deployed a previous version of ActivClient with Microsoft SMS or SCCM, then you can deploy the new package with the same methodology. For more information, see "Deploying Using Systems Management Server" on page 103 or "Deploying using Microsoft System Center Configuration Manager" on page 123.
- If you deployed a previous version of ActivClient with Active Directory Push, then you can deploy the new package with the same methodology. For more information, see "Deploying Using Active Directory Push" on page 100.
- If you used the ActivClient Auto-Update feature, see "Using ActivClient Auto-Update" on page 125.

For a detailed description of the prerequisites and upgrade procedure, see the *ActivClient for Windows Installation Guide*.

Using ActivClient Auto-Update

This section describes how to update and configure ActivClient using Auto-Update in order to access your company's internal Web site, and how to configure Stunnel to secure the protocol.

Because configuration is site dependant, ActivIdentity cannot pre-configure the ActivClient package with your auto-update settings. However, you can create a custom setup including configuration settings that are specific to your deployment.

ActivClient Auto-Update Overview

The Auto-Update system uses a standard Web server to publish ActivClient software updates. The Auto-Update client uses the HTTP and HTTPS protocols to communicate with the web server. The Web server can reside on your company intranet, the DMZ, or on the Internet. You can use any standard web server.

ActivClient periodically checks your company's Web site for new versions and acts as follows:

If...	Then...
ActivClient is already upgraded.	Nothing is done.
A new version is available.	The new version (or patch) is downloaded, and then automatically installed. The Auto-Update client runs with elevated privileges as a service. Therefore, even if the end user does not have enough privileges to run the installer, the client software is updated successfully.

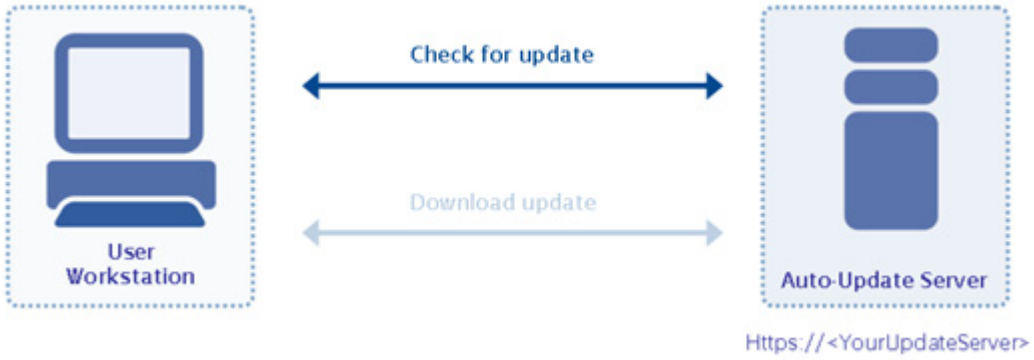
Important

In order to update ActivClient, the Auto-Update service runs with elevated privileges. Always use the Auto-Update service with an SSL protected AutoUpdate server.

Using the Auto-Update service without SSL protection could lead to malicious software being installed on the client workstation.

Use the Auto-Update service without SSL protection only for testing and troubleshooting purposes.

Figure 5.1: Updating ActivClient



On the user workstation, the following tasks are performed by the Auto-Update tool:

- Starts the update wizard at regular times (set up in registry)
- Checks to confirm that communication is secure and that the server trusted
- Reads the Auto-Update configuration file on the host
- Checks the local version number against that of the server
- Downloads a new version of the installer
- Runs the new installer
- Updates the local version number

The Auto-update Server:

- Contains Auto-Update configuration file
- Stores the new version number
- Stores the URL to the new installer

The Auto-Update server can be configured to apply updates using either the:

- Microsoft Install (using an `.msi` file) method, see "Configure ActivClient Auto-Update for MSI Updates" on page 127
- Microsoft Patch (using an `.msp` file) method, see "Configure ActivClient Auto-Update for MSP Updates" on page 128

To configure the Auto-Update Server, you must obtain:

- Web certificates from your Web server (Server Authentication certificate)
- A Root Certificate (Certification Path)

Enable ActivClient Auto-Update

The ActivClient Auto-Update component is not installed during a typical setup. Install the ActivClient Auto-Update component on the user workstation. You then must configure the following ActivClient configuration options. See Chapter 2, "Policy Definition," on page 16 for details on product customization.

1. Confirm that the ActivClient Auto-Update component is installed.
2. If you are using HTTPS, ensure that the Auto-Update server SSL certificate is trusted by the client.
   a. Download the trusted certificate in `.cer` format (for example, `activclient.cer`).
   b. Trust the certificate for the client machine by using `acregcrt.exe` (installed in ActivClient install path):
   `acregcrt.exe-regcrt activclient.cer`.

acregcrt.exe

This executable is provided in the \Admin\Auto Update directory on the ActivClient distribution.

Note

This tool does not accept path for the certificate file and does not return any feedback. Use Internet Explorer to check if the certificate is correctly trusted (Tools/Internet Options/Content/Certificates.../ Trusted Root Certification Authorities).

Configure ActivClient Auto-Update for MSI Updates

To configure auto-updates for ActivClient 6.2 (32-bit edition) and ActivClient 6.2 (64-bit edition) on the same server, you must create two different configuration files.

Select the Web server you want to use and, if you are using HTTPS, configure SSL on the server by following these steps:

1. Create a virtual directory and create an `autoupdate.ini` file in it.
2. In `autoupdate.ini`, replace `AC_XX.msi` with the name of the `.msi` file that must be installed.

Note

`.msi` files typically are larger than `.msp` files and network traffic can be higher as a result of using this method.

Example:

```
[AUTOUPDATE]

BuildNumber=6.2.0.40

FileName=ActivClient x86 6.2.msi CmdLine=/qr
```

Configure ActivClient Auto-Update for MSP Updates

To configure auto-updates for ActivClient 6.2 (32-bit edition) and ActivClient 6.2 (64-bit edition) on the same server, you must create two different configuration files.

Select the Web server you want to use and, if you are using HTTPS, configure SSL on the server by following these steps:

1. Create a virtual directory and create an `autoupdate.ini` file in it.
2. In `autoupdate.ini`, replace *`FIX_XX.msp`* with this hot fix filename:

```
[AUTOUPDATE]

BuildNumber=6.2.0.40

FileName=FIXS0XXXXXX.msp CmdLine=REINSTALL=ALL REINSTALLMODE=vomus
/qr
```

Use the Windows Installer command line when installing patches. Using this option allows you to control the user interface displayed during the update process.

ActivIdentity highly recommends that you:

- Set `REINSTALLMODE=vomus` in the command line in order to ensure that a Windows Installer repair operation does not reinstall an older version of ActivClient that does not contain the latest patches. Because “v” requires access to the original setup (“v” forces updates of `msi` cached locally on the machine), the installation using that option must have easy access to the original installation package.
- If the Auto-Update service does not have sufficient rights to access the original installation directory on the network, you can achieve the same result without the “v” switch in the MSI command line. However, this requires installing windows Installer 2.0. Windows Installer 2.0 is not available on older Windows operating systems.
- Place the `.msp` file (Microsoft Patch file) in the same virtual directory as the `autoupdate.ini` file.

Sample files

To help set up and test the auto-update capability, a hot fix sample (in both x86 and x64 versions) is provided in the \Admin\Update Sample directory on the ActivClient distribution.

An associated `autoupdate.ini` is also provided in the directory.

- Refer to published hot fixes and patches. Patches are cumulative, so only the latest ones need to be on the Auto-Update server.
- Check the version number needed for the Auto-Update client.

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Chapter 6: Uninstallation

This chapter explains how to uninstall ActivClient and its components.

In This Chapter

130 ActivClient Uninstallation Methods

130 Managing Remaining Components

ActivClient Uninstallation Methods

You can uninstall ActivClient either locally or remotely from a group of computers with Systems Management Server (SMS) using a command line:

```
msiexec /x "<code>"
```

where <*code*> is one of the following (including the {}):

- For ActivClient and ActivClient CAC x86 6.2:

  {1BE8806A-84F8-4655-A381-0D5524430944}
- For ActivClient and ActivClient CAC x64 6.2:

  {86E45973-5352-439F-A115-2E8EE4D40140}

For previous versions of ActivClient or ActivCard Gold, see the corresponding Resource Kit documentation. For more information about SMS, see "Deploying Using Systems Management Server" on page 103.

Managing Remaining Components

During the uninstallation process, ActivClient removes all installed files and registry keys. However, some components remain. These remaining components fall into these categories:

- Components left behind by design—These elements are intentionally left on the workstation by ActivClient, usually to ensure that third-party applications will continue working properly. See "Components Left Behind by Design" on page 131.
- Components left behind unexpectedly—These elements are unintentionally left on the workstation by ActivClient, due to setup limitations. See "Components Left Behind Unexpectedly" on page 134.
- Components managed by Windows—When installing and using ActivClient, the Windows operating system creates elements for its internal use. ActivClient setup does not manage these elements, which might then be left behind after ActivClient uninstallation. See "Components Managed by Windows" on page 138.

In the referenced sections, the following information is provided for each element:

- Element's identifier
- Comment or description of the element
- Consequence of leaving the element of the workstation
- Action you can take to cleanup the machine

Components Left Behind by Design

Files Left Behind by Design

Element	Mfc80 files
Comment	If necessary, ActivClient setup installs or upgrades MFC80. During uninstall, MFC is not uninstalled nor downgraded.
Consequence	None (except using disk space).
Action	None. Removing these files may prevent other applications to work properly.

Registries Left Behind by Design

Element	**HKCU\Software\ActivCard\ ActivClient\ Settings\ Settings xx-yy-zz-nn\ (several values) and sub-keys**
Comment	When using ActivClient User Console, the user interface configuration is stored on the workstation such as menus or icons. This allows displaying the User Console with the desired user preference each time it displays. Setup cannot / does not uninstall such user preferences.
Consequence	When uninstalling and reinstalling ActivClient, user configuration is kept.
Action	It is possible to remove these registries keys. However, to completely cleanup the machine, it is necessary to do that for each user that has been logged to this machine.

Element	**HKCU\Software\ActivCard\ActivClient\Diagnostics\ And sub-keys**
Comment	When using ActivClient Advanced Diagnostics, the configuration is stored on the workstation (warning display, …). This allows displaying ActivClient Advanced Diagnostics with the desired user preference. Setup cannot / does not uninstall these user preferences.
Consequence	When uninstalling and reinstalling ActivClient, user configuration is kept.
Action	It is possible to remove these registries keys. However, to completely cleanup the machine, it is necessary to do that for each user that has been logged to this machine.

Element	**HKCU\Software\ActivCard\ActivClient\GlobalConfig\ And sub-keys**
Comment	When using ActivClient Advanced Configuration Manager, the configuration is stored on the workstation such as warning display. This allows displaying ActivClient Advanced Configuration Manager with the desired user preference. Setup cannot and does not uninstall these user preferences.
Consequence	When uninstalling and reinstalling ActivClient, user configuration is kept.
Action	It is possible to remove these registries keys. However, to completely cleanup the machine, it is necessary to do that for each user that has been logged to this machine.

Element	HKCU\Software\ActivCard\ActivClient\SmartCardAgent\ And sub-keys.
Comment	When using ActivClient Agent, the configuration is stored on the workstation such as warning display. This allows displaying ActivClient Agent with the desired user preference. Setup cannot / does not uninstall these user preferences.
Consequence	When uninstalling and reinstalling ActivClient, user configuration is kept.
Action	It is possible to remove these registries keys. However, to completely cleanup the machine, it is necessary to do that for each user that has been logged to this machine.

Element	HKLM\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\xxxxx
Comment	Root certificates installed by the setup are not removed. To remove them, use Internet Explorer options.
Consequence	None.
Action	Use Netscape or Internet Explorer interface to remove them manually.

Other Components Left Behind by Design

Element	Security profiles, contacts and certificates added to Microsoft Outlook Contacts by Microsoft Outlook Usability Enhancements are not removed.
Comment	None.
Consequence	None.
Action	Use Outlook interface to remove them manually.

Element	Root Certificates are not removed from Netscape or Internet Explorer during uninstall.
Comment	None.
Consequence	None.
Action	Use Netscape or Internet Explorer interface to remove them manually.

Components Left Behind Unexpectedly

Files Left Behind Unexpectedly

Element	C:\Program Files\Common Files\acbackupreg.reg
Comment	This file is created when installing a hot-fix or upgrading from ActivClient 5.5. This is a backup of the configuration. Not applicable to ActivClient x64.
Consequence	None (except using disk space). This file is overwritten when installing a hot-fix.
Action	You may delete this file with no impact to the system.

Element	C:\Program Files\ActivCard\ActivClient\ Platform Control folder
Comment	This will occur during an upgrade from ActivClient 5.4. It is a limitation of ActivClient 5.4. Not applicable to ActivClient x64. **Note:** The directory name can differ depending on the installation directory.
Consequence	None (expect using disk space). This directory is no more used.
Action	You may delete this directory with no impact to the system.

Element	C:\Program Files\ActivCard\ActivClient\ NewRestoreSharedCount.reg file
Comment	This will occur during an upgrade from ActivClient 5.4. Not applicable to ActivClient x64. **Note:** The directory name can differ depending on the installation directory.
Consequence	None (except using disk space). This file is overwritten when installing ActivClient 6.2.
Action	You may delete this file with no impact to the system.

Element	C:\Program Files\Common Files\ActivCard folder
Comment	This will occur during an upgrade from ActivClient 5.4. It is a limitation of ActivClient 5.4. Not applicable to ActivClient x64.

Element	C:\Program Files\Common Files\ActivCard folder
Consequence	None (except using disk space).
Action	You may delete this directory (if empty) with no impact to the system. Note that the directory may be used by other ActivIdentity applications (if it is not be empty), in which case you must not delete it.

Element	ACoutCom.dll in system folder
Comment	This will occur during an upgrade from ActivCard Gold 3.0. Not applicable to ActivClient x64.
Consequence	None (except using disk space).
Action	You may delete this file with no impact to the system.

Registries Left Behind Unexpectedly

Element	**HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ ActivCard Auto-Update Service HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ ActivClient Authentication HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ ActivClient Event Service**
Comment	These registry keys are used by Microsoft event viewer to display ActivClient information.
Consequence	None. As the file are no longer stored on the machine, event viewer will display only ID information (expected behavior as ActivClient is no longer present).
Action	You may delete these registry keys with no impact to the system.

Element	**HKEY_CLASSES_ROOT\TypeLib\{14693D63-AD77-11D3-A629-00104BB6307C} And sub-keys**
Comment	This will occur during an upgrade. This is a limitation of previous versions of ActivCard Gold and ActivClient. The data cache COM object (accoca) was not properly unregistered.
Consequence	None. COM object is used by ActivClient. Installing ActivClient will overwrite this information.
Action	You may delete these registry keys with no impact to the system.

Element	**HKLM\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\Include "lsass"="C:\\WINNT\\system32\\lsass.exe" "acdiagcd"="C:\\Program Files\\ActivCard\\ActivClient\\acdiagcd.exe"**
Comment	This will occur during an upgrade from ActivClient 5.4. It is a limitation of ActivClient 5.4. Not applicable to ActivClient x64.
Consequence	None. These registry keys are used only by ActivClient. Installing ActivClient will overwrite this information.
Action	You may delete these registry keys with no impact to the system.

Element	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\ActivCard ActivClient (Oberthur CosmopolIC 32K V4 Fast ATR) HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\ActivCard ActivClient (Oberthur CosmopolIC 32K V4) HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\ActivCard ActivClient (Oberthur CosmopolIC 64K v5) HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\ActivCard ActivClient (Oberthur CosmopolIC 64K V5.2) And sub-keys
Comment	This will occur during an upgrade from ActivClient 5.4. Not applicable to ActivClient x64.
Consequence	None. The error message that displays when trying to use these cards for a Windows PKI logon may differ, but it is no longer possible to use them (as ActivClient is uninstalled).ient. Installing ActivClient will overwrite this information.
Action	You may delete these registry keys with no impact to the system.

Element	HKLM\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard "AutoRegOutlook"=dword:00000001
Comment	This will occur during an upgrade from ActivClient 5.4. Not applicable to ActivClient x64.
Consequence	None. These registry keys are used only by ActivClient. Installing ActivClient will overwrite this information.
Action	You may delete these registry keys with no impact to the system.

Element	HKLM\SYSTEM\CurrentControlSet\Services\acautsrv
Comment	This will occur during an upgrade from ActivClient 5.4. Not applicable to ActivClient x64.
Consequence	None. As sub-keys are not set, Windows ignores this service.
Action	You may delete these registry keys with no impact to the system.

Element	HKLM\Software\ActivCard\ASPCOM
Comment	This will occur during an upgrade from ActivCard Gold for CAC 2.2. Not applicable to ActivClient x64.
Consequence	None. These registry keys are used only by ActivClient. Installing ActivClient will overwrite this information.
Action	You may delete these registry keys with no impact to the system.

Other Components Left Behind Unexpectedly

Element	**PATH (added values): C:\Program Files\ActivCard\ActivCard Gold\Resources C:\Program Files\ActivIdentity\ActivClient**
Comment	This will occur during an upgrade from ActivCard Gold or ActivClient. It is a limitation of ActivCard Gold and previous versions of ActivClient. Not applicable to ActivClient x64.
Consequence	None. No more files (used only by ActivClient) are stored in these directories.
Action	You may remove these values from PATH with no impact to the system.

Element	**Start Menu\Programs\ActivIdentity\ActivClient shortcuts (registry HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Explorer\MenuOrder\Start Menu\Programs\ActivIdentity\ActivClient)**
Comment	These shortcuts are created by Windows when creating/updating a user profile.
Consequence	None. Windows will try to find the target when trying to use them (just cancel the dialog box).
Action	You may remove these shortcuts with no impact to the system

Components Managed by Windows

Files Managed by Windows and Left Behind

Element	**C:\Config.Msi\xxx.rbf**
Comment	Windows Installer 3.0 backup files when installing an ActivClient hot fix in MSP format (see http://filext.com/detaillist.php?extdetail=RBF for further information).
Consequence	None (except using disk space). Files will be overwritten by Windows Installer when installing another MSP.
Action	None. As files are renamed by Windows installer, it is not possible to know which corresponds to an ActivClient file. Deleting all files may prevent uninstallation of hot-fixes for other products.

Element	**C:\WINDOWS\Prefetch\ ACACHSRV.EXE-1012A658.pf ACADVCFM.EXE-08294250.pf ACADVCFM.EXE-2D5D2F84.pf ACAUTOUP.EXE-25F623E1.pf ACCOCA.EXE-0B1B0F17.pf ACCRDSUB.EXE-35F4282C.pf ACDIAGWZ.EXE-302FC847.pf ACEVENTS.EXE-0E8FEC57.pf ACREGCRT.EXE-0634B271.pf ACSAGENT.EXE-309F3296.pf ACTSWZDG.EXE-2B2673C5.pf ACUSCONS.EXE-0613D964.pf AIPINCH.EXE-19F1D0A8.pf**
Comment	To improve performance on Windows XP, Windows stores some information about applications (see http://msdn.microsoft.com/msdnmag/issues/01/12/XPKernel/ for further information).
Consequence	None (except using disk space).
Action	None. It is possible to delete all files in this directory (see http://support.microsoft.com/default.aspx/kb/915163/us), Windows will recreate automatically all necessary files whenever needed.

Note

The identifers (such as, 1012A658) of the .exe files will vary for each workstation but the names will be the same (such as, acachsrv.exe).

