ActivID® ActivClient® for Windows Administration Guide

DOCUMENT REFERENCE: AC_WIN_7.1_AG_07.2016

PRODUCT VERSION: 7.1

JULY 2016



Copyright

© 2008-2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved. This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID, HID Global, the HID Blue Brick logo, the Chain Design and 4TRESS, ActivIdentity and ActivID are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Revision History

Date	Description	Document Version
July 2016	Initial release of rebranded document and major technical updates.	1.0

Contacts

Americas		Asia Pacific
United States: +1 510.574.0100	U.S. Federal: +1 571.522.1000	+61 (0) 3.9809.2892
Europe		**Corporate**
+33 (0) 1.42.04.84.00		+1 800.237.7769

Technical Support

If you purchased your product from a third party, then please contact that third party for Technical Support. For products purchased directly from HID Global, please go to http://www.hidglobal.com/support

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
`Code samples`	`Highlights code samples`
	**WARNING**: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
	**Important**: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	**Note**: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

List of Tables **11**

List of Figures **11**

1.0 Introduction **12**

1.1 Product Overview 12
1.2 Document Scope and Audience 12

2.0 ActivClient Deployment **13**

2.1 Deployment and Policy Planning 13
2.2 Preparation 13
2.3 Deployment 13
2.4 Upgrading 13
2.5 ActivClient Management 14
2.6 Administrative Tools 14

3.0 Defining the ActivClient Policies **15**

3.1 ActivClient Customization Methods 15
3.2 Using Active Directory Group Policy Objects on Microsoft Windows Server 15
3.2.1 Add the ActivClient Administrative Template and Create the Group Policy 16
3.2.2 Configure the Policy Settings 17
3.2.3 Customizing ActivClient Using the Microsoft Windows Local Computer Policy Editor 21
3.3 Importing and Exporting Policies 24
3.3.1 Domain Machines 24
3.3.2 Non-Domain Machines 24
3.4 Viewing Active Policies 24
3.4.1 About Group Policy Processing in a Microsoft Windows Environment 24
3.4.2 ActivClient Resultant Set of Policies 25

4.0 ActivClient Policy Settings **27**

4.1 Certificate Availability 28
4.1.1 Display certificate replacement warning 28
4.1.2 Remove certificates from Microsoft Windows on logoff 28
4.1.3 Remove certificates from Microsoft Windows on smart card removal 29
4.1.4 Turn off automatic configuration of Microsoft Windows EFS smart card certificate 29
4.2 Login Window 29
4.2.1 Static Logon Banner—high resolution 29
4.3 Notification Area Icon (ActivClient Agent) 30
4.3.1 Clipboard One-Time Password expiration (in seconds) 30
4.3.2 Hide Advanced Diagnostics menu 30
4.3.3 Hide Get One-Time Password menu 31
4.3.4 Hide notification area icon 31
4.3.5 Hide Open menu 31
4.3.6 Hide PIN Initialization Tool menu 31

4.3.7 One-Time Password window duration (in seconds) 31
4.4 Notifications Management 32
4.4.1 Blocked Card Manager message (Windows 7 and earlier) 33
4.4.2 Blocked Card Manager message (Windows 8 and later) 33
4.4.3 Blocked Card Manager title (Windows 8 and later) 33
4.4.4 Card Auto-Update Alert duration (in seconds) 34
4.4.5 Card Auto-Update Alert message (Windows 7 and earlier) 34
4.4.6 Card Auto-Update Alert message (Windows 8 and later) 34
4.4.7 Card Auto-Update Alert title (Windows 8 and later) 35
4.4.8 Delay before checking expiration after card insertion (in seconds) 35
4.4.9 Display Card Expiration notification 35
4.4.10 Display Certificate Expiration notification 36
4.4.11 Display New Card window on card insertion 36
4.4.12 Expiration notification period (in days) 36
4.4.13 Expiration warning message 37
4.4.14 Expiration warning period (in days) 37
4.4.15 Hide Blocked Card Manager message when a smart card with a blocked card manager is inserted 37
4.4.16 Hide No Smart Card Reader Alert 37
4.4.17 Locked Card Message (Windows 7 and earlier) 38
4.4.18 Locked Card Message (Windows 8 and later) 38
4.4.19 Locked Card Title (Windows 8 and later) 38
4.4.20 No Smart Card Reader Alert duration (in seconds) 39
4.4.21 No Smart Card Reader Alert message (Windows 7 and earlier) 39
4.4.22 No Smart Card Reader Alert message (Windows 8 and later) 39
4.4.23 No Smart Card Reader Alert title (Windows 8 and later) 40
4.4.24 Prevent Unlock Card window prompt when a locked card is inserted 40
4.4.25 Unattended Smart Card Alert 40
4.4.26 Unattended Smart Card Alert Sound 41
4.5 Outlook Enhancements 42
4.5.1 Allow different email addresses in smart card certificate and Microsoft Exchange account 42
4.5.2 Check CRL for Microsoft Outlook security profile creation and Publish to GAL 43
4.5.3 Check CRL timeout for Microsoft Outlook security profile creation and Publish to GAL 43
4.5.4 Disable audit for Microsoft Outlook security profile creation and Publish to GAL 43
4.5.5 Encryption algorithm configured in Security Profile on card insertion 44
4.5.6 Hash algorithm configured in Security Profile on card insertion 44
4.5.7 Microsoft Outlook Auto-Contact destination folder 45
4.5.8 Turn off automatic addition of sender's certificates to Microsoft Outlook contacts 45
4.5.9 Turn off setup email certificates in Microsoft Outlook on card insertion 45
4.5.10 Turn on automatic decryption of encrypted emails 45
4.5.11 Turn on automatic publication of certificates to the Global Address List 46
4.6 PIN Caching 46
4.6.1 Allow per-process PIN caching 46
4.6.2 Disable PIN cache clearance on workstation lock 46
4.6.3 Enable PIN caching for "PIN Always" private keys 47
4.6.4 Number of minutes before PIN cache is cleared 47
4.7 PIN Initialization Tool 47
4.7.1 Turn Off OTP Initialized Card Re-initialization 47

4.8 PIN Management 48
4.8.1 Allow ActivClient to validate the PIN code against the PIN policy before validating the PIN code against the smart card 48
4.8.2 Allow entry of PIN code longer than the maximum PIN length 48
4.8.3 Prevent alphabetic characters in PIN code 48
4.8.4 Prevent cancellation of Change PIN at first use 49
4.8.5 Prevent entry of PIN code shorter than the minimum PIN length 49
4.8.6 Prevent users from reusing current PIN during Change PIN 49
4.8.7 Unlock card contact telephone number 49
4.9 Smart Card 50
4.9.1 Turn on US Department of Defense configuration 50
4.9.2 Disable smart card discovery information caching 51
4.10 Smart Card Auto-Update 51
4.10.1 CMS MDIDC timeout (in seconds) 52
4.10.2 CMS Server URL 52
4.10.3 CMS Synchronization Manager timeout (in seconds) 52
4.10.4 Enable Card Auto-Update 53
4.10.5 Frequency of update (in days) 53
4.10.6 Maximum delay for card update check after card insertion 53
4.10.7 Maximum delay for card update check after Windows Logon 54
4.10.8 Maximum number of CMS MDIDC card update retries 54
4.10.9 Maximum number of CMS Synchronization Manager retries 54
4.11 Smart Card Readers 55
4.11.1 Enable the PIN Pad Readers Support 55
4.11.2 Smart Card Readers Black List 55
4.12 Software Auto-Update 56
4.12.1 Enable software auto update 56
4.12.2 Delay between update retries (in minutes) 56
4.12.3 Frequency of update (in days) 57
4.12.4 Maximum number of update retries 57
4.13 User Console 58
4.13.1 Disable deletion of user certificates 59
4.13.2 Disable One-Time Password generation 59
4.13.3 Disable One-Time Password synchronization 59
4.13.4 Hide Advanced Diagnostics icon 59
4.13.5 Hide CA Certificates folder 59
4.13.6 Hide Check for Card Update menu 60
4.13.7 Hide Export Certificate menu 60
4.13.8 Hide Help menu 60
4.13.9 Hide Import Certificate menu 60
4.13.10 Hide My Certificates folder 60
4.13.11 Hide My Personal Info option 61
4.13.12 Hide New Card menu 61
4.13.13 Hide Publish to GAL menu 61
4.13.14 Hide Reset Card menu 61
4.13.15 Hide Tasks View from Explorer bar 61
4.13.16 Hide the Smart Card Info icon 62
4.13.17 Hide Tree View from Explorer bar 62

4.13.18 Hide Unlock Card menu ... 62
4.13.19 Hide Use Reader menu and Reader list icon ... 62
4.13.20 Hide View Policy Settings menu ... 62
4.13.21 Hide View Unlock Code menu ... 63
4.13.22 Image displayed on the lower right corner of List view ... 63
4.13.23 Prevent users from switching between icon and detail view ... 63
4.14 Advanced Diagnostics ... 64
4.14.1 Email address where the diagnostics report will be sent ... 64
4.14.2 Hide Email menu in Advanced Diagnostics ... 64
4.14.3 Turn off smart card diagnostics in Advanced Diagnostics ... 64
4.15 Logging ... 65
4.15.1 Turn on ActivClient logging ... 65
4.15.2 Enable ActivClient performance logging for Microsoft Windows PKI Smart Card Logon ... 66
4.15.3 Full path to log files folder ... 66
4.15.4 Maximum number of backup files ... 66
4.15.5 Maximum log file size in MB ... 67
4.16 Microsoft Policies Relevant to ActivClient ... 67
4.16.1 Microsoft Windows Policies ... 67
4.16.1.1 Card Removal ... 67
4.16.1.2 Certificate Registration ... 68
4.16.1.3 Card Auto Registration (PIV Cards Only) ... 68
4.16.1.4 Smart Card PIN Unlock ... 69
4.16.2 Microsoft Outlook Policies ... 70
4.17 Citrix XenApp Configuration ... 72

5.0 Customizing the Setup ... 74

5.1 Setup Customization Methods ... 74
5.1.1 Using a Command Line ... 74
5.1.1.1 Basic Install Command Line ... 75
5.1.1.2 Remove Features ... 75
5.1.1.3 Force Features ... 76
5.1.2 Using Orca ... 76
5.1.3 Using InstallShield Admin Studio (or Wize Package Studio) ... 77
5.2 ActivClient Setup Customization Options ... 78
5.2.1 Customize the Feature Installation ... 78
5.2.2 Customize the Installation Path ... 80
5.2.3 Customize the Setup Behavior ... 80
5.2.3.1 Customize the Setup Restart Behavior ... 80
5.2.3.2 Run a Blind Setup ... 81
5.2.3.3 Avoid Conflict with Other MSI Products ... 82
5.2.3.4 Install Root Certificates Automatically ... 82

6.0 Deploying the Setup ... 83

6.1 Deploying Using Standard Methods ... 83
6.2 Deploying Using Active Directory Push ... 83
6.2.1 Create a Distribution Point ... 84
6.2.2 Assign a Package ... 84
6.2.3 Test a Package ... 86

6.2.4 Redeploy a Package ... 86
6.3 Deploying using Microsoft System Center Configuration Manager ... 87
6.3.1 Configure the Client Computers ... 88
6.3.2 Prepare Collections ... 88
6.3.3 Create a Package ... 88
6.3.4 Create and Update a Distribution Point ... 96
6.3.5 Create a Program ... 100
6.3.6 Create a Distributed Advertisement ... 108
6.3.6.1 Monitoring the Software Distribution ... 115
6.3.7 Run an Advertised Program on a Client ... 115

7.0 Upgrading and Updating ... 116

7.1 Upgrading ActivClient ... 116
7.1.1 Supported ActivClient Upgrades ... 116
7.1.2 Supported HID Global Mini Driver Upgrades ... 117
7.1.3 Upgrading Methods ... 117
7.2 Using ActivClient Auto-Update ... 117
7.2.1 ActivClient Auto-Update Overview ... 117
7.2.2 Prerequisites ... 119
7.2.3 Configure ActivClient Auto-Update ... 119
7.2.4 Configure ActivClient Auto-Update on the Client Machines ... 121

8.0 Uninstallation ... 122

8.1 ActivClient Uninstallation Methods ... 122
8.2 Uninstall the ActivClient Administrative Templates ... 122
8.2.1 Delete the Settings for a Local User ... 122
8.2.2 Delete the Settings for a Domain User ... 123
8.3 Restore Microsoft Settings ... 123

9.0 Outlook Usability Enhancements ... 124

9.1 Environment ... 124
9.1.1 Overview ... 124
9.1.2 Microsoft Outlook Email Clients ... 125
9.1.3 Microsoft Exchange Server ... 126
9.1.4 Emails From and To Any Email Client on Any Platform ... 126
9.2 Outlook Security Profile Configuration ... 126
9.2.1 Outlook Security Profile Settings ... 126
9.2.2 Outlook Security Profile Update ... 128
9.2.2.1 Profile Selection and Conditions for Security Profile Update ... 128
9.2.2.2 Security Profile Updated Values ... 130
9.2.3 Publish Certificate to GAL ... 132
9.2.3.1 Profile Selection and Email Account ... 133
9.2.3.2 Configuration ... 133
9.2.3.3 Workflow ... 133
9.2.3.4 Environment Considerations ... 134
9.2.3.5 Interactive Process ... 134
9.2.4 Audit ... 135
9.3 Auto-Contact ... 137

9.4 Auto-Decrypt 139

10.0 PIN Caching Service 140

10.1 Overview 140
10.2 Per Session or Per Process PIN Caching 141
10.2.1 Policy Name: Allow per-process PIN caching 141
10.2.2 Example 1: Per Process Mode 141
10.2.3 Example 2: Per Session Mode 141
10.2.4 Example 3: Per Session Mode 142
10.3 PIN Cache Timeout 142
10.3.1 Policy Name: Number of minutes before PIN cache is cleared 142
10.3.2 Exceptions 143
10.3.3 Example: PIN Cache Timeout of One Hour 143
10.4 PIN Caching for "PIN Always" Private Keys 143
10.4.1 Policy Name: Enable PIN caching for "PIN Always" private keys 144
10.4.2 Example 144
10.5 PIN Cache Clearance on Workstation Lock 145
10.5.1 Policy Name: Disable PIN cache clearance on workstation lock 145

11.0 Auto-Update with ActivID CMS 147

11.1 Overview 147
11.2 Configuration 147
11.3 Client Card Auto-Update Configuration 148
11.3.1 Policy Name: Enable Card Auto-Update 148
11.3.2 Policy Name: CMS Server URL 149
11.3.3 Policy Name: Maximum delay for card update check after Windows Logon 149
11.3.4 Policy Name: Maximum delay for card update check after card insertion 150
11.3.5 Policy Name: Frequency of update (in days) 151
11.4 ActivID CMS Connection Configuration 151
11.4.1 Policy Name: CMS Synchronization Manager timeout 151
11.4.2 Policy Name: CMS Synchronization Manager retry 152
11.4.3 Policy Name: CMS MDIDC timeout 152
11.5 Card Auto-Update Experience 152

12.0 Security Guidelines 154

12.1 FIPS Compliance 154
12.1.1 Microsoft CNG Versions 154
12.1.2 FIPS Policy Flag 154
12.1.3 ActivClient Compatibility with FIPS Approved Cryptographic Algorithms, Modes, and Key Sizes 155
12.1.4 FIPS Compliance for Firefox 155
12.1.5 FIPS Compliance for PKCS#11 155
12.1.6 FIPS Compliance for Terminal Services 156
12.1.6.1 Microsoft Remote Desktop Sessions 156
12.1.6.2 Citrix XenApp Sessions 156
12.2 SHA-2 Compliance 157
12.2.1 Card Content Signed with SHA-2 157
12.2.2 Using SHA-2 for Digital Signature Operations 158
12.3 PIN Policies 160

12.4 Log Handling 160
12.5 ActivClient Policies 160
12.6 Code Integrity 161
12.7 Hardening Desktop Security 161
12.8 Additional Recommendations 162

13.0 Troubleshooting 163

13.1 ActivClient Troubleshooting Tools 163
13.1.1 ActivClient Diagnostics Wizard 163
13.1.2 Advanced Customer Support Logging 163
13.2 Troubleshooting Strategies 163
13.2.1 Check Common Issues and Known Problems 164
13.2.2 Analyze Symptoms and Factors 164
13.2.3 Isolate the Error Condition and Reproduce the Error 164
13.2.4 Ask for Technical Support Resources 164

Appendix A: ActivClient Files and Processes 165

A.1. ActivClient 7.1 Installed Files (32-bit Edition) 165
A.2. ActivClient 7.1 Installed Files (64-bit Edition) 173
A.3. File Update After Installation 181

Appendix B: Registry Keys 182

B.1. Registry Keys Installed by ActivClient 7.1 (32-bit Edition) 182
B.2. Registry Keys Installed by ActivClient 7.1 (64-bit Edition) 185
B.3. Registry Keys Updated After Installation 189

Appendix C: Terms and Acronyms 190

C.1. Terms 190
C.2. Acronyms 192

List of Tables

Table 1: Microsoft Outlook enhancements policies 70
Table 2: ActivClient Setup Filenames and Editions 74
Table 3: Customizable Features 78
Table 4: Base Component Features 79
Table 5: Security Profile Configured Values 130
Table 6: Audited Event ID Codes 136
Table 7: ActivClient 7.1 32-bit Edition 165
Table 8: ActivClient 7.1 64-bit Edition 173
Table 9: Registry Keys Installed by ActivClient 7.1 (32-bit Edition) 182
Table 10: Registry Keys Installed by ActivClient 7.1 (64-bit Edition) 185

List of Figures

Figure 1: Updating ActivClient 118

1.0 Introduction



ActivID® ActivClient® guards against an ever-changing threat landscape by providing organizations with risk-appropriate and secure access to corporate IT assets.

1.1 Product Overview

HID Global's ActivID ActivClient is the latest smart card and USB token middleware from that allows enterprise and government customers to easily use smart cards and USB tokens to protect workstations and networks.

ActivClient enables the use of PKI certificates and keys and one-time passwords 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

ActivClient provides the following range of services:

- PKI services
- Remote access and One-Time Password (OTP) services
- Remote session services
- Management services (for end users and administrators)
- Development services with a Software Development Kit (SDK)

1.2 Document Scope and Audience

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

HID Global 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 document is for system administrators and integrators. You must have a good understanding of Microsoft® Windows® administrative templates (for ActivClient product customization) and Windows installer (for ActivClient setup customization).

2.0 ActivClient Deployment

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

Note: It is recommended that you first test the policy settings with a limited population of users before deploying to your wider organization.

2.1 Deployment and Policy Planning

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

  For further information, see the *ActivID 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 section 3.0 Defining the ActivClient Policies on page 15.

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

- Outlook Usability Enhancements on page 124
- PIN Caching Service on page 140
- Auto-Update with ActivID CMS on page 147

2.2 Preparation

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

For further information, see section 5.0 Customizing the Setup on page 74.

2.3 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 section 6.0 Deploying the Setup on page 83.

2.4 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 section 7.0 Upgrading and Updating on page 116.

2.5 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 section 13.0 Troubleshooting on page 163).

2.6 Administrative Tools

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

- Administrative setups − unsigned versions of the ActivClient MSI to use if you want to customize the setup. For further information, see section 5.0 Customizing the Setup on page 74.
- Configuration − Active Directory administrative template for ActivClient (in ADMX format) to use if you want to deploy ActivClient policies in an Active Directory environment. For further information, see section 3.0 Defining the ActivClient Policies on page 15.

3.0 Defining the ActivClient Policies

This section explains how to customize ActivClient using its policies.

For full details of the ActivClient policy settings, see section 4.0 ActivClient Policy Settings on page 27.

3.1 ActivClient Customization Methods

ActivClient policies are defined as Microsoft Windows administrative templates. You have two main methods to customize ActivClient:

- Using Active Directory Group Policy Objects on Microsoft Windows Server 2008 (or later) – this method enables organizations to define, manage and deploy policies for the whole organization.

  See section 3.2 Using Active Directory Group Policy Objects on Microsoft Windows Server on page 15.

- Using the Microsoft Windows Local Computer Policy editor – this method enables individual users to define policies specific to individual computers.

  See section 3.2.3 Customizing ActivClient Using the Microsoft Windows Local Computer Policy Editor on page 21.

If your organization uses an Enterprise Management product other than Active Directory, you can also customize the policies. See the technical documentation provided with your enterprise management product for more information about Microsoft Windows policy management.

3.2 Using Active Directory Group Policy Objects on Microsoft Windows Server

This section applies to Microsoft Windows Server 2008 or later.

The Active Directory Group Policy allows you to remotely set the configuration for a group of computers or users.

The ActivClient Administrative Template files are installed with the Configuration Management component during ActivClient setup. They are then copied to the standard **C:\Windows\PolicyDefinitions** folder.

The files are also provided on the ActivClient distribution, in the **Admin\Configuration** folder.

You can define the values of the ActivClient policies with the Active Directory Group Policy Editor. You can then push the values to all ActivClient users in the domain.

The following ActivClient Administrative Template files are provided:

- *HIDGlobal.admx* (and *HIDGlobal.adml*) that configures the root node under Administrative template under which all *HIDGlobal* settings are configured.
- *HIDGlobal.ActivClient.admx* (and *HIDGlobal.ActivClient.adml*) that contains all settings related to ActivClient. This node is defined under *HIDGlobal*.
- *HIDGlobal.Logging.admx* (and *HIDGlobal.Logging.adml*) that contains general logging settings defined as true policies. This node is defined under *HIDGlobal*.

- *HIDGlobal.AdvancedDiagnostics.admx* (and *HIDGlobal.AdvancedDiagnostics.adml*) that contains settings related to the Advanced Diagnostics tool. This node is defined under *HID Global*.

The policy deployed using the Active Directory Group Policy Object (GPO) overwrites the values configured locally.

You can also customize the setup to install the modified policy settings at installation. For further information, see section 5.0 Customizing the Setup on page 74.

Setting an GPO with default permissions causes the application to deploy for every user or computer within the domain.

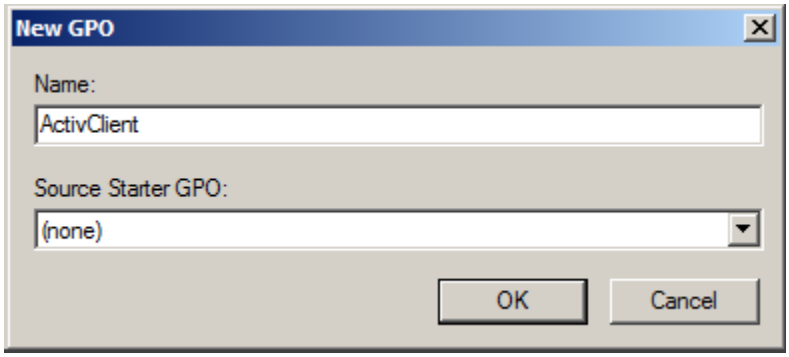
To deploy ActivClient policies you must first load ActivClient policies as a new Administrative Template. Then you need to make sure that only specified users receive the application.

Notes:

- You must have domain administration access rights to deploy the Group Policy.
- The ActivClient Administrative template defines only ActivClient policies. It does not provide 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 Microsoft Windows Server.

3.2.1 Add the ActivClient Administrative Template and Create the Group Policy

1. If you did not install the ActivClient Configuration Management component on the machine, you must copy the template files from the distribution:
   - Locate the ActivClient *.admx* template files in the **\Admin\Configuration** folder on your ActivClient distribution and copy them to **C:\Windows\PolicyDefinitions**.
   - Locate the ActivClient *.adml* template files in the **\Admin\Configuration\EN-US** folder on your ActivClient distribution and copy them to **C:\Windows\PolicyDefinitions\en-US**.
2. From the Start menu, go to **Administrative Tools**, and then select **Group Policy Management**.
3. In the console tree, right-click the domain or Organizational Unit that you want to configure, then select **Create a GPO in this domain...**.



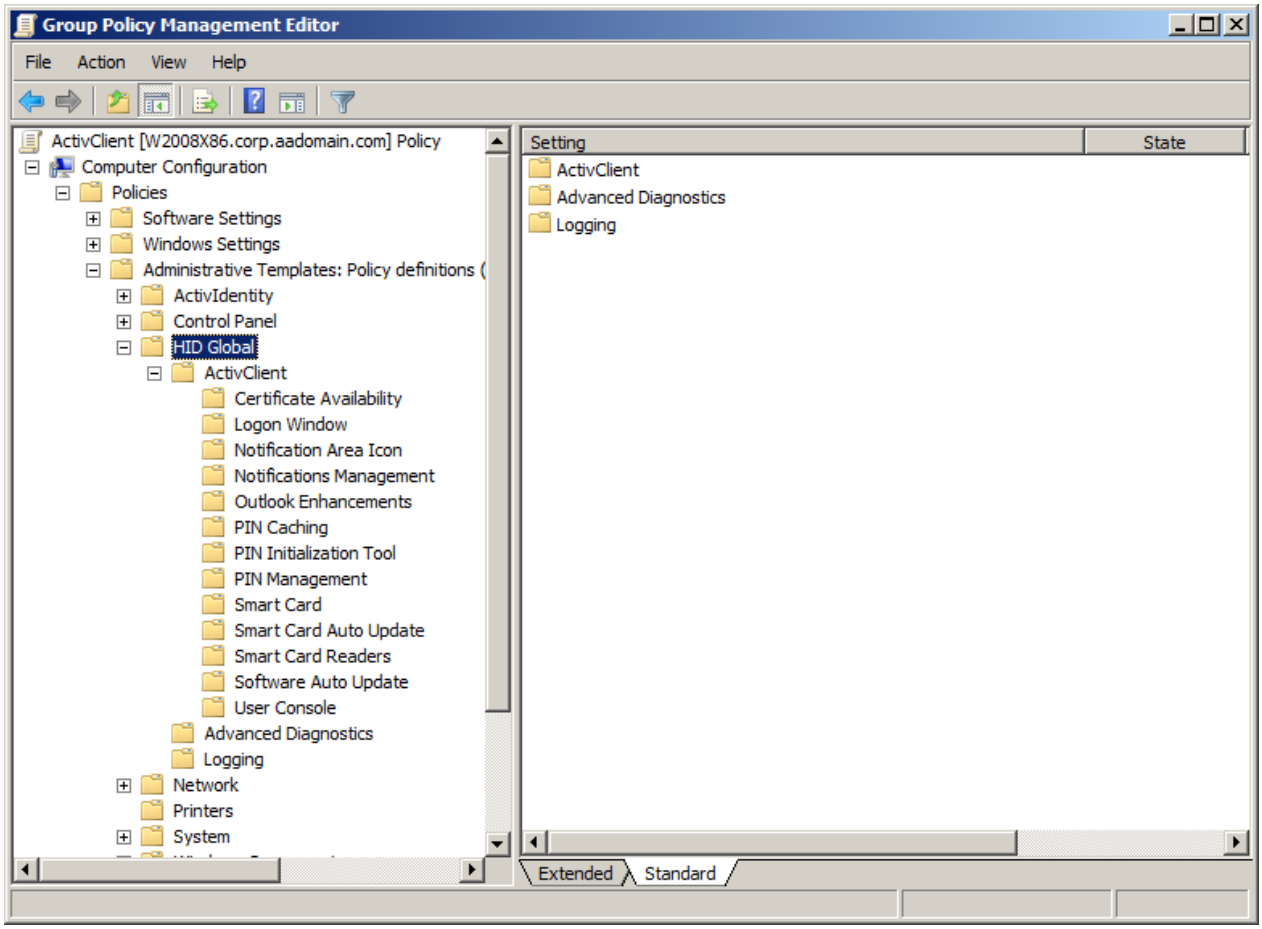
4. Create a Group Policy Object (GPO) called, for example, ActivClient, and click **OK**.

3.2.2 Configure the Policy Settings

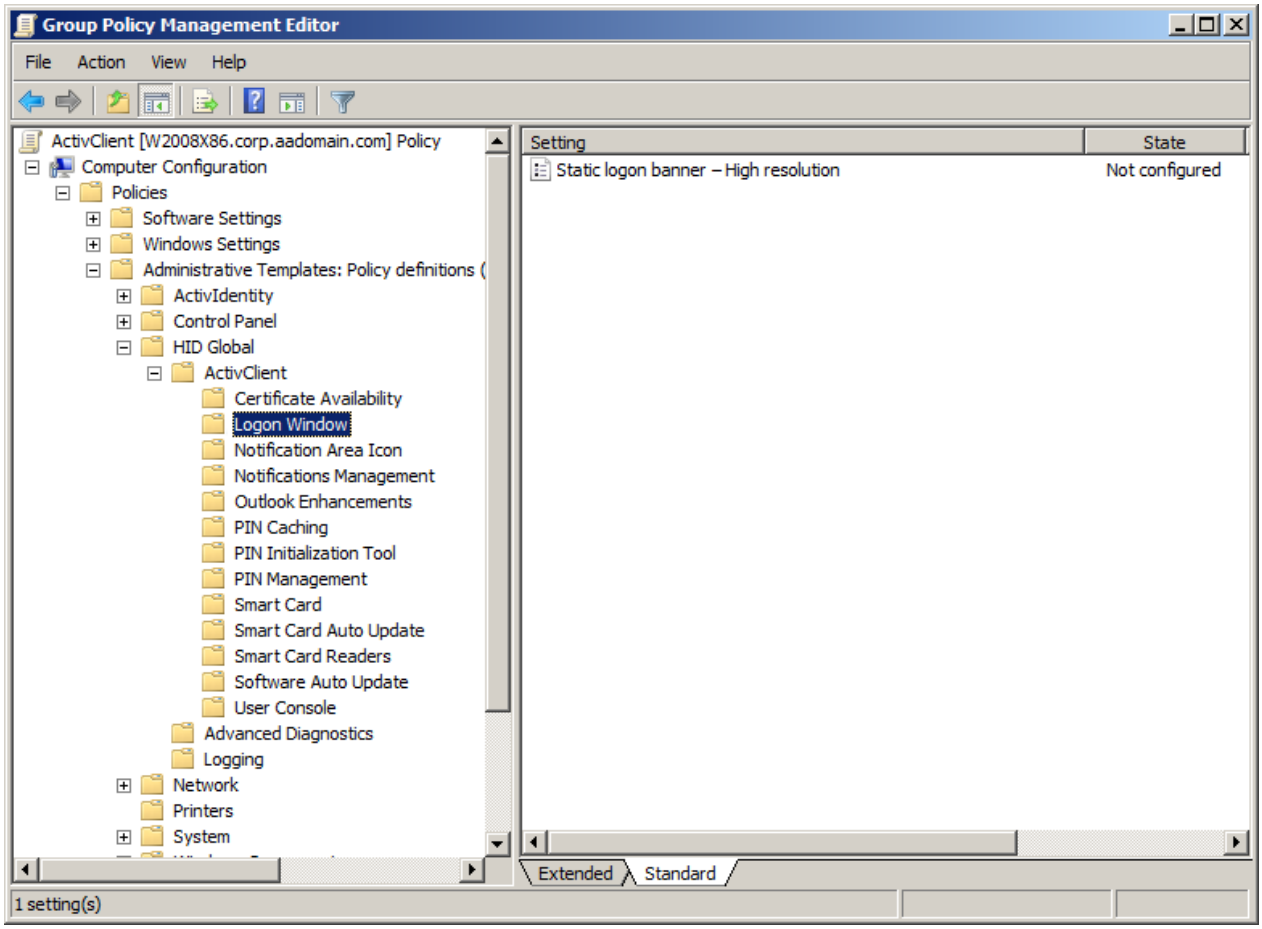
1. To modify the policy settings, right-click on the group policy you just created and select **Edit**.

   The Group Policy Management Editor opens.