Registries Managed by Windows and Left Behind

Element	**HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ActivCard Auto-Update Service HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ActivClient Authentication HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ActivClient Event Service HKLM\SYSTEM\ControlSet002\Services\Eventlog\Application\ActivCard Auto-Update Service HKLM\SYSTEM\ControlSet002\Services\Eventlog\Application\ActivClient Authentication HKLM\SYSTEM\ControlSet002\Services\Eventlog\Application\ActivClient Event Service**
Comment	Windows stores the last known configuration in HKLM\SYSTEM\ControlSet00x registry keys. See http://www.windowsitlibrary.com/Content/405/11/3.html for further information.
Consequence	None.
Action	Do not remove these registry keys. This may prevent Windows to boot to the last known configuration.

Chapter 7: Outlook Usability Enhancements

In This Chapter

140 Environment
142 Outlook Security Profile Configuration
154 Auto-Contact
156 Auto-Decrypt

This chapter describes the following topics:

- Supported environments
- Outlook security profile configuration and Publish to GAL, on card insertion
- Auto-Contact
- Auto-Decrypt

The purpose of the ActivClient Microsoft Outlook Usability Enhancements is to ease the configuration and usage of Microsoft Outlook for email signature, encryption and decryption using certificates stored on a smart card.

They also enable administrators to enforce corporate policies regarding email security.

The capabilities of the ActivClient Outlook Usability Enhancements are:

- Outlook security profile configuration on card insertion:
  - Setup Email certificate in Outlook on card insertion
  - Publish to GAL
- Outgoing e-mail management:
  - Encrypt content and attachments for outgoing messages
  - Add digital signature for outgoing messages
  - Send clear text signed messages when sending signed messages
  - Auto-request return receipt for outgoing emails
- Incoming e-mail management:
  - Automatically add sender's certificates to Outlook Contacts
  - Outlook Auto-Contact Destination Folder
  - Automatically decrypt encrypted e-mails
- Outlook security icons management:
  - Add Outlook Security icons in the compose e-mail windows

Environment

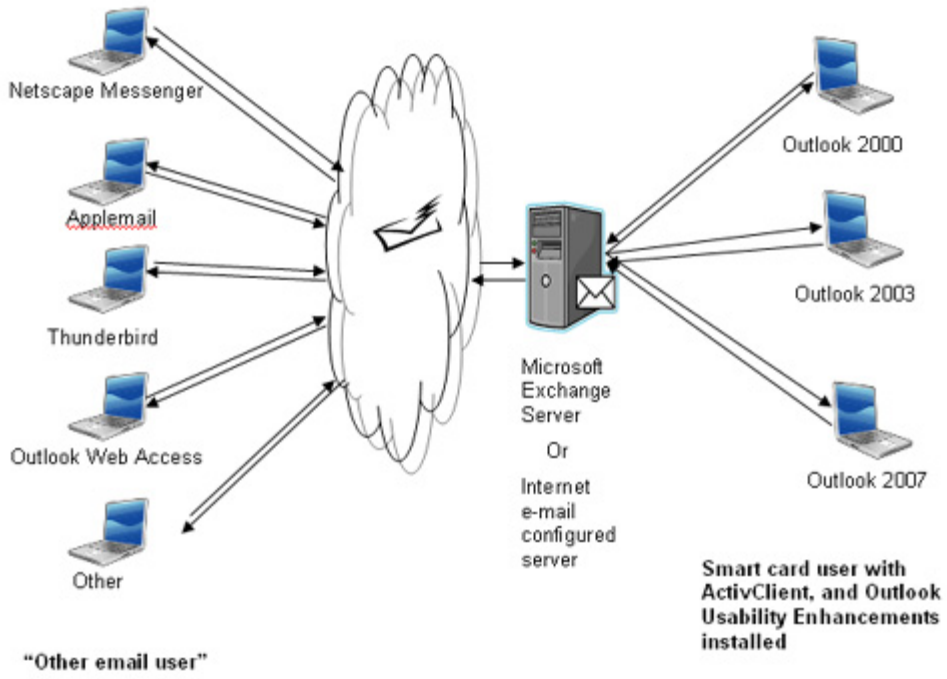
This section details the ActivClient Microsoft Outlook Usability Enhancements environment, including supported software versions and configurations.

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Overview

The environment involved in email exchanges using Microsoft Outlook and ActivClient Outlook Usability Enhancements are:

- The end user's Microsoft Outlook client (on any supported Windows platform), (for the complete list of supported versions, see "Microsoft Outlook Email Clients" on page 141).
- Microsoft Outlook Exchange Server (for the complete list of supported versions, see "Microsoft Exchange Server" on page 142).
- Emails from and to any email client on any platform (for examples, see "Emails From and To Any Email Client on Any Platform" on page 142).



Microsoft Outlook Email Clients

Supported versions of Microsoft Outlook are:

- Microsoft Office 2000 – Outlook 2000 SP3
- Microsoft Office XP – Outlook 2002 SP3
- Microsoft Office 2003 – Outlook 2003 SP3
- Microsoft Office 2007– Outlook 2007 SP1 and SP2

Email accounts configurations can be either:

- Internet emails (POP3, IMAP, HTTP, other email server)
- Exchange Server

Microsoft Exchange Server

Supported versions of Microsoft Exchange Server are:

- Microsoft Exchange Server 2000 Service Pack 3
- Microsoft Exchange Server 2003 Service Pack 2
- Microsoft Exchange Server 2007 and 2007 Service Pack 1

Emails From and To Any Email Client on Any Platform

There is no limitation regarding the email client sending the incoming managed emails and receiving the outgoing managed emails.

The following list below gives examples of such email clients:

- Microsoft Outlook
- Outlook Web Access: OWA as a feature of Exchange 2003 SP2 and 2007 (SP1 optional)
- Outlook Express
- Windows Mail
- Netscape Messenger
- AppleMail
- Microsoft Entourage (on MacOS)
- Thunderbird

Outlook Security Profile Configuration

This section describes Outlook security profile management through the ActivClient Outlook Usability enhancements settings:

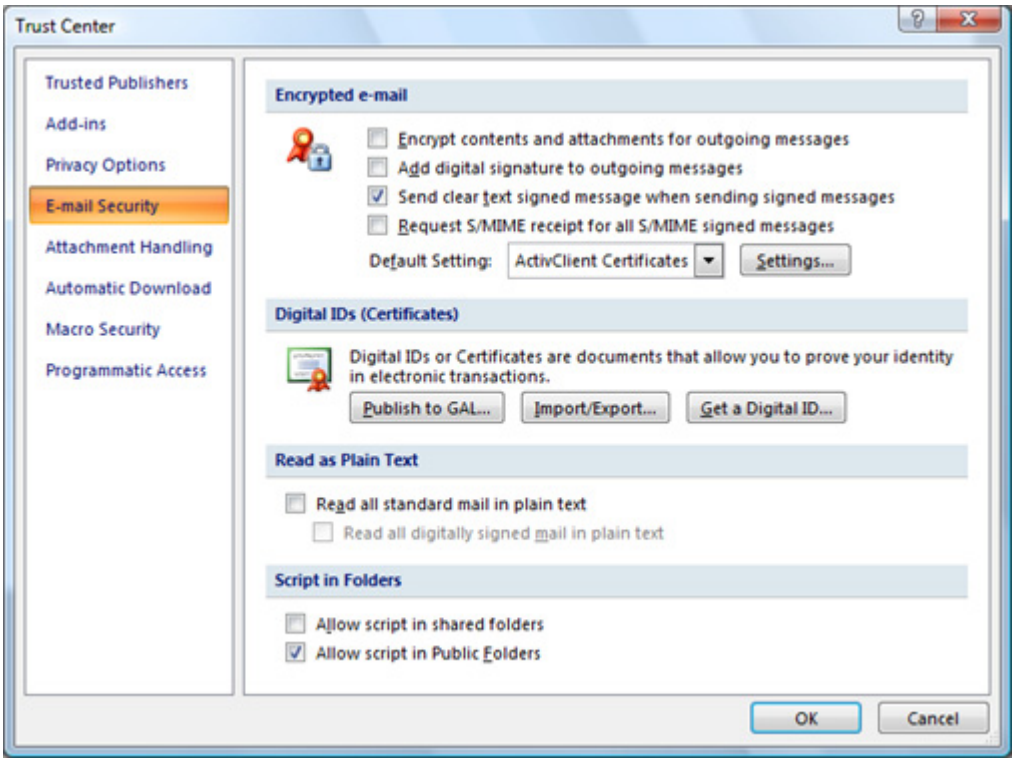
- "Setup email certificates in Outlook on card insertion" on page 42
- "Automatically publish certificates to the Global Address List" on page 43

Note

- Some ActivClient features might not be supported if Outlook is configured in the Internet modes
- Outlook (32-bit) installed on Windows x64 (platforms supported by ActivClient) is also supported
- Outlook Express (any version) and Windows Mail are not supported

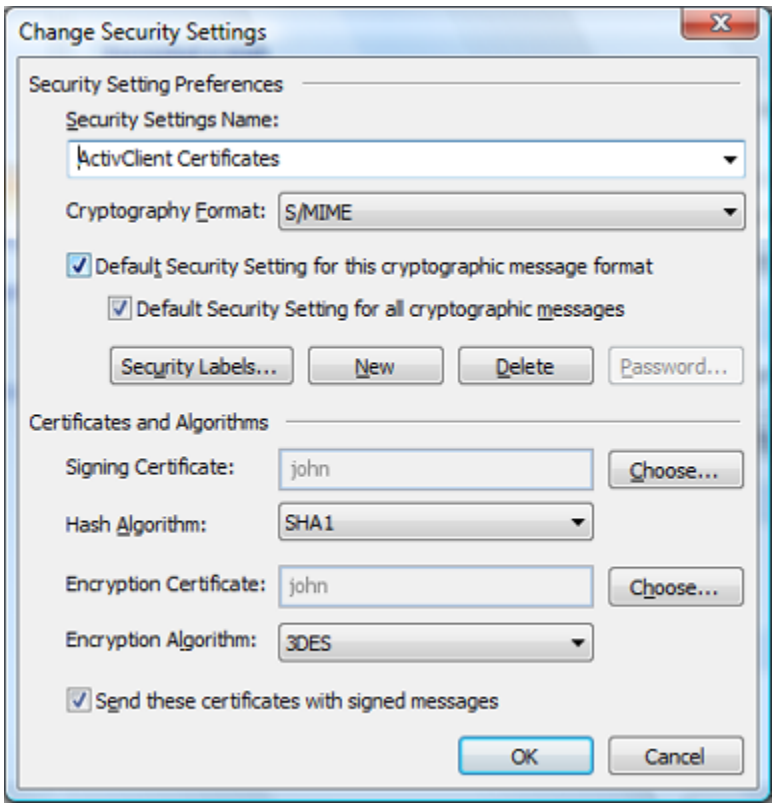
Outlook Security Profile Settings

1. The view the security settings for Outlook 2007, open the **Trust Center**.



2. In the left pane, click **Email Security**.
3. In the Encrypted e-mail section, click **Settings...**.

   The Change Security Settings window is displayed.



Outlook 2003

If you use Outlook 2003, you will find the same information in the Security tab of the Options dialog box.

The Outlook security profile as created by ActivClient is based on:

- Settings from the user's Outlook profile related to the Security Profile:
  - Security settings name
  - Signature certificate and hash algorithm
  - Cryptography format
- Encryption and signature options:
  - Encryption certificate and encryption algorithm
  - Outgoing email and attachment encryption
  - Outgoing email signature and format for signature sent
  - S/MIME receipt request for outgoing emails
- Additional settings fully managed by ActivClient:
  - Automatically add sender's certificates to Outlook Contacts
  - Outlook Auto-Contact Destination Folder
  - Automatically decrypt encrypted e-mails
  - Add Outlook Security icons in the compose e-mail windows

These settings are configured automatically at smart card insertion depending on the smart card inserted and ActivClient MS Outlook Usability Enhancements settings and environment conditions as described in following section.

Outlook Security Profile Update

Profile Selection and Conditions for Security Profile Update

When “Setup Email certificate in Outlook on card insertion” is enabled, ActivClient updates the profile at card insertion if the following conditions are met:

- Certificate propagation is enabled (either ActivClient certificate propagation or Windows certificate propagation).
- A default Microsoft Outlook profile is defined, and an Exchange account is set for this profile (for example POP accounts are ignored).
- An encryption certificate on the smart card inserted meets the following conditions (if several certificates meet the conditions, the most recent one (Valid From date) is selected):
  - Key usage - the certificate key usage must contain the value “Key Encipherment”
  - Extended Key usage - the certificate extended key usage must contain the value "Secure Email" or "<All>"
  - Validity - current date being between Valid From and Valid To date
  - User account - the certificate email address corresponds to the email address configured for the Exchange account. The comparison is performed by retrieving the email address in the certificate from the subjectaltName attribute, or if missing, from the “E=” value in the subject attribute. On the Exchange side, the comparison is performed by checking all email addresses defined in the Exchange account (prefixed by “SMTP:” or “smtp:”). This allows supporting email aliases.
  - The certificate is valid (the certificate status is verified via CRL checking). A configuration option allows some flexibility:
    - CRL check may be disabled
    - CRL check may be enabled and enforced
    - CRL check may be enabled but not enforced (an event is then created mentioning that the certificate is used even though CRL check failed: timeout, certificate expired or on hold).

Notes

- The CRL check timeout is also configurable
- The whole certificate chain is checked
- For performance reasons, the CRL check is performed only if the security profile needs to be updated (that is, after comparing with the current configuration)

- A signature certificate on the smart card inserted meets the following conditions (if several certificates meet the conditions, the most recent one (Valid From date) is selected):
  - Key usage - the certificate key usage must contain the value “Digital Signature”
  - Extended Key usage - the certificate extended key usage must contain the value "Secure Email" or "<All>"
  - Validity - current date being between Valid From and Valid To date
  - User account - the certificate email address corresponds to the email address configured for the Exchange account. The comparison is performed by retrieving the email address in the certificate from the subjectaltName attribute, or if missing, from the “E=” value in the subject attribute. On the Exchange side, the comparison is performed by checking all email addresses defined in the Exchange account (prefixed by “SMTP:” or “smtp:”). This allows supporting email aliases.
  - The certificate is valid (the certificate status is verified via CRL checking). A configuration option allows some flexibility:
    - CRL check may be disabled
    - CRL check may be enabled and enforced
    - CRL check may be enabled but not enforced (an event is then created mentioning that the certificate is used even though CRL check failed: timeout, certificate expired or on hold).

The description above applies if the workstation is connected to the corporate network (Active Directory is accessible). If it is not and the Active Directory is not accessible, then the automatic configuration is still performed but with two differences:

- No user account check is performed
- No CRL check is performed (whatever the configuration for the CRL check)

Once the conditions above are met, the security profile and the encryption/signature options are always updated:

- If a security profile named “ActivClient Certificates” already exists, it is overwritten. The default profile setting is unchanged if it was:
  - The default profile, it remains the default profile
  - Not the default profile; it is not set as the default profile
- If no security profile named “ActivClient Certificates” exists, the profile is created and set as default.
- All other security profiles (not named “ActivClient Certificates”) are not altered.

The profile creation or update is executed whether Outlook is running or not, yet Outlook needs to be restarted to see the updates in effect.

Note

The security profile is updated only if the user certificates are updated. It is not updated if only the profile policies (such as "Add digital signature to outgoing messages") are updated.

Security Profile Updated Values

The values updated by the ActivClient configuration are retrieved either from the smart card (certificates) or from the registry (configured settings). The following table lists the configured value for each setting when the profile is created or updated.

Table 7.1: Security Profile Configured Values

Setting	Value
Security settings name “Default Setting” field	“ActivClient Certificates” (always – not configurable)
Encrypt contents and attachments for outgoing messages	Value configured in ActivClient MS Outlook Usability Enhancements setting “Encrypt contents and attachments for outgoing messages”. Default is disabled.
Add digital signature to outgoing messages	Value configured in ActivClient MS Outlook Usability Enhancements setting “Add digital signature to outgoing messages”. Default is enabled
Send clear text signed message when sending signed messages	Value configured in ActivClient MS Outlook Usability Enhancements setting “Send clear text signed message when sending signed messages”. Default is enabled
Request S/MIME receipt for all S/MIME signed messages	Value configured in ActivClient MS Outlook Usability Enhancements setting “Auto-request return receipt for outgoing emails”. Default is disabled
Cryptography format	S/MIME (always – not configurable through ActivClient)
‘Default security setting for this cryptographic message format’ check box	Checked (always – not configurable through ActivClient)
‘Default security setting for all cryptographic messages’ check box	Checked (always – not configurable through ActivClient)

Note

The created profile might be altered if the ActivClient setting “Remove certificate from Windows on smart card removal” is enabled or if the user certificates are deleted from the Internet Explorer (CAPI) store.

In this case, the user needs to insert the smart card prior to sending signed emails in order to restore the security profile; otherwise, no “insert smart card” window will be displayed when sending a signed email.

Signing Certificate selected	The selected certificate is the most recent certificate (the most recent Valid From date) from the smart card that verifies the conditions: • Key usage - the certificate key usage must contain the value “Digital Signature” • Extended Key usage - the certificate extended key usage must contain the value "Secure Email" or "<All>" • Validity - current date being between Valid From and Valid To date • User account (only if workstation is online) - the certificate email address corresponds to the email address configured for the Exchange account. The comparison is performed by retrieving the email address in the certificate from the subjectaltName attribute, or if missing, from the “E=” value in the subject attribute. On the Exchange side, the comparison is performed by checking all email addresses defined in the Exchange account (prefixed by “SMTP:” or “smtp:”). This allows supporting email aliases • The certificate is valid (the certificate status is verified via CRL checking). Only if workstation is online. This CRL check can be configured with an ActivClient policy
Signing Certificate displayed name	Certificate friendly name (depends on the certificate propagation method)
Hash algorithm	SHA-1 (always – not configurable through ActivClient)

Note

The security profile is updated only if the user certificates are updated. It is not updated if only the profile policies (such as "Add digital signature to outgoing messages") are updated.

Encryption certificate selected	The selected certificate is the most recent certificate (the most recent Valid From date) from the smart card that verifies the conditions: • Key usage - the certificate key usage must contain the value “Key Encipherment” • Extended Key usage - the certificate extended key usage must contain the value "Secure Email" or "<All>" • Validity - current date being between Valid From and Valid To date • User account (only if workstation is online) - the certificate email address corresponds to the email address configured for the Exchange account. The comparison is performed by retrieving the email address in the certificate from the subjectaltName attribute, or if missing, from the “E=” value in the subject attribute. On the Exchange side, the comparison is performed by checking all email addresses defined in the Exchange account (prefixed by “SMTP:” or “smtp:”). This allows supporting email aliases • The certificate is valid (the certificate status is verified via CRL checking). Only if workstation is online. This CRL check can be configured with an ActivClient policy
Encryption certificate displayed name	Certificate friendly name (depends on the certificate propagation method)
Encryption algorithm	3DES (always – not configurable through ActivClient)
‘Send these certificates with signed message’ check box	Checked (always – not configurable)
Automatically add sender’s certificates to Outlook Contacts	Value configured in ActivClient MS Outlook Usability Enhancements setting “Automatically add sender’s certificates to Outlook Contacts”. Default is enabled.
Outlook Auto-Contact Destination Folder	Value configured in ActivClient MS Outlook Usability Enhancements setting “Outlook Auto-Contact Destination Folder”. Default is “Contacts” folder.
Automatically decrypt encrypted e-mails	Value configured in ActivClient MS Outlook Usability Enhancements setting “Automatically decrypt encrypted e-mails”. Default is disabled.
Add Outlook Security icons in the compose e-mail windows	Value configured in ActivClient MS Outlook Usability Enhancements setting “Add Outlook Security icons in the compose e-mail windows”. Default is enabled. Applicable to MS Outlook 2000 and MS Outlook 2002 only.

Note

The security profile is updated only if the user certificates are updated. It is not updated if only the profile policies (such as "Add digital signature to outgoing messages") are updated.

Publish Certificate to GAL

The ActivClient Publish Certificate to GAL feature consists of publishing the user's encryption certificate used for secure e-mail to the user's object in the Active Directory. This allows other Exchange users using Outlook or Outlook Web Access to automatically access the encryption certificate to send the user encrypted emails.

The feature is the equivalent of the “Publish to GAL” option that can be found on the Outlook Security tab of the Options dialog box (Outlook 2003) or in the Trust Center (Outlook 2007).

Profile Selection and Email Account

The email account selection is the same as for the security profile update: applicable to Exchange accounts (that is, not applicable for Outlook accounts configured for a third-party server or using a POP3 configuration).

Configuration

The “Automatically publishes certificates to the Global Address List” setting is applicable only if the setting “Setup Email certificates in Outlook on card insertion” is enabled (that is, to enable ActivClient Publish to GAL, the administrator must configure both settings to 1).

The setting is disabled by default.

Workflow

On card insertion, the certificate publication to the GAL is executed after the Outlook security profile automatic update:

If the smart card content is appropriate, the Outlook security profile is updated (see "Security Profile Updated Values" on page 147), then, if the Publish to GAL feature is enabled, ActivClient publishes the user's encryption certificate that has been set in the Outlook security profile to the GAL by updating the certificate in the following locations:

- The userSMIMECertificate attribute of the user's object in Active Directory (certificate in PKCS #7 format):
  - This attribute (defined in RFC 2798) contains the user’s S/MIME configuration; it is multi-valued and includes the user’s encryption certificate and the user’s signature certificate (all certificate chains).
  - ActivClient Publish to GAL will erase the content of this attribute and publish the user’s encryption and signature certificates.
  - ActivClient Publish to GAL has the same result as the native Outlook “Publish to GAL” feature.

Note

In full Microsoft environments (that is, using Windows-based CA), the Active Directory attributes are automatically updated when the certificates are created.

In this case, the ActivClient Publish to GAL and the Outlook Publish to GAL features are not necessary. On the contrary, they could lead to mismatched certificates. This is why the ActivClient Publish to GAL feature is disabled by default.

- The userCertificate attribute of the user's object in Active Directory (certificate in DER encoded format):
  - This attribute is multi-valued. It may contain all user certificates (signature, encryption, logon, EFS, etc) if certificates are issued by Microsoft CA.
  - The native Outlook “Publish to GAL” feature adds the encryption certificate without deleting earlier values – which may lead to multiple encryption certificates, and to issues in some configurations.
  - ActivClient Publish to GAL will erase the content of this attribute and publish the user’s encryption certificate. This behavior, different from the native Outlook behavior, guarantees that the Active Directory configuration is the same as the local configuration, therefore ensuring email exchanges with the latest configuration.

Once the certificate is published, any other online Exchange user (accessing the GAL) can send an encrypted email without having configured the contact information to set the encryption certificate prior to sending the email.

If the user cancels the PIN code prompt (that might display for the userSMIMECertificate attribute), no certificates are published to GAL – neither in the userSMIMECertificate attribute nor the userCertificate attribute.

If errors occur during the Publish to GAL, they are reported in the Windows Event Viewer of the user workstation – no error message is displayed to the user.

For further information, see "Audit" on page 152.

Environment Considerations

- Users must have permission to update their Active Directory object. This implies that:
  - Cases where the email account is configured for a different user name than that of the Windows account user are not supported.
  - If the user is not authenticated to Active Directory, the Publish to GAL will fail.
- If the Exchange server is configured in cached mode, there might be a delay up to 24 hours before OWA users can access the updated GAL.

Interactive Process

In addition to the Publish to GAL operations described above (performed in the background on card insertion), an option is available in the ActivClient User Console (in the Tools, Advanced menu) that provides a similar feature which.

- Performs both the Outlook profile configuration and the Publish to GAL as described above (whether these features are enabled or disabled in the ActivClient configuration).

Notes

- In order to limit the write operations to the directory, ActivClient first reads the attributes to check if an update is needed (that is, it verifies that the certificate(s) is the same as the one(s) configured in the local Outlook security profile).
- The smart card is used to sign the certificates in a PKCS#7 format (for the userSMIMECertificate attribute).
  Depending on the PIN caching policy, the user might see a PIN prompt when the certificate is published to Active Directory. This happens only if there is a certificate change; it does not happen if the certificates published in Active Directory do not need to be updated.
- If you enable the ActivClient feature, Publish to GAL, then you might want to disable the Outlook Publish to GAL feature. This will avoid conflicting updates of Active Directory for the userCertificate attribute. You can do so using an Outlook policy; see the Microsoft documentation for details.

- Displays success or errors via dialog boxes (in addition to the Event Viewer).
- If necessary, it prompts the user to authenticate to the Active Directory.
- The CRL checks follow the same configuration options as used in the automatic mode.

Audit

ActivClient enables the auditing of the two operations described earlier: Outlook security profile configuration and Publish certificate to GAL.

ActivClient audits the successes and failures of these operations and logs them in the Windows Event Viewer.

To be notified of unexpected events, we recommend filtering the audited information using the Event Viewer filters.

By default, the ActivClient auditing function is enabled. To disable the option, see "Enable audit for Outlook security profile creation and Publish to GAL" on page 43.

The ActivClient events are formatted following Microsoft logging guidelines and are:

- On Windows XP:
  - Logged in the Application section of the Windows Event Viewer display
  - Labeled with ActivClient as the Source
- On Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008:
  - Logged in the ActivIdentity section of the Applications and Services Logs of the Windows Event Viewer
  - Labeled with ActivClient as the Source

Each event contains the following elements:

- Event Type:
  - Information
  - Warning
  - Error
- Event ID

  For the complete list of ID codes, see Table7.2 on page 153.
- Event Description

  Specifies the username and domain; and reason of failure when applicable.

Note

You can also audit changes performed directly in Active Directory (changes performed during the Publish to GAL operation).

To do so, on the domain controller, open the "Default Domain Controller Security Settings", Security Settings, Local Policies, Audit Policy, and enable "Audit directory service access".

Then, for each user, specify the attributes that should be audited: open the Advanced Security Settings for the user, Auditing tab, and select "Write userSMIMECertificate" and "Write userCertificate".

For further information, see the Microsoft documentation.

Table 7.2: Audited Event ID Codes

Message ID	Event Type	Category	Description
257	Information	Outlook Profile Update	Outlook security profile updated
258	Information	Publish to GAL	Publish to GAL completed
513	Warning	Outlook Profile Update	No update applicable
514	Warning	Publish to GAL	No update applicable
515	Warning	Outlook Profile Update	CRL check failed for signing certificate for the following reason: Revoked, Offline, or Other
516	Warning	Outlook Profile Update	CRL check failed for encryption certificate for the following reason: Revoked, Offline, or Other
517	Warning	Publish to GAL	CRL check failed for signing certificate for the following reason: Revoked, Offline, or Other
518	Warning	Publish to GAL	CRL check failed for encryption certificate for the following reason: Revoked, Offline, or Other
519	Warning	Outlook Profile Update	Impossible to reach Active Directory
520	Warning	Publish to GAL	Impossible to reach Active Directory
521	Warning	Publish to GAL	Your certificates were not published to the Global Address List.To publish successfully, start the Publish to GAL operation again, and enter the PIN when prompted to do so.
769	Error	Outlook Profile Update	No Exchange account
770	Error	Outlook Profile Update	No valid certificate found
771	Error	Outlook Profile Update	No valid email address in signing certificate
772	Error	Outlook Profile Update	No valid email address in encryption certificate
773	Error	Publish to GAL	Access Denied
774	Error	Outlook Profile Update	CRL check failed for signing certificate for the following reason: Revoked, Offline, or Other
775	Error	Outlook Profile Update	CRL check failed for encryption certificate for the following reason: Revoked, Offline, or Other
776	Error	Publish to GAL	CRL check failed for signing certificate for the following reason: Revoked, Offline, or Other
777	Error	Publish to GAL	CRL check failed for encryption certificate for the following reason: Revoked, Offline, or Other
778	Error	Publish to GAL	Your certificates were not published to the Global Address List. MAPI error code

Auto-Contact

When the “Automatically add sender’s certificates to Outlook Contacts” policy is enabled (see page 45), ActivClient enables saving your contact certificate to your Outlook account.

When you receive a signed email, the encryption email of the sender is attached to the email – when you open this email, ActivClient allows you to automatically save this certificate to the “Contact” associated to the sender. This contact is created or updated in a specific Contacts folder that you can also configure: “Outlook Auto-Contact Destination Folder” (see page 45).

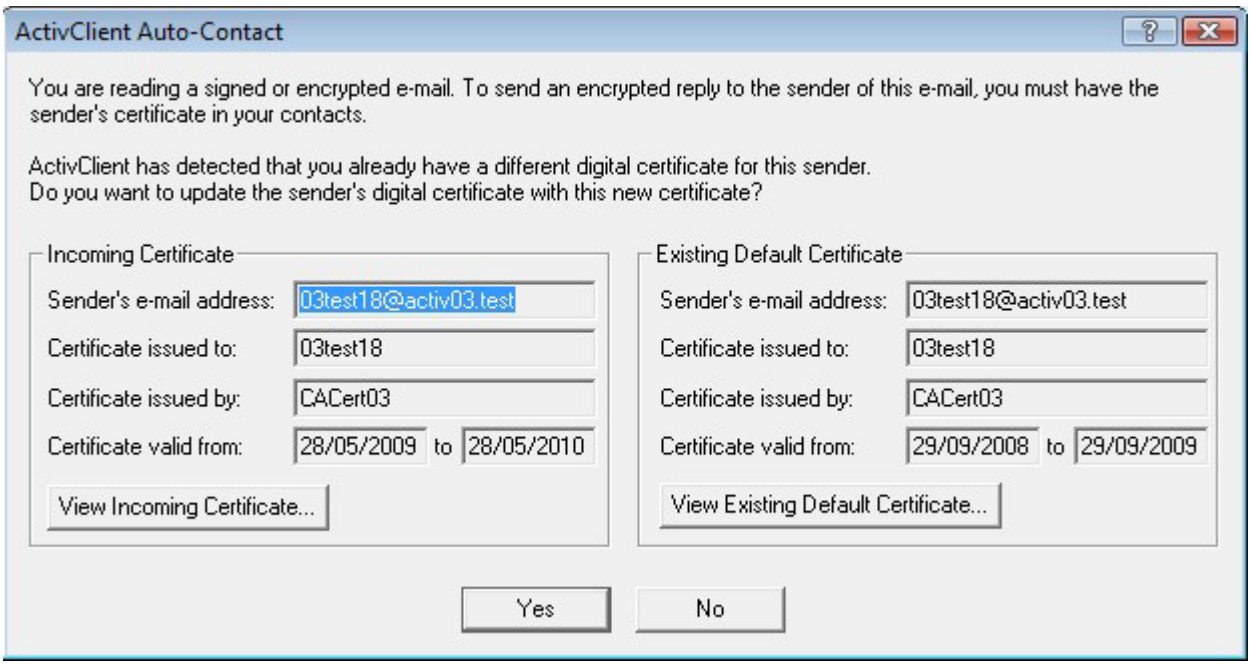
Depending on the scenario, ActivClient asks the user to confirm the operation:

- Scenario 1: If a contact already exists in the Contacts folder with the same email address and without any associated certificate, the following window is displayed.



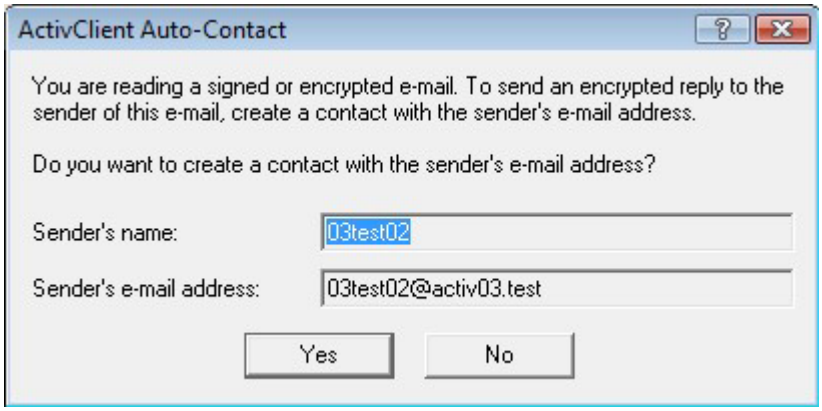
  The user can view the certificate before adding it to the Contacts. It then becomes the default certificate for this contact.

- Scenario 2: If a Contact already exists in the Contacts folder with the same email address and has a default certificate that is different from the received email encryption certificate, the following window is displayed.



The user can easily compare the 2 certificates. By accepting the update, the new certificate is added to the Contact and it becomes the default certificate for this Contact.

- Scenario 3: If a Contact already exists in the Contacts folder with the same email address and has a default certificate identical to the received email encryption certificate, ActivClient does not modify the contact.
- Scenario 4: If there is no Contact in the Contacts folder associated to the received email, the following window is displayed.



The user can confirm that the new Contact should be created in the Contacts folder. If the user accepts and creates the Contact, then another window displays to confirm the addition of the certificate to this user (same as in scenario 1). The

Note

If the signed email that the user receives is encrypted as well, then ActivClient needs to decrypt the email first in order to determine if the email is signed, and if the add-to contact is applicable.

A PIN prompt might then display in order to decrypt the email and access the sender's certificate. Depending on ActivClient PIN caching configuration, PIN authentication might be required several times.

user can view the certificate before accepting that it is added to the Contact. It then becomes the default certificate for this Contact.

Auto-Decrypt

When the “Automatically decrypt encrypted e-mails” policy is enabled (see page 46), ActivClient saves a decrypted version of encrypted emails in order to provide access to the email later, even when the decryption key is no longer available. This feature is specifically useful for deployments that do not have a key backup and recovery mechanism in place.

The auto-decryption process is as follows:

1. User opens the received encrypted email.
2. Email and attachment are decrypted (it might require PIN authentication).
3. A decrypted copy of the encrypted email is saved in the current folder. Any, email digital signature is preserved.
4. The encrypted version of the email is moved to the Deleted Items folder.

These steps apply to the initial email, regardless of its location, including when the initial email is in the Deleted Items folder. In the latter case, both the decrypted and encrypted versions of the email are located in the Deleted Items folder at the end of the process.

Note

Depending on ActivClient PIN caching configuration, PIN authentication might be required several times.

Chapter 8: PIN Caching Service

In This Chapter

157 Overview
158 Enabling or Disabling PIN Caching
159 Per Session or Per Process PIN Caching
161 PIN Cache Timeout
163 Force PIN Re-authentication
165 Application Lists

The purpose of ActivClient PIN Caching service is to enable users to use the smart card without entering the PIN for every card operation, while preserving the security of the smart card solution.

ActivClient PIN Cache is configurable to enable customers to determine the best compromise between security (more PIN prompts) and usability (less PIN prompts), as needed for their specific business requirements.

Chapter 2 provides a list of the policies relevant to PIN Cache configuration (starting on page 31). This chapter provides more in-depth information about this ActivClient component.

Overview

To provide two-factor authentication, most smart card operations are PIN-protected: users need to have the card, and know the card PIN, in order to use the card.

Some smart card middleware leave the card open after a PIN entry, meaning that any application can then use the card without the user entering the PIN again. This provides a high level of usability (only one PIN entry is required until the card is removed from the reader), but lacks in terms of security. For example, a virus or Trojan horse could use the card to perform an authentication to a secure site, or sign a financial transaction, or decrypt sensitive documents – without the user's consent or even knowledge. Non repudiation cannot be guaranteed.

Other middleware might "close" the card after each operation, meaning that once the user has entered the PIN and the card operation has been performed (for example an authentication to a secure site), the card is closed. The user will need to enter the PIN again for the next card operation: access to another site, sign a transaction, etc. As some functional operations require several actual card operations (for example, a Windows smart card logon requires four digital signatures), this can easily lead to repeated PIN prompts, causing user frustration. This model is very secure, but highly inconvenient to the user.

ActivClient PIN cache has been designed to address these two concerns:

- The PIN authentication status is reset (that is, the card is closed) after the user has authenticated to the card with the PIN, the PIN entry could be in ActivClient user interface or in a third-party interface (such as Windows Logon or Firefox).

- The PIN value is cached securely by ActivClient until the user logs off, the workstation is locked, the workstation shuts down, the card is removed, or the PIN cache timeout is reached.
- ActivClient seamlessly re-authenticates to the card using the cached PIN before each PIN protected operation.
- The PIN authentication status is reset (that is, the card is closed) after each PIN protected operation.
- ActivClient PIN cache includes policies to further customize whether the PIN cache will submit the PIN seamlessly to applications, or whether it will request the user to enter the PIN – this enables a more granular control of the PIN prompts. For example, you can configure ActivClient to force a PIN prompt for specific applications (for example, Microsoft Outlook), or for specific operations (for example, signature operations).

PIN Caching Policy - Detailed Description

This section provides more detailed information on the PIN Caching Service policy, compared to the corresponding section in Chapter 2, "PIN Caching Service" on page 31.

Enabling or Disabling PIN Caching

The default ActivClient behavior is to enable the PIN caching; this provides a higher level of security and usability.

When you disable the ActivClient PIN caching, ActivClient does not cache the PIN and leaves the card open after the PIN authentication – until the user removes the card from the reader, or until an application specifically logs off / disconnects the card.

ActivIdentity highly recommends keeping the PIN caching service enabled.

The ActivClient policies described in this chapter are only applicable if the PIN caching service is enabled.

Policy name: Enable PIN Caching

Description	Avoids PIN re-authentication requests for every operation by allowing PIN caching. When disabled, PIN caching is handled at the smart card level, PIN re-authentication is needed whenever the smart card requires it.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Allow`
Type	DWORD

Per Session or Per Process PIN Caching

ActivClient PIN cache can be configured to apply either per session (this refers to the Windows session) or per process (this refers to a Windows process).

Per session mode (the default configuration) allows all the processes in the user's Windows session to share the same PIN cache (that is, user authentication is required once for the entire session whatever the applications used during the session).

In per process mode, the PIN cache is separate for each Windows process (that is, users need to enter their PIN at least once per process that will use the card).

In both modes, you can further customize the PIN cache behavior for specific applications by using the Include list, Exclude list and Open card list (see the following tables).

Policy name: Allow per-process PIN caching

Description	Allows users to avoid sharing the PIN cache between Windows processes. When the default (No) setting is applied, all Windows processes running in the same Windows session share the same PIN cache.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\AllowPerProcess`
Type	DWORD

Example 1: Per Process Mode

The following steps are an example of processes running on a workstation:

1. Set ‘AllowPerProcess’ to 1.
2. Open Outlook with your smart card inserted.
3. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
4. Send a second signed email, you are not prompted for the PIN because it is already cached.
5. Close Outlook.
6. Open Outlook again.
7. Send a signed email, you are prompted for the PIN again because it is a different Windows process.

The same behavior would occur if one process was Outlook and the other was Internet Explorer (running simultaneously), or if two Internet Explorer processes were running simultaneously.

Example 2: Per Session Mode

The following steps are an example of processes running on a workstation:

1. Set ‘AllowPerProcess’ to 0.
2. Open Outlook with your smart card inserted.
3. Send a signed email, you are prompted for the PIN.
4. Send a second signed email, you are not prompted for the PIN because it is already cached.
5. Close Outlook.
6. Open Outlook again.
7. Send a signed email, you are not prompted for the PIN because it is cached and shared between processes.