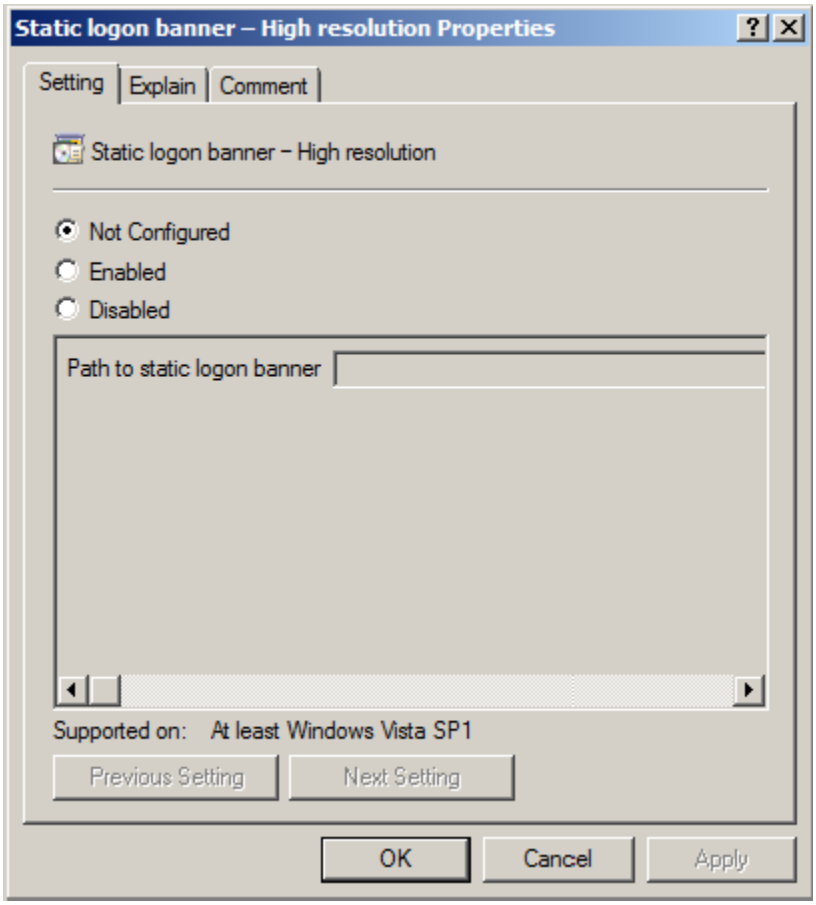
2. In the console tree, go to **Computer Configuration**, **Policies**, and then **Administrative Templates: Policy definitions**.



3. Expand the **HID Global** directory to display the available ActivClient settings.



4. Double-click on a policy setting (for example, Static logon banner) to display the properties.

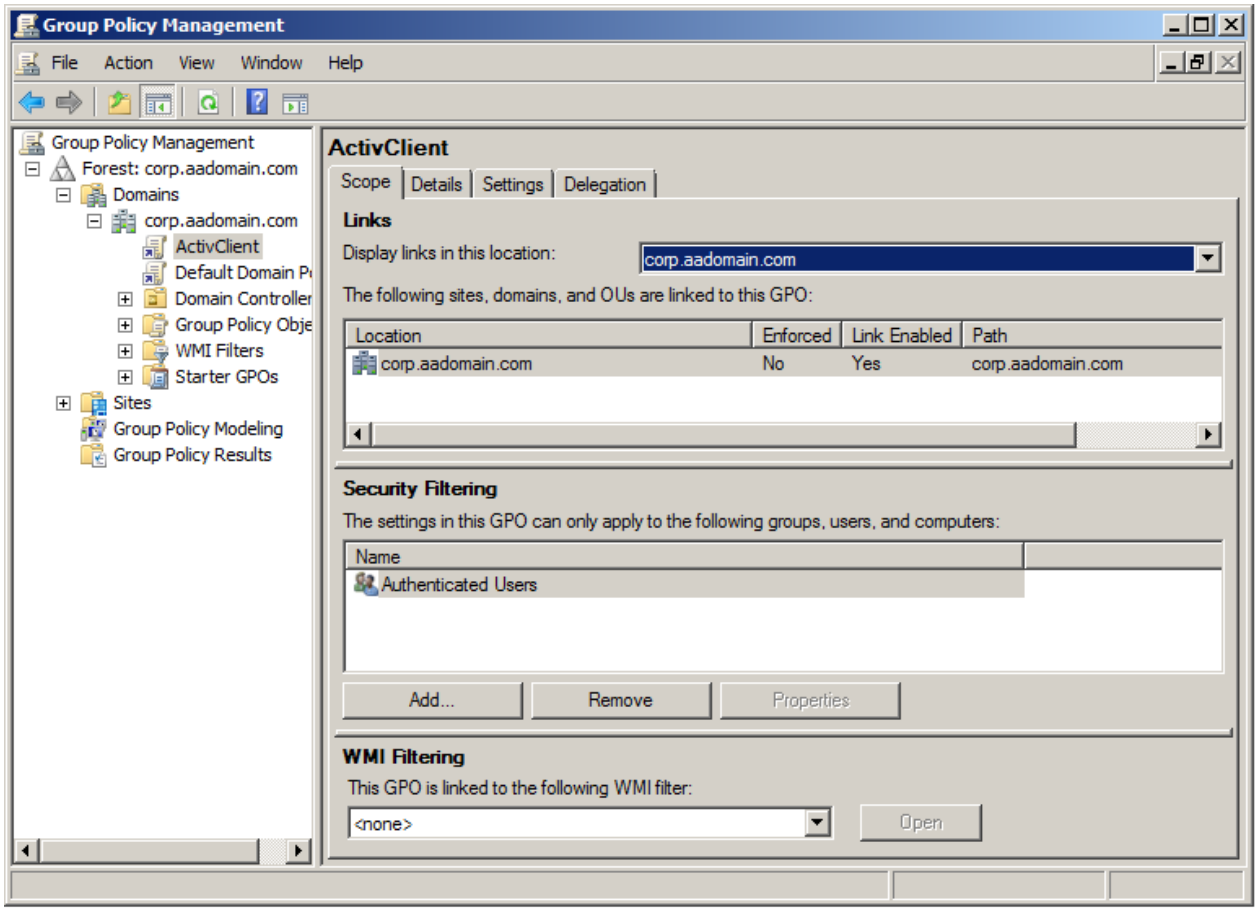


5. For settings that do not require a specific value (such as timeouts), you can set the status with the following options:

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 policy. 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 policy. If the default value is used, the policy is empty.
Disabled	When the status is Disabled and you click Apply, the setting is disabled. Any values remain in the policy and are used when the setting is Enabled.

Note: The Enabled behavior is the opposite of the default behavior (that is, Not Configured).

6. To apply the policy to specific users or group of users, return to the Group Policy Management console and double-click your group policy (in this example, ActivClient).



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

3.2.3 Customizing ActivClient Using the Microsoft Windows Local Computer Policy Editor

If your workstations are not managed centrally, you can customize ActivClient policies via the Windows Local Computer Policy editor.

The ActivClient Administrative Template files are installed with the Configuration Management component during ActivClient setup. They are then copied to the standard **C:\Windows\PolicyDefinitions** folder.

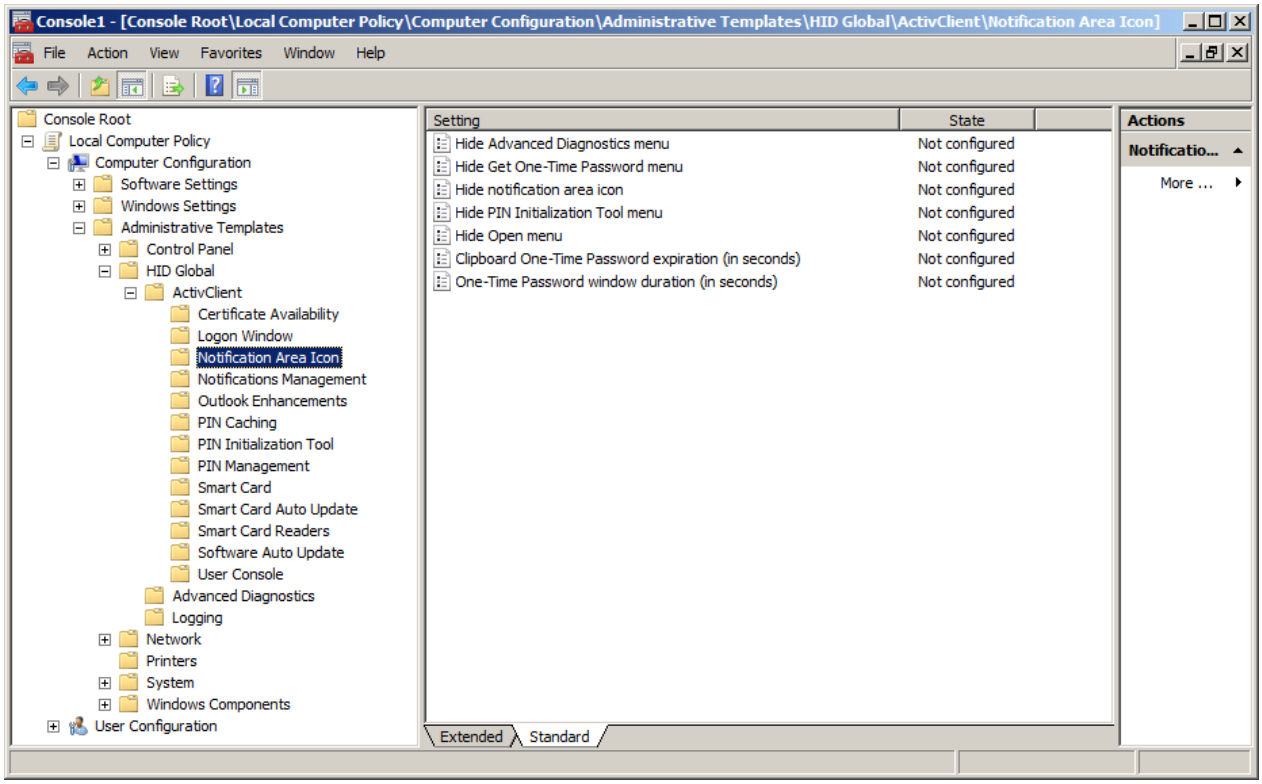
The files are also provided on the ActivClient distribution, in the **Admin\Configuration** folder.

The following ActivClient Administrative Template files are provided:

- *HIDGlobal.admx* (and *HIDGlobal.adml*) that configures the root node under Administrative template under which all *HIDGlobal* settings are configured.

- *HIDGlobal.ActivClient.admx* (and *HIDGlobal.ActivClient.adml*) that contains all settings related to ActivClient. This node is defined under *HIDGlobal*.
- *HIDGlobal.Logging.admx* (and *HIDGlobal.Logging.adml*) that contains general logging settings defined as true policies. This node is defined under *HIDGlobal*.
- *HIDGlobal.AdvancedDiagnostics.admx* (and *HIDGlobal.AdvancedDiagnostics.adml*) that contains settings related to the Advanced Diagnostics tool. This node is defined under *HIDGlobal*.

1. Start the Microsoft Management Console (*mmc.exe*) and, from the **File** menu, click **Add/Remove Snap-in**.
2. Add the **Group Policy Object Editor** snap-in, select the **Local Computer**, and click **OK**.
3. Under **Computer Configuration**, go to **Administrative Templates**, and then **HID Global**.
4. View and edit ActivClient product settings (ActivClient, Advanced Diagnostics and Logging).



5. For settings that do not require a specific value (such as timeouts), you can set the status with the following options:

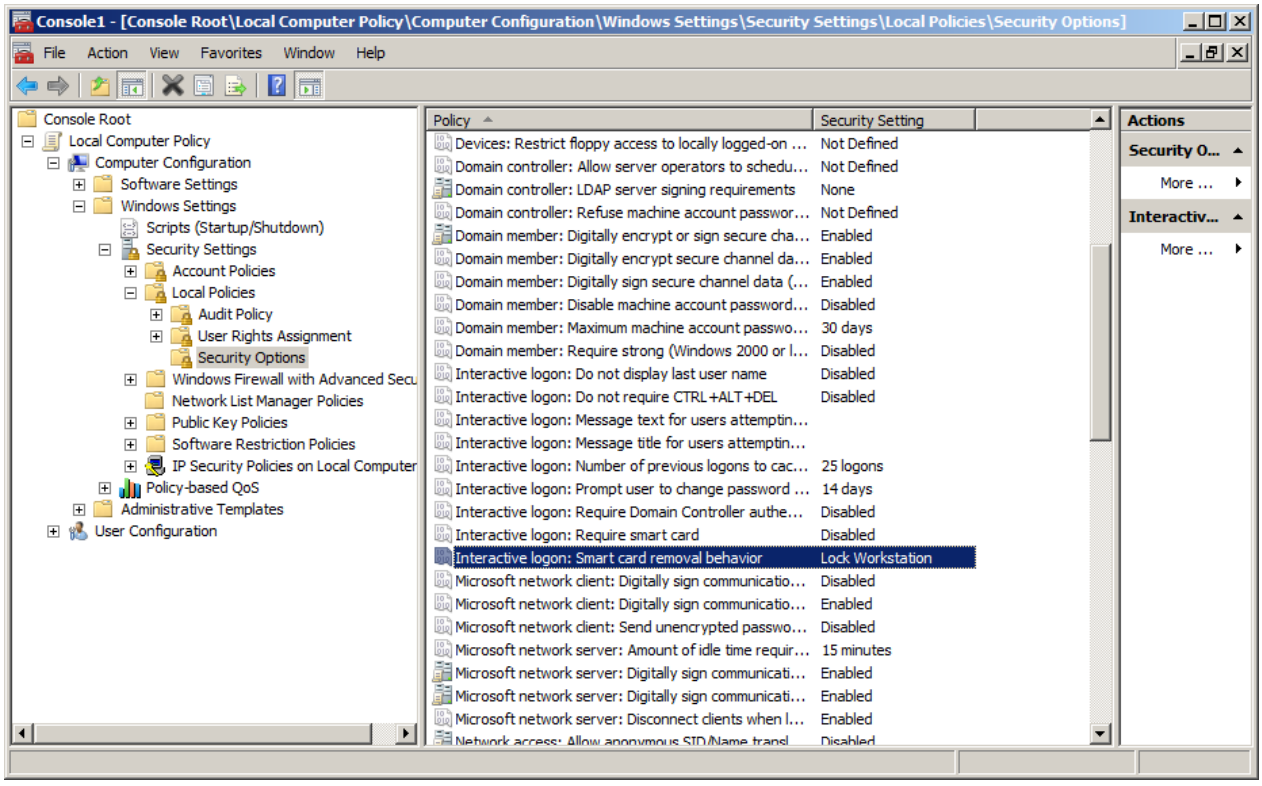
Status	Description
Not Configured	When the status is Not Configured and you click Apply, the setting is disabled and any previous values are cleared from the policy. New values are required when the setting is Enabled.

Status	Description
Enabled	When the status is Enabled and you click Apply, the values you enter are stored in the policy. If the default value is used, the policy is empty.
Disabled	When the status is Disabled and you click Apply, the setting is disabled. Any values remain in the policy and are used when the setting is Enabled.

Note: The Enabled behavior is the opposite of the default behavior (that is, Not Configured).

6. You can also view and edit relevant Microsoft settings.

   The following example illustrates the smart card removal behavior policy.



Note: All ActivClient settings are available for configuration and/or update, even settings related to features that have not been installed on the local computer.

If settings related to non-installed features are modified, changes will not be taken into account.

3.3 Importing and Exporting Policies

3.3.1 Domain Machines

If you deploy ActivClient in an Active Directory domain, then ActivClient policies should be configured via GPOs at the domain level. The Group Policy Management Console gives access to machines and OUs where the policies have to be set.

Once the Group Policy is defined, the policy will be applied to the user or machine at the next group policy update either:

- At logon.
- AI specified intervals.
- When a `gpupdate /force` command is executed.

Microsoft provides recommendations on the Group Policy phased deployment at http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx#BKMK_GP_STAGE

Microsoft Windows Server 2008 also introduces the *Starter GPO* concept (http://technet.microsoft.com/en-us/library/cc753200.aspx) that allows defining the GPO settings and import or export them as required. The starter GPO, when created, is configured with the default settings of the policy template.

3.3.2 Non-Domain Machines

If you deploy ActivClient on standalone machines, you can configure policies using the Windows Local Computer Policy Editor. You can then export these policies and import them on other machines by following a simple procedure:

1. Go to **%systemroot%\system32\grouppolicy**.
2. Copy the machine and user folder to the same location of the targeted machine.
3. Run the `gpupdate /force` command on the target machine to apply the new policy.

3.4 Viewing Active Policies

If ActivClient policies are configured by GPOs or by local policies, there can be several policies affecting the behavior on the local workstation.

3.4.1 About Group Policy Processing in a Microsoft Windows Environment

- Group Policy settings for computers are processed in the following order:
  - Local
  - Site

- Domain
- Organizational units (from the highest OU in hierarchy to the lowest, meaning that the lowest OU setting takes precedence over higher ones)

  This order means that the local Group Policy object is processed first, and Group Policy objects that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites the earlier Group Policy objects. Go to http://technet.microsoft.com/en-us/library/cc778890(WS.10).aspx for more information.

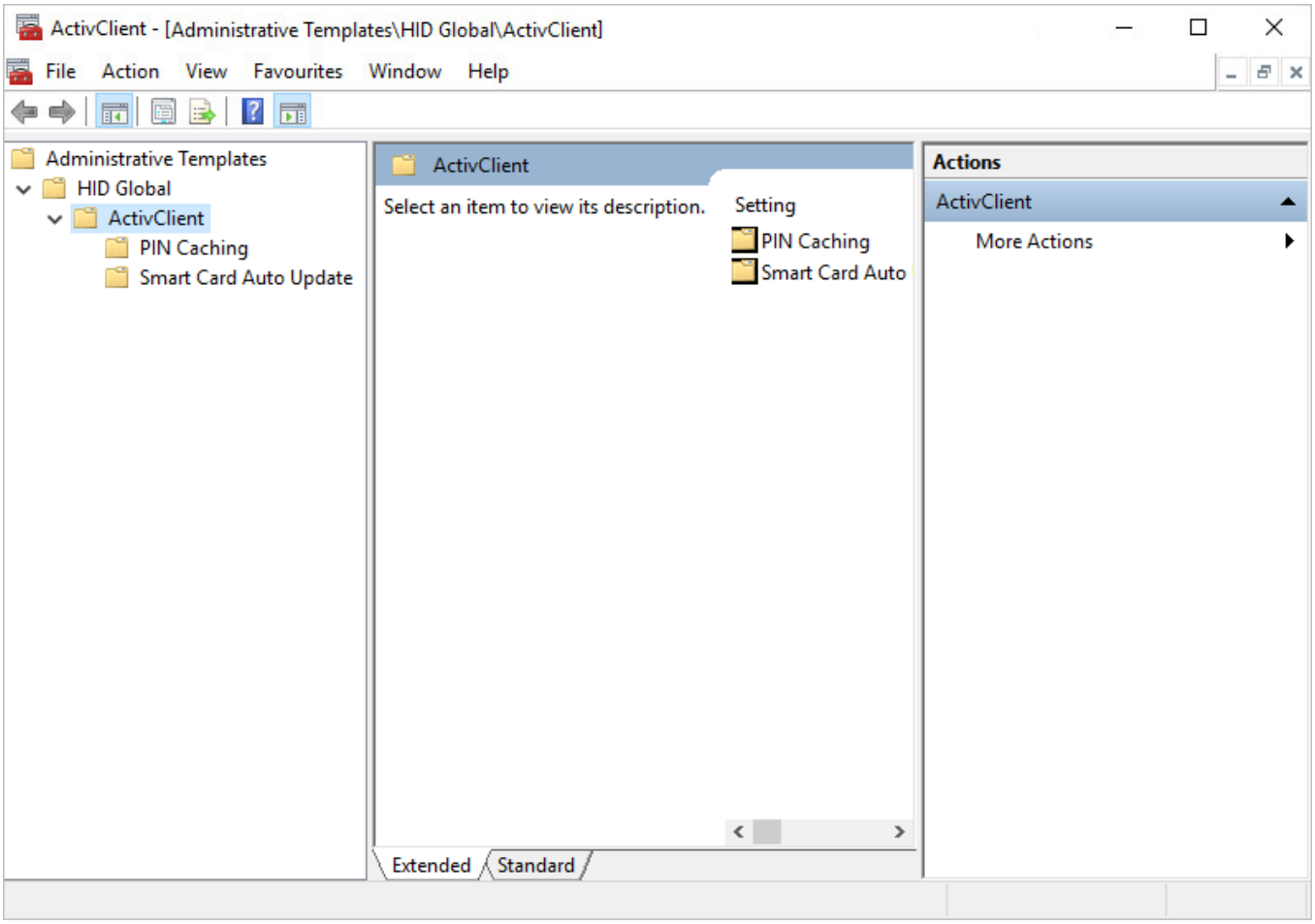
- Group policies are applied to the computer when they are connected to the domain. So even if a user logs on to Microsoft Windows offline, with cached domain credentials, the last group policy objects are applied and cannot be modified.
- Group Policy refreshes policy settings at a regular interval, which is every 90 minutes by default. This value is configurable by a Group Policy administrator.
- Group policy refresh can also be enforced by executing the command line `gpupdate /force`.

3.4.2 ActivClient Resultant Set of Policies

ActivClient includes a utility that displays the 'resultant set of policies' active on the workstation. It is recommended that you use this utility to check that policies set on the domain controller are properly pushed to the workstations.

1. From the ActivClient User Console, select **Tools**, then **Advanced** and then **View Policy Settings…**.

   You are prompted for administrative privileges, if applicable.



2. You can view the HID Global ActivClient policies in the **Administrative Templates** folder.

   For each policy, you can view, but not edit, the policy value.

Only the configured policies (that is, policies set to Enabled or Disabled) are displayed.

If policies are Not Configured (which is the default), they do NOT display. In other words, this tool displays only the policies that differ from the default ActivClient configuration. In a default configuration (no customization), the ActivClient folder under Administrative Templates will not display.

4.0 ActivClient Policy Settings

You can customize the behavior of ActivClient by updating the settings described in this section:

- For details on how to modify these settings at installation, see section 5.0 Customizing the Setup on page 74.
- For details on how to propagate these settings, see section 3.2 Using Active Directory Group Policy Objects on Microsoft Windows Server on page 15.

The ActivClient policy settings are divided into the following categories:

Policy category (by section)	Action for changes to be applied
Certificate Availability on page 28	Restart the workstation
Login Window on page 29	Restart the workstation
Notification Area Icon (ActivClient Agent) on page 30	Restart ActivClient Agent
Notifications Management on page 32	Restart the workstation
Outlook Enhancements on page 42	Restart Outlook
PIN Caching on page 46	Restart the workstation
PIN Initialization Tool on page 47	Restart the PIN Initialization Tool
PIN Management on page 48	Restart the workstation
Smart Card on page 50	Restart the workstation
Smart Card Auto-Update on page 51	Restart the workstation
Smart Card Readers on page 55	Restart the workstation
Software Auto-Update on page 56	Restart the workstation
User Console on page 58	Restart the User Console
Advanced Diagnostics on page 64	Restart the Advanced Diagnostics Tool
Logging on page 65	Restart 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.

4.1 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, Microsoft Edge and Microsoft Outlook) require the certificates to be available in Microsoft Windows (specifically registered to the Microsoft Windows CAPI store) prior to using them.

ActivClient leverages a Microsoft Windows feature to automatically register smart card certificates in the Microsoft Windows CAPI store on card insertion (this is often referred to as 'certificate propagation'). This feature is controlled by a Microsoft Windows policy. See section 4.16.1.2 Certificate Registration on page 68 for details.

The following are ActivClient policies that complement the Microsoft Windows policy:

- Display certificate replacement warning on page 28
- Remove certificates from Microsoft Windows on logoff on page 28
- Remove certificates from Microsoft Windows on smart card removal on page 29
- Turn off automatic configuration of Microsoft Windows EFS smart card certificate on page 29

RESTART THE WORKSTATION

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

4.1.1 Display certificate replacement warning

Description: Defines if a warning is displayed before the default certificate is replaced during certificate download with Microsoft Internet Explorer.

If this setting is not configured or disabled, then the warning is not displayed.

4.1.2 Remove certificates from Microsoft 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 is inserted in the card reader during the log-off operation.

Description: Defines if user certificates are removed from Microsoft Windows when users log off.

Enable this feature if you are using a shared Microsoft 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.

If this setting is not configured or disabled, then certificates are not removed from Microsoft Windows on logoff.

When this setting is enabled, the smart card must remain inserted during logoff for certificates to be removed from Microsoft Windows properly.

4.1.3 Remove certificates from Microsoft Windows on smart card removal

Description: Removes user certificates from Microsoft Windows when users remove their smart card.

Enable this feature 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.

If this setting is not configured or disabled, then certificates are not removed from Microsoft Windows on card removal.

4.1.4 Turn off automatic configuration of Microsoft Windows EFS smart card certificate

Description: Disables the automatic configuration of the Encrypting File System feature with a smart card certificate after Microsoft Windows PKI smart card logon. This feature automatically selects which certificate will be used for EFS.

If this setting is not configured or disabled, then the certificate that will be used for EFS is automatically selected.

4.2 Login Window

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

The following section details the Login Window policy settings that enable you to select the banner you want to apply.

> **RESTART WORKSTATION**
>
> For the Login Window policy changes to be applied, you must restart the workstation.

The default static logon banner is:



Size = 413 x 72.

4.2.1 Static Logon Banner—high resolution

Description: In the Value column, select a path to a banner (*.bmp* format) to be displayed in the Enter PIN window in high resolution mode.

If this setting is not configured or disabled, then the ActivID ActivClient static banner is displayed.

Possible Values:

- Not Configured
- Enabled – enter the path to the required image.
- Disabled

4.3 Notification Area Icon (ActivClient Agent)

Some policies are only available if the associated ActivClient components are installed. For example, the policy allowing to access the Advanced Diagnostics tool.

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:

- Clipboard One-Time Password expiration (in seconds) on page 30
- Hide Advanced Diagnostics menu on page 30
- Hide Get One-Time Password menu on page 31
- Hide notification area icon on page 31
- Hide Open menu on page 31
- Hide PIN Initialization Tool menu on page 31
- One-Time Password window duration (in seconds) on page 31

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.

4.3.1 Clipboard One-Time Password expiration (in seconds)

Description: Defines for how long (in seconds) the One-Time Password is available on the Clipboard.

If this setting is not configured, then the One-Time Password is available for 30 seconds on the Clipboard.

If this setting is disabled, the generated One-Time Password is not automatically copied to the Clipboard.

Possible Values:

- Not Configured
- Enabled – displays the default value, 30, and can be updated
- Disabled

4.3.2 Hide Advanced Diagnostics menu

Description: Defines if the Advanced Diagnostics menu item is displayed in the ActivClient Agent menu. This option starts the Advanced Diagnostics tool, allowing users and help desk operators to diagnose ActivClient.

This menu is not displayed if the Troubleshooting feature is not installed.

If this setting is not configured or disabled, then the Advanced Diagnostics menu is displayed.

4.3.3 Hide Get One-Time Password menu

Description: Defines if the Get One-Time Password menu is displayed, allowing users to generate a smart card-based One-Time Password from the ActivClient Agent.

If this setting is not configured or disabled, the Get One-Time password menu is displayed.

4.3.4 Hide notification area icon

Description: Defines if the ActivClient Smart Card agent icon is displayed in the Microsoft Windows notification area.

If this setting is not configured or disabled, then the ActivClient Agent icon is displayed.

4.3.5 Hide Open menu

Description: Defines if the Open menu item is displayed in the ActivClient Agent menu. This option opens the ActivClient User Console.

If this setting is not configured or disabled, the Open menu item is displayed.

4.3.6 Hide PIN Initialization Tool menu

Description: Defines if the PIN Initialization Tool menu item is displayed in the ActivClient Agent menu. This option starts the PIN Initialization Tool, allowing users to initialize smart cards.

This menu is not displayed if the PIN Initialization Tool feature is not installed.

If this setting is not configured or disabled, then the PIN Initialization Tool menu is displayed.

4.3.7 One-Time Password window duration (in seconds)

Description: Defines for how long (in seconds) the One-Time Password notification window is displayed.

If this setting is not configured, the One-Time Password notification window is displayed for 10 seconds.

If this setting is disabled, the generated One-Time Password is not displayed in a notification window.

Possible Values:

- Not Configured
- Enabled – displays the default value, 10, and can be updated
- Disabled

4.4 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:

- Blocked Card Manager message (Windows 7 on page 33
- Blocked Card Manager message (Windows 8 on page 33
- Blocked Card Manager title (Windows 8 on page 33
- Card Auto-Update Alert duration (in seconds) on page 34
- Card Auto-Update Alert message (Windows 7 on page 34
- Card Auto-Update Alert message on page 34
- Card Auto-Update Alert title on page 35
- Delay before checking expiration after card insertion (in seconds) on page 35
- Display Card Expiration notification on page 35
- Display Certificate Expiration notification on page 36
- Display New Card window on card insertion on page 36
- Expiration notification period (in days) on page 36
- Expiration warning message on page 37
- Expiration warning period (in days) on page 37
- Hide Blocked Card Manager message when a smart card with a blocked card manager is inserted on page 37
- Hide No Smart Card Reader Alert on page 37
- Locked Card Message (Windows 7 and earlier) on page 38
- Locked Card Message (Windows 8 and later) on page 38
- Locked Card Title (Windows 8 and later) on page 38
- No Smart Card Reader Alert duration (in seconds) on page 39
- No Smart Card Reader Alert message on page 39
- No Smart Card Reader Alert message on page 39
- No Smart Card Reader Alert title on page 40

RESTART WORKSTATION

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

- Prevent Unlock Card window prompt when a locked card is inserted on page 40
- Unattended Smart Card Alert on page 40
- Unattended Smart Card Alert Sound on page 41

4.4.1 Blocked Card Manager message (Windows 7 and earlier)

Description: Specifies the message displayed to users when a smart card with a blocked Card Manager is inserted.

Note: To be displayed properly, the message must not exceed 243 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Your smart card's Card Manager is blocked; please contact the person or organization who gave you this card.", and can be updated
- Disabled

4.4.2 Blocked Card Manager message (Windows 8 and later)

Description: Specifies the message displayed to users when a smart card with a blocked Card Manager is inserted.

Note: To be displayed properly, the message must not exceed 60 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Please contact your administrator to unblock your smart card.", and can be updated
- Disabled

4.4.3 Blocked Card Manager title (Windows 8 and later)

Description: Specifies the title displayed on Windows 8 to users when the Card Manager is blocked.

Note: To be displayed properly, the message must not exceed 40 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Card Manager Blocked", and can be updated

- Disabled

4.4.4 Card Auto-Update Alert duration (in seconds)

Description: Defines for how long (in seconds) the Card Auto-Update Alert is displayed.

If this setting is not configured or disabled, then the Card Auto-Update Alert is displayed for 5 seconds.

The minimum value allowed is 1 second.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

4.4.5 Card Auto-Update Alert message (Windows 7 and earlier)

Description: Specifies the message displayed to users when a card auto-update request is available.

Note: To be displayed properly, the message must not exceed 243 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Smart Card Update \n\nActivClient has detected that an update is available for your card. \n\nPlease click the link below in order to proceed with the update.", and can be updated
- Disabled

4.4.6 Card Auto-Update Alert message (Windows 8 and later)

Description: Specifies the message displayed on Windows 8 to users when a card auto-update request is available.

Note: To be displayed properly, the message must not exceed 60 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Please log on to the My Digital ID Card portal to update your card.", and can be updated
- Disabled

4.4.7 Card Auto-Update Alert title (Windows 8 and later)

Description: Specifies the title displayed on Windows 8 to users when a card auto-update request is available.

Note: To be displayed properly, the message must not exceed 40 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Card Update available.", and can be updated
- Disabled

4.4.8 Delay before checking expiration after card insertion (in seconds)

Description: Defines for how long (in seconds) ActivClient should wait after smart card insertion or Microsoft Windows logon/unlock before checking for smart card or certificate expiration.