Example 3: Per Session Mode

The following steps are an example of processes running on a Microsoft Terminal Server and on a user workstation:

1. On the user workstation and on the server, set 'AllowPerProcess' to 0.
2. Open Outlook on the workstation, with your smart card inserted.
3. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
4. Send a second signed email, you are not prompted for the PIN because it is already cached.
5. Close Outlook.
6. Open the session to Terminal Server. In this remote session, open Outlook.
7. Send a signed email, you are prompted for the PIN again because it is cached only for the local workstation. ActivClient running on Terminal Server has a separate Windows session with its separate PIN cache.

PIN Cache Timeout

Whether the PIN cache is configured per session or per process, the PIN cache is set to expire after a period of smart card inactivity. This is designed to guarantee that, if a user leaves their desk without locking their workstation, an intruder would not be able to perform any PIN-protected operation with the smart card.

The timeout corresponds to the period (in minutes) without any PIN protected operation performed on the smart card. When the timeout expires, the PIN is deleted from the PIN cache. The user will be prompted for the PIN at the next PIN-protected operation.

Note that the timer is reset each time a PIN protected operation occurs.

Policy name: Number of minutes before PIN cache is cleared

Description	Defines the number of minutes before PIN cache is cleared.
Values	15 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Minutes`
Type	DWORD

Exceptions:

- 'Minutes'=0
  When 'Minutes' is set to 0, the expiration is immediate. In this case, the user will see a PIN prompt every time a protected card operation occurs, regardless if the PIN was previously cached. This configuration might cause some issues with applications that manage their own user interface and do not allow ActivClient to prompt the user for PIN authentication as often as needed.

  However, processes in the 'Include' list (described below) have a special behavior when 'Minutes' is set to 0. In this case, the PIN cache reacts internally as if 'Minutes' is set to 0x80000000 and sets an infinite expiry on the credential. The PIN stored in the cache is then only accessible by processes in the 'Include' list. Processes not in the 'Include' list are not able to access the cached PIN. Note that this is required for example by the Windows processes involved in Windows Logon (which performs four digital signature operations and only one PIN prompt is used, displayed by Windows).
- 'Minutes'=0x80000000

  When 'Minutes' is set to 0x80000000, the maximum PIN inactivity period is infinite. In this case, no timer is maintained: the PIN cache is cleared at workstation lock, Windows log off, Windows shutdown, Windows session disconnect, card removal and explicit card logout.

Example: PIN Cache Timeout of One Hour

1. Set 'Minutes' to 60.
2. Open Outlook with your smart card inserted.
3. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
4. Wait for 45 minutes.
5. Send a second signed email, you are not prompted for the PIN because it is already cached.
6. Wait another 45 minutes.
7. Send a third signed email, you are not prompted for the PIN because it is already cached.
8. Wait another 75 minutes.
9. Send a fourth signed email, you are prompted for the PIN because the PIN cache timeout expired and the cached PIN was deleted.

Force PIN Re-authentication

Various policies allow ActivClient to provide access, or deny access, to the cached PIN for certain types of card operations and not for others, offering greater granularity of control when PIN caching is used.

If an organization decides that private key signing operations must be treated in a very secure manner, then setting ‘Sign’=0 forces the user to enter the PIN every time a signing operation occurs, regardless if the PIN is already cached. The same behavior can be specified for private key decryption and other (that is, everything except signing and decryption) PIN-protected operations.

The ‘Sign’ policy means controls access to the cached PIN for digital signature operations. If the policy is disabled (‘Sign’ = 1, the default configuration), then the user will see a PIN prompt depending only on other PIN cache policies (for example, per process, timeout, etc). If the policy is enabled (‘Sign’ = 0), then the user will see a PIN prompt for every digital signature operation.

Policy name: Always prompt for the PIN code before performing any private key signature operation

Description	Forces PIN authentication for any private key signature operation.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Sign`
Type	DWORD

The ‘Decrypt’ policy controls access to the cached PIN for decryption operations. If the policy is disabled (‘Decrypt’ = 1, the default configuration), then the user will see a PIN prompt depending only on other PIN cache policies (for example, per process, timeout, etc). If the policy is enabled (‘Decrypt’ = 0), then the user will see a PIN prompt for every decryption operation.

Note

Per FIPS 201 compliance, for PIV cards used in PIV mode (it does not apply to CAC PIV cards used in GSC-IS mode), the digital signature key is configured for PIN Always.

This means that a user will see a PIN prompt every time the digital signature key is used.

This behavior is enforced in ActivClient. It is independent of this ActivClient PIN cache policy; this means that for PIV cards, the ‘Sign’ policy does not matter; ActivClient will always behave as if ‘Sign’ was enabled (set to 0).

Policy name: Always prompt for the PIN code before performing any private key decryption operation

Description	Forces PIN authentication for any private key decryption operation.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Decrypt`
Type	DWORD

The 'Other' policy controls access to the cached PIN for all other operations requiring a PIN (that is, operations other than digital signature and decryption operations). This applies for example to reading PIN-protected personal information stored on PIV cards. If the policy is disabled ('Other' = 1, the default configuration), then the user will see a PIN prompt depending only on other PIN cache policies (for example, per process, timeout, etc). If the policy is enabled ('Other' = 0), then the user will see a PIN prompt for every PIN-protected operation other than signature and decryption.

Policy name: Always prompt for the PIN code before performing any other operation

Description	Forces PIN authentication for any PIN protected operation except for private key signature and private key decryption operations.
Values	Yes = 0 No = 1(default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\Other`
Type	DWORD

Note

ActivIdentity recommends keeping the default setting (Other = 1). If you enable this option (Other = 0), the user experience might not be acceptable, as some functional operations (1 user click) cause several card-level operations (several read commands), which would cause repeated PIN prompts to display.

Example: Force PIN Re-authentication in Outlook

1. Set 'Sign' to 0, 'Decrypt' to 1 and 'Other' to 1.
2. Open Outlook with your smart card inserted.
3. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
4. Decrypt an encrypted email that you received, you are not prompted for the PIN because it is already cached.

5. Send a second signed email, you are prompted for the PIN because the sign operation is not allowed to access the cache.

6. Decrypt a second encrypted email, you are not prompted for the PIN because it is already cached.

7. Open ActivClient User console.

8. Access the personal information (CAC and PIV cards), you are not prompted for the PIN because it is already cached because it is already cached.

Application Lists

Various policies allow ActivClient to provide access, or deny access, to the cached PIN for specific applications, offering greater granularity of control when PIN caching is used.

Exclude List

Applications listed in the ‘Exclude’ list never have access to the PIN cache, even if the PIN has been already cached by the application itself, and regardless of other ActivClient PIN cache policies. The user needs to provide the PIN for every single PIN-protected operation.

This policy enables organizations to improve the security with regards to specific un-trusted applications.

The complete full path name of the application must be in the ‘Exclude’ list to enable this feature.

In the default configuration, the Exclude policy is disabled and the Exclude list is empty.

Note

Changing the applications listed in the Exclude, Include and OpenCard lists can impact the usability and security of the smart card deployment.

ActivIdentity recommends that you keep the default values for these lists for most deployments.

If you do implement some changes, we recommend that you test them before deployment.

Policy name: Enable "Exclude" application list

Description	Prevents access to the PIN cache by applications listed in the "Exclude" list. Select **Yes** if you want to exclude applications in PIN caching. Then, follow the steps indicated in the next table.
Values	Yes = 1 No = 0 (default)
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Exclude`
Type	DWORD

Policy name: Applications "excluded" from PIN caching

Description	Lists the applications that are not allowed access to the PIN cache. The applications listed behave as if PIN caching was disabled. To exclude applications from PIN caching: 1. Double click on <application list> in the Value column to open the **Applications to be excluded from the PIN caching window.** 2. Click  and, in the row that displays, click the drop-down list. 3. Locate the application you want to exclude and click **Open**. 4. Repeat steps 5 and 6 for each application you want to exclude. 5. When you have finished, click **OK**.
Values	<application list> Each application must be created as a new STRING, under the Exclude registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Exclude\`
Type	REG_SZ

Example: Outlook an "Excluded" (Un-trusted) Application

1. Set Exclude to 1.
2. In Exclude\, create a new STRING with the value *"C:\Program Files\Microsoft Office\Office\Outlook.exe"* (adapt the path name as relevant to your configuration).
3. Set 'Sign' to 1, 'Decrypt' to 1 and 'Other' to 1 (meaning that there is no restriction per card operation type).
4. Open Outlook with your smart card inserted.
5. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
6. Send a second signed email, you are prompted for the PIN again because processes in the 'Exclude' list are never allowed to access the PIN cache.

Include List

Applications listed in the 'Include' list always have access to the PIN cache, regardless of other ActivClient PIN cache policies.

This policy enables organizations to improve the ease of use with regards to specific trusted applications.

The complete full path name of the application must be in the 'Include' list to enable this feature.

In the default configuration, the Include policy is enabled and the Include list contains specific Windows and ActivClient processes that are considered trusted.

Policy name: Enable "Include" application list

Description	Grants permanent access to the PIN cache to applications listed in the "Include" list. Select Yes if you want to include applications in PIN caching and follow the steps indicated in the next table.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Include`
Type	DWORD

Policy name: Applications "included" in PIN caching

Description	Lists the applications that have permanent access to the PIN cache, including in the per-process mode. To include applications in PIN caching: 1. Double click on <application list> in the Value column to open the **Applications "included" in PIN caching** window. 2. Click  and, in the row that displays, click the drop-down list. 3. Locate the application you want to include and click **Open**. 4. Repeat steps 5 and 6 for each application you want to include. 5. When you have finished, click **OK**.
Values	<application list> The following processes are included by default in the "include" application list: • ActivClient User Console (acuscons) • Diagnostics Tool (actswzdg) • ActivClient middleware (accrdsub.exe) • Troubleshooting Wizard (acDiagWz.exe) • Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) Each application is a new STRING, under the Include registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\Include\`
Type	REG_SZ

Important

The Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) do not appear in the Advanced Configuration Manager but are included in the registry.

Do NOT remove them from the Include list, or the Windows Logon process will no longer work.

Exceptions:

- Processes in the 'Include' list also have a special behavior with regards to the PIN cache timeout ('Minutes' registry entry). When 'Minutes' is set to 0, and when we consider a process in the 'Include' list, the PIN cache reacts internally as if 'Minutes' is set to 0x80000000 and sets an infinite expiry on the credential. The PIN stored in the cache is then only accessible by processes in the 'Include' list. Processes not in the 'Include' list are not able to access the cached PIN. Note that this is required for example by the Windows processes involved in Windows Logon (which performs four digital signature operations and only one PIN prompt is used, displayed by Windows).
- The 'Exclude' list has higher priority than the 'Include' list. This means that when a process is part of both 'Exclude' and 'Include' lists, it has the behavior of an 'Exclude' list process and the presence of the process in the 'Include' list is ignored.

Example: Outlook an "Included" (Trusted) Application

1. Set Include to 1 (the default behavior).
2. In Include\, create a new STRING with the value *"C:\Program Files\Microsoft Office\Office\Outlook.exe"* (adapt the path name as relevant to your configuration).
3. Set 'Sign' to 0, 'Decrypt' to 0 and 'Other' to 0 (meaning that all card operations would require a PIN prompt).
4. Open Outlook with your smart card inserted.
5. Send a signed email, you are prompted for the PIN, and you type the correct PIN.
6. Send a second signed email, you are not prompted for the PIN because processes in the 'Include' list are always allowed to access the PIN cache.

OpenCard List

Applications listed in the 'OpenCard' list are allowed within a limited period (two seconds) to perform successive PIN protected operations without resetting the card authentication status (that is, without "closing" the card) after each operation. The authentication state of the card is actually reset (the card is "closed") following a period of two seconds without any card operation.

This policy improves the performance of certain critical and trusted applications that perform many protected card operations in a very short period of time (such as the Windows Logon process).

The complete full path name of the application must be in the 'OpenCard' list to enable this feature.

In the default configuration, the OpenCard policy is enabled and the OpenCard list contains specific Windows processes that are considered trusted and that require multiple card operations without intermediate PIN prompts.

Policy name: Enable "OpenCard" application list

Description	Allows users to enable OpenCard optimization. Applications listed in the Optimized PIN caching list can perform several card-based operations in a short time (2 seconds) without the need for multiple PIN prompts. Select **Yes** if you want to enable “OpenCard” applications list. Then, follow the steps indicated in Applications “optimized” for PIN caching next table.
Values	Yes = 1 (default) No = 0
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\OpenCard`
Type	DWORD

Policy name: Applications "optimized" for PIN caching

Description	Allows a user to select one or several more applications to be optimized for PIN caching. To enable the “OpenCard” applications list: 1. Double click <Application list> in the **Value** column to open the **Applications “optimized” for PIN caching** window 2. Click  and, in the row that displays, click the drop-down list. 3. Select the application you want to optimize and click **Open**. 4. Repeat for each application you want to optimize. 5. Click **OK**.
Values	<Application list> The following processes are included by default in the “optimized” application list: Microsoft Winlogon processes (lsass, lsass_mount, winlogon, winlogon_mount). Each application is a new STRING, under the OpenCard registry key.
Registry Key	`HKEY_LOCAL_MACHINE\Software\GSC\Policies\PIN\Authentication\ActivCard\OpenCard\`
Type	DWORD

Important

The Microsoft Winlogon processes (lsass_mount, winlogon, winlogon_mount) do not appear in the Advanced Configuration Manager but are included in the registry.

Do NOT remove them from the OpenCard list, or the Windows Logon process will no longer work.

Example: Winlogon is in the OpenCard List

1. Keep all ActivClient PIN cache policies to their default values; this includes OpenCard set to 1.
2. *"C:\WINNT\System32\winlogon.exe"* is registered in the 'OpenCard' list.
3. Perform a Windows smart card (PKI-based) logon operation, enter the PIN at the Windows prompt.
4. winlogon.exe performs several signature and decryption operations during the logon and the card authentication status is not reset between the operations in order to increase performance.
5. Two seconds pass before the Windows desktop is fully enabled and the authentication state of the card is reset.
6. Open Outlook with card inserted.

7. Send a signed email, you are not prompted for the PIN because it is already cached.

8. The card is reset after the sign operation.

Chapter 9: Auto-Update with ActivID CMS

In This Chapter

173 Overview
174 Configuration
174 Card Auto-Update Policies
180 Card Auto-Update Experience

The purpose of ActivClient Smart Card Auto-Update feature is to automate updating the smart card content, for cards managed by ActivID Card Management System (CMS). This removes the need for administrators to send emails to end users, asking them to click on a link in order to access the CMS self help portal.

Overview

ActivClient Smart Card Auto-Update is a component providing a high level of integration with ActivIdentity card management system: ActivID CMS version 4.2 and higher. When card updates are available in CMS (for example, a replacement certificate for a certificate about to expire, or the addition of new certificates on the card), administrators would typically need to inform users to access CMS self help portal; this would traditionally be achieved by sending emails to end users, with a link to the relevant URL. This model has its limits, as it requires users to actually read emails, and to click on the URL when they are connected to the corporate network.

The smart card auto update component automates the process: when a smart card is inserted, ActivClient automatically contacts CMS to determine if a card update request is available for the smart card. This process happens on a regular basis (by default, weekly), to guarantee that updates happen in a timely manner. If no update is available, there is no disruption to the user: the process happens behind the scenes. If an update is available, ActivClient lets the user decide if the update should be performed or not.

For example, if the user is about to disconnect from the network, about to remove the card, or if it's just "a bad time", ActivClient offers to cancel the update. In this case, ActivClient will offer the update again a bit later (after the next card insertion).

If the user is ready to perform the update, ActivClient opens a window connected to the CMS self-help portal. The user can then authenticate and easily perform the card update. At the end of the process, the card is ready for usage with the updated content, and with minimal disruption to the user's activities.

In addition, users can start this card update process from the ActivClient User Console (from the Tools, Advanced menu). This provides a mechanism to connect to CMS to check for card updates without waiting for the recurrent (weekly) automatic check. This capability is mostly designed for troubleshooting purposes.

Configuration

If an organization intends to use the card auto-update feature, they should follow these steps:

1. Configure CMS to enable the card auto-update (see the CMS technical documentation).
2. Install the ActivClient "Card auto-update with ActivID CMS" feature on user workstations (it is not installed in the default ActivClient setup).
3. Configure the ActivClient policies described in "Client Card Auto-Update Configuration" on page 174 and "CMS Connection Configuration" on page 178.
4. Configure the user workstations to support CMS self help portal (My Digital ID Card). See the CMS documentation for details for the following steps.
   a. Install the CMS root certificates on the user workstations.
   b. Install the CMS Synchronization Client (ActiveX control) on the user workstations.

      You can do this either in advance (for example, installing the ActiveX at the same time you install ActivClient), or you can automatically install the ActiveX component when the user first accesses CMS My Digital ID Card (this might not be possible depending on your workstation configuration - for example, if users do not have local administrative privileges, they migt not be able to install the ActiveX component - the specific behavior depends on the user's access rights, Windows UAC configuration and Internet Explorer version and security configuration).

Card Auto-Update Policies

This section provides detailed information on the Smart Card Auto Update policy, compared Chapter 2, "Smart Card Auto-Update" on page 72.

Prerequisite

The Smart Card Auto-Update is only available if "Enable smart card discovery information caching" on page 76 is enabled.

Client Card Auto-Update Configuration

When the "Card auto-update with ActivID CMS" component is installed during ActivClient setup, it:

- Installs components specific to the card auto-update feature.
- Configures the "Enable Card Auto-Update" policy to Enabled.
- Configures the "Display Check for Card Update menu" policy to Yes (see "Display Check for Card Update menu" on page 52).

However, card auto-update is operational only after you configure the CMS connection information with the data specific to your environment.

Policy name: Enable Card Auto-Update

Description	Enables ActivClient to automatically check if inserted smart cards can be updated with card content updates available in the ActivID Card Management System. Starts the smart card update process if updates are available.
Values	0: Card auto-update is disabled (default) 1: Card auto-update is enabled
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\Enabled`
Type	DWORD

The ActivClient card auto-update feature contacts CMS to check if a card update request is available for the inserted smart card. This check starts shortly after card insertion.

For corporations that use the smart card for Windows Logon, we expect that many users will insert their card at about the same time, when they arrive at their desk and connect to the network (between 8am and 9am). As many processes start at Windows Logon, they compete for resources. To avoid this resource constraint, ActivClient delays the connection to CMS by a few minutes. Also, to avoid overloading CMS with too many simultaneous connections, ActivClient automatically spreads the load: ActivClient will contact CMS after a randomized number of minutes after card insertion; this random number is between 0 (that is, at card insertion) and a configurable number. The default is 120 minutes (two hours), which means that ActivClient will contact CMS between 0 and 120 minutes after Windows Logon.

We recommend selecting the maximum value between five minutes and 120 minutes. If a value higher than 120 minutes is selected, we expect that many users will remove their card from the reader before ActivClient connects to CMS, therefore losing the opportunity to check for a card update.

If the user removes the card before the check is performed, then the process happens again at the next card insertion - with a different random delay.

Policy name: Maximum delay for card update check after Windows Logon

Description	ActivClient contacts CMS to determine if smart card updates are available a few minutes after Windows logon. To spread the requests received by CMS, this delay is a random value - between 0 and the maximum delay defined in this policy (in minutes). Recommended values are between 5 and 120.
Values	120 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMaximumDelayAtLogin`
Type	DWORD

For corporations that do not use the smart card for Windows Logon, we expect that the smart card will be inserted only for few minutes, that is only when the smart card-enabled application is used (for example, VPN client for smart card authentication, email client for email signature / decryption, internet browser for secure web access). To cater for this type of use cases, ActivClient uses another policy to define when to contact CMS: ActivClient checks if card updates are available after a randomized number of minutes after card insertion. This random number is between 0 (that is, at card insertion) and a configurable number. The default is five minutes, which means that ActivClient will contact CMS between 0 and five minutes after card insertion.