If this setting is not configured or disabled, the delay is 20 seconds.

Possible Values:

- Not Configured
- Enabled – displays the default value, 20, and can be updated
- Disabled

4.4.9 Display Card Expiration notification

Description: Defines if the Card Expiration notification is displayed to users when their smart card has expired or will expire soon.

If this setting is not configured or disabled, the Card Expiration notification is not displayed.

A setup preference also exists for this setting, which might affect the behavior if this policy setting is not configured.

The goal of this setup preference is to enable you to install ActivClient with the US Department of Defense configuration option and automatically have access to the specified configuration, without having to configure additional policies:

- If the US Department of Defense configuration option is selected in the ActivClient setup and if the Display Card Expiration notification policy is not configured or disabled, then the expiration notification is displayed.
- If the US Department of Defense configuration option is not selected in the ActivClient setup and if the Display Card Expiration notification policy is not configured or disabled, then the expiration notification is not displayed.
- If the Display Card Expiration notification policy is Enabled, then it takes precedence over the preference set in the ActivClient setup.

4.4.10 Display Certificate Expiration notification

Description: Defines if the Certificate Expiration notification is displayed to users when their certificates have expired or will expire soon.

If this setting is not configured or disabled, then the Certificate Expiration notification is not displayed.

A setup preference also exists for this setting, which might affect the behavior if this policy setting is not configured.

The goal of this setup preference is to enable you to install ActivClient with the US Department of Defense configuration option and automatically have access to the specified configuration, without having to configure additional policies:

- If the US Department of Defense configuration option is selected in the ActivClient setup and if the Display Certificate Expiration notification policy is not configured or disabled, then the expiration notification is displayed.
- If the US Department of Defense configuration option is not selected in the ActivClient setup and if the Display Certificate Expiration notification policy is not configured or disabled, then the expiration notification is not displayed.
- If the Display Certificate Expiration notification policy is Enabled, then it takes precedence over the preference set in the ActivClient setup.

4.4.11 Display New Card window on card insertion

Description: Defines if users are prompted 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 ActivID Authentication Server or ActivID CMS, as these products manage the PIN instead of ActivClient.

If this setting is disabled or not configured, then ActivClient does not prompt users to initialize their smart card.

4.4.12 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.

If this setting is not configured or disabled, then the notification period is 5 days.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

4.4.13 Expiration warning message

Description: Specifies the message displayed when the user's smart card or a certificate has expired or will expire soon.

Note: To be displayed properly, the message must not exceed 190 characters.

If this setting is not configured or disabled, then then default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Contact the person or organization who gave you this smart card.", and can be updated
- Disabled

4.4.14 Expiration warning period (in days)

Description: Defines for how long (in days), before smart card or certificate expiration, the warning message should start to be displayed.

If this setting is not configured or disabled, then the message starts to be displayed 60 days before expiration.

Possible Values:

- Not Configured
- Enabled – displays the default value, 60, and can be updated
- Disabled

4.4.15 Hide Blocked Card Manager message when a smart card with a blocked card manager is inserted

Description: Defines if the Blocked Card Manager message is displayed when users insert a smart card with a blocked Card Manager.

If this setting is not configured or disabled, the message is displayed when users insert a smart card with a blocked Card Manager.

4.4.16 Hide No Smart Card Reader Alert

Description: Defines if an alert to inform users that no smart card reader is connected to the workstation is displayed.

If this setting is not configured or disabled, then the alert is displayed when no reader is connected.

4.4.17 Locked Card Message (Windows 7 and earlier)

Description: Specifies the message displayed to users when a locked smart card is inserted and that cannot be unlocked with ActivClient (static unlock code or challenge/response unlock are unavailable).

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "ActivClient has detected that the inserted smart card PIN is locked. Please contact the person or organization who gave you this card ", and can be updated
- Disabled

4.4.18 Locked Card Message (Windows 8 and later)

Description: Specifies the message displayed to users when a locked smart card is inserted and that cannot be unlocked with ActivClient (static unlock code or challenge/response unlock are unavailable).

Note: To be displayed properly, the message must not exceed 60 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Please contact your administrator to unlock your smart card", and can be updated
- Disabled

4.4.19 Locked Card Title (Windows 8 and later)

Description: Specifies the title displayed to users when a locked smart card is inserted and that cannot be unlocked with ActivClient (static unlock code or challenge/response unlock are unavailable).

Note: To be displayed properly, the message must not exceed 40 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "PIN Blocked", and can be updated
- Disabled

4.4.20 No Smart Card Reader Alert duration (in seconds)

Description: Defines for how long (in seconds) the No Smart Card Reader Alert is displayed.

If this setting is not configured or disabled, then the alert is displayed for 5 seconds. The minimum value allowed is 1 second.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

4.4.21 No Smart Card Reader Alert message (Windows 7 and earlier)

Description: Specifies the message displayed to users when no smart card reader is connected to the workstation.

Note: To be displayed properly, the message must not exceed 243 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Card Reader Not Detected \n\nActivClient was unable to detect a smart card reader connected to your computer.\n\nPlease verify that your smart card reader is properly connected.", and can be updated
- Disabled

4.4.22 No Smart Card Reader Alert message (Windows 8 and later)

Description: Specifies the message displayed on Windows 8 to users when no smart card reader is connected to the workstation.

Note: To be displayed properly, the message must not exceed 60 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Please check your card reader connection.", and can be updated
- Disabled

4.4.23 No Smart Card Reader Alert title (Windows 8 and later)

Description: Specifies the title displayed on Windows 8 to users when no smart card reader is connected to the workstation.

Note: To be displayed properly, the message must not exceed 40 characters.

If this setting is not configured or disabled, then the default text is displayed.

Possible Values:

- Not Configured
- Enabled – displays the default text, "Card Reader Not Detected", and can be updated
- Disabled

4.4.24 Prevent Unlock Card window prompt when a locked card is inserted

Description: Disables prompting users with the Unlock Card window when users insert a locked smart card if this feature does not suit your deployment (for example, if you do not provide a card unlock service via the telephone).

If this setting is disabled or not configured, then ActivClient prompts users with the Unlock Card window.

4.4.25 Unattended Smart Card Alert

Description: Defines when to warn users if their smart card is still inserted in the smart card reader at log off or screen lock.

ActivClient can be configured to notify user at log off and screen lock, at log off only, or never.

ActivClient offers audio-only notification (three beeps).

If this setting is not configured or disabled, users are notified of the unattended smart card at log off and screen lock.

Possible Values:

- Not Configured
- Enabled – displays the default value, 'At log off and screen lock', and can be updated with a value from the drop-down list:
  - Only at log off
  - At log off and screen lock
  - Never
- Disabled

4.4.26 Unattended Smart Card Alert Sound

Description: Specifies the full path to an audio file (*.wav*) to be played when a smart card is still inserted in the smart card reader at log off or screen lock.

If this setting is not configured or disabled, users are notified of the unattended smart card by the default sound (three beeps).

Possible Values:

- Not Configured
- Enabled – enter the full path to the audio file to be played
- Disabled

4.5 Outlook Enhancements

For a full description of Outlook enhancements, see section 9.0 Outlook Usability Enhancements on page 124.

ActivClient policies complement some Microsoft Outlook policies related to the Microsoft Outlook security profile. See section 4.16.2 Microsoft Outlook Policies on page 70 for details.

The following sections detail the ActivClient policy settings for the Microsoft Outlook enhancements:

- Allow different email addresses in smart card certificate and Microsoft Exchange account on page 42
- Check CRL for Microsoft Outlook security profile creation and Publish to GAL on page 43
- Check CRL timeout for Microsoft Outlook security profile creation and Publish to GAL on page 43
- Disable audit for Microsoft Outlook security profile creation and Publish to GAL on page 43
- Encryption algorithm configured in Security Profile on card insertion on page 44
- Hash algorithm configured in Security Profile on card insertion on page 44
- Microsoft Outlook Auto-Contact destination folder on page 45
- Turn off automatic addition of sender's certificates to Microsoft Outlook contacts on page 45
- Turn off setup email certificates in Microsoft Outlook on card insertion on page 45
- Turn on automatic decryption of encrypted emails on page 45
- Turn on automatic publication of certificates to the Global Address List on page 46

RESTART OUTLOOK

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

4.5.1 Allow different email addresses in smart card certificate and Microsoft Exchange account

Description: Defines if ActivClient checks that the smart card certificates used to configure the Microsoft Outlook profile (and also published to the GAL) are associated to the current Microsoft Outlook user. Specifically, it validates that the certificate email address corresponds to the email address configured for the Microsoft Exchange account.

If this setting is not configured or disabled, then the email address in certificate is checked against the address configured for the user in Microsoft Exchange account.

4.5.2 Check CRL for Microsoft Outlook security profile creation and Publish to GAL

Description: Defines if a CRL check is required in order to automatically configure email certificates in Microsoft 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 Microsoft 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.

If the setting is not configured, it is set to 'Enabled and enforced'.

Possible Values:

- 0: Disabled
- 1: Enabled and enforced (default)
- 2: Enabled and not enforced

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

Description: Defines the 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.

If this setting is not configured or disabled, the value is set to 0.

Possible Values:

- Not Configured
- Enabled – displays the default value, 20000, and can be updated
- Disabled

4.5.4 Disable audit for Microsoft Outlook security profile creation and Publish to GAL

Description: Disables the audit of Microsoft Outlook security profile creation and certificate publication to the Global Address List.

If this setting is not configured or disabled, then audit is performed.

4.5.5 Encryption algorithm configured in Security Profile on card insertion

Description: Defines the encryption algorithm configured in the Microsoft Outlook security profile on smart card insertion.

If this setting is not configured or disabled, then 3DES is used.

Possible Values:

- Not Configured
- Enabled – select one of the following values from the drop-down list:
  - 3DES (default)
  - AES (128-bit)
  - AES (192-bit)
  - AES (256-bit)
  - DES
  - RC2 (40-bit)
  - RC2 (64-bit)
  - RC2 (128-bit)
- Disabled

4.5.6 Hash algorithm configured in Security Profile on card insertion

Description: Defines the hashing algorithm configured in the Microsoft Outlook security profile on smart card insertion.

If this setting is not configured or disabled, then SHA-1 is used.

Possible Values:

- Not Configured
- Enabled – select one of the following values from the drop-down list:
  - SHA-1 (default)
  - SHA-256
  - SHA-384
  - SHA-512
  - MD5

    Note: The MD5 algorithm is not supported in Microsoft Outlook 2010.

- Disabled

4.5.7 Microsoft Outlook Auto-Contact destination folder

Description: Specifies the location where contacts are updated in Microsoft Outlook. This folder must already have been created.

If this setting is not configured or disabled, contacts are updated in the Microsoft Outlook Contacts folder.

Possible Values:

- Not Configured
- Enabled – displays the default value, Contacts, and can be updated
- Disabled

4.5.8 Turn off automatic addition of sender's certificates to Microsoft Outlook contacts

Description: Disables the automatic creation and update of contact information with the sender's certificate attached to the opened email.

If this setting is not configured or disabled, then the sender's certificates are automatically added to the Microsoft Outlook contacts.

4.5.9 Turn off setup email certificates in Microsoft Outlook on card insertion

Description: Disables the automatic configuration of the Microsoft Outlook security profile on smart card insertion.

If this setting is not configured or disabled, the Microsoft Outlook security profile is updated with the certificate from the smart card on card insertion.

4.5.10 Turn on automatic decryption of encrypted emails

Description: Enables the automatic decryption of opened emails. It also allows saving copies of emails locally in non-encrypted format.

Automatically decrypted emails remain decrypted. Consider the security implications before using this setting.

4.5.11 Turn on automatic publication of 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.

If this setting is not configured or disabled, then certificates are not published to the GAL on card insertion.

4.6 PIN Caching

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 section 10.0 PIN Caching Service on page 140.

The following sections detail the PIN Caching Service policy settings:

- Allow per-process PIN caching on page 46
- Disable PIN cache clearance on workstation lock on page 46
- Enable PIN caching for "PIN Always" private keys on page 47
- Number of minutes before PIN cache is cleared on page 47

RESTART THE WORKSTATION

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

4.6.1 Allow per-process PIN caching

Description: Defines if the PIN cache is shared between Microsoft Windows processes.

If this setting is not configured or disabled, then all processes running in the same session share the same PIN cache.

4.6.2 Disable PIN cache clearance on workstation lock

Description: Disables the clearance of the PIN cache when the workstation is locked.

If this setting is not configured or disabled, then the PIN is cleared from the cache when the workstation is locked.

Disabling PIN cache clearance when the workstation is locked lowers the smart card deployment security.

4.6.3 Enable PIN caching for "PIN Always" private keys

Description: Defines if the PIN cache is applicable for operations with a private key configured for "PIN Always".

If enabled, a confirmation dialog guarantees non-repudiation for these operations.

If this setting is not configured or disabled, then PIN entry is required for all operations with a private key configured for "PIN Always".

If this setting is enabled, per-process PIN caching is recommended for improved security, and is required for FIPS 201 compliance.

Note: This policy complies with NISTIR 7863

4.6.4 Number of minutes before PIN cache is cleared

Description: Defines the number of minutes before the PIN cache is cleared. The default value is 15.

If this value is set to 9999, the PIN cache timeout is infinite. This means that PIN cache is cleared at log off or shutdown or session disconnect or card removal or workstation lock (depending on the Disable PIN cache clearance on workstation lock setting).

If this setting is disabled or not configured, the default value is used.

Possible Values:

- Not Configured
- Enabled – displays the default value, 15, and can be updated
- Disabled

4.7 PIN Initialization Tool

4.7.1 Turn Off OTP Initialized Card Re-initialization

Description: Defines if users can re-initialize a card with One-Time Password personalized.

If this setting is not configured or disabled, then the One-Time Password card can be re-initialized.

4.8 PIN Management

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

- Allow ActivClient to validate the PIN code against the PIN policy before validating the PIN code against the smart card on page 48
- Allow entry of PIN code longer than the maximum PIN length on page 48
- Prevent alphabetic characters in PIN code on page 48
- Prevent cancellation of Change PIN at first use on page 49
- Prevent entry of PIN code shorter than the minimum PIN length on page 49
- Prevent users from reusing current PIN during Change PIN on page 49
- Unlock card contact telephone number on page 49

RESTART THE WORKSTATION

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

4.8.1 Allow ActivClient to validate the PIN code against the PIN policy before validating the PIN code against the smart card

Description: Defines if, during PIN authentication, ActivClient checks the compliance of the entered PIN code with the PIN length policy before verifying the PIN code against the smart card.

If this setting is not configured or disabled, then ActivClient does not validate the PIN code against the PIN policy first.

4.8.2 Allow entry of PIN code longer than the maximum PIN length

Description: Defines if users can enter a PIN code for verification against the smart card that is longer than the maximum PIN length.

If this setting is disabled or not configured, then users cannot enter a PIN code that is longer than the maximum PIN length to the smart card.

4.8.3 Prevent alphabetic characters in PIN code

Description: Defines if users can enter alphabetic characters in their PIN code.

If this setting is disabled or not configured, then ActivClient accepts alphabetic characters in the PIN code.

4.8.4 Prevent cancellation of Change PIN at first use

Description: Disallows users from canceling the Change PIN process when they use their smart card for the first time.

If this setting is disabled or not configured, then users can cancel the Change PIN process at first use.

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

4.8.5 Prevent entry of PIN code shorter than the minimum PIN length

Description: Defines if users can enter a PIN code for verification against the smart card that is shorter than the minimum PIN length.

If this setting is disabled or not configured, then users can enter a PIN code that is shorter than the minimum PIN length to the smart card.

4.8.6 Prevent users from reusing current PIN during Change PIN

Description: Defines if users can reuse the current PIN code as the new PIN during a Change PIN operation.

If this setting is disabled or not configured, then users can enter the current PIN code as a new PIN code during the Change PIN operation.

4.8.7 Unlock card contact telephone number

Description: Specifies the contact telephone number that is displayed in the Unlock Card window prompt.

If this setting is not configured or disabled, then no contact telephone number is displayed in the Unlock Card window prompt.

Possible Values:

- Not Configured
- Enabled – enter the contact telephone number in the field
- Disabled

4.9 Smart Card

The following sections detail the Smart Card middleware policy settings:

- Turn on US Department of Defense configuration on page 50
- Disable smart card discovery information caching on page 51

RESTART WORKSTATION

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

4.9.1 Turn on US Department of Defense configuration

Description: For smart cards that comply with both the US government GSC-IS and PIV standards, defines which standard takes precedence for the middleware.

If this setting is enabled, GSC-IS takes precedence for the middleware.

If this setting is not configured or disabled, then the PIV standard takes precedence.

Possible Values:

- Not Configured
- Enabled
- Disabled

A setup preference also exists for this setting, which might affect the behavior if this policy setting is not configured.

The goal of this setup preference is to enable you to install ActivClient with the US Department of Defense configuration option and automatically have access to the specified configuration, without having to configure additional policies.

- If the US Department of Defense configuration option is selected in the ActivClient setup and if the Turn on US Department of Defense configuration policy is not configured or disabled, then GSC-IS is chosen as the preferred interface.
- If the US Department of Defense configuration option is not selected in the ActivClient setup and if the Turn on US Department of Defense configuration policy is not configured or disabled, then PIV End Point is chosen as the preferred interface.
- If the Turn on US Department of Defense configuration policy is Enabled, then it takes precedence over the preference set in the ActivClient setup, and GSC-IS is chosen as the preferred interface.

4.9.2 Disable smart card discovery information caching

It is recommended that you enable 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.

Description: Disables the smart card discovery information caching.

When this setting is not configured or disabled, performances are optimized by caching smart card discovery information. This smart card discovery process is repeated at each smart card insertion

Note: Discovery information caching needs to be enabled if you use the Smart Card Auto-Update with ActivID CMS capability.

4.10 Smart Card Auto-Update

ActivClient provides an Automatic Smart Card Update feature.

For a full description of the Smart Card Auto-Update feature, see section 11.0 Auto-Update with ActivID CMS on page 147.

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

- CMS MDIDC timeout (in seconds) on page 52
- CMS Server URL on page 52
- CMS Synchronization Manager timeout (in seconds) on page 52
- Enable Card Auto-Update on page 53
- Frequency of update (in days) on page 53
- Maximum delay for card update check after card insertion on page 53
- Maximum delay for card update check after Windows Logon on page 54
- Maximum number of CMS MDIDC card update retries on page 54
- Maximum number of CMS Synchronization Manager retries on page 54

RESTART WORKSTATION

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

Prerequisite

The Smart Card Auto-Update is only available if smart card discovery information caching is enabled (that is, if Disable smart card discovery information caching on page 51 is not configured or disabled).

4.10.1 CMS MDIDC timeout (in seconds)

Description: Defines the maximum time (in seconds) allocated to perform a smart card update using CMS My Digital ID Card. When this timeout is reached, the process running the browser is terminated.

If this setting is not configured or disabled, then the timeout is set to 600 seconds.

Possible Values:

- Not Configured
- Enabled – displays the default value, 600, and can be updated
- Disabled

4.10.2 CMS Server URL

Description: Defines the connection URL for the ActivID CMS server (see the ActivID CMS documentation). The port number must be included in the URL.

Example: http://cms.mycompany.com:89898

If this setting is not configured or disabled, then no automatic update check is performed on card insertion.

Possible Values:

- Not Configured
- Enabled – enter the ActivID CMS server URL
- Disabled

4.10.3 CMS Synchronization Manager timeout (in seconds)

Description: Defines the maximum time (in seconds) allocated to check with ActivID CMS if smart card updates are available.

If this setting is not configured or disabled, then the timeout is set to 5 seconds.

A value of zero (0) means there is no client timeout, in which case the client timeout is determined by the server settings.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

4.10.4 Enable Card Auto-Update

Description: Defines if ActivClient will automatically check if inserted smart cards can be updated with card content updates available in the ActivID CMS. The smart card update process starts if updates are available.

If this card auto-update is enabled, then the ActivID CMS server URL must be specified for ActivClient to perform the Auto-update check.

Possible Values:

- Not Configured
- Enabled
- Disabled

4.10.5 Frequency of update (in days)

Description: Defines the interval (in days) between checks for smart card updates.

If this setting is not configured or disabled, then the update frequency is set to 7 days.

Possible Values:

- Not Configured
- Enabled – displays the default value, 7, and can be updated
- Disabled

4.10.6 Maximum delay for card update check after card insertion

Description: Defines how long (in minutes) ActivClient waits after card insertion before it contacts ActivID CMS to determine if smart card updates are available. This delay is a random value – between 0 and the maximum delay defined in this setting (in minutes).

Recommended values are between 1 and 10.

If this setting is not configured or disabled, then the delay is set to 5 minutes.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

4.10.7 Maximum delay for card update check after Windows Logon

Description: Defines how long (in minutes) ActivClient waits after Microsoft Windows logon before it contacts ActivID CMS to determine if smart card updates are available.

To spread the requests received by ActivID CMS, this delay is a random value – between 0 and the maximum delay defined in this setting (in minutes).

Recommended values are between 5 and 120.

If this setting is not configured or disabled, then the delay is set to 120 minutes.

Possible Values:

- Not Configured
- Enabled – displays the default value, 120, and can be updated
- Disabled

4.10.8 Maximum number of CMS MDIDC card update retries

Description: Defines the maximum number of attempts to update the smart card and check the synchronization result after the CMS MDIDC timeout expires.

Number of attempts should be between 0 and 10.

If this setting is not configured, 2 attempts are configured. By enabling this setting, the number of attempts can be updated. If this setting is disabled, this means that no retry is executed. This is equivalent to setting the number of retries to 0.

Possible Values:

- Not Configured
- Enabled – displays the default value, 2, and can be updated
- Disabled

4.10.9 Maximum number of CMS Synchronization Manager retries

Description: Defines the maximum number of attempts to connect to the CMS Synchronization Manager after timeout.

If this setting is not configured or disabled, the number of attempts is set to 2.

Possible Values:

- Not Configured
- Enabled – displays the default value, 2, and can be updated
- Disabled

4.11 Smart Card Readers

The following section details the Smart Card Readers policy setting that allows you to customize ActivClient behavior regarding hardware devices.

- Enable the PIN Pad Readers Support on page 55
- Smart Card Readers Black List on page 55

RESTART WORKSTATION

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

4.11.1 Enable the PIN Pad Readers Support

Description: Defines if ActivClient uses the PIN Pad reader with secure PIN.

If this setting is not configured or disabled, then ActivClient uses the PIN Pad reader as a standard smart card reader.

Possible Values:

- Not Configured
- Enabled
- Disabled

4.11.2 Smart Card Readers Black List

Description: Defines the list of smart card readers not authorized for use with ActivClient.

If this setting is not configured or disabled, then ActivClient uses any connected smart card reader.

This list is populated with the full reader name or a substring starting with the prefix of the reader name.

Possible Values:

- Not Configured
- Enabled – enter the full reader name in the field to add it to the list
- Disabled

Notes:

- ActivClient 6.x included a policy for smart card reader 'white list'. As the policy with ActivClient 7.x is a black list, the reader list needs to be adapted accordingly.
- The reader name field is case sensitive. Use the reader name as reported in the Reader menu in the User Console.

4.12 Software Auto-Update

ActivClient provides an Automatic Software Update feature.

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

- Enable software auto update on page 56
- Delay between update retries (in minutes) on page 56
- Frequency of update (in days) on page 57
- Maximum number of update retries on page 57

RESTART WORKSTATION

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

4.12.1 Enable software auto update

Description: Defines if ActivClient will automatically check if software update is made available.

Enabling this setting requires to specify the network location (URL) where ActivClient Auto-Update service looks for the software updates, and the path to the local folder where the software updates are downloaded. The ActivClient Auto-Update service must have read and write permissions to the folder.

If this setting is not configured or disabled, then the values remain empty and so no automatic update is performed.

Possible Values:

Software automatic update URL

- Not Configured
- Enabled – enter the URL where ActivClient looks for software updates
- Disabled

Download path for software update

- Not Configured
- Enabled – enter the path to local folder where software updates are downloaded
- Disabled

4.12.2 Delay between update retries (in minutes)

Description: Defines the waiting period (in minutes) before the ActivClient Auto-Update service retries to update the software when a failure occurs.

If this setting is not configured or disabled, then the delay is set to 15 minutes.

If this setting is configured to 0, an update attempt is immediately performed after a failure.

Possible Values:

- Not Configured
- Enabled – displays the default value, 15, and can be updated
- Disabled

4.12.3 Frequency of update (in days)

Description: Defines the interval (in days) between checks for software updates.

If this setting is not configured or disabled, then the delay is set to 1 day.

Possible Values:

- Not Configured
- Enabled – displays the default value, 1, and can be updated
- Disabled

4.12.4 Maximum number of update retries

Description: Defines the number of times the ActivClient Auto-Update service retries to update the software.

If this setting is not configured or disabled, the delay is set to 3.

Possible Values:

- Not Configured
- Enabled – displays the default value, 3, and can be updated
- Disabled

4.13 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 Diagnostics Wizard).

The following sections detail the User Console policy settings:

- Disable deletion of user certificates on page 59
- Disable One-Time Password generation on page 59
- Disable One-Time Password synchronization on page 59
- Hide Advanced Diagnostics icon on page 59
- Hide CA Certificates folder on page 59
- Hide Check for Card Update menu on page 60
- Hide Export Certificate menu on page 60
- Hide Help menu on page 60
- Hide Import Certificate menu on page 60
- Hide My Certificates folder on page 60
- Hide My Personal Info option on page 61
- Hide New Card menu on page 61
- Hide Publish to GAL menu on page 61
- Hide Reset Card menu on page 61
- Hide Tasks View from Explorer bar on page 61
- Hide the Smart Card Info icon on page 62
- Hide Tree View from Explorer bar on page 62
- Hide Unlock Card menu on page 62
- Hide Use Reader menu and Reader list icon on page 62
- Hide View Policy Settings menu on page 62
- Hide View Unlock Code menu on page 63
- Image displayed on the lower right corner of List view on page 63
- Prevent users from switching between icon and detail view on page 63

RESTART USER CONSOLE

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

4.13.1 Disable deletion of user certificates

Description: Defines if users can delete their certificates.

If this setting is not configured or disabled, then the certificate deletion option is available.

If the smart card is issued by a card/credential management system (such as ActivID CMS) that prevents cards from being updated by users, then this policy is not applicable.

ActivClient does not allow updating a card if it is prohibited at the card/applet level. For example, CAC and PIV cards can be considered read-only at the workstation level – users cannot delete current certificates, nor import new certificates on their card. Card update operations are then driven by the card management used to issue the cards, such as ActivID CMS.

4.13.2 Disable One-Time Password generation

Description: Defines if users can generate a smart card-based One-Time Password in the User Console.

If this setting is not configured or disabled, then the One-Time Password generation option is available.

4.13.3 Disable One-Time Password synchronization

Description: Defines if users can resynchronize the smart card-based One-Time Password in the User Console.

If this setting is not configured or disabled, then the One-Time Password resynchronization option is available.

4.13.4 Hide Advanced Diagnostics icon

Description: Defines if the Advanced Diagnostics icon is displayed in the User Console standard toolbar, allowing users to access and use the Advanced Diagnostics tool.

This menu is not displayed if the Troubleshooting feature is not installed.

If this setting is not configured or disabled, then the Advanced Diagnostics icon is displayed in the User Console.

4.13.5 Hide CA Certificates folder

Description: Defines if the CA Certificates folder is displayed in the User Console, allowing users to view CA Certificates stored on their smart card.

If this setting is not configured or disabled, then the CA certificates folder is displayed in the User Console.

4.13.6 Hide Check for Card Update menu

Description: Defines if the Check for Card Update menu is displayed in the User Consoled, allowing users to check with ActivID CMS if an update is available for the inserted smart card.

This menu is not displayed if the Card auto-update service with ActivID CMS feature is not installed.

If this setting is not configured or disabled, then the Check for Card Update menu is displayed in the User Console.

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.

4.13.7 Hide Export Certificate menu

Description: Defines if the Export Certificate menu is displayed in the User Console, allowing users to export certificates from their smart card to a file.

If this setting is not configured or disabled, then the Export Certificate menu is displayed in the User Console.

4.13.8 Hide Help menu

Description: Defines if the Help standard tool bar button and the ActivClient Help command in the Help menu are displayed in the User Console.

If this setting is not configured or disabled, the Help menu and button are displayed in the User Console.

4.13.9 Hide Import Certificate menu

Description: Defines if the Import Certificate menu is displayed in the User Console, allowing users to import a certificate onto their smart card.

If this setting is not configured or disabled, then the Import Certificate menu is displayed in the User Console.

4.13.10 Hide My Certificates folder

Description: Defines if the My Certificates folder is displayed in the User console, allowing users to view their smart card certificates.

If this setting is not configured or disabled, then the My Certificates folder is displayed in the User Console.

4.13.11 Hide My Personal Info option

Description: Defines if My Personal Info icon is displayed in the User Console, allowing users to view the personal information (demographic data) available on their smart card.

If this setting is not configured or disabled, then the My Personal Info icon is displayed in the User Console.

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

4.13.12 Hide New Card menu

Description: Defines if New Card menu is displayed in the User Console, allowing users to access and use the PIN Initialization Tool.

This menu is not displayed if the PIN Initialization Tool feature is not installed.

If this setting is not configured or disabled, then the New Card menu is displayed in the User Console.

4.13.13 Hide Publish to GAL menu

Description: Defines if the Publish to GAL menu is displayed in the User Console, allowing users to set up email certificates in Microsoft Outlook and publish certificates to the Global Address List.

This menu is not displayed if the Microsoft Outlook Usability Enhancements feature is not installed.

If this setting is not configured or disabled, then the Publish to GAL menu is displayed in the User Console.

4.13.14 Hide Reset Card menu

Description: Defines if the Reset Card menu is displayed in the User Console, allowing users to reset their smart cards. This is only applicable to standalone smart cards.

If this setting is not configured or disabled, the Reset Card menu is displayed in the User Console.

4.13.15 Hide Tasks View from Explorer bar

Description: Defines if the Tasks View is displayed in 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.

If this setting is not configured or disabled, then the Tasks View is displayed.

4.13.16 Hide the Smart Card Info icon

Description: Defines if the Smart Card Info icon is displayed in the right pane of the User Console, allowing users to view information such as smart card user name, manufacturer, model and serial number.

If this setting is not configured or disabled, then the Smart card Info icon is displayed in the User Console.

4.13.17 Hide Tree View from Explorer bar

Description: Defines if the Tree View is displayed in 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.

If this setting is not configured or disabled, the Tree View is displayed.

4.13.18 Hide Unlock Card menu

Description: Defines if the Unlock Card menu is displayed in the User Console, allowing users to access the Unlock Card tool in order to unlock their smart card.

If this setting is not configured or disabled, then the Unlock Card menu is displayed in the User Console.

4.13.19 Hide Use Reader menu and Reader list icon

Description: Defines if the Use Reader menu and the Reader List toolbar icon are displayed in the User Console.

If this setting is not configured or disabled, then the Use Reader menu and the Reader List toolbar icon are displayed in the User Console and available for use.

4.13.20 Hide View Policy Settings menu

Description: Defines if the View Policy Settings menu is displayed in the User Console, allowing users to view the policy settings applied to this computer

This menu is not displayed if the Configuration Management feature is not installed.

If this setting is not configured or disabled, then the View Policy Settings menu is displayed in the User Console.

4.13.21 Hide View Unlock Code menu

Description: Defines if the View Unlock Code menu is displayed in the User Console, allowing users to view their unlock code. This is only applicable to standalone smart cards.

If this setting is not configured or disabled, the View Unlock Code menu is displayed in the User Console.

4.13.22 Image displayed on the lower right corner of List view

Description: Defines the path to the customized background image (lower right corner) of the User Console. The image must be in the *.bmp* format.

If this setting is not configured or disabled, then the ActivClient background image is used (smartcard).