We recommend selecting the maximum value between one minute and ten minutes. If a value higher than ten minutes is selected, we expect that many users will remove their card from the reader before ActivClient connects to CMS, therefore losing the opportunity to check for a card update.

If the user removes the card before the check is performed, then the process happens again at the next card insertion - with a different random delay.

Note

This policy also includes the case of a card used for Windows screen unlock.

Policy name: Maximum delay for card update check after card insertion

Description	ActivClient contacts CMS to determine if smart card updates are available a few minutes after a smart card is inserted. This delay is a random value - between 0 and the maximum delay defined in this policy (in minutes). Recommended values are between 1 and 10.
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMaximumDelayAfterCardInsertion`
Type	DWORD

ActivClient includes a policy to define the frequency to check for card updates. The default value is seven days, which represents a weekly check.

When the number of days has passed, ActivClient will contact CMS a few minutes after card insertion - delay defined in the policies described above. If the card is removed before the check happens, or if CMS is not available, or if the user cancels the card update request, then ActivClient will contact CMS again at the next card insertion (after the usual delay).

If ActivClient manages to contact CMS, and if there is no update request available, ActivClient resets the "counter" for the frequency. The next check will be performed a week later.

If ActivClient manages to contact CMS, where an update is available, and if the user proceeds with the card update, then ActivClient resets the "counter" for the frequency. The next check will be performed a week later.

If ActivClient manages to contact CMS, where an update is available, but if the user does not proceed with the card update, then ActivClient will repeat the process at the next card insertion (after the usual delay).

Policy name: Frequency of update

Description	Frequency (in days) of smart card update checks.
Values	7 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\UpdateFrequency`
Type	DWORD

CMS Connection Configuration

To use the ActivClient card auto-update feature, you need to configure the connection information for your ActivID CMS installation: the connection URL.

Until this URL is defined, the card auto-update will not operate.

Policy name: CMS Server URL

Description	Connection URL for the CMS server (see the ActivIdentity CMS documentation). The port number is included in the URL. Example: http://www.mycompany.com:89898
Values	None
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerServerURL`
Type	STRING

The following policies configure additional CMS connection parameters. The default values apply to most configurations. For further information, see the CMS technical documentation.

If CMS does not answer the "CMS check" request sent by ActivClient (timeout reached, defined by "CMS Synchronization Manager timeout"), then other connection attempts are performed (the number of attempts is defined by "CMS Synchronization Manager retry"). The attempts are performed immediately after failure. If the multiple attempts fail, then they will be restarted at the next card insertion.

Policy name: CMS Synchronization Manager timeout

Description	Maximum time (in seconds) allocated to check with CMS if smart card updates are available
Values	5 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerTimeout`
Type	DWORD

Policy name: CMS Synchronization Manager retry

Description	Number of attempts to connect to the CMS Synchronization Manager after timeout.
Values	2 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSSyncManagerRetry`
Type	DWORD

If ActivClient manages to contact CMS, and identifies that a card update request is available, ActivClient opens a window connecting to CMS My Digital ID Card (MDIDC). If the card update in MDIDC is not performed after a certain time (CMS MDIDC timeout), then the update is not done. There is no repeated attempt performed that would disrupt the user. The next attempt will be performed at the next card insertion.

Policy name: CMS MDIDC timeout

Description	Maximum time (in seconds) allocated to perform a smart card update using CMS My Digital ID Card. When this timeout is reached, the process started to run the browser is terminated.
Values	600 (default)
Registry Key	`HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Auto Update\CMSMDIDCTimeout`
Type	DWORD

Card Auto-Update Experience

When ActivClient has detected that a card update request is available, and when the user accepts the card update, ActivClient opens a window connecting to CMS My Digital ID Card (MDIDC).

When the card update process is running, the user should make sure that they:

- Do not use the card for operations (such as email signature).
  Such card requests will be automatically be blocked until the card update process is complete.
- Do not lock the screen or logoff until the process is complete.
- Do not remove the card until the process is complete.

When the card update is complete, MDIDC informs the user that he should remove and re-insert the card in order to use it. This operation guarantees that all ActivClient and Windows components are aware of the new credentials present on the card. For example, if the Windows Logon certificate is updated, removing and re-inserting the card publishes the new certificate to the Windows CAPI store, a requirement for a successful Windows Logon.

Chapter 10: Troubleshooting

The chapter describes the ActivClient troubleshooting tools and suggested strategies.

In This Chapter

181 ActivClient Troubleshooting Tool
181 ActivClient Diagnostics Wizard
182 Advanced Customer Support Logging
182 Check Common Issues and Known Problems
182 Analyze Symptoms and Factors
183 Isolate the Error Condition and Reproduce the Error
183 Ask for Technical Support Resources

ActivClient Troubleshooting Tools

ActivClient Troubleshooting Tool

The ActivClient Troubleshooting Tool helps users solve common installation and usage issues, such as:

- Reader not connected
- Smart card inserted incorrectly
- No reader driver installed

This tool can be accessed from the ActivClient User Console or the Start menu.

For more information, see the *ActivClient for Windows User Guide*.

ActivClient Diagnostics Wizard

The ActivClient Diagnostics wizard provides advanced information for the help desk and administrators, such as

- Operating system, browser and service pack versions
- Smart card reader presence tests
- Smart card health-check tests
- List of installed ActivClient files and registry entries

The output of the diagnostics can be viewed on the screen, printed, saved to a file, or sent by email.

The Advanced Diagnostics tool is available from the ActivClient User Console, the ActivClient Agent left or right-click menu, or the Start menu.

For more information, see the *ActivClient for Windows User Guide*.

Advanced Customer Support Logging

To help diagnose problems, you can configure ActivClient to generate log files. You can enable it using either:

- **User Console** - from the **Tools** menu, select **Advanced** and the **Log File Options**
- **Advanced Configuration Manager** - configure the **Logging** settings

Log files do not require any change in installed DLLs and do not compromise the system's security - PIN code and personal information are never exposed.

Troubleshooting Strategies

To troubleshoot a problem in ActivClient, follow these basic steps:

1. "Check Common Issues and Known Problems" on page 182
2. "Analyze Symptoms and Factors" on page 182
3. "Isolate the Error Condition and Reproduce the Error" on page 183
4. "Ask for Technical Support Resources" on page 183

Check Common Issues and Known Problems

To check common issues and known problems, consider the following:

- Check to see if your problem was reported in the `ActivClient ReadMe.htm` of your original ActivClient distribution.
- Check the ActivIdentity web site for the latest support information.

Analyze Symptoms and Factors

To analyze the conditions of the error, consider the following questions:

- Has the default configuration been modified from the original installation?
- Has the system ever worked? Is there a similar working system in the same environment?
- Are the operating system and service packs listed in the ActivClient supported configurations?
- Which ActivClient previous version has the system been upgraded with?
- Is there another application using the smart card?

- Does the error depend on the smart card being used?

Isolate the Error Condition and Reproduce the Error

To isolate and, if possible, reproduce the error, consider the following checklist:

- Run the **Troubleshooting** wizard and apply suggestions.
- Run the **Advanced Diagnostics** wizard, save the result file, and compare the same output with a reference identical working platform.
- Restore the default registry settings and try again.
- Replace the smart card reader.
- Try another smart card.
- Consider removal and reinstallation of ActivClient and try again.

Ask for Technical Support Resources

Run the **Advanced Diagnostics Wizard**, save the result file, and contact your ActivIdentity reseller's technical support organization for analysis.

Chapter 11: Customizing the Help File

In This Chapter

184 Extract the HTML Files
187 Create a New Help Project
187 Configure the Context-Sensitive Controls
194 Integrate Customized Help

The ActivClient Help file is provided in the .chm format and accessible from various ActivClient user interfaces, such as the User Console or the Advanced Diagnostics tool.

As well as the standard HTML files, the Help also contains context-sensitive content linked to ActivClient functions.

The Help can be fully customized, from the actual content to the look and feel of the pages. You can customize some ActivClient help pages to match your internal processes (for example, you can customize the smart card unlock help page to describe your own help desk process).

You can also customize the dimensions of the Help viewer if necessary.

To customize the Help file, you can either create a version from scratch based on your organization's requirements, or you can modify the existing files.

The following sections explain how to:

- "Modify the Existing ActivClient Help" on page 184
- "Configure the Context-Sensitive Controls" on page 187
- "Integrate Customized Help" on page 194

While the creation of a Help system from scratch is outside the scope of this guide, the context-sensitive and integration procedures must still be applied.

Modify the Existing ActivClient Help

Extract the HTML Files

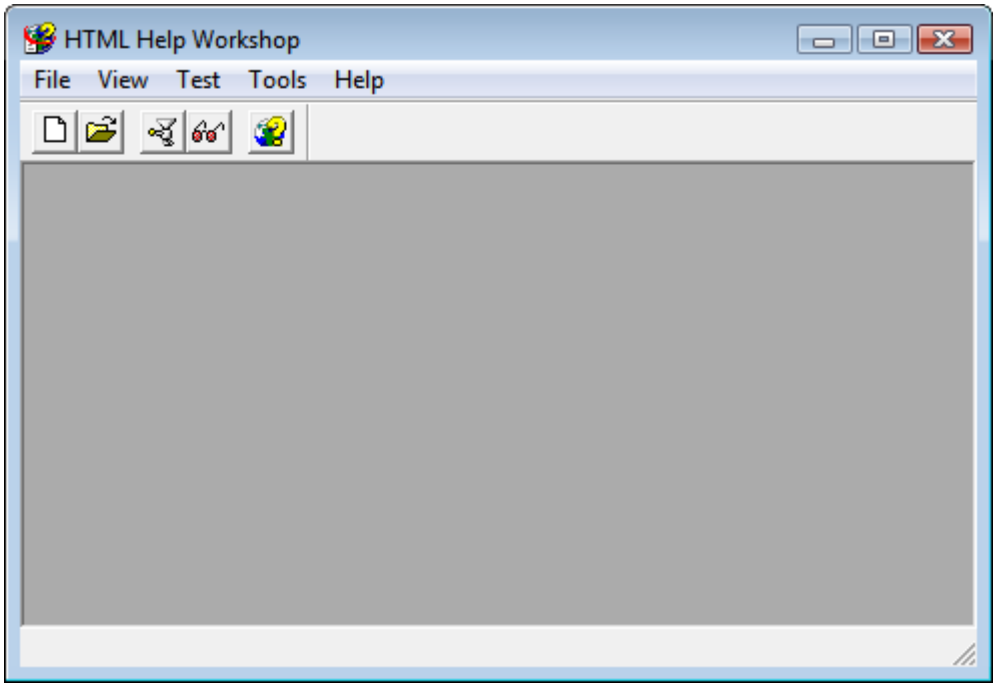
In order to modify the Help, you must first extract (or decompile) the HTML files from the `ActivClient.chm`. During the extraction process, the HTML files are copied to a specified directory without modifying the original help file.

To extract the files, there are several tools available, such as Microsoft's HTML Help Workshop (used as the example in this chapter), and a simple command line switch.

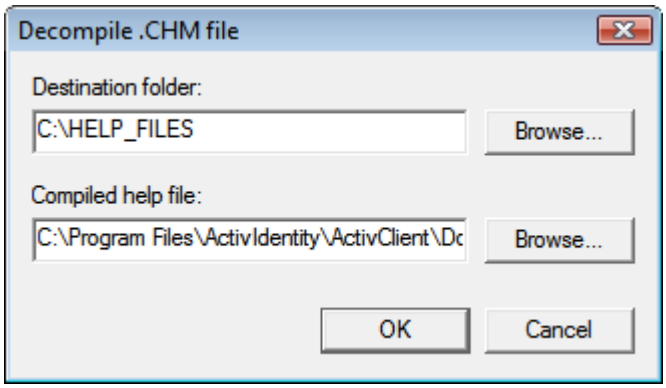
Decompile with HTML Help Workshop

1. Create the destination folder for the decompiled HTML files.

2. From the **Start** menu, point to **All Programs**, **HTML Help Workshop** and click **HTML Help Workshop**.



3. From the **File** menu, click **Decompile...**.



4. In the **Destination folder** field, browse to the folder you created above.

5. In the **Compiled help file** field, browse to the `ActivClient.chm` file in the ActivClient program directory.

HTML Help Workshop

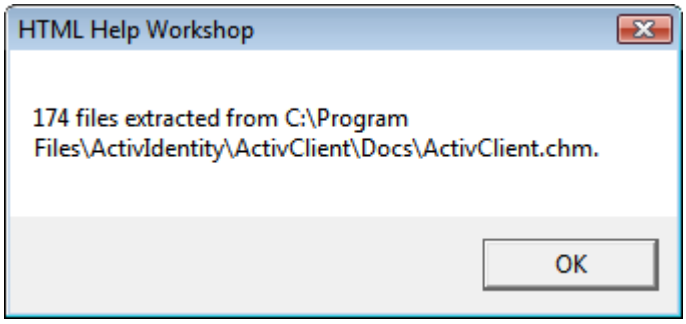
The HTML Help Workshop can be downloaded for free from the Microsoft web site:

http://www.microsoft.com/downloads/details.aspx?familyid=00535334-c8a6-452f-9aa0-d597d16580cc&displaylang=en

By default, this is *C:\Program Files\ActivIdentity\ActivClient\Docs*.

6. Click **OK**.

   The contents of the ActivClient Help are extracted and copied to the specified folder, maintaining the hierarchy established by the table of contents.



   The process also generates the:

   – Table of contents (_Temp.hhc)
   – Index (_Temp.hhk)
   – Glossary (.htm)

   The images and style sheets are organized in the Resources folder.

7. Go to the destination folder and verify that the help file was decompiled successfully.

Decompile from the Command Line

Microsoft Windows operating systems support for HTML Help includes the executable program, **hh.exe**, which does not require the HTML Help Workshop. The executable provides the decompile command to extract the files.

1. Create the destination folder for the decompiled HTML files.

2. Either from a **DOS prompt** or the **Run** command, type:

   ```
   hh.exe -decompile <folder> <chm>
   ```

   where:

   – <folder> is the path to and name of the destination folder for the extracted files.
   – <chm> is path to and filename of the `ActivClient.chm` compiled help file in the ActivClient program directory.
   By default, this is *C:\Program Files\ActivIdentity\ActivClient\Docs*.

For example:

```
hh.exe -decompile c:\Help_Files\ c:\Program
   Files\ActivIdentity\ActivClient\Docs\ActivClient.chm
```

The contents of the ActivClient Help are extracted and copied to the specified folder, maintaining the hierarchy established by the table of contents.

The process also generates the:

- Table of contents (_Temp.hhc)
- Index (_Temp.hhk)
- Glossary (.htm)

The images and style sheets are organized in the Resources folder.

3. Go to the destination folder and verify that the help file was decompiled successfully.

Create a New Help Project

The procedure to import the files into a help project depends on the help authoring tool being used. The key steps are as follows:

1. Create a new help project in the same folder as the extracted files and organize the project folder as required by the tool you are using.
   - The output must be **HTML Help** (that is, a .chm file).
   - The output file must be called **ActivClient.chm**.
2. If you are not using Microsoft HTML Help Workshop, you will also have to build the table of contents and add the topic links.
3. Modify the help content as required.

Note

If you are using HTML Help Workshop, the New Project wizard enables you to specify the extracted table of contents (.hhc) and index (.hhk) files.

Configure the Context-Sensitive Controls

To ensure the ActivClient context-sensitive content works, you need to include an alias and header file in your help project.

- The header file (or map) lists the map names and corresponding numerical IDs for all the content-sensitive controls in a program. The file extension is .h.

  A copy of the ActivClient Help header file, `contexthelp.h`, is provided in the *Admin/Custom Help* folder on the ActivClient distribution.

- The Alias file associates the context-sensitive HTML files with the map and IDs.

  A text file containing the list of aliases, `Alias.txt`, is provided in the *Admin/Custom Help* folder on the ActivClient distribution.

Table 11.1 on page 188 lists the map names, identifiers and linked files of the ActivClient context-sensitive help topics.

Table 11.1: Context-sensitive identifiers and files

Map name	Identifier	Linked file for alias
CHELP_ADVCONF_FRAME	1000	AC_Components/TOPS0702008.htm
CHELP_TRBSHOOTWZ_FRAME	1001	AC_Components/TOPS0702064.htm
CHELP_ADVDIAG_FRAME	1002	AC_Components/TOPS0702009.htm
CHELP_PINCHGTOOL_FRAME	1003	AC_Components/TOPS0702041.htm
CHELP_PININITOOL_FRAME	1004	Managing_your_smart_card_and_its_PIN/PIN_Initialization_Tool/TOPS0702042.htm
CHELP_PININITOOL_NEWPIN	1005	Managing_your_smart_card_and_its_PIN/PIN_Initialization_Tool/TOPS0702042.htm
CHELP_PININITOOL_INIT	1006	Managing_your_smart_card_and_its_PIN/PIN_Initialization_Tool/TOPS0702042.htm
CHELP_PININITOOL_SELECTREADER	1007	Managing_your_smart_card_and_its_PIN/PIN_Initialization_Tool/TOPS0702042.htm
CHELP_PININITOOL_RESET	1008	Managing_your_smart_card_and_its_PIN/TOPS0702051.htm
CHELP_USRCONS_GENOTP	1009	Managing_your_remote_access_One_Time_Password/TOPS0702038.htm
CHELP_USRCONS_CONFGOTP	1010	Managing_your_remote_access_One_Time_Password/TOPS0702013.htm
CHELP_USRCONS_UNLOCKCODE	1011	Managing_your_smart_card_and_its_PIN/TOPS0702065.htm
CHELP_NOTIF_CARDEXPIRATION	1012	Managing_your_smart_card_and_its_PIN/TOPS0702056.htm
CHELP_PINUNLOCK	1013	Managing_your_smart_card_and_its_PIN/TOPS0702066.htm
CHELP_NOTIF_CARDMGRBLOCKED	1014	Managing_your_smart_card_and_its_PIN/TOPS0702057.htm
CHELP_AUTHENT_PIN	1015	Managing_your_smart_card_and_its_PIN/TOPS0702021.htm
CHELP_NOTIF_NOREADER	1017	Managing_your_smart_card_and_its_PIN/TOPS0702045.htm
CHELP_USRCONS_FRAME	1018	AC_Components/ActivClient_User_Console/TOPS0702005.htm

Note

The alias paths to the linked help files in Table 11.1 on page 188 assume that your help project file is stored at the same directory level as the extracted help files. For example, your project file is stored in c:\Help_Files.

If your directory organization differs, you must adjust the alias paths accordingly.

Map name	Identifier	Linked file for alias
CHELP_USRCONS_CERTIFICATES	1019	Managing_your_Digital_Certificates/TOPS0702011.htm
CHELP_USRCONS_PERSODATA	1020	Using_Personal_Information/TOPS0702074.htm
CHELP_USRCONS_RESET	1021	Managing_your_smart_card_and_its_PIN/TOPS0702050.htm
CHELP_CHECKPOINT_LOGONVPN	1022	Using_remote_access_One_Time_Passwords/TOPS0702032.htm
CHELP_CHECKPOINT_CONNECTION	1023	Using_remote_access_One_Time_Passwords/TOPS0702032.htm
CHELP_USRCONS_SYNCOTP	1024	Managing_your_remote_access_One_Time_Password/ TOPS0702062.htm
CHELP_ACAGENT_GENOTP	1025	Using_remote_access_One_Time_Passwords/TOPS0703001.htm
CHELP_USRCONS_INCORRECTPIN	1027	Managing_your_smart_card_and_its_PIN/TOPS0702021.htm

Table 11.2 on page 189 lists the actions required to call each context-sensitive help topic.

Table 11.2: Context-sensitive help call actions

Map name	Identifier	Call action
CHELP_ADVCONF_FRAME	1000	From the Advanced Configuration Manager interface: • Help menu • F1 • Alt+H shortcut • Help icon  in the window title bar Calls the topic describing the Advanced Configuration Manager.
CHELP_TRBSHOOTWZ_FRAME	1001	From the Troubleshooting Wizard interface: • F1 • Help icon  in the window title bar Calls the topic describing the Troubleshooting Wizard and how to diagnose issues.
CHELP_ADVDIAG_FRAME	1002	From the Advanced Diagnostic Tool interface: • Help menu • F1 • Alt+H shortcut • Help icon  in the window title bar Calls the topic describing the Advanced Diagnostic Tool and how to generate reports.

Map name	Identifier	Call action
CHELP_PINCHGTOOL_FRAME	1003	From the PIN Change Tool interface: • F1 • Help icon in the window title bar Calls the topic describing the PIN change procedure.
CHELP_PININITOOL_FRAME	1004	From the PIN Initialization Tool interface: • F1 • Help icon in the window title bar Calls the topic describing the PIN Initialization Tool and how to initialize a smart card.
CHELP_PININITOOL_NEWPIN	1005	From the PIN Initialization Tool interface: • F1 • Help icon in the window title bar Calls the topic describing the PIN Initialization Tool and how to initialize a smart card.
CHELP_PININITOOL_INIT	1006	From the PIN Initialization Tool interface: • F1 • Help icon in the window title bar Calls the topic describing the PIN Initialization Tool and how to initialize a smart card.
CHELP_PININITOOL_SELECTREADER	1007	From the PIN Initialization Tool interface: • F1 • Help icon in the window title bar Calls the topic describing the PIN Initialization Tool and how to initialize a smart card.
CHELP_PININITOOL_RESET	1008	From the PIN Initialization Tool interface when ActivClient detects that the smart card is already initialized: • F1 • Help icon in the window title bar Calls the topic explaining how to reset a smart card using the PIN Initialization Tool.

Map name	Identifier	Call action
CHELP_USRCONS_GENOTP	1009	From the User Console interface when the One-Time Passwords folder is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic explaining how to generate one-time passwords.
CHELP_USRCONS_CONFGOTP	1010	From the User Console interface when the Configure One-Time Password window is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic explaining how to configure the username for remote access.
CHELP_USRCONS_UNLOCKCODE	1011	From the User Console interface when the Unlock card window is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic explaining how to view the unlock code.
CHELP_NOTIF_CARDEXPIRATION	1012	From the smart card expiration notification message: • F1 • Help icon  in the window title bar Calls the topic describing the smart expiration warning message.
CHELP_PINUNLOCK	1013	From the smart card locked notification message: • F1 • Help icon  in the window title bar Calls the topic explaining how to unlock the smart card.
CHELP_NOTIF_CARDMGRBLOCKED	1014	From the smart card manager blocked notification message: • F1 • Help icon  in the window title bar Calls the topic describing the smart card manager blocked status.

Map name	Identifier	Call action
CHELP_AUTHENT_PIN	1015	From the ActivClient PIN authentication prompt: • F1 • Help icon  in the window title bar Calls the topic describing the PIN entry procedure.
CHELP_NOTIF_NOREADER	1017	The **Learn more about this** link in the No smart card reader notification message: Calls the topic describing the no smart card reader detected status.
CHELP_USRCONS_FRAME	1018	From the User Console interface: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic describing the User Console, its menus and toolbars.
CHELP_USRCONS_CERTIFICATES	1019	From the User Console interface when the My Certificates or CA Certificates folder is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic describing digital certificates and how to view certificate information.
CHELP_USRCONS_PERSODATA	1020	From the User Console interface when the My Personal Info folder is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic describing the View *Personal Information feature*.
CHELP_USRCONS_RESET	1021	From the User Console interface when the Reset card window is open: • Help menu • F1 • Alt+H shortcut • Help icon  on the toolbar Calls the topic explaining how to reset a smart card using the User Console.

Map name	Identifier	Call action
CHELP_CHECKPOINT_LOGONVPN	1022	From Check Point VPN-1 logon window: • F1 • Help icon in the window title bar Calls the topic explaining how to log on to Check Point VPN with a one-time password.
CHELP_CHECKPOINT_CONNECTION	1023	From Check Point VPN-1 authentication result window: • F1 • Help icon in the window title bar Calls the topic explaining how to log on to Check Point VPN with a one-time password.
CHELP_USRCONS_SYNCOTP	1024	From the User Console interface when the Synchronize One-Time Password window is open: • Help menu • F1 • Alt+H shortcut • Help icon on the toolbar Calls the topic explaining how to synchronize a smart card for remote access.
CHELP_ACAGENT_GENOTP	1025	The **Learn more about this** link in the Generate a One-Time Password notification message. Calls the topic explaining how to generate one-time passwords.
CHELP_USRCONS_INCORRECTPIN	1027	From the ActivClient Incorrect PIN warning message: • F1 • Help icon in the window title bar Calls the topic describing the PIN entry procedure.

Add the Header File

Copy the ActivClient Help header file, `contexthelp.h`, from the *Admin/Custom Help* folder on the ActivClient distribution to the required location in your help project directory.

You can also create the file using the information provided in Table 11.1 on page 188. Set each context-sensitive control with the following format:

```
#define <map name> <identifier>
```

For example:

```
#define CHELP_ADVCONF_FRAME 1000
```

Configure the Alias Links

The procedure to configure the context-sensitive alias links depends on the help authoring tool being used. For further details, see the documentation provided with the tool.

Using the information provided in Table 11.1 on page 188, set the link to the required help topic for each map name/identifier.

Integrate Customized Help

1. Exit ActivClient and any of its components.
2. Backup the original `ActivClient.chm` in the ActivClient program directory (by default, *C:\Program Files\ActivIdentity\ActivClient\Docs*).
3. Compile your customized help project, making sure the output is called **ActivClient.chm**.
4. Paste the compiled help into the ActivClient program directory.
5. Open the ActivClient User Console and verify that the customized help is working correctly.

   Either:

   – From the User Console **Help** menu, click **ActivClient Help**.
   – Click the ActivClient Help icon  on the toolbar.
   – Press F1.
6. Verify that the context-sensitive help is working correctly.

   For example, either:

   – Generate a One-Time Password and, in the notification message, click the **Learn more about this** link.
   – Open one of the ActivClient tools (such as the PIN Change Tool or Advanced Diagnostics) and click the help icon  in the window title bar.

   For the complete list of the actions that call each context-sensitive help topic, see Table 11.2 on page 189.

Important

Due to Microsoft security restrictions, the content of the customized help file might not display correctly.

To resolve this issue, either:

- Right-click on the .chm, click **Properties** and then click **Unblock**.
- Double-click the .chm and, in the warning message, clear the **Always ask before opening this file** option.

For further information, see the Microsoft Knowledge Base article.

Appendix A: Packages

This appendix describes the ActivClient distribution packages, including the DoD root certificates provided with the CAC editions.

ActivClient Packages

ActivClient comes in four different packages:

- ActivClient x86
- ActivClient x64
- ActivClient CAC x86
- ActivClient CAC x64

The differences between the basic and CAC editions are small. The CAC edition is a customized version of the ActivClient product and includes the following differences:

In the CAC edition:

- Installation and trust of the DoD Root certificates
- Certificate and card expiration notification is enabled by default
- The configuration option “Prefer GSC-IS over PIV EndPoint” is enabled (it is disabled in ActivClient)
- There are some minor differences in the default setup options. For example, the Advanced Configuration Manager is installed by default

In the 64-bit editions of ActivClient, there are small functional differences compared to the 32-bit editions:

- In addition to the 64-bit ActivClient APIs, 32-bit wrappers are available for the ActivClient APIs in order to support compatibility with 32-bit applications running on the 64-bit operating system.
- The Entrust Desktop Solution support module is not available in the 64-bit edition.
- The Check Point SAA support module is not available in the 64-bit edition.
- Netscape, Mozilla, Firefox, and Thunderbird are supported with the ActivClient PKCS#11 library (64- or 32-bit). However, ActivClient 64-bit does not automatically register the PKCS#11 library to these applications. Manual registration is required.

DoD Root Certificates

The DOD Root Certificates included in the ActivClient CAC editions are:

- DODCA_11.cer
- DODCA_12.cer
- DODCA_13.cer
- DODCA_14.cer
- DODCA_15.cer
- DODCA_16.cer
- DODCA_17.cer
- DODCA_18.cer
- DODCLASS3CA_3.cer
- DODCLASS3CA_4.cer
- DODCLASS3CA_5.cer
- DODCLASS3CA_6.cer
- DODCLASS3CA_7.cer
- DODCLASS3CA_8.cer
- DODCLASS3CA_9.cer
- DODCLASS3CA_10.cer
- DODCLASS3EMAILCA_3.cer
- DODCLASS3EMAILCA_4.cer
- DODCLASS3EMAILCA_5.cer
- DODCLASS3EMAILCA_6.cer
- DODCLASS3EMAILCA_7.cer
- DODCLASS3EMAILCA_8.cer
- DODCLASS3EMAILCA_9.cer
- DODCLASS3EMAILCA_10.cer
- DoDClass3RootCA.cer
- DoDEMAILCA_11.cer
- DoDEMAILCA_12.cer
- DoDEMAILCA_13.cer
- DoDEMAILCA_14.cer
- DoDEMAILCA_15.cer
- DoDEMAILCA_16.cer
- DoDEMAILCA_17.cer
- DoDEMAILCA_18.cer
- DoDRootCA2.cer

Appendix B: ActivClient Files and Processes

This appendix describes files installed and used by ActivClient. It also provides an overview of the key ActivClient processes.

Installed Files

The installed files are presented here in two tables.

- Table B.1 lists the files in the ActivClient 6.2 32-bit edition
- Table B.2 lists the files in the ActivClient 6.2 64-bit edition

Table B.1: ActivClient 6.2 32-bit edition

Location	Name
CommonFilesFolder\ActivIdentity	acadvcfm.exe
CommonFilesFolder\ActivIdentity	acdiagwz.exe
CommonFilesFolder\ActivIdentity\Resources	
CommonFilesFolder\ActivIdentity\Resources\Common	acadvcrc_common.dll
CommonFilesFolder\ActivIdentity\Resources\Common	acdiazrc_common.dll
CommonFilesFolder\ActivIdentity\Resources\Localized	acadvcrc.dll
CommonFilesFolder\ActivIdentity\Resources\Localized	acdiazrc.dll
CommonFilesFolder\ActivIdentity\Resources\Merged	
ProgramFilesFolder\ActivIdentity	
INSTALLDIR	acacia.dll
INSTALLDIR	acautoup.exe
INSTALLDIR	acbcgpro.dll
INSTALLDIR	accoca.exe
INSTALLDIR	accocaps.dll
INSTALLDIR	accrdsub.exe

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
INSTALLDIR	accrypto.dll
INSTALLDIR	accuvoplite.dll
INSTALLDIR	acdiagno.dll
INSTALLDIR	acdiagtoolplugin.dll
INSTALLDIR	acevents.exe
INSTALLDIR	acnstool.exe
INSTALLDIR	acregcrt.exe
INSTALLDIR	acsagent.exe
INSTALLDIR	actse.dll
INSTALLDIR	actsinit.exe
INSTALLDIR	actswzdg.exe
INSTALLDIR	acunlock.dll
INSTALLDIR	acuscons.exe
INSTALLDIR	acvop.dll
INSTALLDIR	acvopsm.cfg
INSTALLDIR	acvopsm.dll
INSTALLDIR	acvopsvr.dll
INSTALLDIR	aicfgreg.dll
INSTALLDIR	aipinch.exe
INSTALLDIR	aipinit.exe
INSTALLDIR	aiwjpg.dll
INSTALLDIR	apduengine.dll
INSTALLDIR	libnspr4.dll
INSTALLDIR	libplc4.dll
INSTALLDIR	libplds4.dll
INSTALLDIR	modutil.exe
INSTALLDIR	nspr4.dll
INSTALLDIR	nss3.dll

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
INSTALLDIR	persodatasnapin.dll
INSTALLDIR	plc4.dll
INSTALLDIR	plds4.dll
INSTALLDIR	skisnapin.dll
INSTALLDIR	smime3.dll
INSTALLDIR	softokn3.dll
INSTALLDIR	ucsnapinhelper
INSTALLDIR\Certificates	
INSTALLDIR\Docs	ActivClient ReadMe.htm
INSTALLDIR\Docs	ActivClient.chm
INSTALLDIR\Docs	ActivIdentity End User License Agreement.rtf
INSTALLDIR\Docs	Third Party Software Component License Terms.rtf
INSTALLDIR\Profiles	ACMini-20110000000000000000B9-AxaltoV2C.ini
INSTALLDIR\Profiles	ACMini-20110000000000000000B9-GnD64K.ini
INSTALLDIR\Profiles	ACMini-20110000000000000000B9-OCS5.2D.ini
INSTALLDIR\Profiles	ACMini-20110000000000000000BA-ATMEL-09.FA.ini
INSTALLDIR\Profiles	ACMini-20110000000000000000BA-AxaltoV1SM2.1.ini
INSTALLDIR\Profiles	ACMini-20110000000000000000BA-GXP3-64K-STD-VERSION.ini
INSTALLDIR\Profiles	ACMini-Blank-ATMEL-09.FA.ini
INSTALLDIR\Profiles	ACMini-Blank-AxaltoV1SM2.1.ini
INSTALLDIR\Profiles	ACMini-Blank-AxaltoV2C.ini
INSTALLDIR\Profiles	ACMini-Blank-GnD64K.ini
INSTALLDIR\Profiles	ACMini-Blank-GXP3-64K-STD-VERSION.ini

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
INSTALLDIR\Profiles	ACMini-Blank-OCS5.2D.ini
INSTALLDIR\Profiles	ZIN-20110000000000000000000052.ini
INSTALLDIR\Profiles\Capfiles	GCapplet_SLB_1_0_0_31.cry
INSTALLDIR\Profiles\Capfiles	IDapplet_SLB_1_0_0_27.cry
INSTALLDIR\Profiles\Capfiles	PKIapplet_SLB_1_0_0_34.cry
INSTALLDIR\Profiles\Capfiles	SKIapplet_SLB_1_0_0_20.cry
INSTALLDIR\Resources	acautrc.dll
INSTALLDIR\Resources	acc16krc.dll
INSTALLDIR\Resources	acc8krc.dll
INSTALLDIR\Resources	accobapirc.dll
INSTALLDIR\Resources	accocarc.dll
INSTALLDIR\Resources	acdiagnorc.dll
INSTALLDIR\Resources	acdiagtoolplgrc.dll
INSTALLDIR\Resources	acjavarc.dll
INSTALLDIR\Resources	acjpivrc.dll
INSTALLDIR\Resources	acjsc2rc.dll
INSTALLDIR\Resources	acpkcs201-en6rc.dll
INSTALLDIR\Resources	acpkcs201-nsrc.dll
INSTALLDIR\Resources	acpkcs201rc.dll
INSTALLDIR\Resources	acpkcs211rc.dll
INSTALLDIR\Resources	acsaarc.dll
INSTALLDIR\Resources	persodatasnapinrc.dll
INSTALLDIR\Resources\Common	accsprc_common.dll
INSTALLDIR\Resources\Common	acerrmrc_common.dll
INSTALLDIR\Resources\Common	acexchrc_common.dll
INSTALLDIR\Resources\Common	acsagtrc_common.dll
INSTALLDIR\Resources\Common	actswzrc_common.dll
INSTALLDIR\Resources\Common	acunlockrc_common.dll

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
INSTALLDIR\Resources\Common	aicfgregrc_common.dll
INSTALLDIR\Resources\Common	aipinchrc_common.dll
INSTALLDIR\Resources\Common	aipinguirc_common.dll
INSTALLDIR\Resources\Common	aipinitrc_common.dll
INSTALLDIR\Resources\Common	asphatrc_common.dll
INSTALLDIR\Resources\Common	skisnapinrc_common.dll
INSTALLDIR\Resources\Localized	accsprc.dll
INSTALLDIR\Resources\Localized	acerrmrc.dll
INSTALLDIR\Resources\Localized	acexchrc.dll
INSTALLDIR\Resources\Localized	acsagtrc.dll
INSTALLDIR\Resources\Localized	actswzrc.dll
INSTALLDIR\Resources\Localized	acunlockrc.dll
INSTALLDIR\Resources\Localized	aicfgregrc.dll
INSTALLDIR\Resources\Localized	aipinchrc.dll
INSTALLDIR\Resources\Localized	aipinguirc.dll
INSTALLDIR\Resources\Localized	aipinitrc.dll
INSTALLDIR\Resources\Localized	asphatrc.dll
INSTALLDIR\Resources\Localized	skisnapinrc.dll
INSTALLDIR\Resources\Merged	
ProgramFilesFolder\ActivIdentity\CheckPoint	
ProgramFilesFolder\ActivIdentity\CheckPoint\ SecuRemote	
ProgramFilesFolder\ActivIdentity\CheckPoint\ SecuRemote\bin	acsaa.dll
SystemFolder	acbsi21.dll
SystemFolder	acbsij.dll
SystemFolder	acbsiprov.dll
SystemFolder	accsp.dll
SystemFolder	accsp.sig

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
SystemFolder	acerrmes.dll
SystemFolder	acevtsub.dll
SystemFolder	acexchex.dll
SystemFolder	acflex16.dll
SystemFolder	acflex8.dll
SystemFolder	acfscrfs.dll
SystemFolder	acjavasc.dll
SystemFolder	acjscpiv.dll
SystemFolder	acjscrfs.dll
SystemFolder	acjsys.jar
SystemFolder	acjvscv2.dll
SystemFolder	ackpbsc.dll
SystemFolder	aclibeay.dll
SystemFolder	aclog.dll
SystemFolder	acomx.dll
SystemFolder	acoutcom.dll
SystemFolder	acpicom.dll
SystemFolder	acpimeta.dll
SystemFolder	acpipint.dll
SystemFolder	acpipint.jar
SystemFolder	acpivapi.dll
SystemFolder	acpkcs201-en6.dll
SystemFolder	acpkcs201-ns.dll
SystemFolder	acpkcs201.dll
SystemFolder	acpkcs211.dll
SystemFolder	acwpipint.dll
SystemFolder	aijnipiv.dll
SystemFolder	aijnipiv.jar

Table B.1: ActivClient 6.2 32-bit edition (Continued)

Location	Name
SystemFolder	aipingui.dll
SystemFolder	aspcom.dll
SystemFolder	asphat32.dll
SystemFolder	bsi21classes.jar
SystemFolder	bsi21interf.jar
SystemFolder	jnibsi21.dll
SystemFolder	xsi.jar
SystemFolder	xsi.zip

Table B.2: ActivClient 6.2 64-bit edition

Location	Name
CommonFilesFolder\ActivIdentity	acadvcfm.exe
CommonFilesFolder\ActivIdentity	acdiagwz.exe
CommonFilesFolder\ActivIdentity\Resources	
CommonFilesFolder\ActivIdentity\Resources\Common	acadvcrc_common.dll
CommonFilesFolder\ActivIdentity\Resources\Common	acdiazrc_common.dll
CommonFilesFolder\ActivIdentity\Resources\Localized	acadvcrc.dll
CommonFilesFolder\ActivIdentity\Resources\Localized	acdiazrc.dll
CommonFilesFolder\ActivIdentity\Resources\Merged	
ProgramFilesFolder\ActivIdentity	
INSTALLDIR	acacia.dll
INSTALLDIR	acautoup.exe
INSTALLDIR	acbcgpro.dll
INSTALLDIR	accoca.exe