Possible Values:

- Not Configured
- Enabled – enter the path to the required image
- Disabled

4.13.23 Prevent users from switching between icon and detail view

Description: Defines if users can choose a view type from the Large Icons, Small Icons, List, and Details options.

If this setting is not configured or disabled, then users can choose the view type. If this setting is enabled, users cannot choose between the view type and the User Console uses Large Icons.

4.14 Advanced Diagnostics

The Advanced Diagnostics tool is designed to help diagnose issues with HID Global 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 64
- Hide Email menu in Advanced Diagnostics on page 64
- Turn off smart card diagnostics in Advanced Diagnostics on page 64

RESTART ADVANCED DIAGNOSTICS TOOL

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

4.14.1 Email address where the diagnostics report will be sent

Description: Specifies an email address where the diagnostics report will be sent.

Possible Values:
- Not Configured
- Enabled – enter the email address where the diagnostics will be sent
- Disabled

4.14.2 Hide Email menu in Advanced Diagnostics

Description: Defines if users can access the Email menu in the Advanced Diagnostics interface, and sending the diagnostics report by email.

If this setting is disabled or not configured, then the Email menu is displayed in the Advanced Diagnostics interface.

4.14.3 Turn off smart card diagnostics in Advanced Diagnostics

Description: Disables advanced diagnostics on inserted smart cards.

If this setting is disabled or not configured, advanced diagnostics are performed on inserted smart cards.

4.15 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. Additional policies are available and presented in this section.

The following sections detail the Logging policy settings:

- Turn on ActivClient logging on page 65
- Enable ActivClient performance logging for Microsoft Windows PKI Smart Card Logon on page 66
- Full path to log files folder on page 66
- Maximum number of backup files on page 66
- Enable ActivClient performance logging for Microsoft Windows PKI Smart Card Logon on page 66

RESTART WORKSTATION

For the Logging policy changes to be applied, you must restart 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).

4.15.1 Turn on ActivClient logging

Description: Defines if users can generate log files for every action performed by ActivClient. No security sensitive information is logged.

This might affect performance and should be activated only when required by Technical Support for troubleshooting purposes.

If this setting is not configured or disabled, then ActivClient actions are not logged.

Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Logging\ActivClientEnabled

Type: DWORD

4.15.2 Enable ActivClient performance logging for Microsoft Windows PKI Smart Card Logon

Description: Enables the creation of entries in the Microsoft Windows Event Viewer when a Microsoft Windows PKI Smart Card Logon starts and ends. This is used to troubleshoot Microsoft 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 Microsoft Windows Event Viewer.

If this setting is not configured or disabled, then Microsoft Windows PKI Smart Card Logon performances are not logged.

4.15.3 Full path to log files folder

Description: Specifies the full path to the generated log files.

The folder where logs are generated must be created and end users must be granted write permissions to this folder.

Possible Values:

- Not Configured
- Enabled – displays the default value, **%CommonProgramFiles%\HID Global\Logs**, and can be updated
- Disabled

Note: The policy does not configure the path for log files of restricted processes:

- The logs of processes running in low level integrity will always be generated in **%APPDATA%\..\LocalLow\HID Global\Logs**.
- The logs of processes running in an AppContainer will always be generated in **%LOCALAPPDATA%\Packages\<AppContainerName>\AC\HID Global\Logs**.

4.15.4 Maximum number of backup files

Description: Defines the maximum number of log file backups. The default value is 3.

It cannot be set to 0.

Possible Values:

- Not Configured
- Enabled – displays the default value, 3, and can be updated
- Disabled

4.15.5 Maximum log file size in MB

Description: Defines the maximum size (in megabytes) of the log files. The default size is 20 MB.

It cannot be set to 0.

Possible Values:

- Not Configured
- Enabled – displays the default value, 20, and can be updated
- Disabled

4.16 Microsoft Policies Relevant to ActivClient

4.16.1 Microsoft Windows Policies

The following Microsoft Windows policies are relevant to ActivClient. For convenience, some are configured automatically by ActivClient setup.

Notes:

- ActivClient does not restore these settings to their default values at uninstallation. You must manually reset the settings. For further information, see section 8.3 Restore Microsoft Settings on page 123.
- ActivClient 6.x included policies that had some redundancy with Microsoft policies. In ActivClient 7, ActivClient relies on Microsoft policies when it is relevant.

4.16.1.1 Card Removal

Description: This setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

Possible Values:

- No Action = 0
- Lock Workstation = 1
- Force Logoff = 2
- Disconnect if a remote Terminal Services session = 3

Policy setting: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon : Smart card removal behavior

Registry key: scremoveoption

Comments During ActivClient installation:

- The setting 'Interactive logon: Smart card removal behavior' is automatically set to Lock on Card removal.
- The Smart Card Removal Policy service (SCPolicySvc) is also updated to Automatic.

4.16.1.2 Certificate Registration

Description: This policy setting allows you to manage the certificate propagation that occurs when a smart card is inserted.

If you enable or do not configure this policy setting then certificate propagation will occur when you insert your smart card.

Possible Values:

- Not Configured = 0
- Enabled = 1
- Disabled = 2

Policy setting: Computer Configuration\Administrative Templates\Windows Components\Smart Card\Turn on certificate propagation from smart card

Registry key: CertPropEnabled

Comments: During ActivClient installation:

- The setting 'Turn on certificate propagation from smart card' is set to Enabled.
- The Certificate Propagation service is also set to Automatic.

4.16.1.3 Card Auto Registration (PIV Cards Only)

ActivClient supports new PIV cards (including PIV-compatible CAC cards) without requiring any software update. ActivClient leverages the Windows card auto-registration (or Plug and Play) feature, which needs to be enabled.

Description: This policy setting allows you to control whether Smart Card Plug and Play is enabled.

If you enable or do not configure this policy setting, Smart Card Plug and Play will be enabled and the system will attempt to install a Smart Card device driver when a card is inserted in a Smart Card Reader for the first time.

Possible Values:

- Not Configured = 0
- Enabled = 1
- Disabled = 2

Policy setting: Computer Configuration\Administrative Templates\Windows Components\Smart Card\Turn on Smart Card Plug and Play service

Registry key: EnableScPnP

Comments

- Available on Microsoft Windows 7, Server 2008 R2 and later.
- During ActivClient installation:
  - The setting 'Turn on Smart Card Plug and Play service' is set to Enabled.
  - The Smart Card service is set to Automatic.

4.16.1.4 Smart Card PIN Unlock

In order to enable the Unblock feature at logon, the following policy must be configured.

Description: This policy setting lets you determine whether the integrated unblock feature will be available in the logon User Interface (UI).

In order to use the integrated unblock feature, your smart card must support this feature. Please check with your hardware manufacturer to see if your smart card supports this feature.

If you enable this policy setting, the integrated unblock feature will be available.

If you disable or do not configure this policy setting then the integrated unblock feature will not be available.

Possible Values:

- Not Configured = 0
- Enabled = 1
- Disabled = 2

Policy setting: Computer Configuration\Administrative Templates\Windows Components\Smart Card\Allow Integrated Unblock screen to be displayed at the time of logon

Comments This Windows feature is compatible with smart cards that are configured for unblocking with an External Authentication mechanism. Most card profiles issued by ActivID CMS with ActivID Applets are compatible with the unlock feature at logon.

For further information about profile selection, refer to the ActivID CMS documentation.

4.16.2 Microsoft Outlook Policies

The following Microsoft Outlook policies are relevant to ActivClient Outlook Enhancement feature.

Note: ActivClient 6.x included policies that had some redundancy with Microsoft policies. In ActivClient 7, ActivClient relies on Microsoft policies when it is relevant.

The Microsoft Outlook administrative templates can be downloaded from:

- For Microsoft Office 2007:

  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=73d955c0-da87-4bc2-bbf6-260e700519a8&displaylang=en

- For Microsoft Office 2010:

  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=64b837b6-0aa0-4c07-bc34-bec3990a7956&displaylang=en

- For Microsoft Outlook 2016:

  http://www.microsoft.com/en-us/download/details.aspx?id=49030

The following table lists the policies that you should configure in order to finalize support of the Microsoft Outlook enhancements feature:

Table 1: Microsoft Outlook enhancements policies

Microsoft Office Outlook Setting	Description
Sign all e-mail messages	This setting is defined under: User Configuration\Administrative Templates\Microsoft Outlook 20xx\Security\Cryptography Sign all e-mail messages: • Not Configured • Enabled • Disabled Sets the value for the corresponding UI option.

Microsoft Office Outlook Setting	Description
Request an S/MIME receipt for all S/MIME signed messages	This setting is defined under: User Configuration\Administrative Templates\Microsoft Outlook 20xx\Security\Cryptography Request an S/MIME receipt for all S/MIME signed messages: • Not Configured • Enabled • Disabled Sets the value for the corresponding UI option.
Encrypt all e-mail messages	This setting is defined under: User Configuration\Administrative Templates\Microsoft Outlook 20xx\Security\Cryptography Encrypt all e-mail messages: • Not Configured • Enabled • Disabled Sets the value for the corresponding UI option.
Send all signed messages as clear signed messages	This setting is defined under: User Configuration\Administrative Templates\Microsoft Outlook 20xx\Security\Cryptography Send all signed messages as clear signed messages: • Not Configured • Enabled • Disabled Sets the value for the corresponding UI option.
Enable Cryptography Icons	This setting is defined under: User Configuration\Administrative Templates\Microsoft Outlook 20xx\Security\Cryptography Enable Cryptography Icons: • Not Configured • Enabled • Disabled Sets the value for the corresponding UI option.

4.17 Citrix XenApp Configuration

ActivClient is designed to support smart cards in a Citrix XenApp deployment. However, there is no specific ActivClient configuration required for Citrix deployments.

Citrix provides a large set of documentation about XenApp configuration for smart card deployments. This section provides pointers to these Citrix documents and configuration recommendations. For the latest up-to-date documentation, go to the official Citrix web site.

To decide which Citrix client is needed for your deployment, see http://support.citrix.com/proddocs/topic/online-plugin-112-windows/ica-clients-deciding-v2.html. The Citrix Online plug-in is recommended for smart card services.

To configure Citrix Web Interface with smart card authentication, see http://support.citrix.com/proddocs/topic/web-interface-impington/wi-authenticate-wrapper-gransden.html. Choose Smart card or Pass-through with smart card depending on your configuration.

This document also includes the following authentication recommendations:

If you plan to enable pass-through, pass-through with smart card, or smart card authentication, be aware of the following:

- If users log on to their computers using smart cards and you want to enable pass-through authentication, select the option to use Kerberos authentication.
- If users log on to their computers using explicit credentials, do not enable smart card or pass-through with smart card authentication for those users to access the Web Interface.

Note: Users who log on to Windows using explicit credentials and then subsequently access a site configured for pass-through with smart card authentication are presented with a Welcome to Windows dialog box when accessing resources. To cancel this dialog box, users must press right-ALT (ALT GR) + DELETE. Citrix recommends creating separate sites for users logging on with smart cards and users logging on with explicit credentials.

To enable smart card authentication for Web Interface, see http://support.citrix.com/proddocs/topic/web-interface-impington/wi-enable-smart-card-authentication-gransden.html.

As you configure Microsoft Windows for the smart card removal behavior, you also need to configure the smart card removal behavior for Citrix sessions. To enable smart card authentication for XenApp Services sites:

1. From the Windows **Start** menu, point to **All Programs**, **Citrix**, **Management Consoles** and then select **Citrix Web Interface Management**.
2. In the left pane of the Citrix Web Interface Management console, click **XenApp Services Sites** and select your site in the results pane.
3. In the **Action** pane, click **Authentication Methods** and select the **Smart card or Pass-through with smart card** option, as appropriate.
4. Click **Properties** and select **Roaming**.
5. To configure the behavior of the Web Interface when a smart card is removed, select **Enable roaming** and choose one of the following options:

- To disconnect a user's session when the smart card is removed, select **Disconnect sessions when smart card removed**.
- To log off a user's session when the smart card is removed, select **Log off sessions when smart card removed**.

6. If you enabled pass-through with smart card authentication and you want to use Kerberos authentication between the plug-in and the XenApp Services site, click **Kerberos Authentication** and select the **Use Kerberos to authenticate to the XenApp Services site** option.

5.0 Customizing the Setup

This section explains how to customize the ActivClient setup. It describes the possible customization methods and details the ActivClient setup options.

5.1 Setup Customization Methods

5.1.1 Using a Command Line

This section describes how to use a command line.

To...	See...
Use the basic command line to install a product.	5.1.1.1 Basic Install Command Line on page 75
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.	5.1.1.2 Remove Features on page 75
Start ActivClient setup program in blind mode i.e. default features installation without any user interface displayed	5.2.3.2 Run a Blind Setup on page 81

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 2: ActivClient Setup Filenames and Editions.

Table 2: ActivClient Setup Filenames and Editions

ActivClient edition	ActivClient Setup file name
ActivClient 7.1 (32-bit)	ActivClient x86 7.1.msi
ActivClient 7.1 (64-bit)	ActivClient x64 7.1.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 2: ActivClient Setup Filenames and Editions.

5.1.1.1 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 command line are necessary when there are spaces in the file name.

5.1.1.2 Remove Features

To remove one or several features from the setup program, use the following command:

```
msiexec /i "<path>\<ActivClient setup>.msi" Remove=<FeatureName>
```

where:

- <path> is the ActivClient setup path.
- <ActivClient setup> is the ActivClient setup .msi file name.
- <FeatureName> is the name of the feature to remove. See section 5.2.1 Customize the Feature Installation on page 78 for more information.

For example, to remove the User Console feature, use the following command:

```
msiexec.exe /i "<path>\<ActivClient setup>.msi" Remove=UserConsole
```

Notes:

- The quotation marks shown in the command line are necessary when there are spaces in the file name.
- Once ActivClient is installed, you can modify the installed features using the Add or Remove Programs function in the Windows Control Panel.

  Features removed during initial installation (that is, the features that are not installed) are displayed in the ActivClient Custom Setup screen as unselected, with a red cross, where you can select them for installation.

5.1.1.3 Force Features

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

```
msiexec.exe /i "<path>\<ActivClient setup>.msi" AddLocal= FeatureName1
```

where:

- <path> is the ActivClient setup path.
- <ActivClient setup> is the ActivClient setup .msi file name.
- <FeatureName1> is the name of the feature to install. See section 5.2.1 Customize the Feature Installation on page 78 for more information.

When installing ActivClient, you need to list all the features that you want to install. For example:

```
msiexec.exe /i "<path>\<ActivClient setup>.msi" AddLocal=MiniDriver,OutLook,PKCS,SoftwareAutoUpdate
```

You can use `AddLocal=ALL` if you want to install all the ActivClient features.

When modifying an existing installation, you can use `AddLocal` to add only the features that you want to install.

5.1.2 Using Orca

This section describes how to edit the *.msi* file in order to hide or display the setup features by changing the appropriate feature values.

This can be done with Orca, a free resource editor program distributed by Microsoft. Orca is part of the Microsoft Windows Installer SDK. The default values can be updated directly in the MSI.

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

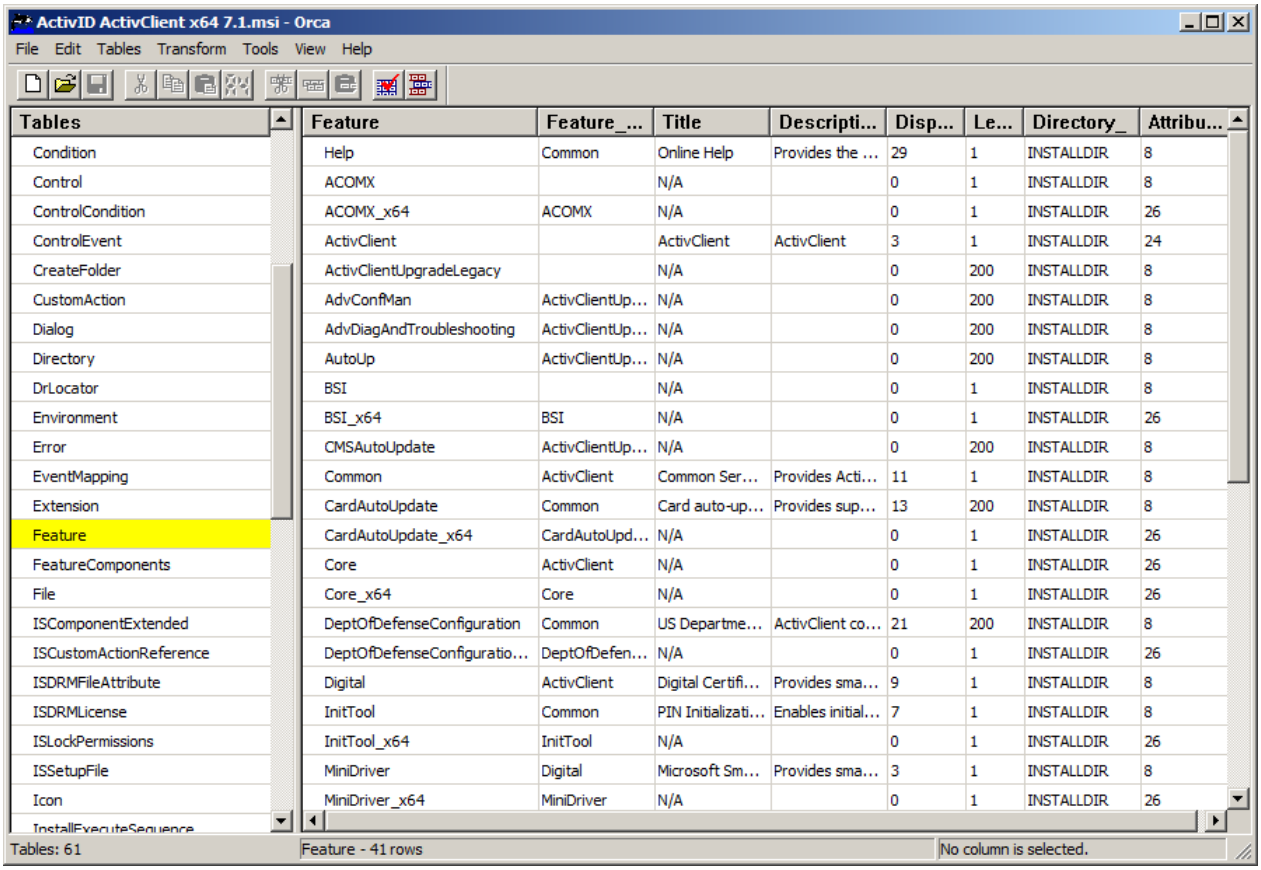
1. Download the Microsoft Windows Install SDK from:

   http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3138

2. Install the Microsoft 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 7.1.msi*
   - *ActivClient x64 7.1.msi*



4. Select **Feature** in the **Tables** column to display all the ActivClient features.
5. Locate and select the feature you want to change.

   You can refer to the ActivClient features in section 5.2.1 Customize the Feature Installation on page 78.
6. Change the feature's Display value to either:
   - 0 (to hide it)
   - 1 (to force it to display)
7. Repeat the procedure for all other features you want to edit.
8. Save the file.
9. You can then place this setup program on the network for use by all end users.

5.1.3 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 section 5.2 ActivClient Setup Customization Options on page 78.
- ActivClient MSI file together with an MST file.

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

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

Both programs allow setup customization (MSI and MST management) and packages integrity validation.

Their user interfaces hide typical setup complexity for the following customization operations:

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

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

5.2 ActivClient Setup Customization Options

5.2.1 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.

MSI customization must be done on the unsigned MSI file (located in the **\Admin\Administrative setups** folder in the ActivClient distribution). If it is done on the signed MSI, the update will invalidate the MSI digital signature.

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.

The following table lists the features that you can use to customize the setup program.

Table 3: Customizable Features

Feature Name	Feature Title
MiniDriver	Microsoft Smart Card Mini Driver Support
Outlook	Microsoft Outlook Usability Enhancements
PKCS	PKCS#11 Support
MozillaSupport	Mozilla Firefox and Thunderbird configuration
UserConsole	User Console

Feature Name	Feature Title
Troubleshooting	Troubleshooting
SoftwareAutoUpdate	Auto-Update Service
CardAutoUpdate	Card auto-update service with ActivID CMS
DeptOfDefenseConfiguration	US Department of Defense configuration
SettingsManagement	Configuration Management
Help	Online Help

Notes:

- When you install the ActivClient PKCS#11 library, for compliance with the US Government GSC-IS specifications, ActivClient records the location of the PKCS#11 library in a standard registry:

  HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\ActivIdentity

- The Troubleshooting feature includes the Advanced Diagnostics tool.

In addition to the features visible in the ActivClient installation user interface, there are also additional properties that enable you to prevent the installation of components that are otherwise always installed as part of the Base Components:

Table 4: Base Component Features

Property Name	Property Description
PIVAPIREMOVE	PIV API support is automatically installed with the common services. This property can be used to remove this support. This customization can only be executed once at ActivClient installation (first installation or upgrade) and cannot be updated through a modify command execution afterwards.
BSIAPIREMOVE	GSC-IS BSI API support is automatically installed with the common services. This property can be used to remove this support. This customization can only be executed once at ActivClient installation (first installation or upgrade) and cannot be updated through a modify command execution afterwards.

For example, if you do not want to install the PIV API, use the command:

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

5.2.2 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.

5.2.3 Customize the Setup Behavior

5.2.3.1 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.

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.

5.2.3.2 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).

/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.

5.2.3.3 Avoid Conflict with Other MSI Products

To avoid installing ActivClient with some incompatible MSI products, 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.

5.2.3.4 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**.
3. Copy all root certificate files that must be installed into the **Certificates** folder.

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 install root certificates.

6.0 Deploying the Setup

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

6.1 Deploying Using Standard Methods

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

- *ActivClient x86 7.1.msi*
- *ActivClient x64 7.1.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.

Once ActivClient MSI is deployed, you can deploy ActivClient policies, as described in section 3.0 Defining the ActivClient Policies on page 15. ActivClient uses administrative templates, also supported by most enterprise management products.

Before deploying ActivClient MSI and ActivClient policies on your production network, it is strongly recommended that you perform a test with ActivClient in a separate test environment.

6.2 Deploying Using Active Directory Push

This section describes how to deploy ActivClient using the automated software push capabilities in Microsoft Windows Server Active Directory.

Note: The following procedure is illustrated using Microsoft Windows Server 2008. The steps and interface might vary with newer versions of Microsoft Windows Server. Refer to the Microsoft documentation for further information.

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.

See section 5.0 Customizing the Setup on page 74 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	Task Description	See
1	Create a shared network folder as a distribution point.	6.2.1 Create a Distribution Point on page 84

Task	Task Description	See
2	Limit deployment to a predefined user population.	3.2 Using Active Directory Group Policy Objects on Microsoft Windows Server on page 15
3	Distribute a package containing ActivClient to computers.	6.2.2 Assign a Package on page 84
4	Test the package.	6.2.3 Test a Package on page 86
5	Redeploy a package.	6.2.4 Redeploy a Package on page 86

6.2.1 Create a Distribution Point

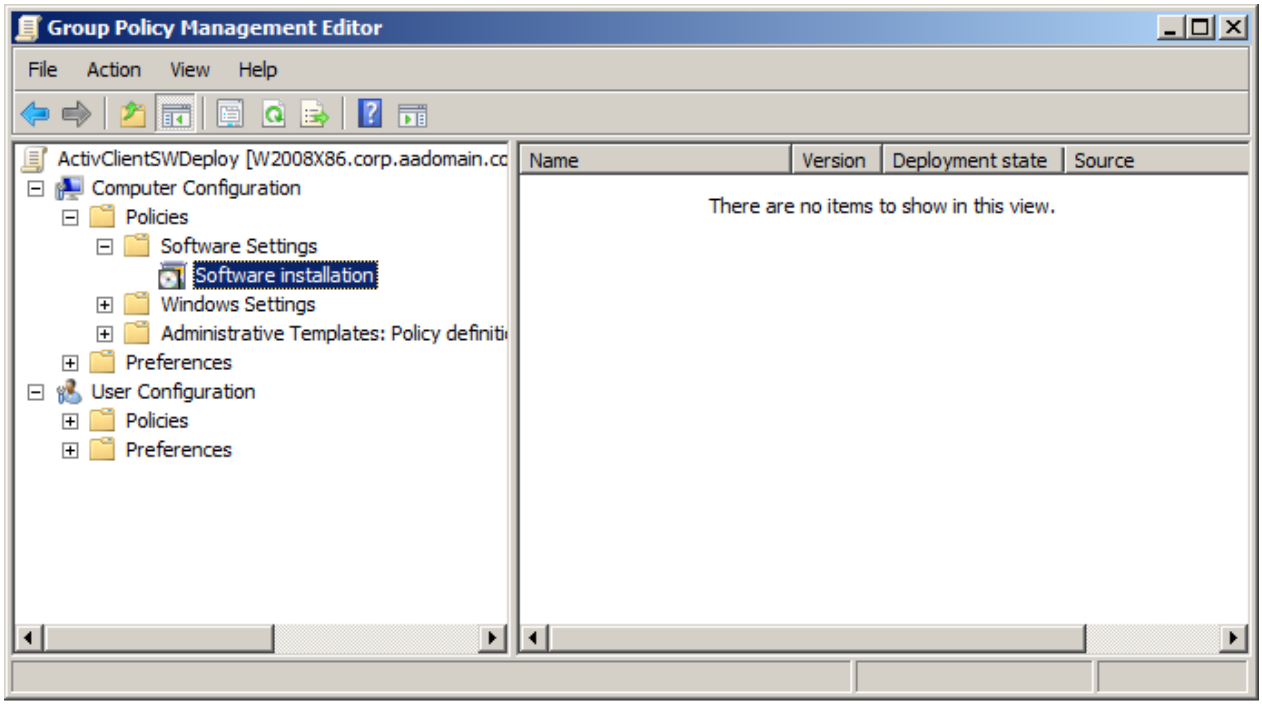
1. Log on to the server computer as an administrator.
2. Create a shared network folder in which to place an ActivClient *.msi* file for each ActivClient edition to be deployed.
3. Set permissions on the shared network folder to allow access to the distribution point.
4. Copy each ActivClient edition *.msi* file (*ActivClient x86 7.1.msi, ActivClient x64 7.1.msi*, or both) to the distribution point.

6.2.2 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 7.1 32-bit and one with ActivClient 7.1 64-bit. For both deployments, follow these steps:

1. On the domain controller, start the **Server Manager**, and expand the **Features** node.
2. In the **Group Policy Management** node, expand **Forest** and **Domains** and then select the domain containing the organizational unit(s) to which you want to deploy ActivClient.
3. Depending on the scope of the deployment, right-click on the domain or OU and select **Create a GPO in this domain and Link it here** (or edit an existing GPO).
4. In the Group Policy Management Editor, expand **Computer Configuration**, then **Policies** and then **Software Settings**.

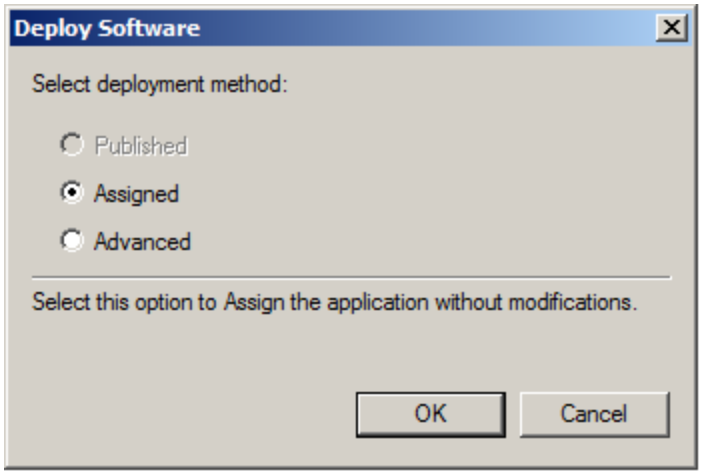


5. Right-click on **Software Installation**, point to **New**, and select **Package**.
6. In the Open dialog box, in the **File name** field, enter the full Universal Naming Convention (UNC) path to the shared folder that contains the MSI package you want to deploy.

Notes:

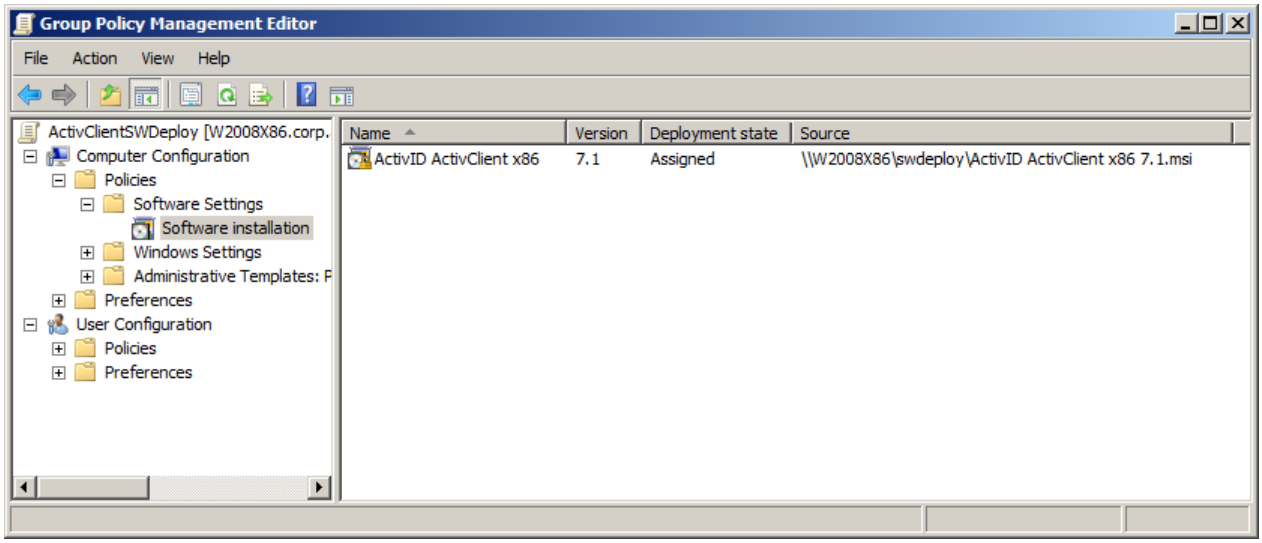
- Do not browse to the location. Make sure that you use the UNC path to the shared folder.
- It is mandatory that the package is assigned to a computer, as opposed to assigning it to a user.

7. Select the package and click **Open**.



8. Select **Assigned** and click **OK**.

The package is listed in the right pane of the Software installation window.



9. Close the console window.

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

6.2.3 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 on to a computer that is part of the target OU.
2. From the Start menu, point to **Settings**, and select **Control Panel**.
3. Double-click **Programs and Features**, and then click **Install a Program from the Network**.
4. 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**.

6.2.4 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. In the Group Policy Management Editor, return to the Software installation container that you created above.
2. Right--click the package, point to **All Tasks**, and select **Redeploy application**.
3. When prompted to accept that the application will be installed everywhere it is already installed, click **Yes**.
4. Close the console window.

6.3 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.

Prerequisites

- All client computers are connected in the same domain.
- The product (CD image) is stored on the server in a shared folder.

The deployment process involves a new wizard-based user interface specific to SCCM.

An SCCM 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.

Task	Task Description	See
1	Configure the client computers	6.3.1 Configure the Client Computers on page 88
2	Prepare the collection	6.3.2 Prepare Collections on page 88
3	Create a package.	6.3.3 Create a Package on page 88
4	Create and update a distribution point.	6.3.4 Create and Update a Distribution Point on page 96
5	Create a program for the package.	6.3.5 Create a Program on page 100
6	Advertise the package.	6.3.6 Create a Distributed Advertisement on page 108
7	Test the package.	6.3.7 Run an Advertised Program on a Client on page 115

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

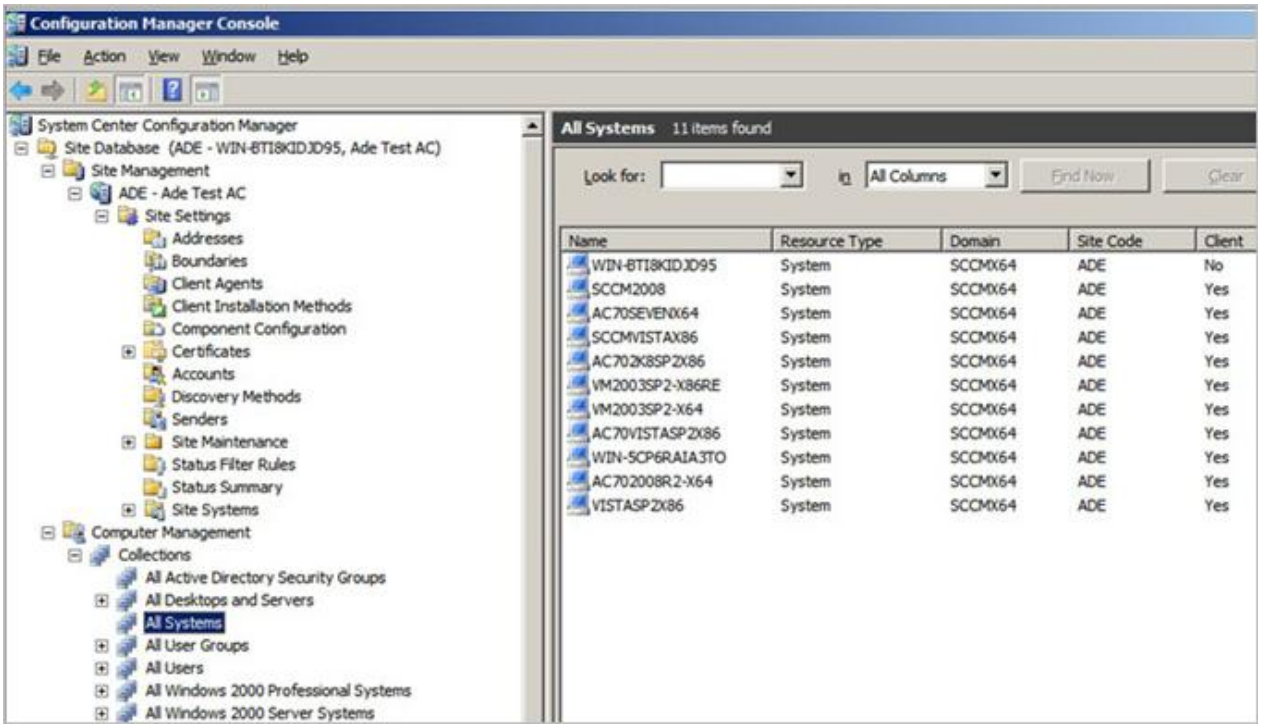
6.3.1 Configure the Client Computers

To support SCCM package deployment, you must configure the client computers with the following settings:

- Configuration Manager
- Program Download Monitor
- Run Advertised Programs
- Remote Control

6.3.2 Prepare Collections

1. Start the System Center Configuration Manager Console, and expand the **Computer Management** node.

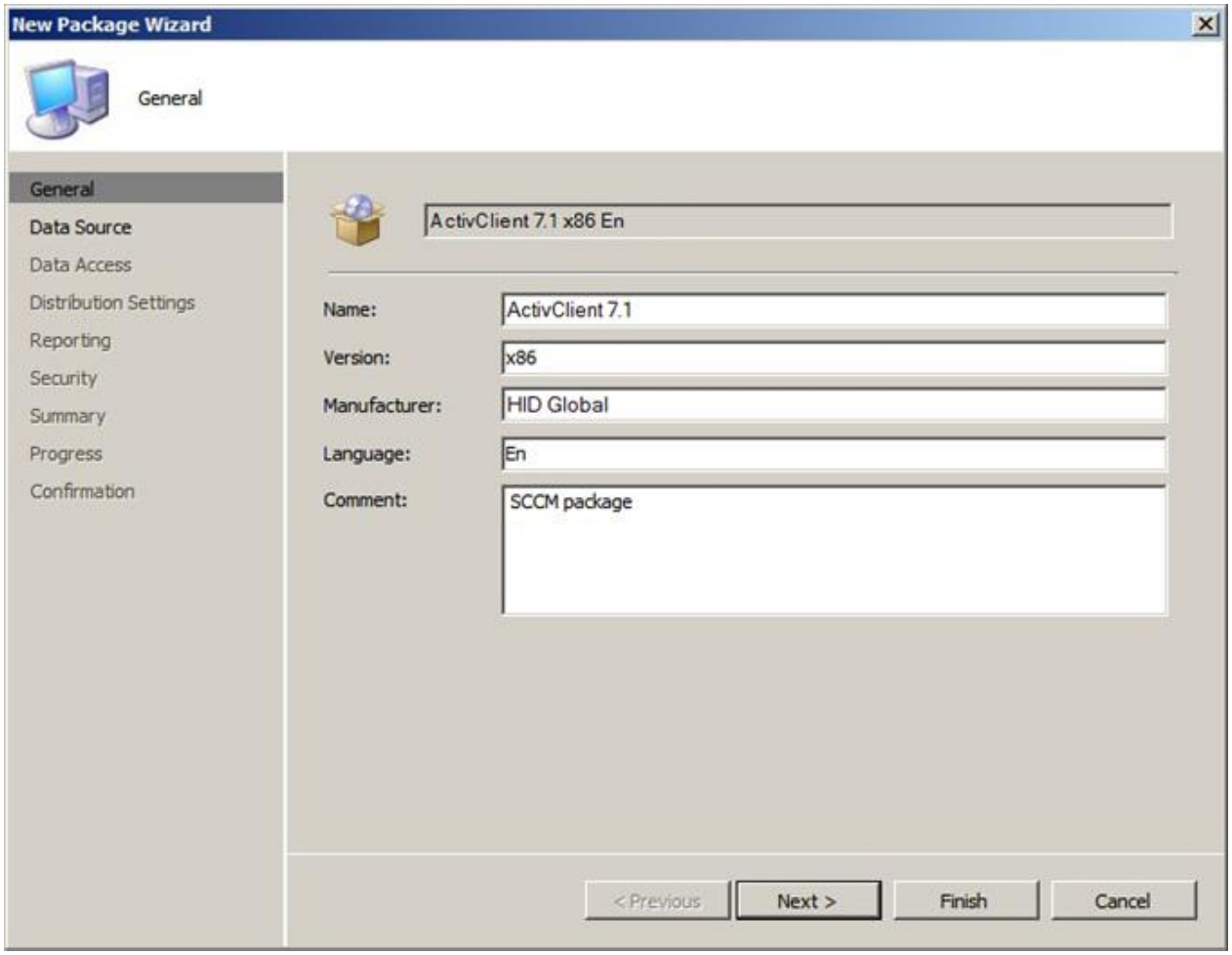


2. Expand **Collections** and either create a new collection or use an existing collection.

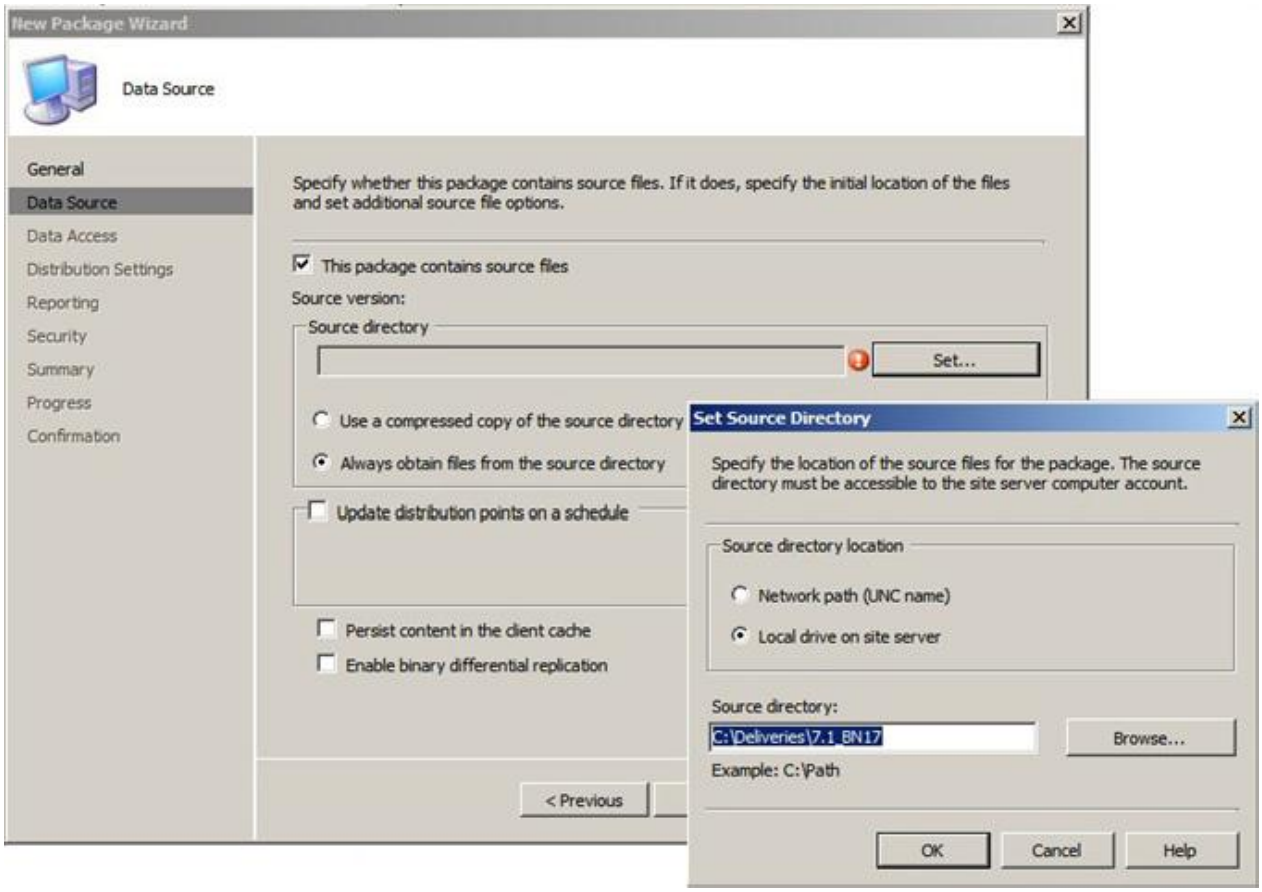
   The collection must contain the clients where you want to remotely install the package.

6.3.3 Create a Package

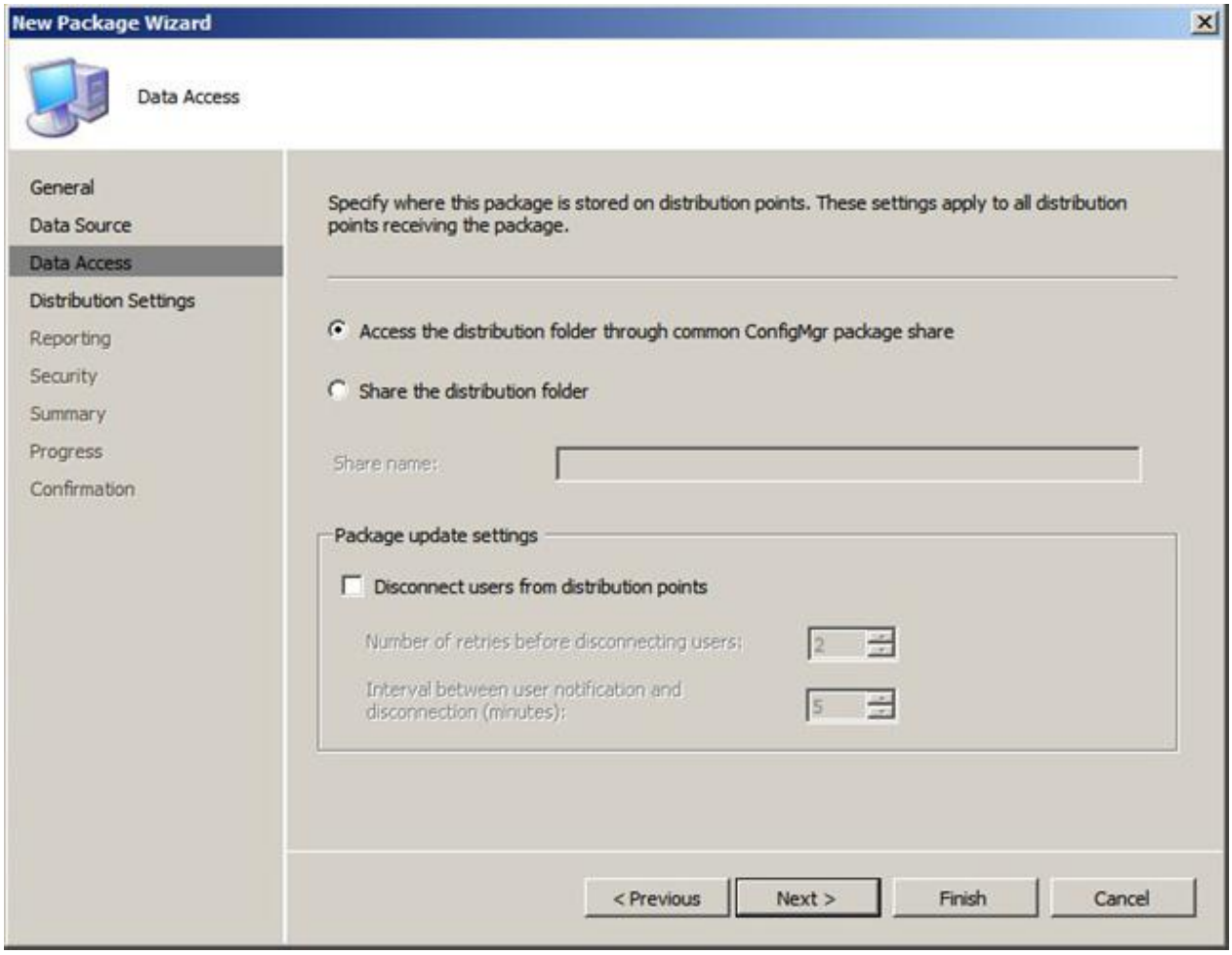
1. Start the System Center Configuration Manager Console, and expand the **Software Distribution** node.
2. Right-click on **Packages** and point to **New**, and then click **Package**.



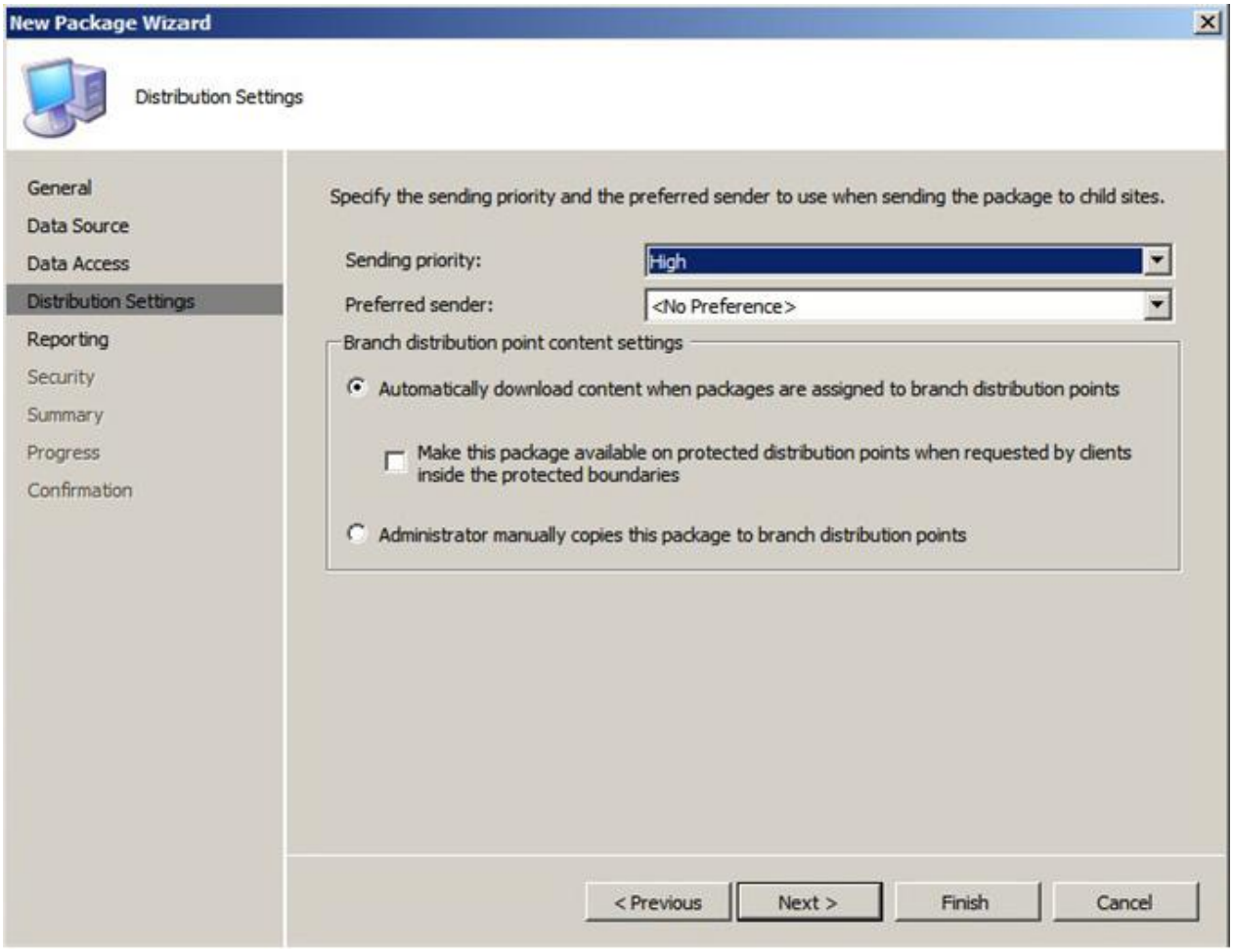
3. In the General page, enter the package information and click **Next**.



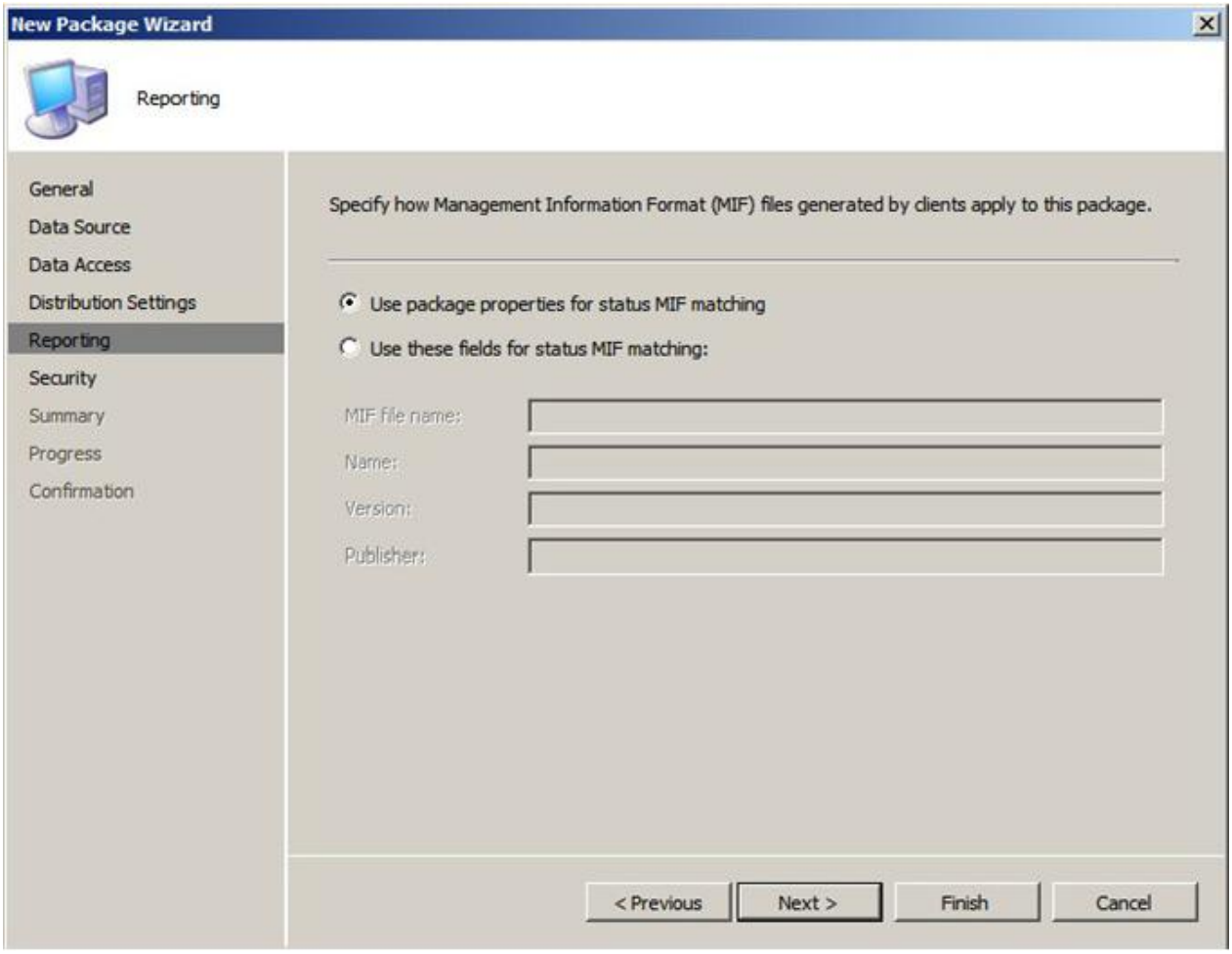
4. In the Data source page:
   a. Click **Set** to specify the directory containing the source files.
   b. Select the directory containing the ActivClient file and click **OK**.
   c. Select **Update distribution points on a schedule**, and click **Schedule**.
   d. Configure a schedule as required, click **OK** and then click **Next**.



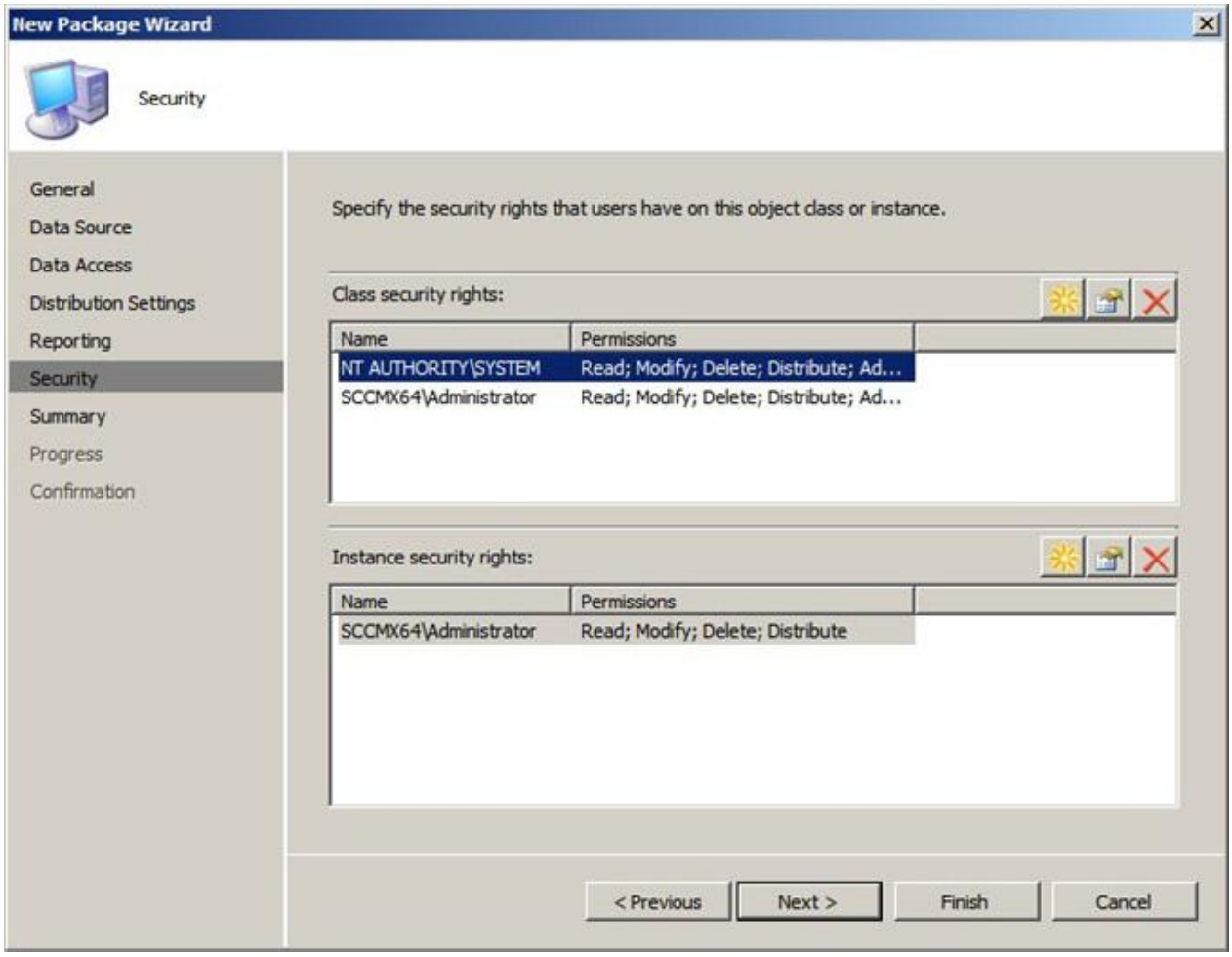
5. In the Data Access page, select the **Access distribution folder through common ConfigMgr package share** option and click **Next**.



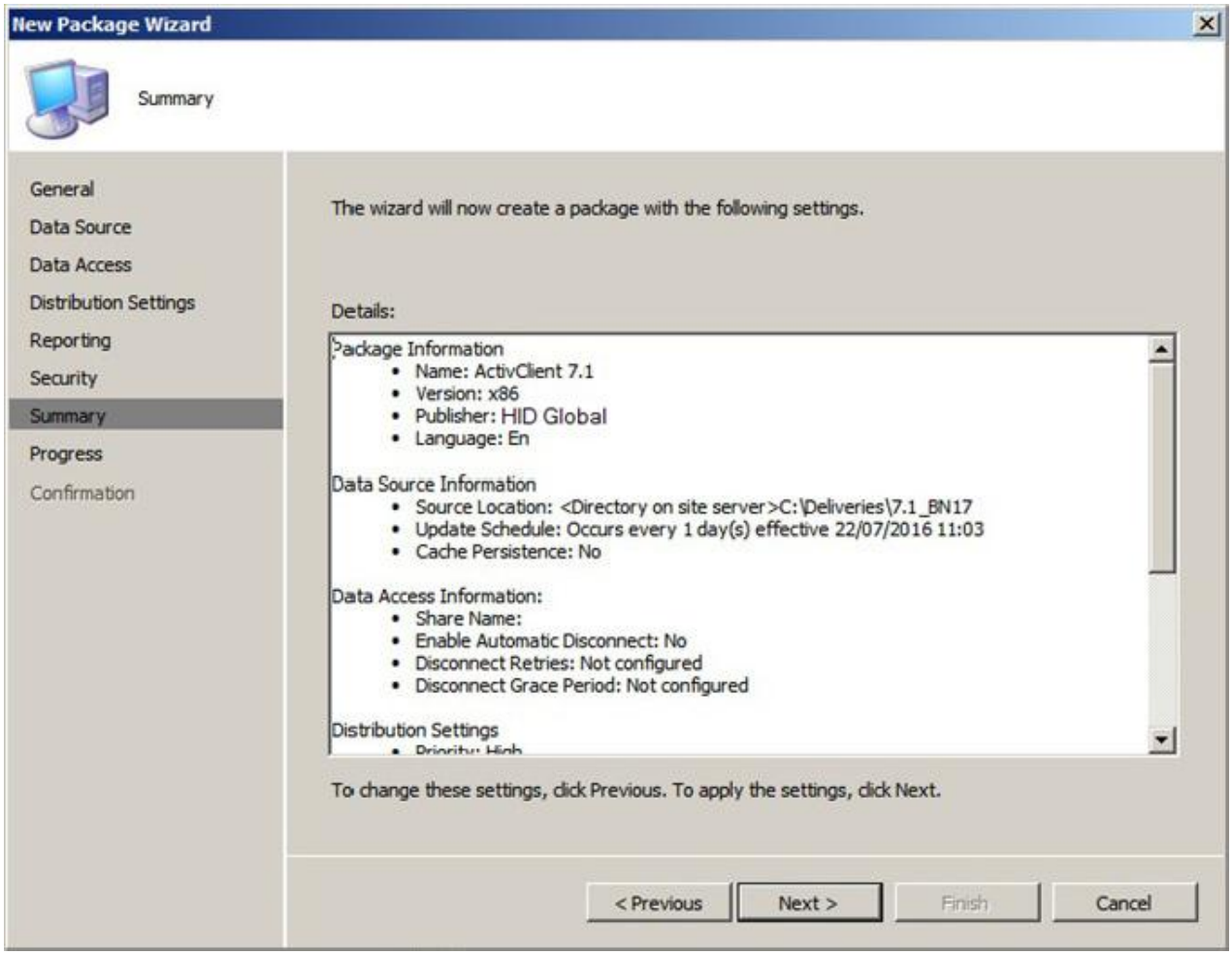
6. In the Distribution Settings page, from the drop-down lists, set the **Sending priority** (medium by default) and **Preferred sender** settings, and click **Next**.



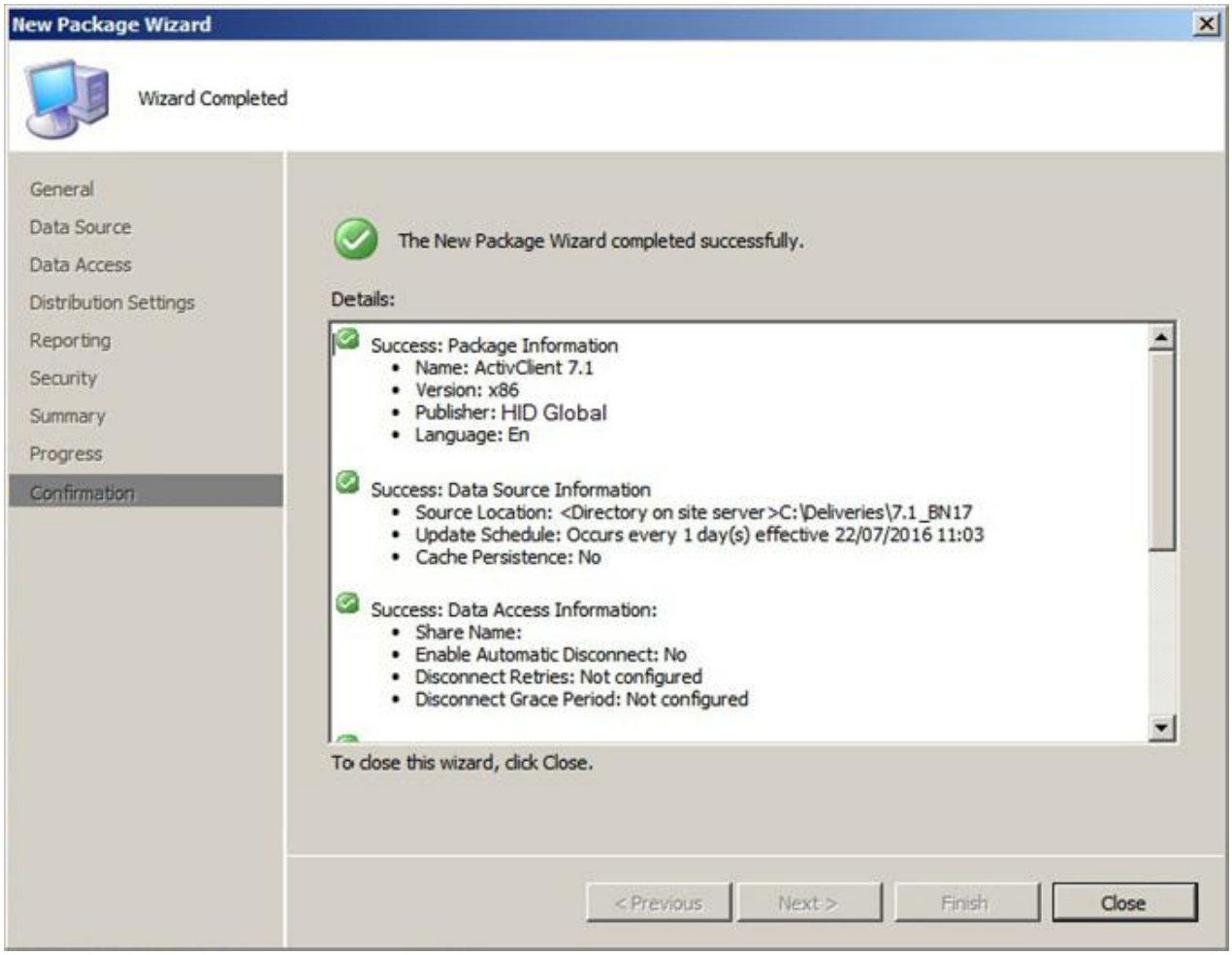
7. In the Reporting page, select **Use package properties for status MIF matching** option and click **Next**.