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
INSTALLDIR	accocaps.dll
INSTALLDIR	acCOMacomx.exe
INSTALLDIR	acCOMbsi21.exe
INSTALLDIR	acCOMcsp.exe
INSTALLDIR	acCOMpiv.exe
INSTALLDIR	acCOMpkcs.exe
INSTALLDIR	acCOMpkcscallback.dll
INSTALLDIR	accrdsub.exe
INSTALLDIR	accrypto.dll
INSTALLDIR	accuvoplite.dll
INSTALLDIR	acdiagno.dll
INSTALLDIR	acdiagtoolplugin.dll
INSTALLDIR	acevents.exe
INSTALLDIR	acjsys.jar
INSTALLDIR	acnstool.exe
INSTALLDIR	acregcrt.exe
INSTALLDIR	acsagent.exe
INSTALLDIR	actse.dll
INSTALLDIR	actsinit.exe
INSTALLDIR	actswzdg.exe
INSTALLDIR	acunlock.dll
INSTALLDIR	acuscons.exe
INSTALLDIR	acvop.dll
INSTALLDIR	acvopsm.cfg
INSTALLDIR	acvopsm.dll
INSTALLDIR	acvopsvr.dll
INSTALLDIR	aicfgreg.dll
INSTALLDIR	aijnipiv.jar

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
INSTALLDIR	aipinch.exe
INSTALLDIR	aipinit.exe
INSTALLDIR	aiwjpg.dll
INSTALLDIR	apduengine.dll
INSTALLDIR	bsi21classes.jar
INSTALLDIR	bsi21interf.jar
INSTALLDIR	persodatasnapin.dll
INSTALLDIR	skisnapin.dll
INSTALLDIR	ucsnapinhelper
INSTALLDIR	xsi.jar
INSTALLDIR	xsi.zip
INSTALLDIR\Certificates	
INSTALLDIR\Docs	ActivClient ReadMe.htm
INSTALLDIR\Docs	ActivClient.chm
INSTALLDIR\Docs	ActivIdentity End User License Agreement.rtf
INSTALLDIR\Docs	Third Party Software Component License Terms.rtf
INSTALLDIR\Profiles	ACMini-201100000000000000000B9-AxaltoV2C.ini
INSTALLDIR\Profiles	ACMini-201100000000000000000B9-GnD64K.ini
INSTALLDIR\Profiles	ACMini-201100000000000000000B9-OCS5.2D.ini
INSTALLDIR\Profiles	ACMini-201100000000000000000BA-ATMEL-09.FA.ini
INSTALLDIR\Profiles	ACMini-201100000000000000000BA-AxaltoV1SM2.1.ini
INSTALLDIR\Profiles	ACMini-201100000000000000000BA-GXP3-64K-STD-VERSION.ini
INSTALLDIR\Profiles	ACMini-Blank-ATMEL-09.FA.ini
INSTALLDIR\Profiles	ACMini-Blank-AxaltoV1SM2.1.ini

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
INSTALLDIR\Profiles	ACMini-Blank-AxaltoV2C.ini
INSTALLDIR\Profiles	ACMini-Blank-GnD64K.ini
INSTALLDIR\Profiles	ACMini-Blank-GXP3-64K-STD-VERSION.ini
INSTALLDIR\Profiles	ACMini-Blank-OCS5.2D.ini
INSTALLDIR\Profiles	ZIN-20110000000000000000000052.ini
INSTALLDIR\Profiles\Capfiles	GCapplet_SLB_1_0_0_31.cry
INSTALLDIR\Profiles\Capfiles	IDapplet_SLB_1_0_0_27.cry
INSTALLDIR\Profiles\Capfiles	PKIapplet_SLB_1_0_0_34.cry
INSTALLDIR\Profiles\Capfiles	SKIapplet_SLB_1_0_0_20.cry
INSTALLDIR\Resources	acautrc.dll
INSTALLDIR\Resources	acc16krc.dll
INSTALLDIR\Resources	acc8krc.dll
INSTALLDIR\Resources	accobapirc.dll
INSTALLDIR\Resources	accocarc.dll
INSTALLDIR\Resources	acdiagnorc.dll
INSTALLDIR\Resources	acdiagtoolplgrc.dll
INSTALLDIR\Resources	acjavarc.dll
INSTALLDIR\Resources	acjpivrc.dll
INSTALLDIR\Resources	acjsc2rc.dll
INSTALLDIR\Resources	acpkcs201-en6rc.dll
INSTALLDIR\Resources	acpkcs201-nsrc.dll
INSTALLDIR\Resources	acpkcs201rc.dll
INSTALLDIR\Resources	acpkcs211rc.dll
INSTALLDIR\Resources	persodatasnapinrc.dll
INSTALLDIR\Resources\Common	accsprc_common.dll
INSTALLDIR\Resources\Common	acerrmrc_common.dll
INSTALLDIR\Resources\Common	acsagtrc_common.dll

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
INSTALLDIR\Resources\Common	actswzrc_common.dll
INSTALLDIR\Resources\Common	acunlockrc_common.dll
INSTALLDIR\Resources\Common	aicfgregrc_common.dll
INSTALLDIR\Resources\Common	aipinchrc_common.dll
INSTALLDIR\Resources\Common	aipinguirc_common.dll
INSTALLDIR\Resources\Common	aipinitrc_common.dll
INSTALLDIR\Resources\Common	asphatrc_common.dll
INSTALLDIR\Resources\Common	skisnapinrc_common.dll
INSTALLDIR\Resources\Localized	accsprc.dll
INSTALLDIR\Resources\Localized	acerrmrc.dll
INSTALLDIR\Resources\Localized	acsagtrc.dll
INSTALLDIR\Resources\Localized	actswzrc.dll
INSTALLDIR\Resources\Localized	acunlockrc.dll
INSTALLDIR\Resources\Localized	aicfgregrc.dll
INSTALLDIR\Resources\Localized	aipinchrc.dll
INSTALLDIR\Resources\Localized	aipinguirc.dll
INSTALLDIR\Resources\Localized	aipinitrc.dll
INSTALLDIR\Resources\Localized	asphatrc.dll
INSTALLDIR\Resources\Localized	skisnapinrc.dll
INSTALLDIR\Resources\Merged	
INSTALLDIR\x64	acCOMacomxPS.dll
INSTALLDIR\x64	acCOMbsi21PS.dll
INSTALLDIR\x64	acCOMcspPS.dll
INSTALLDIR\x64	acCOMpivPS.dll
INSTALLDIR\x64	acCOMpkcscallbackPS.dll
INSTALLDIR\x64	acCOMpkcsPS.dll
INSTALLDIR\x86	acCOMacomxPS.dll
INSTALLDIR\x86	acCOMbsi21PS.dll

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
INSTALLDIR\x86	acCOMcspPS.dll
INSTALLDIR\x86	acCOMpivPS.dll
INSTALLDIR\x86	acCOMpkcscallbackPS.dll
INSTALLDIR\x86	acCOMpkcsPS.dll
System64Folder	acbsi21.dll
System64Folder	acbsij.dll
System64Folder	acbsiprov.dll
System64Folder	accsp.dll
System64Folder	accsp.sig
System64Folder	acerrmes.dll
System64Folder	acevtsub.dll
System64Folder	acflex16.dll
System64Folder	acflex8.dll
System64Folder	acfscrfs.dll
System64Folder	acjavasc.dll
System64Folder	acjscpiv.dll
System64Folder	acjscrfs.dll
System64Folder	acjvscv2.dll
System64Folder	ackpbsc.dll
System64Folder	aclibeay.dll
System64Folder	aclog.dll
System64Folder	acomx.dll
System64Folder	acpicom.dll
System64Folder	acpimeta.dll
System64Folder	acpipint.dll
System64Folder	acpivapi.dll
System64Folder	acpkcs201-en6.dll
System64Folder	acpkcs201-ns.dll

Table B.2: ActivClient 6.2 64-bit edition (Continued)

Location	Name
System64Folder	acpkcs201.dll
System64Folder	acpkcs211.dll
System64Folder	acwpipint.dll
System64Folder	aijnipiv.dll
System64Folder	aipingui.dll
System64Folder	aspcom.dll
System64Folder	asphat32.dll
System64Folder	jnibsi21.dll
SystemFolder	acacia.dll
SystemFolder	acbsi21.dll
SystemFolder	accsp.dll
SystemFolder	accsp.sig
SystemFolder	acexchex.dll
SystemFolder	aclog.dll
SystemFolder	acomx.dll
SystemFolder	acpivapi.dll
SystemFolder	acpkcs211.dll
SystemFolder	aijnipiv.dll
SystemFolder	jnibsi21.dll

Core ActivClient Components

This section presents technical information about a few core ActivClient processes and services.

As ActivClient involves several components that run concurrently, the data cache mechanism is used to improve performance, especially when reading data from the smart card. For instance, reading a certificate from a smart card might take much more time than reading it from memory.

In ActivClient operations, the first component that needs a certificate, reads it from the smart card and then stores it in the data cache for further access. The data cache is invalidated after the card has been removed or after Windows events such as workstation lock or log off. The cached data is limited to certificate, static password and middleware management information.

Table B.3 provides an overview of the key ActivClient system processes.

Table B.3: ActivClient Processes

Process	Description
ac.sharedstore.exe (Shared Store)	This is the component in charge of managing the data and PIN cache. This component implements COM interfaces and is configured to run as a service called ActivIdentity Shared Store Service. This component is used both by ActivClient and by the ActivIdentity Authentication Client. It stores the PIN (encrypted) and the material needed to properly manage per session and per process configuration.
accrdsub.exe	This is a user component started at logon. It subscribes to acevents through a COM interface and manages SCard events and OS events on notification, such as: • Card insertion - registers certificates in the Internet Explorer store, configures Outlook and EFS, publishes certificates to GAL, checks card and certificate expiration, checks for available smart card updates (in CMS), displays relevant prompts in the case of blank card or locked card or change PIN at first use • Card removal - unregisters certificates, locks the workstation of logs the user off • Session lock - removes data and PIN from cache, notification if the card is still inserted
acevents.exe (Event Service)	This is the component in charge of: • Detecting the following events: - SCard events: card insertion/removal, reader plug-in/removal - OS events: lock, logoff, RDP connection and disconnection, Fast User Switching events • Notifying these events to subscriber applications • It also implements certificate caching and card auto-registration On Windows XP and later, this component implements a COM object, instantiated by the OS when needed (that is, when a client application subscribes through its COM interface). There is one acevents.exe instance running per session which is why you can see two instances running simultaneously (SYSTEM + user dependent). **Note:** In a Terminal Server environment, you will see as many instances as users logged in to the TSE server. On Windows 2000, there is a single instance of acevents.exe running from a service.
acsagent.exe	This is a user interface-based component started at logon. It displays the ActivClient smart card icon in the notification area/system tray.

File Update After Installation

Once ActivClient is installed, new files might be created automatically.

To do so, ActivClient software requires write permission to the INSTALLDIR\Downloads directory. The default folder is \Program Files\ActivIdentity\ActivClient\Downloads This folder is used to store downloaded hot-fixes if the ActivClient Auto-Update feature is used.

Appendix C: Registry Keys

This appendix describes all the Windows registry keys used (for read or write) by ActivClient, in two sections:

- "Registry Keys Installed by ActivClient 6.2 (32-bit Edition)" on page 211
- "Registry Keys Installed by ActivClient 6.2 (64-bit Edition)" on page 231

Note: Only the registry keys described in Chapter 2, "Policy Definition," page 16, are supported for updates. All other registry keys are mentioned only for reference. If you want to use reduced permissions for registry access, you must allow the ActivClient software access to (that is, read permission for) these registries.

Registry Keys Installed by ActivClient 6.2 (32-bit Edition)

```
[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore.1]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore.1\CLSID]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier\CLSID]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier\CurVer]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier.1]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier.1\CLSID]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber\CLSID]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber\CurVer]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber.1]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber.1\CLSID]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore\CurVer]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore\CLSID]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}]
```

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\0\win32]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{14693D72-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\CLSID\{83DA5E0D-61FA-4102-9D19-00DF4E435171}]

[HKEY_CLASSES_ROOT\CLSID\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{C824992C-2940-40C6-9A56-EB40E29C5D47}]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\InprocServer32]

```
[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\VERSION]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Implemented Categories]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Implemented Categories\{40FC6ED5-
2438-11CF-A3DB-080036F12502}]

[HKEY_CLASSES_ROOT\ACOutCom.ConnectOutlook]

[HKEY_CLASSES_ROOT\ACOutCom.ConnectOutlook\Clsid]

[HKEY_CLASSES_ROOT\AppID\{CFDD1051-06E1-4446-BFA1-3D63B5CB2B5A}]

[HKEY_CLASSES_ROOT\AppID\acevents.EXE]

[HKEY_CLASSES_ROOT\AppID\{4C94073B-F8E2-41F1-AC23-B7BA8A08B188}]

[HKEY_CLASSES_ROOT\AppID\aicfgreg.DLL]

[HKEY_CLASSES_ROOT\AppID\{14693D64-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\AppID\accoca.EXE]

[HKEY_CURRENT_USER\Software\Microsoft]

[HKEY_CURRENT_USER\Software\Microsoft\Office]

[HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook]

[HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Addins]

[HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Addins\ACOutCom.ConnectOutlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns\AdvancedConfigurationManager]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns\AdvancedDiagnostics]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Cards]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\ACA]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\AIDPIV]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\Card Manager]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\CCC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\CAC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\CAC\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\STANDARD]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data
Model\STANDARD\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\PIV]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\PIV\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC19]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC18]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC17]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC11]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC6]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC2]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile 1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI7]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC6]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC19]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC18]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC17]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\SKI1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\MANAGER]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\DEMOGRAPHIC2]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile
1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI8]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\SnapIns]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\SnapIns\UserConsole]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\AcOutCom.ConnectOutlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client\Extensions]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ActivCard Gold Cryptographic
Service Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ackpbsc]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acunlock]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\Include]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\OpenCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\Exclude]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1\ActivCard]
```

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Logging]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\AutoUpdate]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\AutoUpdate\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\EventService]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPCOM]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MULTOS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MULTOS\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SAGEM]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SAGEM\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SHARP]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SHARP\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\CFLEX16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\CFLEX16\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\GlobalConfig]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\AuthenticationDialog]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card7]

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SAA]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification\NoReaderWarning]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification\SmartCardPresenceWarning]
```

Registry Keys Installed by ActivClient 6.2 (64-bit Edition)

This section provides information on the following:

- "64-bit Registry" on page 231
- "32-bit Registry" on page 267

64-bit Registry

```
[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore.1]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore.1\CLSID]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier\CLSID]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier\CurVer]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier.1]

[HKEY_CLASSES_ROOT\ACEventService.EventNotifier.1\CLSID]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber\CLSID]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber\CurVer]

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber.1]
```

[HKEY_CLASSES_ROOT\ACEventSubscriber.Subscriber.1\CLSID]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore\CurVer]

[HKEY_CLASSES_ROOT\aicfgreg.CBackupRestore\CLSID]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{CC49D6C0-98F0-4320-B3F2-87C3393DECA1}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{80E03EC1-5D9F-440A-B139-AF13D1DF8A0E}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{14693D70-AD77-11D3-A629-00104BB6307C}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{B109E525-FCE1-4894-B80A-4ABEF00EB54A}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\0\win32]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{7A8DD2B5-D2A7-4F8B-A9AC-09FEA003113B}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{78D3D4FD-B8BB-429C-8563-2FC9ADF0AC12}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{14693D72-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\CLSID\{83DA5E0D-61FA-4102-9D19-00DF4E435171}]

[HKEY_CLASSES_ROOT\CLSID\{83DA5E0D-61FA-4102-9D19-00DF4E435171}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{C824992C-2940-40C6-9A56-EB40E29C5D47}]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\VERSION]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Implemented Categories]

[HKEY_CLASSES_ROOT\CLSID\{D97C28A7-D1A3-4718-9E65-E71C2FFC2555}\Implemented Categories\{40FC6ED5-2438-11CF-A3DB-080036F12502}]

[HKEY_CLASSES_ROOT\ACOutCom.ConnectOutlook]

[HKEY_CLASSES_ROOT\ACOutCom.ConnectOutlook\Clsid]

[HKEY_CLASSES_ROOT\AppID\{CFDD1051-06E1-4446-BFA1-3D63B5CB2B5A}]

[HKEY_CLASSES_ROOT\AppID\acevents.EXE]

[HKEY_CLASSES_ROOT\AppID\{4C94073B-F8E2-41F1-AC23-B7BA8A08B188}]

[HKEY_CLASSES_ROOT\AppID\aicfgreg.DLL]

[HKEY_CLASSES_ROOT\AppID\{14693D64-AD77-11D3-A629-00104BB6307C}]

[HKEY_CLASSES_ROOT\AppID\accoca.EXE]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns\AdvancedConfigurationManager]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\SnapIns\AdvancedDiagnostics]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Cards]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge]

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\ACA]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\AIDPIV]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\Card Manager]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Card Edge\CCC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\CAC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\CAC\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\STANDARD]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data
Model\STANDARD\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\PIV]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Data Model\PIV\ServiceList]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC19]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC18]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC17]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC11]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile1\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile5\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC6]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile5\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC
Profile1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\Empty OCS\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC2]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CAC Gemx
Profile1\DEMOGRAPHIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile 1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI7]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Gemx Profile
1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\STATIC1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile2\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx Profile3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Gemx
Profile3\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC6]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC19]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC18]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC17]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\STATIC10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\SKI1]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile1\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\SKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\SKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile2\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile2\MANAGER]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile3\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile3\BIO1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile6\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\DEMOGRAPHIC2]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile6\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile
1\DEMOGRAPHIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\STATIC5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CS Profile 1\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\STATIC1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI8]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI15]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI14]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI13]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI12]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PKI10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1 Profile4\PIN1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Card Discovery\Profiles\CSV1
Profile4\MANAGER]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\SnapIns]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\SnapIns\UserConsole]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\AcOutCom.ConnectOutlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client\Extensions]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ActivCard Gold Cryptographic
Service Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ackpbsc]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acunlock]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\Include]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\OpenCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\ActivCard\Exclude]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration\ActivCard\Outlook]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1]

[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1\ActivCard]
```

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Logging]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\AutoUpdate]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\AutoUpdate\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\EventService]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPCOM]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\COSMOPOLIC\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GALACTIC\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GEMXPRESSO\CARD9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\GND\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MULTOS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MULTOS\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SAGEM]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SAGEM\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SHARP]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\SHARP\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\CFLEX16]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\CFLEX16\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\MFLEX\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD6]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ACCESS\CARD3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL\CARD2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\AspCards\ATMEL\CARD1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\SmartCardAgent]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\GlobalConfig]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\AuthenticationDialog]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card1]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card2]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card3]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card4]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card5]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card7]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card8]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card9]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card10]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\PINInitTool\Card11]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\UserConsole]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification\NoReaderWarning]

[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\Notification\SmartCardPresenceWarning]

[HKEY_CLASSES_ROOT\acCOMpkcscallback.PKCScallbackInterface]

[HKEY_CLASSES_ROOT\acCOMpkcscallback.PKCScallbackInterface\CurVer]

[HKEY_CLASSES_ROOT\acCOMpkcscallback.PKCScallbackInterface\CLSID]

[HKEY_CLASSES_ROOT\acCOMpkcscallback.PKCScallbackInterfa.1]

[HKEY_CLASSES_ROOT\acCOMpkcscallback.PKCScallbackInterfa.1\CLSID]

[HKEY_CLASSES_ROOT\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}]

[HKEY_CLASSES_ROOT\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{668456A8-24D6-4243-B106-B8F53F944640}]

[HKEY_CLASSES_ROOT\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}]

[HKEY_CLASSES_ROOT\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}]

[HKEY_CLASSES_ROOT\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}]

[HKEY_CLASSES_ROOT\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}]

[HKEY_CLASSES_ROOT\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}]

[HKEY_CLASSES_ROOT\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}]