8. In the Security page, set the security rights that each user will have on the object class and instance of the package and click **Next**.



9. Review the package configuration summary and click **Next** to proceed (or Previous to modify a setting).



10. When the wizard successfully creates the package, click **Close**.

6.3.4 Create and Update a Distribution Point

A distribution point acts as distribution center for the package, allowing users to download and run the package files when a package is advertised.

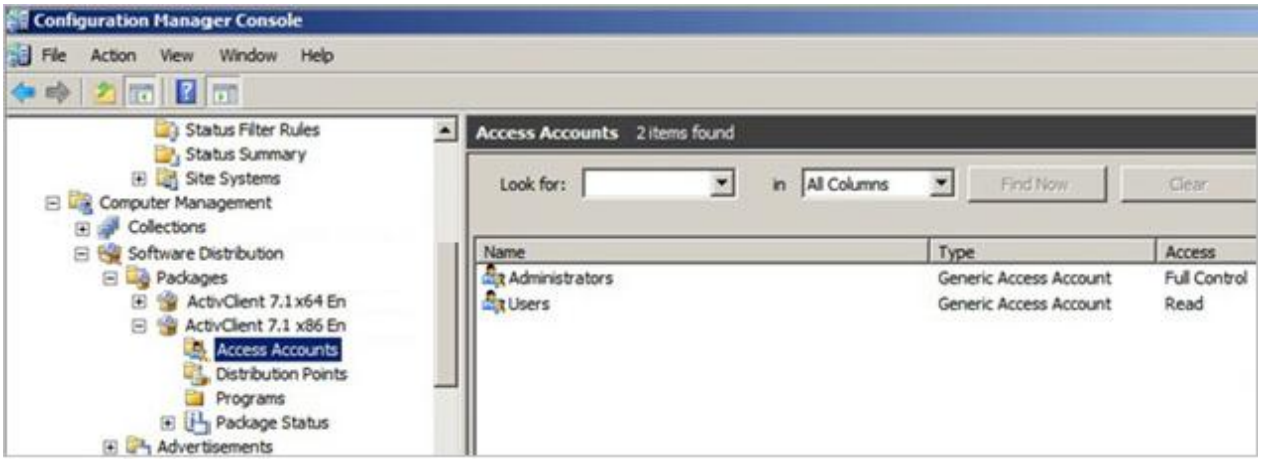
Use the New Distribution Points Wizard to select the distribution points to which you want to add the ActivClient package.

Prerequisite

To use your server as a distribution point for providing packages to distribute packages to client computers, you must first assign the Distribution Point role to the site system.

For further information, see the Microsoft SCCM documentation.

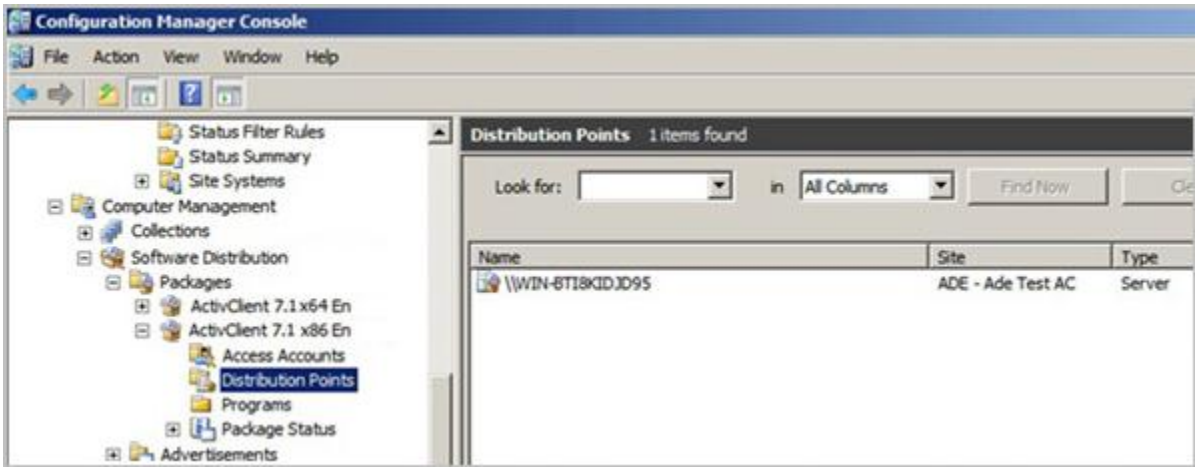
The package you created above is displayed under the Packages node.



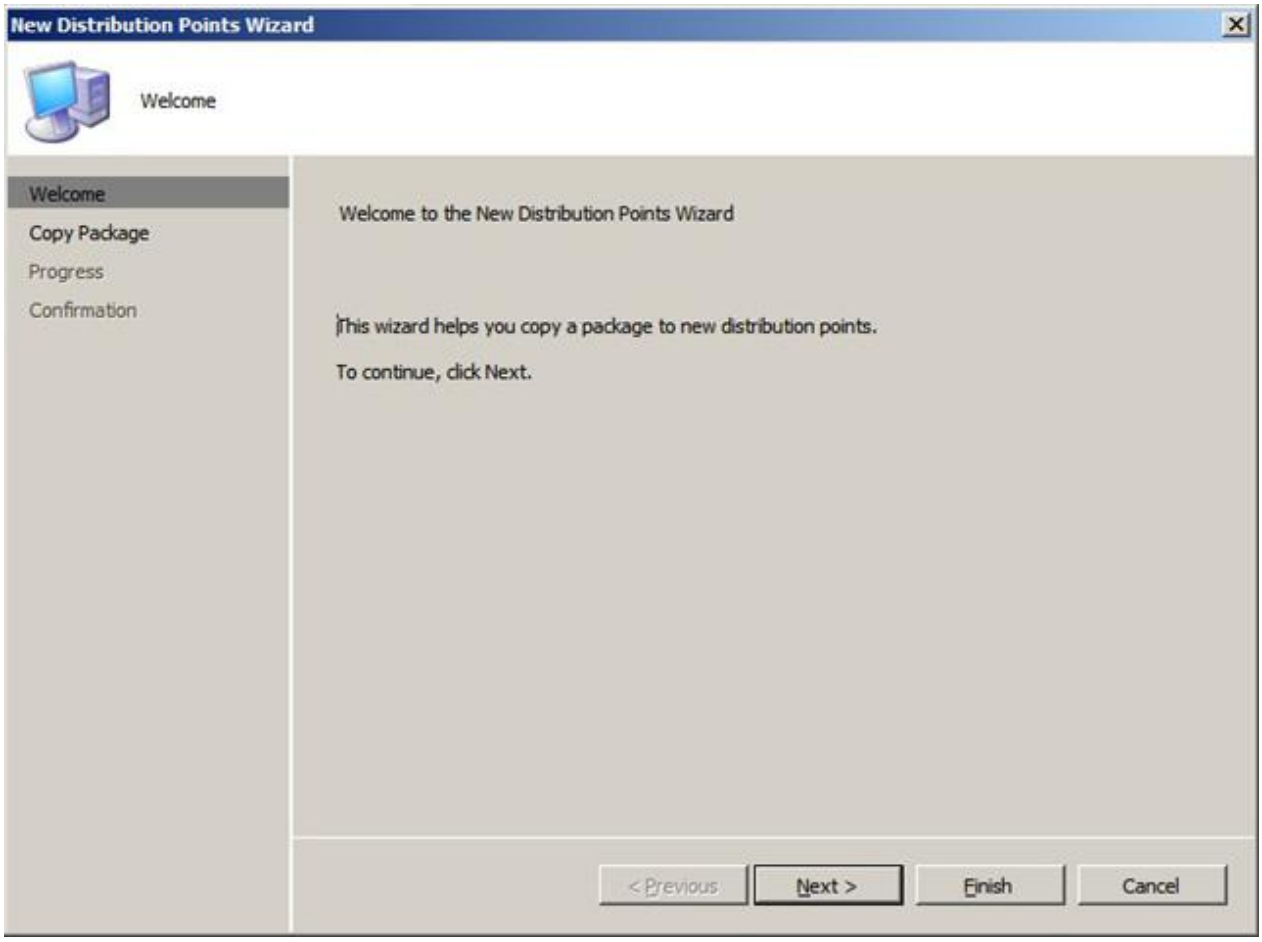
1. Select **Access Accounts** for the package to verify who has access to the package and the permission level.

   By default, the Configuration Manager sets Read access to the local Users group and Full Control to the Administrators group.

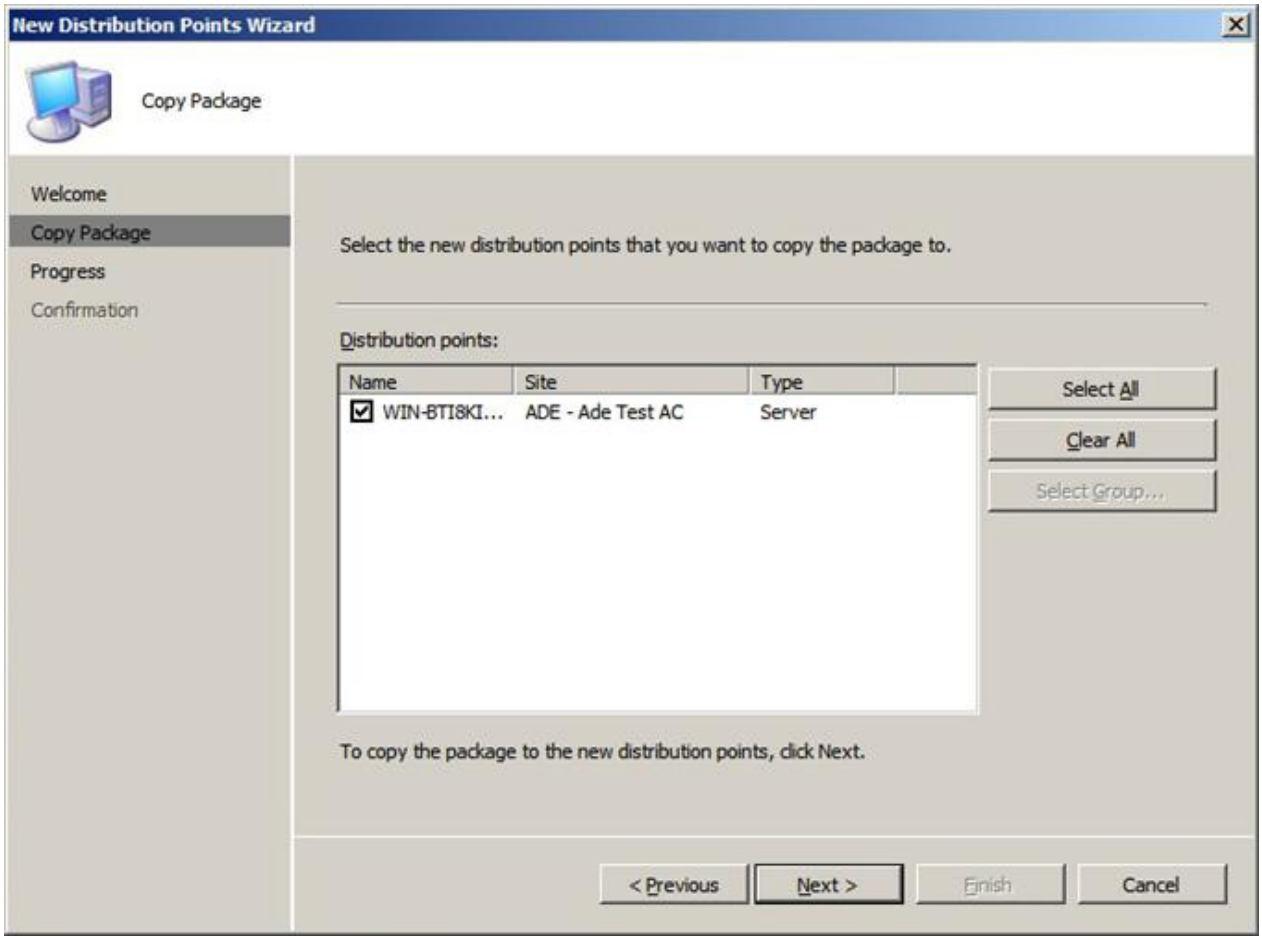
2. Select **Distribution Points** for the package.



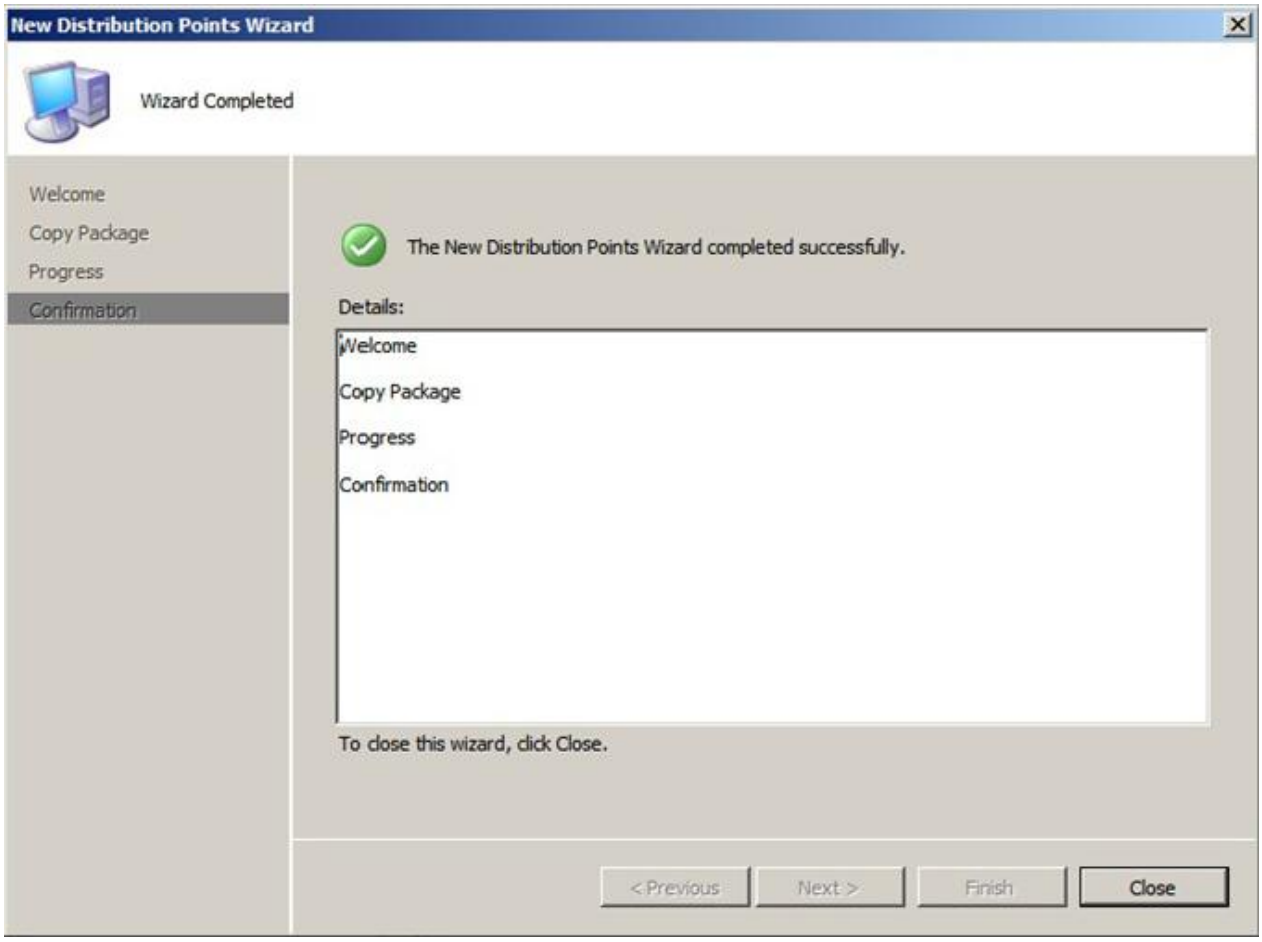
3. To create a new distribution point for the package, right-click on **Distribution Points** and select **New Distribution Points**.


New Distribution Points Wizard
Welcome
Welcome
Copy Package
Progress
Confirmation
Welcome to the New Distribution Points Wizard
This wizard helps you copy a package to new distribution points.
To continue, click Next.
< Previous
Next >
Finish
Cancel

4. Click **Next**.



5. Select your distribution point server and click **Next**.



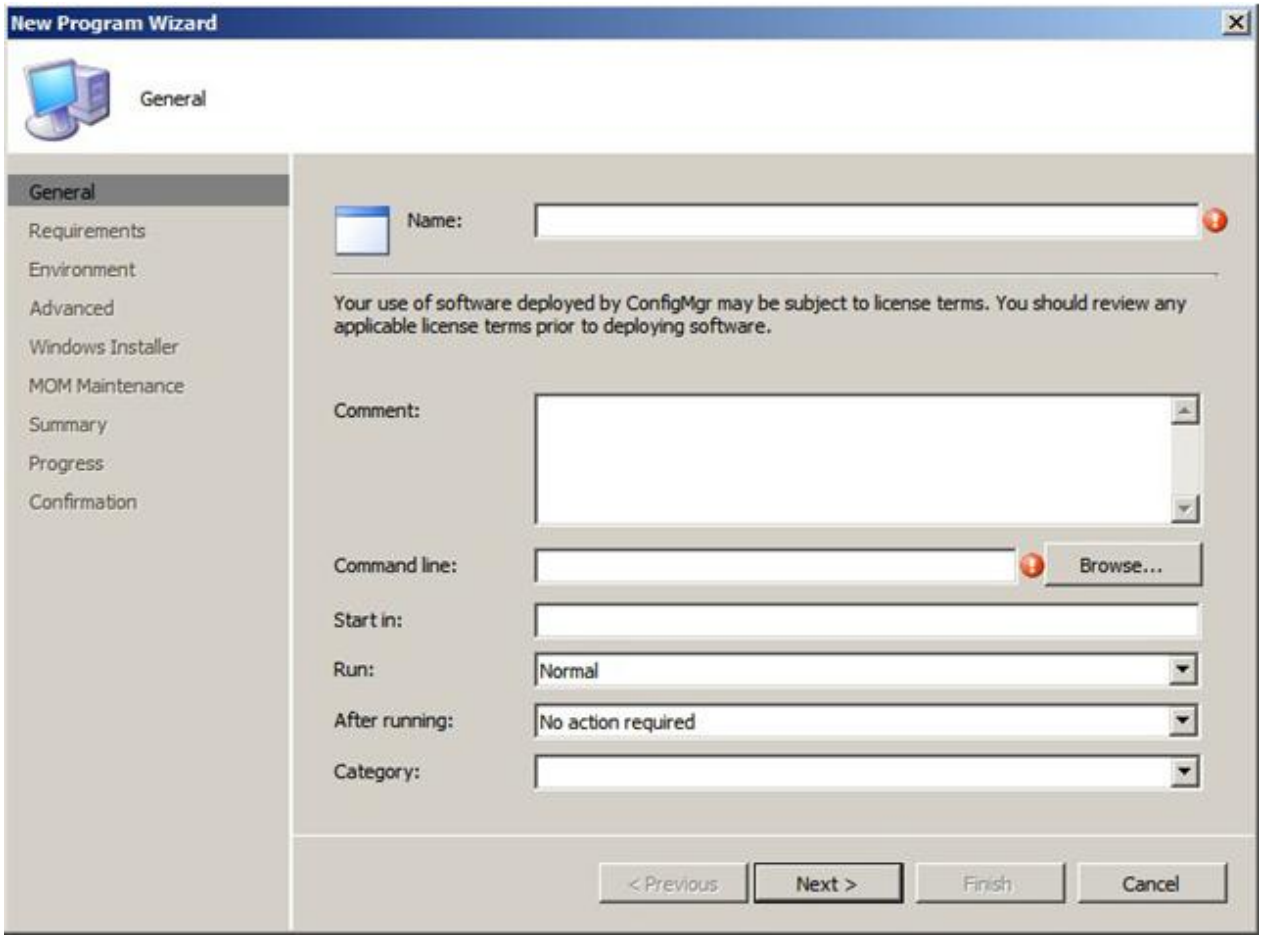
6. When the wizard successfully creates the distribution point, click **Close**.

   The package that you created previously is copied to the designated server for distribution.

6.3.5 Create a Program

Use the following procedure to create a program that contains the package behavior instructions for the client computers.

1. For your package, right-click on **Programs**, point to **New** and select **Program**.



2. In the General page:
   a. Enter a **Name** for the program (for example, Install ActivClient).
   b. Enter the Command line that you want to be executed on the client.
      For example, to install ActivClient, use one of following command lines depending of your operating system:

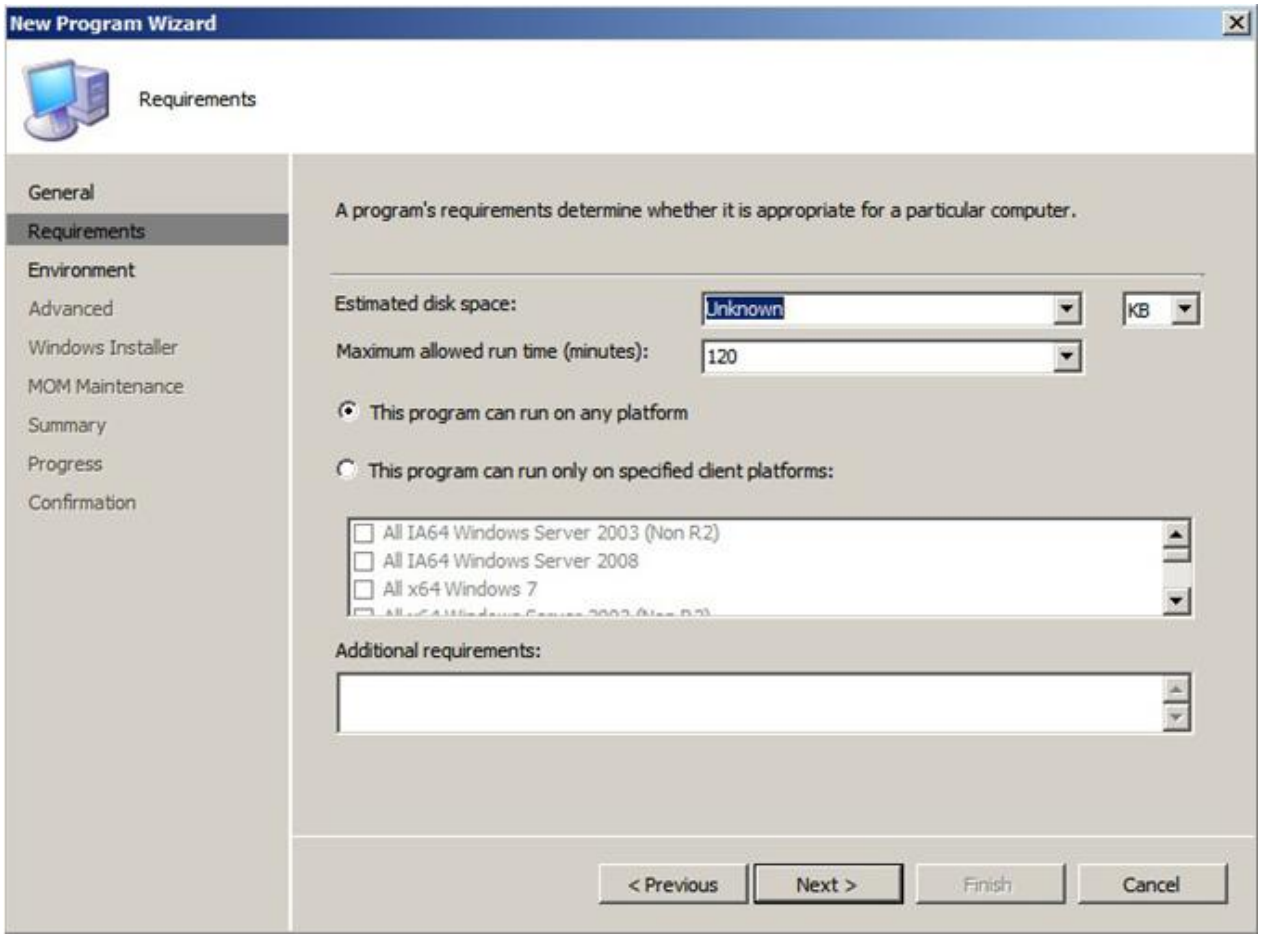
```
"ActivClient x86 7.1.msi /q
```

      or

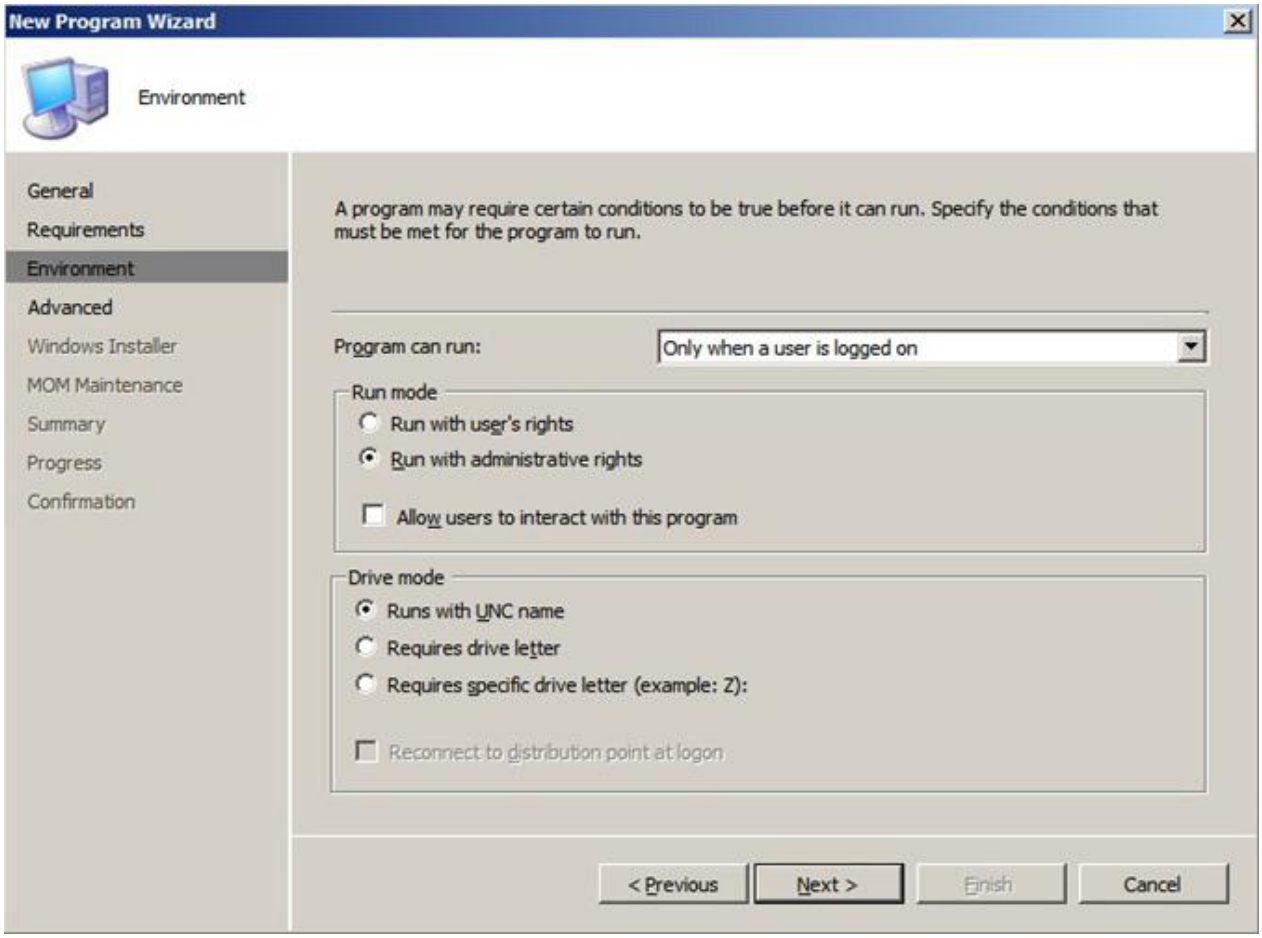
```
"ActivClient x64 7.1.msi /q
```

      If necessary, click **Browse** to navigate to the program file.
   c. Optionally, in the **Start** in field, you can specify the executable folder for the program (either an absolute path on the client or a path relative to the distribution point folder that contains the package).
   d. From the **Run** drop-down list, select **Maximized**.
   e. From the **After running** drop-down list, select **SMS restarts computer**.

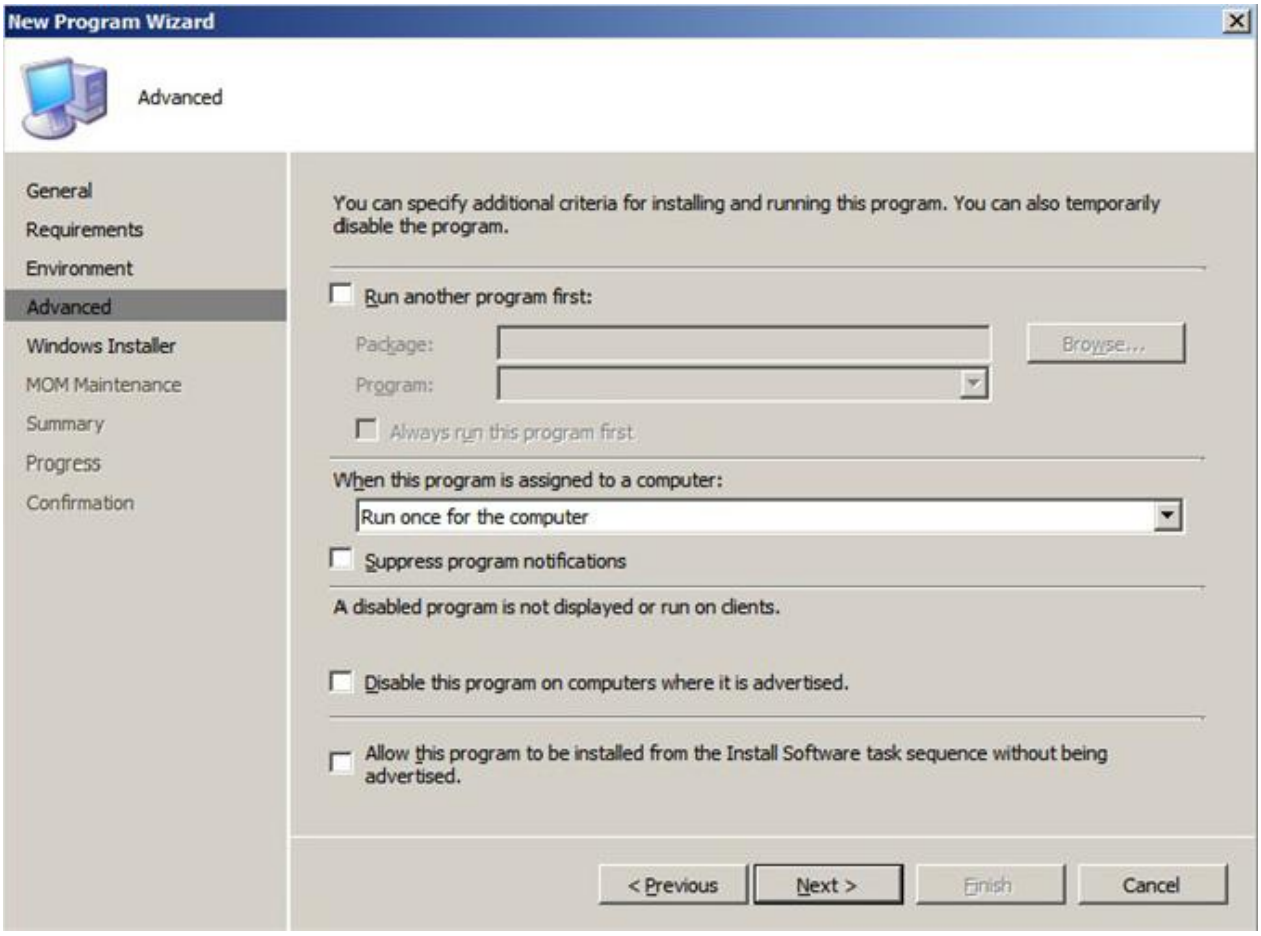
f. From the **Category** drop-down list, select the **cocreator** under which the program will be displayed on the client computer, and click **Next**.



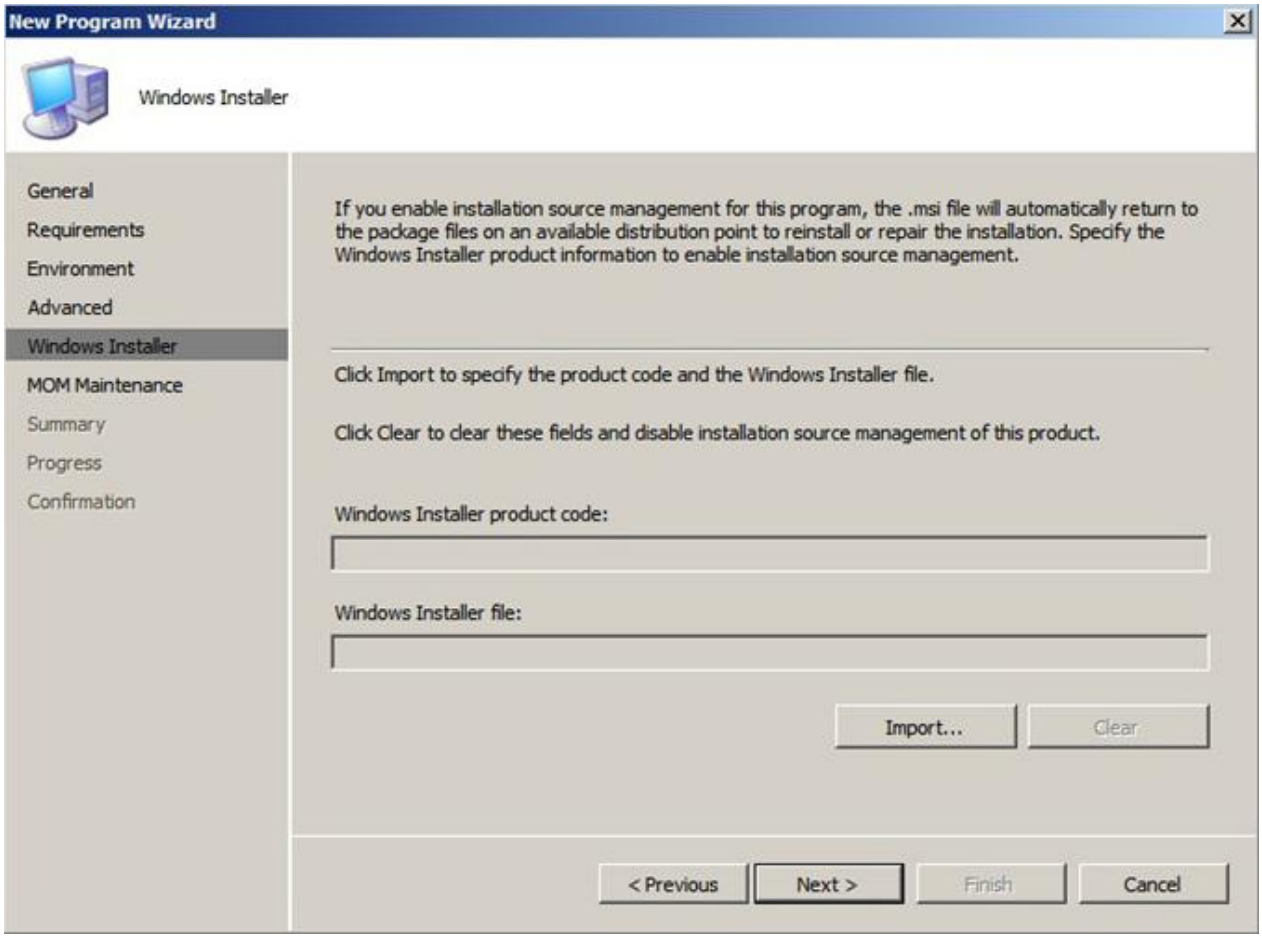
3. In the Requirements page:
   a. From the **Estimated disk space** drop-down list, set the size of the disk space you estimate is required to store this program.
   b. From the **Maximum allowed run time** drop-down list, set the run time you estimate is required to run this program.
   c. If necessary, select **This program can run on any platform** and click **Next**.



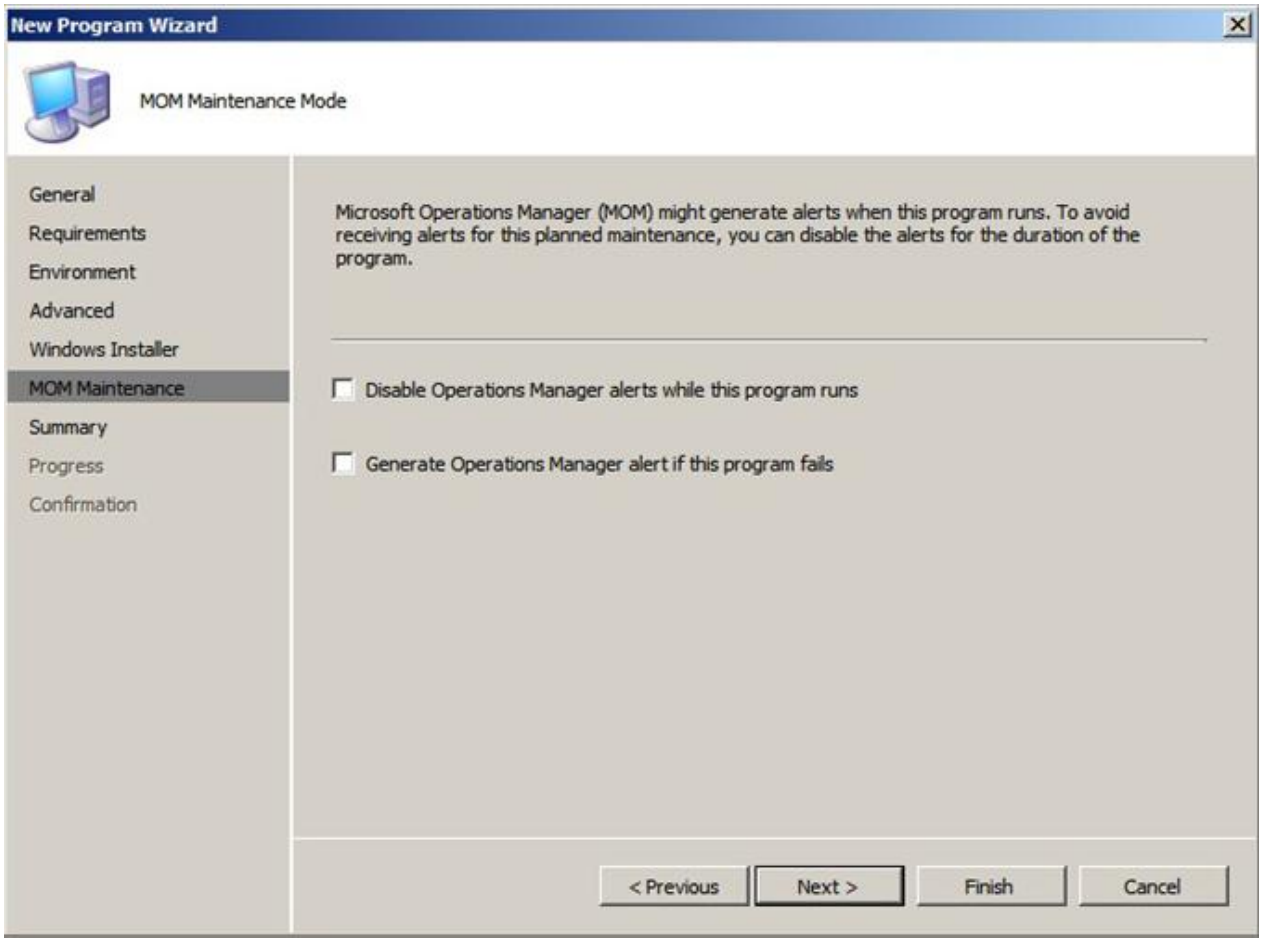
4. In the Environment page:
   a. From the **Program can run** drop-down list, select when the program can run.
   b. Select **Run with administrative rights**.
   c. Select **Allow users to interact with this program** if allowed by your organization's software deployment policy.
   d. Select **Runs with UNC name** and click **Next**.



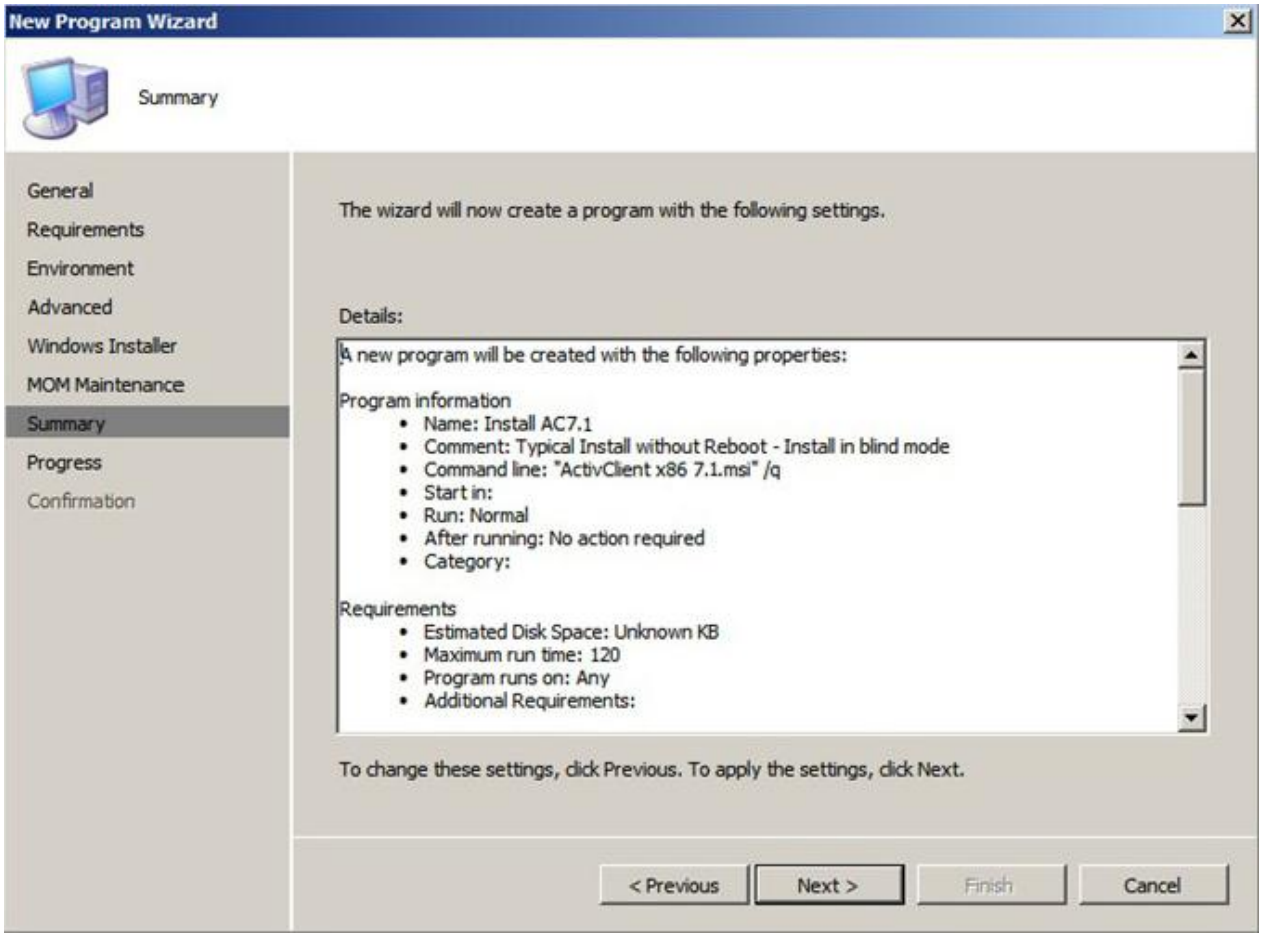
5. In the Advanced page:
   a. If this is an update, select **Run another program first** and use the **Package** and **Program** drop-down lists to select the package and program that must be run before running the current program. For example, the uninstall program.
   b. From the **When program is assigned to a computer** drop-down list, 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 options, and click **Next**.



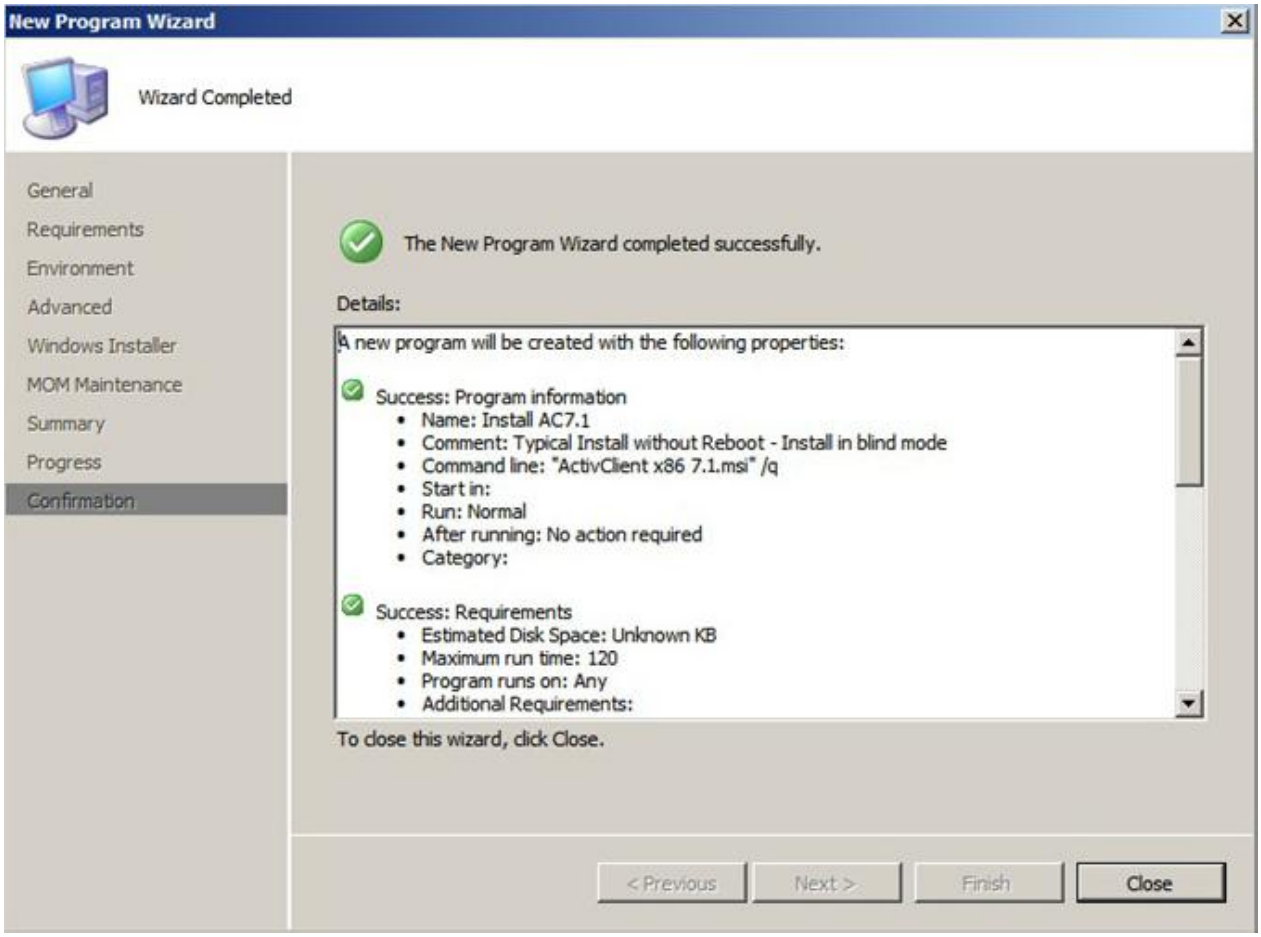
6. If you want to enable installation source management of ActivClient, click **Import** to obtain the product information of the relevant Windows Installer file and click **Next**.



7. If necessary, configure the MOM alert settings and click **Next**.



8. Review the program configuration summary and click **Next** to proceed (or Previous to modify a setting).



9. When the wizard successfully creates the program, click **Close**.

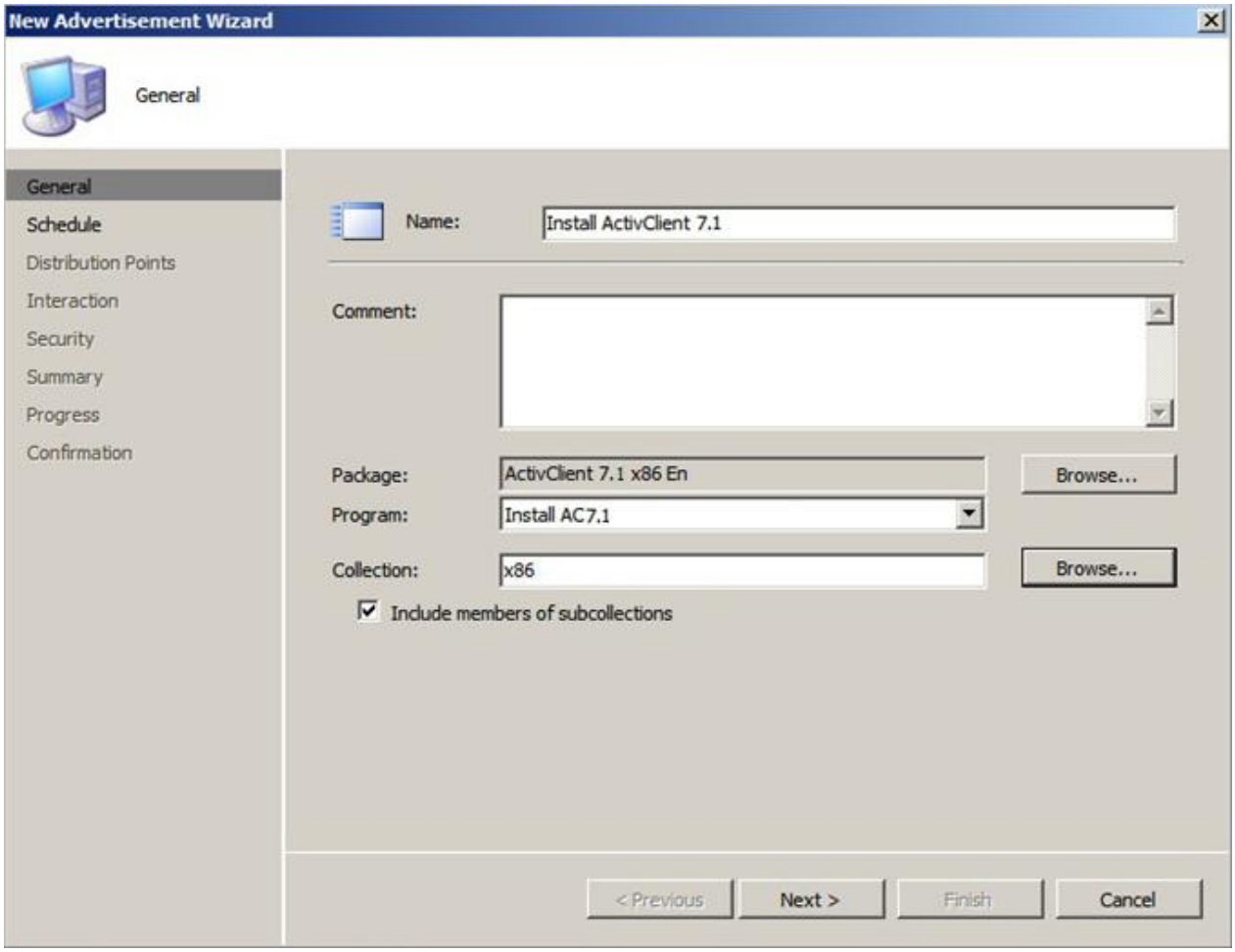
6.3.6 Create a Distributed Advertisement

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

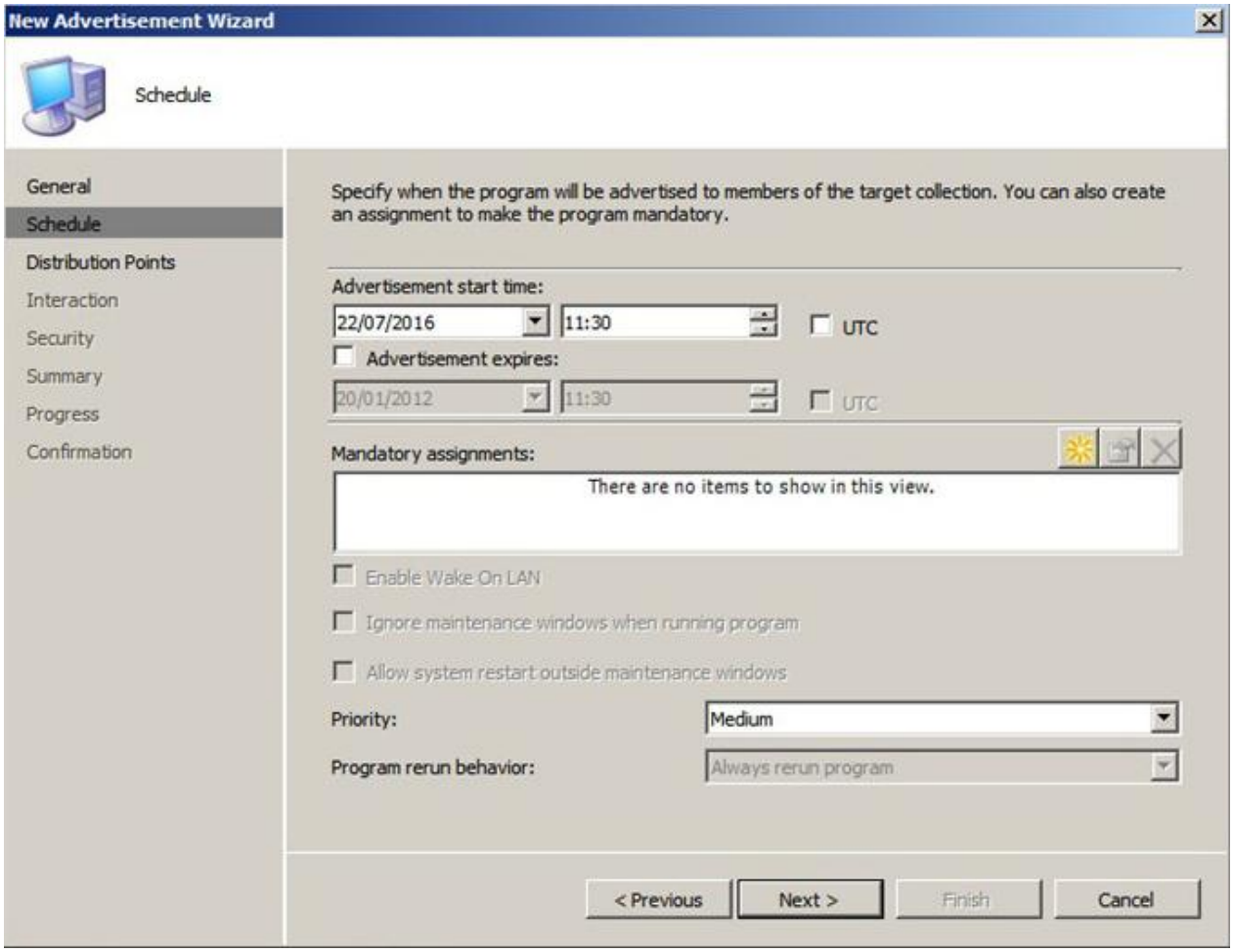
An advertisement defines the:

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

1. Under Software Distribution, right-click on **Advertisements**, point to **New** and select **Advertisement**.



2. In the General page:
   a. Enter a **Name** for the advertisement.
   b. Enter (or Browse to) the **Package**.
   c. Select the **Program** from the drop-down list.
   d. Enter (or Browse to) the **Collection** and select **Include members of subcollections**, and click **Next**.

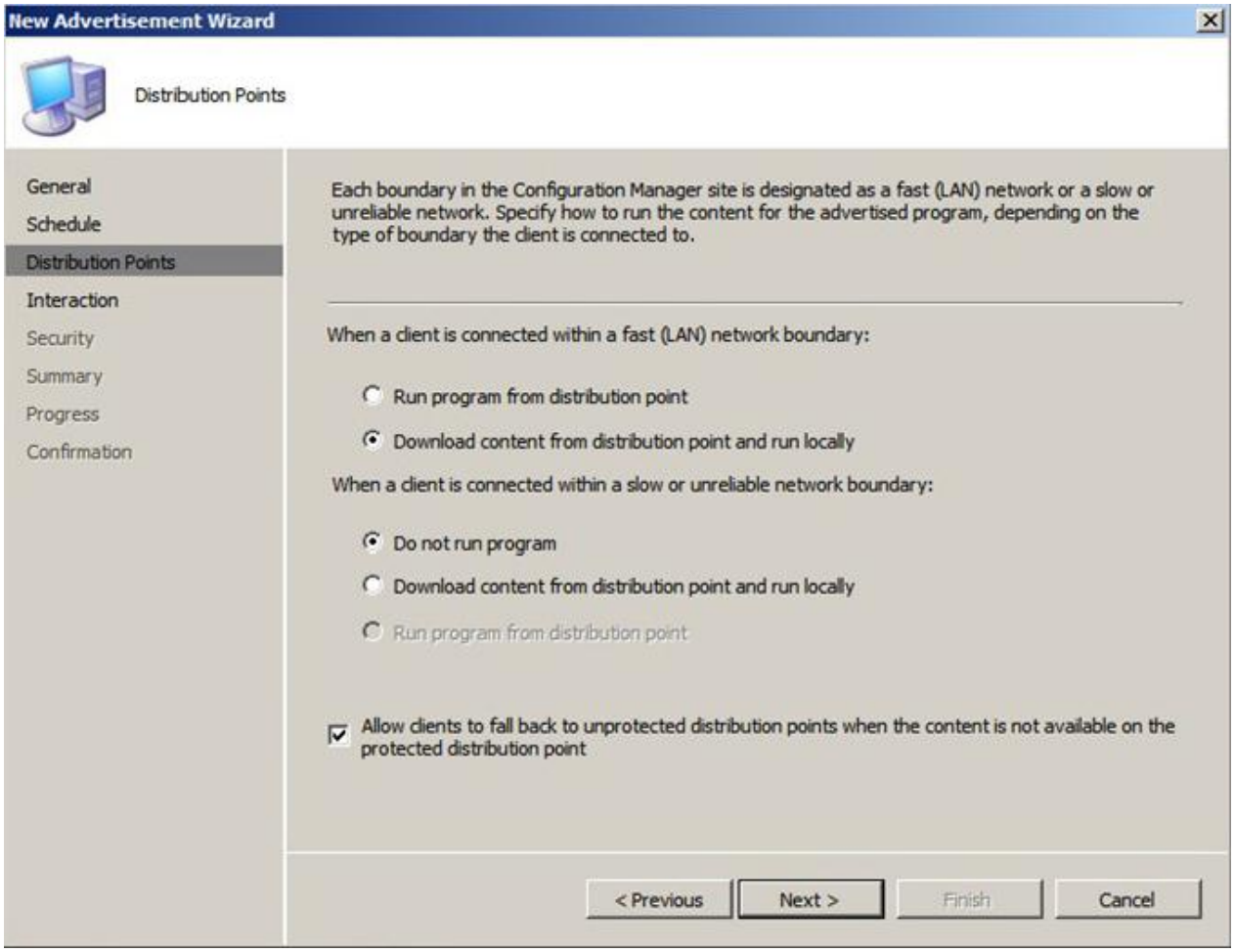


3. Enter a start date and time when the program is advertised and available to run on client machines.

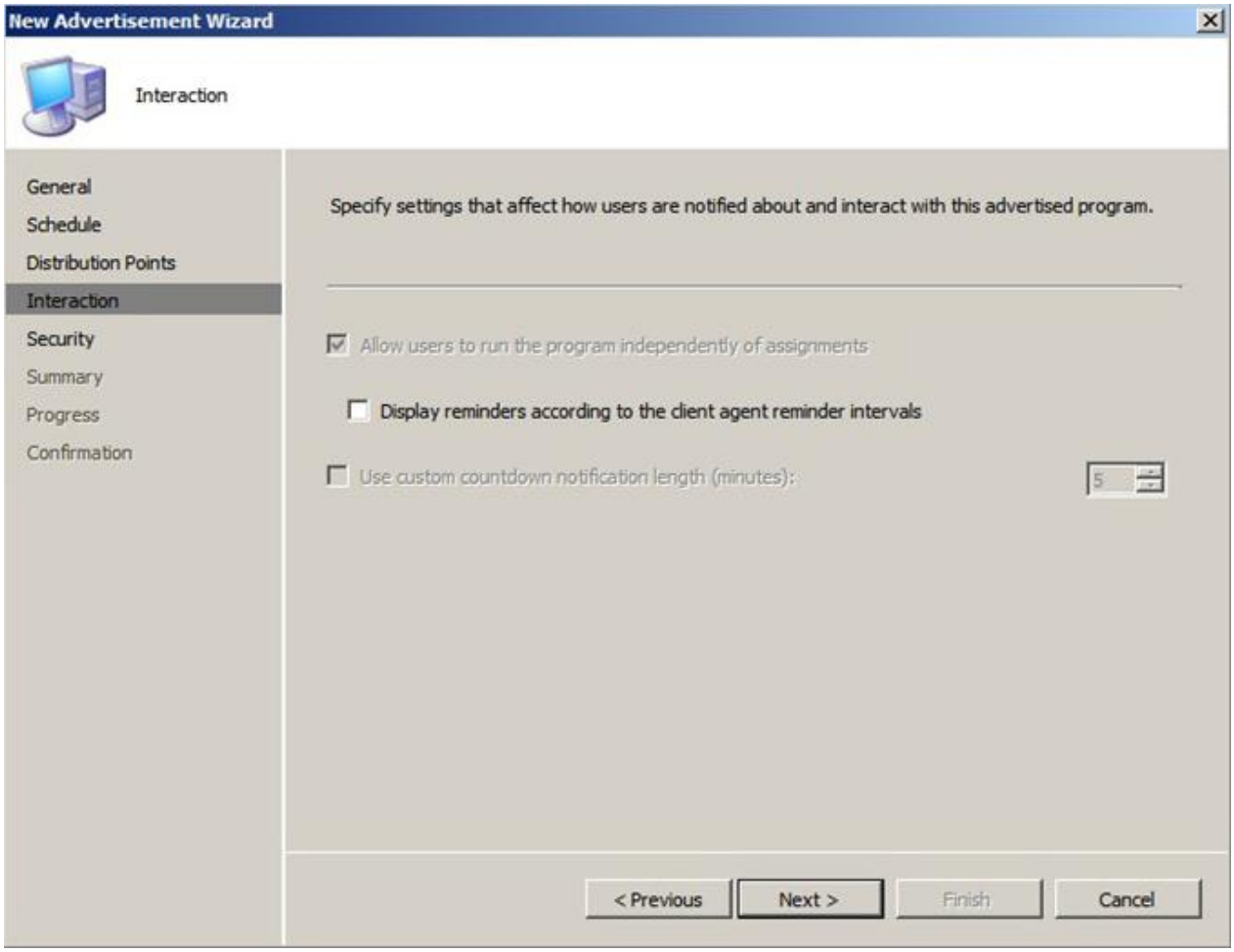
   To remove a program from the list of available programs after a specified period of time, select **Advertisement expires** and then specify the date.