[HKEY_CLASSES_ROOT\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}]

[HKEY_CLASSES_ROOT\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}]

[HKEY_CLASSES_ROOT\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}]

[HKEY_CLASSES_ROOT\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}]

[HKEY_CLASSES_ROOT\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}]

[HKEY_CLASSES_ROOT\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}]

[HKEY_CLASSES_ROOT\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}]

[HKEY_CLASSES_ROOT\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}]

[HKEY_CLASSES_ROOT\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}]

[HKEY_CLASSES_ROOT\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}]

[HKEY_CLASSES_ROOT\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}]

[HKEY_CLASSES_ROOT\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}]

[HKEY_CLASSES_ROOT\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}]

[HKEY_CLASSES_ROOT\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}]

[HKEY_CLASSES_ROOT\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}]

[HKEY_CLASSES_ROOT\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\TypeLib]

[HKEY_CLASSES_ROOT\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\NumMethods]

[HKEY_CLASSES_ROOT\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Interface\88FA504A-1B4F-42B1-9848-AE6209F09447]

[HKEY_CLASSES_ROOT\Interface\88FA504A-1B4F-42B1-9848-AE6209F09447\ProxyStubClsid]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\0\win32]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{A6BF8CB6-5D50-4378-9C6C-F9AF402620EC}\1.0\0\win64]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{5E46E9DF-D73E-4EFC-BB9A-07597C6801E2}\1.0\0\win64]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{DF79E2F5-15E2-4DC6-8C88-B40BB33C7C4B}\1.0\0\win64]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{B2F63BD5-2901-4BDA-8A19-1DC20D1F28F9}\1.0\0\win64]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}\1.0]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}\1.0\0]

[HKEY_CLASSES_ROOT\TypeLib\{D16964CE-4858-47F3-A339-3A42CC5BA327}\1.0\0\win64]

[HKEY_CLASSES_ROOT\CLSID\{05EEE5A9-F903-4D54-999C-A43C547EF034}]

[HKEY_CLASSES_ROOT\CLSID\{05EEE5A9-F903-4D54-999C-A43C547EF034}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{D147D7C6-41F8-45E5-96C5-216657A9C173}]

[HKEY_CLASSES_ROOT\CLSID\{D147D7C6-41F8-45E5-96C5-216657A9C173}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\InprocServer32]

[HKEY_CLASSES_ROOT\CLSID\{668456A8-24D6-4243-B106-B8F53F944640}]

[HKEY_CLASSES_ROOT\CLSID\{668456A8-24D6-4243-B106-B8F53F944640}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{070695CD-CB20-4254-B3EF-6D89228DE220}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{30E61CBC-8DF2-4ED6-9FD8-D977B5698C66}\Programmable]

```
[HKEY_CLASSES_ROOT\CLSID\{2599E050-87CD-49F0-9A49-92DAED39D313}]

[HKEY_CLASSES_ROOT\CLSID\{2599E050-87CD-49F0-9A49-92DAED39D313}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{8EB55F9F-C5DE-4727-BF28-7EA42AADE077}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{193795BC-B81F-4900-B391-349EA9019C0F}]

[HKEY_CLASSES_ROOT\CLSID\{193795BC-B81F-4900-B391-349EA9019C0F}\InProcServer32]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{CF323C11-8F18-4500-8301-0F99CCC2D054}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{5B985AAD-0DC3-4230-BC40-E62AC276FF03}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}]

[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}\LocalServer32]
```

```
[HKEY_CLASSES_ROOT\CLSID\{0D77058D-09A6-4D40-B3C2-FDBA8E77288B}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{38CC0AC0-170A-4FD0-8441-9BD7C7FE6883}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{8F5330A7-4214-45F4-8736-0ED72C96DEB0}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{876DD103-9F92-4960-A705-4EC69B8B0ADA}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{6AAF1B76-370B-427E-9D45-729A56826BD3}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}]

[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}\VersionIndependentProgID]
```

```
[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{2E03C01D-D9A2-419D-BF56-FCFDA14FF879}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{C0879BC8-FE3C-49CB-9D6F-3295F514E12A}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{A082D824-693A-47D0-832A-918F160F839F}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{7030D479-1A29-4935-8B42-B4B619992DFF}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}]

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}\LocalServer32]
```

[HKEY_CLASSES_ROOT\CLSID\{BD1E4BC3-204A-4937-8D1B-62DF084CE8B0}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{08049768-774A-4B91-8B39-87FFBB2BF28E}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{9359DF4E-50D2-419E-989F-FF113D304593}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{1C1451BA-4F87-4944-8111-5E4078C87C87}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{190E1E02-263E-4CF5-8978-F6B5838E0090}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}]

[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}\VersionIndependentProgID]

```
[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{729F85AE-A18C-42F4-8FF1-2861E829866D}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{0D095E72-4D30-42A1-8FEB-DB3F3546D3C0}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}\TypeLib]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}\ProgID]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}\LocalServer32]

[HKEY_CLASSES_ROOT\CLSID\{46E61AEF-B3AE-48E9-B67E-2E9EA4BCF359}\Programmable]

[HKEY_CLASSES_ROOT\CLSID\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}]

[HKEY_CLASSES_ROOT\CLSID\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\InProcServer32]

[HKEY_CLASSES_ROOT\acCOMbsi21.BSI21]

[HKEY_CLASSES_ROOT\acCOMbsi21.BSI21\CurVer]

[HKEY_CLASSES_ROOT\acCOMbsi21.BSI21\CLSID]

[HKEY_CLASSES_ROOT\acCOMbsi21.BSI21.1]

[HKEY_CLASSES_ROOT\acCOMbsi21.BSI21.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMpiv.PIVInterface]

[HKEY_CLASSES_ROOT\acCOMpiv.PIVInterface\CurVer]

[HKEY_CLASSES_ROOT\acCOMpiv.PIVInterface\CLSID]

[HKEY_CLASSES_ROOT\acCOMpiv.PIVInterface.1]
```

[HKEY_CLASSES_ROOT\acCOMpiv.PIVInterface.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMpkcs.PKCSInterface]

[HKEY_CLASSES_ROOT\acCOMpkcs.PKCSInterface\CLSID]

[HKEY_CLASSES_ROOT\acCOMpkcs.PKCSInterface\CurVer]

[HKEY_CLASSES_ROOT\acCOMpkcs.PKCSInterface.1]

[HKEY_CLASSES_ROOT\acCOMpkcs.PKCSInterface.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMcsp.CSPInterface.1]

[HKEY_CLASSES_ROOT\acCOMcsp.CSPInterface.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMcsp.CSPInterface]

[HKEY_CLASSES_ROOT\acCOMcsp.CSPInterface\CurVer]

[HKEY_CLASSES_ROOT\acCOMcsp.CSPInterface\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Acomx]

[HKEY_CLASSES_ROOT\acCOMacomx.Acomx\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.Acomx\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Acomx.1]

[HKEY_CLASSES_ROOT\acCOMacomx.Acomx.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.ACStatic]

[HKEY_CLASSES_ROOT\acCOMacomx.ACStatic\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.ACStatic\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.ACStatic.1]

[HKEY_CLASSES_ROOT\acCOMacomx.ACStatic.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Card]

[HKEY_CLASSES_ROOT\acCOMacomx.Card\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.Card\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Card.1]

[HKEY_CLASSES_ROOT\acCOMacomx.Card.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.CardAccessor]

[HKEY_CLASSES_ROOT\acCOMacomx.CardAccessor\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.CardAccessor\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.CardAccessor.1]

[HKEY_CLASSES_ROOT\acCOMacomx.CardAccessor.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.CardCriteria]

[HKEY_CLASSES_ROOT\acCOMacomx.CardCriteria\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.CardCriteria\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.CardCriteria.1]

[HKEY_CLASSES_ROOT\acCOMacomx.CardCriteria.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PIN]

[HKEY_CLASSES_ROOT\acCOMacomx.PIN\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.PIN\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PIN.1]

[HKEY_CLASSES_ROOT\acCOMacomx.PIN.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PINAccessor]

[HKEY_CLASSES_ROOT\acCOMacomx.PINAccessor\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.PINAccessor\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PINAccessor.1]

[HKEY_CLASSES_ROOT\acCOMacomx.PINAccessor.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PINLogicalCriteria]

[HKEY_CLASSES_ROOT\acCOMacomx.PINLogicalCriteria\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.PINLogicalCriteria\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.PINLogicalCriteria.1]

[HKEY_CLASSES_ROOT\acCOMacomx.PINLogicalCriteria.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Reader]

[HKEY_CLASSES_ROOT\acCOMacomx.Reader\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.Reader\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.Reader.1]

[HKEY_CLASSES_ROOT\acCOMacomx.Reader.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.ReaderManager]

[HKEY_CLASSES_ROOT\acCOMacomx.ReaderManager\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.ReaderManager\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.ReaderManager.1]

[HKEY_CLASSES_ROOT\acCOMacomx.ReaderManager.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SDKCardServiceFactory]

[HKEY_CLASSES_ROOT\acCOMacomx.SDKCardServiceFactory\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SDKCardServiceFactory\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SDKCardServiceFactory.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SDKCardServiceFactory.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKI]

[HKEY_CLASSES_ROOT\acCOMacomx.SKI\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SKI\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKI.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SKI.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKIAccessor]

[HKEY_CLASSES_ROOT\acCOMacomx.SKIAccessor\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SKIAccessor\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKIAccessor.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SKIAccessor.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKILogicalCriteria]

[HKEY_CLASSES_ROOT\acCOMacomx.SKILogicalCriteria\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SKILogicalCriteria\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SKILogicalCriteria.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SKILogicalCriteria.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnection]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnection\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnection\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnection.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnection.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnectionManager]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnectionManager\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnectionManager\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnectionManager.1]

[HKEY_CLASSES_ROOT\acCOMacomx.SmartCardConnectionManager.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticAccessor]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticAccessor\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticAccessor\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticAccessor.1]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticAccessor.1\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticLogicalCriteria]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticLogicalCriteria\CurVer]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticLogicalCriteria\CLSID]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticLogicalCriteria.1]

[HKEY_CLASSES_ROOT\acCOMacomx.StaticLogicalCriteria.1\CLSID]

[HKEY_CLASSES_ROOT\AppID\{194FA587-F460-4E6B-8E20-90212C1851F7}]

[HKEY_CLASSES_ROOT\AppID\acCOMpkcscallback.DLL]

[HKEY_CLASSES_ROOT\AppID\acCOMpiv.EXE]

[HKEY_CLASSES_ROOT\AppID\{884A0BCF-1E9D-4485-97A2-CD1F958B3003}]

[HKEY_CLASSES_ROOT\AppID\acCOMbsi21.EXE]

[HKEY_CLASSES_ROOT\AppID\{2FE87B63-6C6D-457C-B161-4AE6DD6D2D0A}]

[HKEY_CLASSES_ROOT\AppID\{3EA348A7-99E9-4E93-9A24-273081580B17}]

```
[HKEY_CLASSES_ROOT\AppID\acCOMpkcs.EXE]

[HKEY_CLASSES_ROOT\AppID\{4C77A80A-10BB-47C5-8A4D-C0417965CDBD}]

[HKEY_CLASSES_ROOT\AppID\acCOMcsp.EXE]

[HKEY_CLASSES_ROOT\AppID\{2B2D0DFE-BF90-4DBD-BD09-E44C17586E80}]

[HKEY_CLASSES_ROOT\AppID\acCOMacomx.EXE]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ActivClient Cryptographic
Service Provider]
```

32-bit Registry

```
[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{193795BC-B81F-4900-B391-349EA9019C0F}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{193795BC-B81F-4900-B391-349EA9019C0F}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{193795BC-B81F-4900-B391-349EA9019C0F}\ProxyStubClsid32]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\ActivClient
Cryptographic Service Provider]

[HKEY_CLASSES_ROOT\Wow6432Node\acCOMpkcscallback.PKCScallbackInterface]

[HKEY_CLASSES_ROOT\Wow6432Node\acCOMpkcscallback.PKCScallbackInterface\CurVer]

[HKEY_CLASSES_ROOT\Wow6432Node\acCOMpkcscallback.PKCScallbackInterface\CLSID]

[HKEY_CLASSES_ROOT\Wow6432Node\acCOMpkcscallback.PKCScallbackInterfa.1]

[HKEY_CLASSES_ROOT\Wow6432Node\acCOMpkcscallback.PKCScallbackInterfa.1\CLSID]

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{194FA587-F460-4E6B-8E20-90212C1851F7}]

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\acCOMpkcscallback.DLL]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\TypeLib]
```

```
[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\ProxyStubClsid]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-
C176EF0BD17C}\VersionIndependentProgID]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\TypeLib]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\Programmable]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\ProgID]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{A33DFD8D-B211-4E41-8BA9-C176EF0BD17C}\InprocServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\HELPDIR]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\FLAGS]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\0]

[HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{1C58E335-7C7F-4ED7-B4AB-2020BC5C23B3}\1.0\0\win32]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D147D7C6-41F8-45E5-96C5-216657A9C173}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D147D7C6-41F8-45E5-96C5-216657A9C173}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D147D7C6-41F8-45E5-96C5-216657A9C173}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{2599E050-87CD-49F0-9A49-92DAED39D313}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{2599E050-87CD-49F0-9A49-92DAED39D313}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2599E050-87CD-49F0-9A49-92DAED39D313}\ProxyStubClsid32]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GSC]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GSC\Cryptography]

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GSC\Cryptography\PKCS#11]
```

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GSC\Cryptography\PKCS#11\ActivCard]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{05EEE5A9-F903-4D54-999C-A43C547EF034}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{05EEE5A9-F903-4D54-999C-A43C547EF034}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{05EEE5A9-F903-4D54-999C-A43C547EF034}\ProxyStubClsid32]

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\GSC]

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\GSC\BSI]

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\GSC\BSI\2.1]

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\GSC\BSI\2.1\ActivCard]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{668456A8-24D6-4243-B106-B8F53F944640}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{668456A8-24D6-4243-B106-B8F53F944640}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{668456A8-24D6-4243-B106-B8F53F944640}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{668456A8-24D6-4243-B106-B8F53F944640}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}]

[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\InProcServer32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{7006647C-AB15-49D5-AC04-AF39A8BAC71B}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{88FA504A-1B4F-42B1-9848-AE6209F09447}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{D1C5856D-FE18-4DA5-B29B-6CE61B9D2A26}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{67228205-C4C6-45D6-AAAE-CBF72A35D1B3}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DA84C1FE-6148-4676-9D5E-0D92C576248C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{EE59FE67-46FB-4435-A2DD-8277AEAD3D12}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{CEAC0E85-53CE-4C93-A481-2FAB9DE41D8D}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{A88CA4D6-D6F2-445F-9008-E79564B48D5E}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{092C6063-2247-4C0E-B2D2-E961D1486FDD}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{DF978174-43D7-4DAC-8290-6791468C9456}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{AE06D5D4-FB02-4248-9043-349D130B644C}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{250E0ABC-E9A3-40D4-A556-E91384C372DA}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}]

```
[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{F595C96B-A35E-4A6E-A40A-0C940961B1EA}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{9D0FA17A-55A5-4EA4-B687-2286C4D5E9E9}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{87CC499D-B2AB-4800-8301-0A7CB6665411}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B25B7EE-C875-40DC-AA05-991149DB87B6}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{60AC9FBA-C720-4D04-8A29-67821B1D118A}\ProxyStubClsid32]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\NumMethods]

[HKEY_CLASSES_ROOT\Wow6432Node\Interface\{2B48F33B-F761-405F-A7C0-F7CD719A4856}\ProxyStubClsid32]
```

Registry Keys Updated After Installation

These following registries are updated during post-installation usage scenarios. You must guarantee that the ActivClient software has write permissions to them:

- `HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Cards`
  (used for performance optimization)
- `HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Logging`
  (used for logging)
- `HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Diagnostic`
  (used for diagnostics)

Appendix D: Terms and Acronyms

In This Appendix

272 Terms

273 Acronyms

This appendix lists terms and acronyms used throughout the full set of ActivIdentity ActivClient for Windows technical publications. Not all terms and acronyms appear in all documents.

Terms

Certificate Authority (CA) - The CA issues and manages security credentials and public keys for message encryption in a networked environment. As part of a Public Key Infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA issues a certificate.

ActivID Card Management System (CMS) - Formally known as ActivCard Identity Management System (AIMS), CMS is a web-based, smart card, credential and application lifecycle management system. CMS augments and works in concert with an enterprise's primary identity management infrastructure components, including popular directory, database, and PKI components.

Cryptographic Service Provider (CSP) - An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.

Federal Information Processing Standard (FIPS 140-2) - FIPS 140-2 is the standard for crypto-module security. FIPS 140-2 level 3 adds additional requirements to FIPS 140-2 level 2. These requirements concern physical security and a trusted path for entering a Cryptographic Service Provider, such as a PIN. FIPS 140-2 level 3 uses local ports and the key pad to enforce such security.

Federal Information Processing Standard 201 (FIPS 201) - FIPS 201 is the standard for Personal Identity Verification (PIV) cards defined for US Government employees and contractors.

My Digital ID Card (MDIDC) - This CMS component allows end users to access the self-service CMS functions, which includes card and credential management.

One-Time Password (OTP) - A one-time password is a password used only once to authenticate to remote applications. One-Time Passwords are only present on smart cards issued with SKI credentials.

Personal Identification Number (PIN) - Is used to authenticate to your smart card in order to perform actions such as Windows PKI logon, remote access and email signature.

Public Key Infrastructure (PKI) - PKI describes the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.

Registration Authority (RA) - RA is an authority in a network that verifies user requests for a digital certificate and instructs the CA to issue it. An RA is part of a PKI, a networked system that enables companies and users to exchange information safely and securely.

Symmetric Key Infrastructure (SKI) - SKI keys are used to perform strong authentication on remote applications. SKI keys encrypt passwords in:
- Synchronous mode (generates 1 password without any challenge. The server uses the same method to create a password than the smart card)
- Asynchronous: encrypts a challenge

Standalone smart card - Smart card with pre-loaded applets issued by the manufacturer.

Acronyms

Acronym

What does it stand for

CA

Certificate Authority

CAC

Common Access Card (for the United States Department of Defense)

CSP

Cryptographic Service Provider

FIPS

Federal Information Processing Standard

GAL

Global Address List

GP

GlobalPlatform

Replaces OpenPlatform (OP).

OTP

One-Time Password

PKI

Public Key Infrastructure

PIV

Personal Identity Verification

Smart card issued by the United States government to federal employees and contractors.

RA

Registration Authority

SKI

Symmetric Key Infrastructure

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Document Information

ActivIdentity, Inc. welcomes your comments and suggestions.

Your input is an important factor in future revisions of this publication. Please let us know your opinion.

Product: ActivClient for Windows

Document: ActivClient for Windows Administration Guide

Document Reference: AC/WIN/AG/06.2009/v6.2

Please send your feedback via email to: tpd@actividentity.com. If you find errors or have general suggestions for improvement, please indicate the chapter, section and page number. If you would like a reply, please include your name, company, email address, and telephone number.

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

ActivIdentity Intellectual Property: This document or deliverable(s) contain proprietary information of ActivIdentity Corporation and/or its subsidiaries and affiliates (collectively, “ActivIdentity”) embodying confidential information, ideas, and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission from ActivIdentity. This document may not be modified, copied, distributed, transmitted, displayed, performed, reproduced, published, licensed, used to create derivative works therefrom, transferred, or sold unless expressly agreed by ActivIdentity. The furnishing of this document does not imply or expressly provide a license to any of the ActivIdentity intellectual property.

Trademarks: ActivIdentity, ActivIdentity (logo), and/or other ActivIdentity products or marks referenced herein are either registered trademarks or trademarks of ActivIdentity in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the ActivIdentity trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.