   You can also set the program as a mandatory assignment.

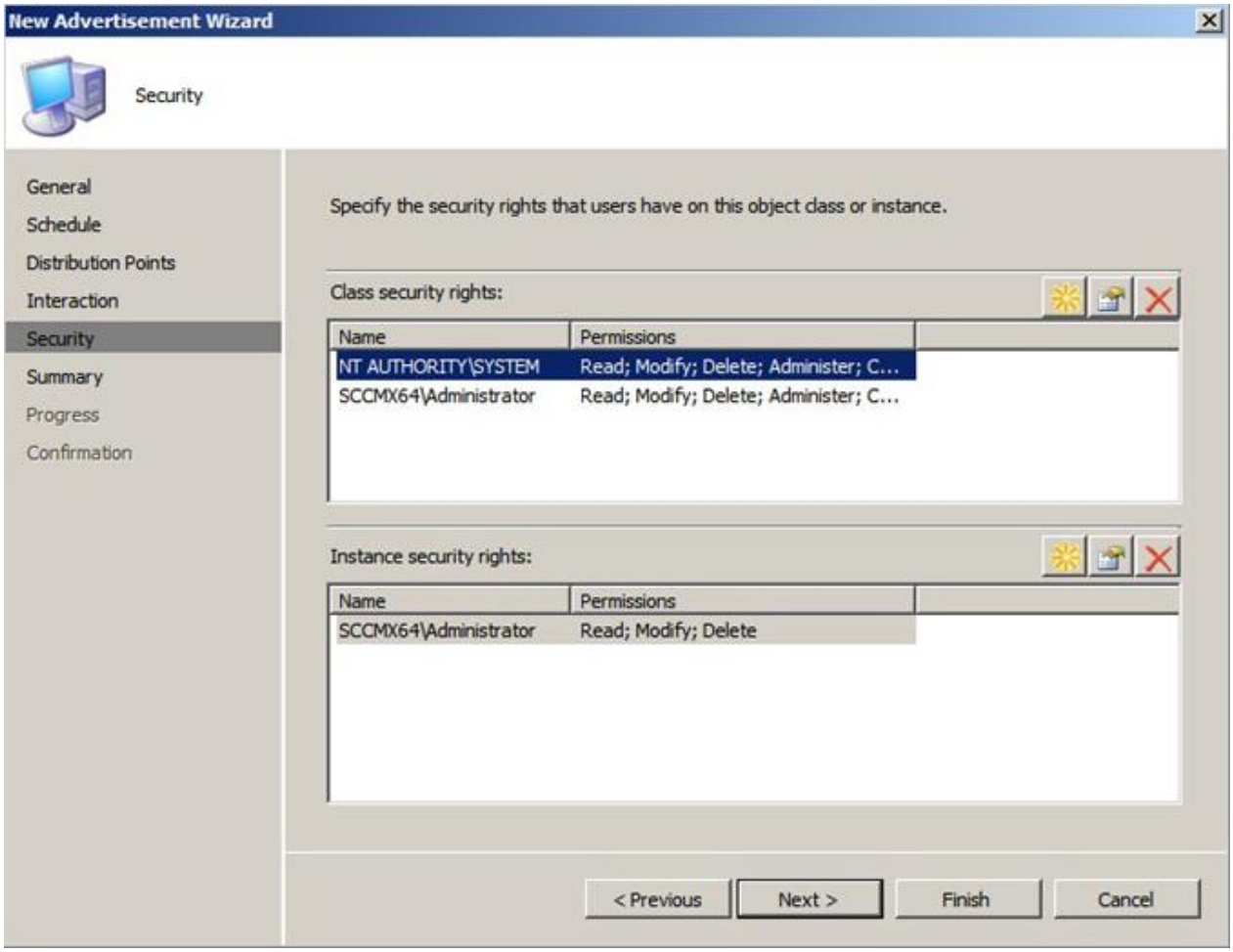
4. Click **Next**.



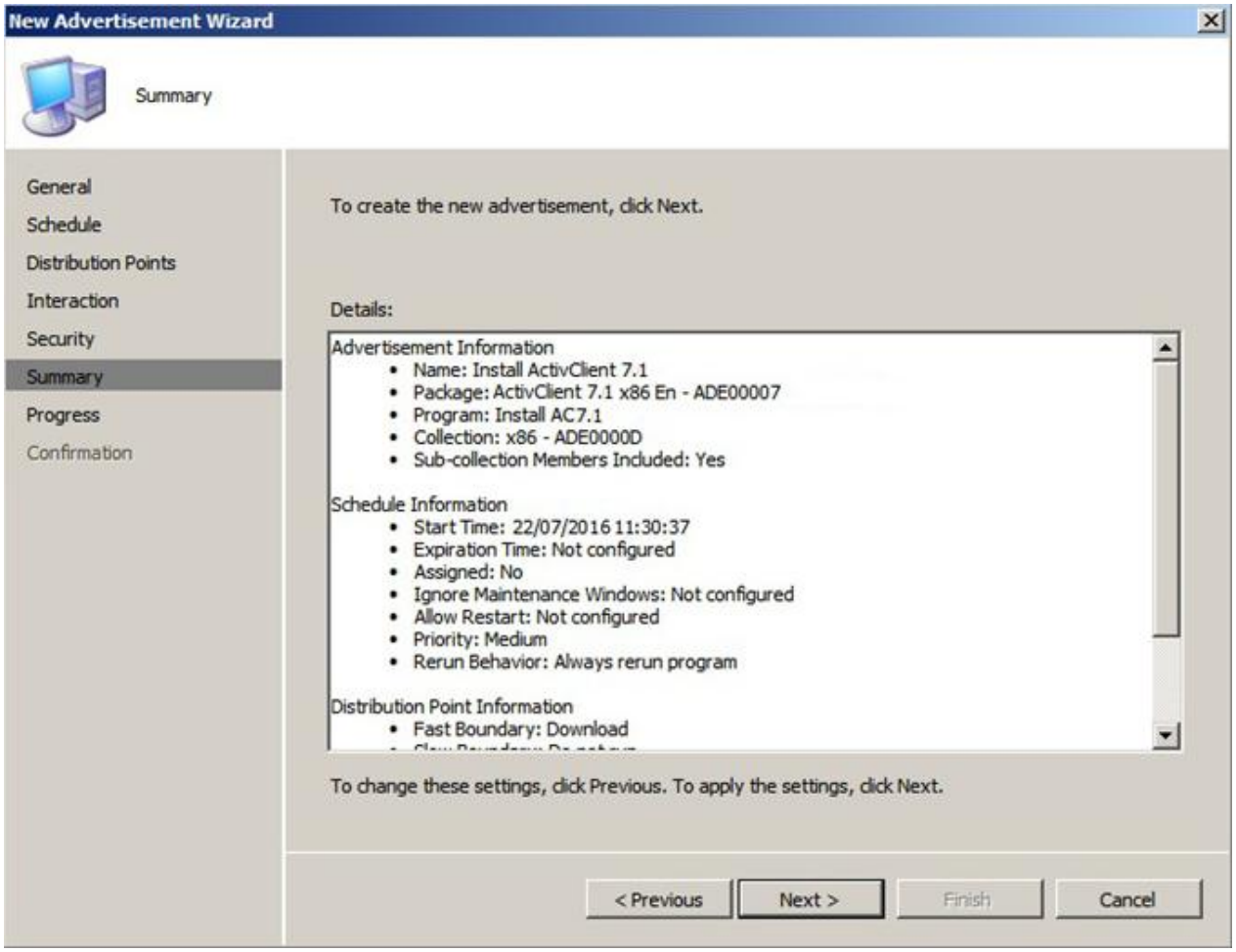
5. In the Distribution Points page, specify how to deliver and run the content for the new advertisement, and click **Next**.



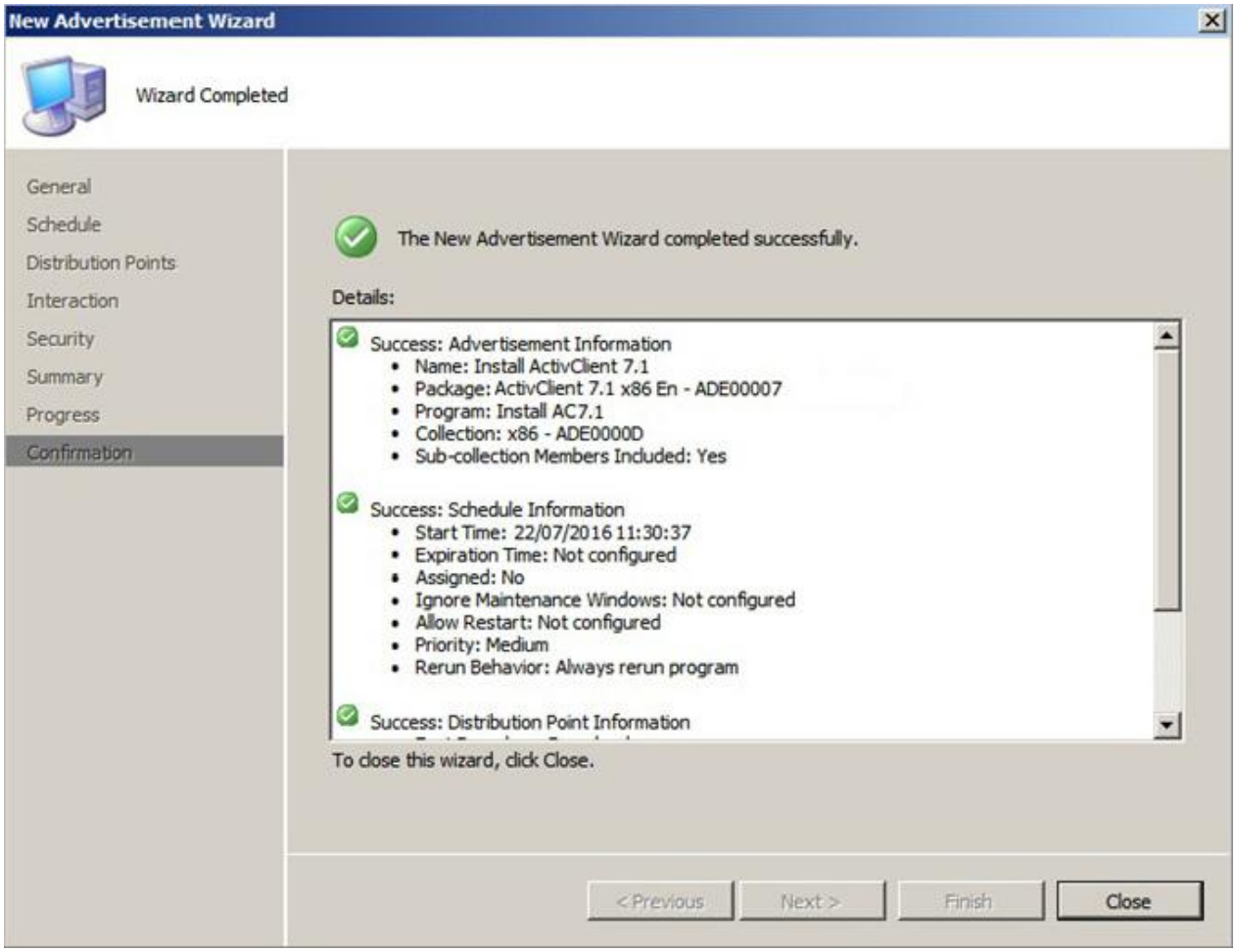
6. In the Interaction page, select whether reminders are displayed to the user and, if required, the length of time that the reminder is displayed, and click **Next**.



7. In the Security page, specify the security rights individual users have on both the class/instance and the specific advertisement, and click **Next**.



8. Review the advertisement configuration summary and click **Next** to proceed (or Previous to modify a setting).



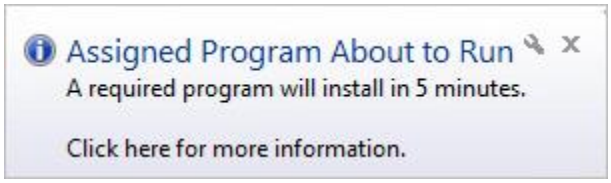
9. When the wizard successfully creates the advertisement, click **Close**.

6.3.6.1 Monitoring the Software Distribution

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

6.3.7 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.

7.0 Upgrading and Updating

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

7.1 Upgrading ActivClient

7.1.1 Supported ActivClient Upgrades

This release of ActivClient allows you to upgrade automatically from previous versions:

- ActivClient 6.2 (32-bit and 64-bit editions)
- ActivClient CAC 6.2 (32-bit and 64-bit editions)
- ActivClient 7.0 (32-bit and 64-bit editions)
- ActivClient 7.0.1 (32-bit and 64-bit editions)
- ActivClient 7.0.2 (32-bit and 64-bit editions)

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

- Upgrading from ActivClient 6.2:
  - If you had customized the previous ActivClient 6.x version by specifying which components to install, the equivalent components will be installed during the upgrade. For example, if you had installed the ActivClient 6.x CSP, the ActivClient 7.x Mini Driver will be installed.
  - If you had customized the previous ActivClient 6.x version by updating some configuration options (registries or administrative templates), this customization is not upgraded automatically.

    The ActivClient customization model has been changed to a new policy model, as described in section 3.0 Defining the ActivClient Policies on page 15. Many policies have changed (for example, the authorized reader list has been replaced by a reader black list), some ActivClient policies have been replaced by similar Microsoft policies (for example, the card removal policy).

    Therefore, it is recommended that you review the policies required in your organization before deploying ActivClient 7.1.
- Upgrading from ActivClient 7.0.x:

  If you are upgrading from ActivClient 7.0.x, previous policy settings are not removed. During the upgrade to ActivClient 7.1, it is recommended that you:

  a. Clear the ActivClient 7.0.x policy settings with Group Policy Editor and uninstall the ActivClient 7.0.x ADMX/ADML files.

  b. Install the ActivClient 7.1 ADMX/ADML files and configure the policies as required.

7.1.2 Supported HID Global Mini Driver Upgrades

If Mini Driver is already installed on the machine, you can upgrade to the version delivered with ActivClient 7.1 in order to have access to more capabilities. The supported upgrades are from:

- Mini Driver 1.0, 1.1 and 1.2 (installed with an MSI package)
- Mini Driver 1.2 (installed via Microsoft Windows update)

7.1.3 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 *ActivID ActivClient for Windows Installation Guide*.
- 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 section 6.2 Deploying Using Active Directory Push on page 83.
- If you deployed a previous version of ActivClient with Microsoft SCCM, then you can deploy the new package with the same methodology. For more information, see section 6.3 Deploying using Microsoft System Center Configuration Manager on page 87.
- If you used the ActivClient Auto-Update feature, see section 7.2 Using ActivClient Auto-Update on page 117.

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

7.2 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.

Because configuration is site dependent, HID Global 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.

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.

7.2.1 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, although it is highly recommended that you use HTTPS for security reasons.

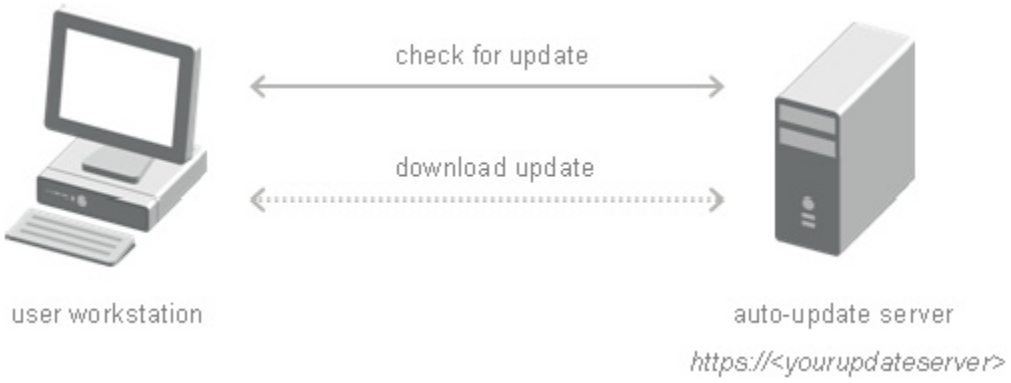
The web server can reside on your company intranet, the DMZ, or on the Internet. You can use any standard web server.

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

- If ActivClient is already upgraded, nothing is done.
- If 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.

Figure 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:

- Major updates – new ActivClient versions (MSI files)

- Maintenance updates – ActivClient hot fixes and service packs (MSP files)

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

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

For further information, see section 7.2.3 Configure ActivClient Auto-Update on page 119.

7.2.2 Prerequisites

- Confirm that the ActivClient Auto-Update component is installed on the client machines.

  The ActivClient Auto-Update component is not installed during a typical setup. Install the ActivClient Auto-Update component on the user workstation using the Custom setup option. For further information, see the *ActivID ActivClient for Windows Installation Guide*.

- If you are using HTTPS (recommended), make sure 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 installed in the ActivClient installation directory.

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 (from the **Tools** menu, go to **Internet Options**, **Content**, **Certificates**, and then **Trusted Root Certification Authorities**).

7.2.3 Configure ActivClient Auto-Update

To configure auto-updates for both 32-bit and 64-bit editions of ActivClient 7.1 on the same server, you must create two different configuration files.

Note: MSI files are typically larger than MSP files and network traffic can be higher as a result of using this method.

1. On the web server you want to use for the updates, create a virtual directory called **AutoUpdate\ActivClient**.
2. In this folder, create an *autoupdate.ini* file.

3. In autoupdate.ini, replace **AC_XX.msX** with the filename of the *.msi* or *.msp* that must be installed.

   For example:

```
[AUTOUPDATE]
BuildNumber=7.1.18
FileName=ActivClient x86 7.1.msi
CmdLine=/qr
```

   Where:

   - BuildNumber is required and indicates the build number to be installed.
   - FileName is required and indicates the update file to be installed.
   - CmdLine is optional and indicates optional options to use with msiexec during installation. For example:
     - For a MSI – `CmdLine=/qr`
     - For a MSP – CmdLine=REINSTALL=ALL REINSTALLMODE=vomus /qr

   It is highly recommended that you:

   - Set `REINSTALLMODE=vomus` in the command line in order to make sure 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.

4. Place the *.msX* file (Microsoft Patch file) in the same virtual directory as the *autoupdate.ini* file.

Note: ActivClient hot fixes are cumulative, so only the latest ones need to be on the Auto-Update server.

7.2.4 Configure ActivClient Auto-Update on the Client Machines

You then must configure ActivClient as follows.

(See section 4.10 Smart Card Auto-Update on page 51 for details on product customization.)

- Enable software auto-update – defines if ActivClient will automatically check if software update is made available:
  - URL (text, empty by default)

    This is the web address of the server where the new version is stored.

    The URL can be a http or https URL. If the URL is SSL, the validity of the certificate must be checked (that is, the certificate must be trusted on the machine).

    Example: http://194.168.2.221/Autoupdate/ActivClient
  - DownloadPath (text, empty by default)

    This file must have restricted access rights (administrator and system) to avoid security issues.

    Example: C:\DownloadedUpdate
- Frequency of update – defines the interval (in days) between checks for software updates:
  - CheckDays (numerical, '1' by default)

    Interval when the check must be done (in days).
- Maximum number of update retries – defines the number of times the AC autoupdate service will attempt to update the software.
  - NumberOfRetries (numerical, '3' by default)

    In case of problem when downloading the patch, numbers of tries before aborting download. If the download is aborted, the next check has a chance to download the patch.
- Delay between update retries – defines the waiting period (in minutes) before AC autoupdate service retires to update the software.
  - TimeBetweenRetry (numerical, '15' by default)

    Time in minutes before retrying the download.

8.0 Uninstallation

This section explains how to uninstall ActivClient and its components.

8.1 ActivClient Uninstallation Methods

You can uninstall ActivClient either locally or remotely from a group of computers with the Microsoft System Center Configuration Manager (SCCM) using a command line:

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

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

- For ActivClient x86 7.1:

  {A2D8C2E3-5CD4-4498-829D-D1E47B4D44A8}

- For ActivClient x64 7.1:

  {BCE4067B-9B40-4316-9235-6A1EEAD55622}

For previous versions of ActivClient, refer to the corresponding administration guide.

For more information about SCCM, see 6.3 Deploying using Microsoft System Center Configuration Manager on page 87.

8.2 Uninstall the ActivClient Administrative Templates

ActivClient, when uninstalled, does not remove the policy settings. You must manually delete these settings.

8.2.1 Delete the Settings for a Local User

1. Launch the Group Editor (*gpedit.msc*) and reset all the ActivClient policy settings to **Not configured**.
2. Apply the changes.
3. Run the `gpupdate /force` command to propagate the changes.
4. Remove the ActivClient administrative templates:
   - Remove the ActivClient *.admx* template files from **C:\Windows\PolicyDefinitions**.
   - Remove the ActivClient *.adml* template files from **C:\Windows\PolicyDefinitions\en-US**.

8.2.2 Delete the Settings for a Domain User

Group policies defined at the domain level can be edited, updated, unlinked or removed through the Group Policy Management Console.

If you unlink or remove a group policy, the policy is no longer be applied and all the associated registry keys are deleted from the client workstations in the domain at the next GPO update.

In order to force propagation and application of the GPO changes, run the `gpupdate /force` command on each domain client machine where the changes have to be applied.

For further information, go to http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx.

8.3 Restore Microsoft Settings

During ActivClient installation, ActivClient configures some Microsoft Windows policies to provide a full smart card experience (see section 4.16 Microsoft Policies Relevant to ActivClient on page 67).

During ActivClient uninstallation, these Microsoft policies are not updated. You can leave them as is as they have no impact if you do not use smart cards anymore, or they can also be relevant to other smart card deployments. Alternatively, you might want to disable these policies.

1. Launch the Microsoft Group Policy Editor (*gpedit.msc*) and reset the following settings to **Not configured**:
   - Card removal – Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**Interactive logon : Smart card removal behavior**
   - Certificate registration – Computer Configuration\Administrative Templates\Windows Components\Smart Card**Turn on certificate propagation from smart card**
   - Card Auto Registration – Computer Configuration\Administrative Templates\Windows Components\Smart Card**Turn on Smart Card Plug and Play service**
2. To propagate and apply the policy changes, run the `gpupdate /force` command on each domain client machine.
3. You can also remove the ActivClient template files:
   - Remove the ActivClient *.admx* template files from **C:\Windows\PolicyDefinitions**.
   - Remove the ActivClient *.adml* template files from **C:\Windows\PolicyDefinitions\en-US**.

9.0 Outlook Usability Enhancements

This section 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:
- Configure Outlook security profile on card insertion
- Publish to GAL on card insertion
- Incoming e-mail management:
- Automatically add sender's certificates to Outlook Contacts (Auto-Contact)
- Automatically decrypt encrypted e-mails (Auto-Decrypt)

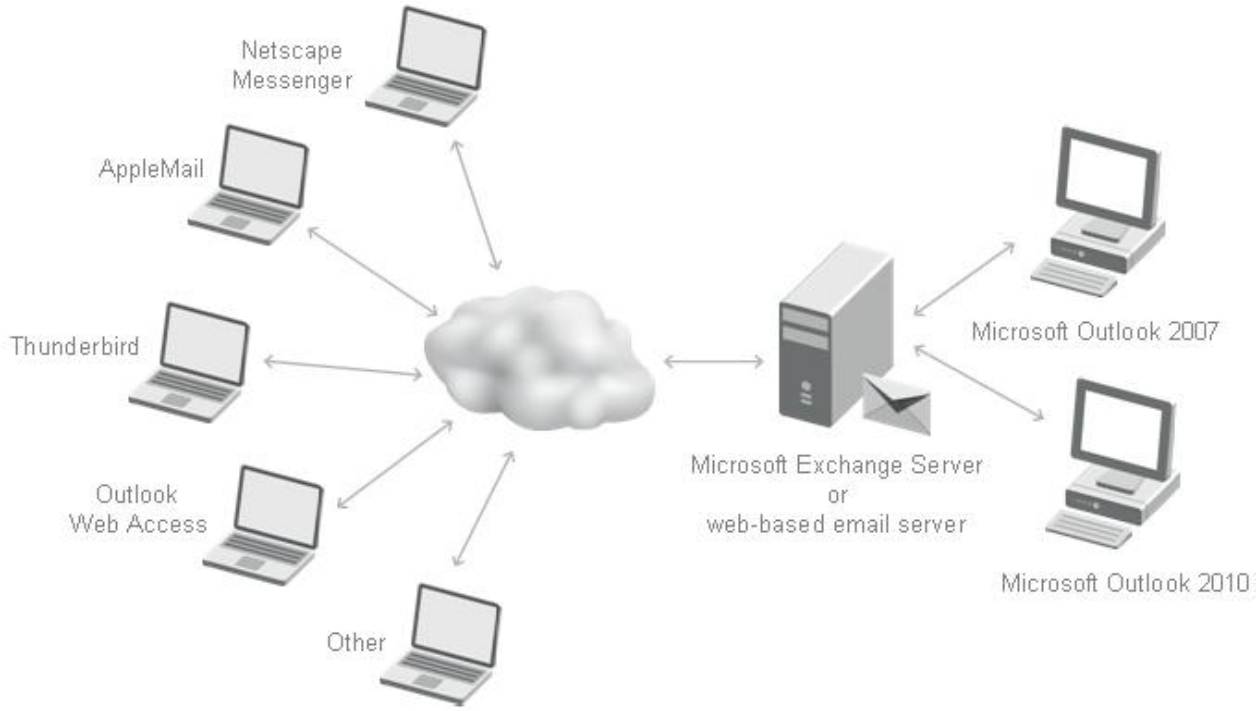
9.1 Environment

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

9.1.1 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 section 9.1.2 Microsoft Outlook Email Clients on page 125.
- Microsoft Outlook Exchange Server (for the complete list of supported versions, see section 9.1.3 Microsoft Exchange Server on page 126).
- Emails from and to any email client on any platform (for examples, see section 9.1.4 Emails From and To Any Email Client on Any Platform on page 126).



Notes:

- Some ActivClient features might not be supported if Microsoft Outlook is configured in the Internet mode.
- Microsoft Outlook Express (any version) and Windows Mail are not supported.

9.1.2 Microsoft Outlook Email Clients

Supported versions of Microsoft Outlook are:

- Microsoft Outlook 2007 SP3 (Office 2007)
- Microsoft Outlook 2010 SP2 (Office 2010)
- Microsoft Outlook 2013 SP1 (Office 2013)
- Microsoft Outlook 2016

Email account configurations can be either:

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

9.1.3 Microsoft Exchange Server

Supported versions of Microsoft Exchange Server are:

- Exchange Server 2007 SP3
- Exchange Server 2010 SP3
- Exchange Server 2013 SP1
- Exchange Server 2016

9.1.4 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 Server
- Outlook Express
- Windows Mail
- Netscape Messenger
- Apple Mail
- Microsoft Entourage (on MacOS)
- Mozilla Thunderbird

9.2 Outlook Security Profile Configuration

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

- 4.5.9 Turn off setup email certificates in Microsoft Outlook on card insertion on page 45.
- 4.5.11 Turn on automatic publication of certificates to the Global Address List on page 46.

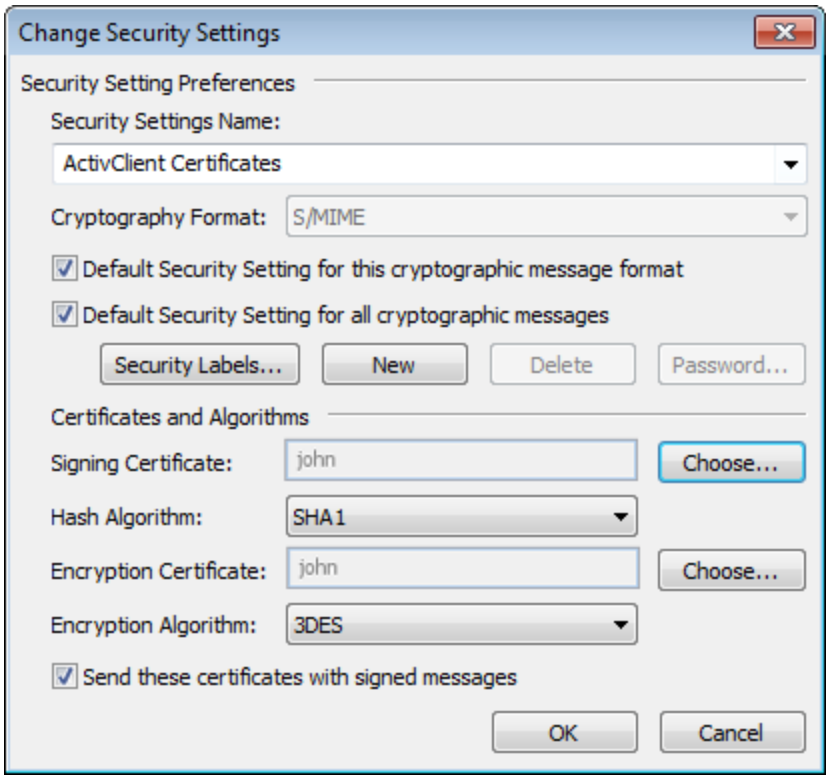
9.2.1 Outlook Security Profile Settings

Note: The following procedure is illustrated using Microsoft Outlook 2010. The steps and interface might vary with newer versions of Microsoft Outlook. Refer to the Microsoft documentation for further information.

1. To view the security settings for Outlook 2010, 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.



The Outlook security profile created by ActivClient defines the:

- Security settings name
- Cryptography format
- Signing certificate
- Hash algorithm
- Encryption certificate
- Encryption algorithm

Other parameters can be defined using Microsoft policies (for example, Add digital signature to outgoing messages).

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

9.2.2 Outlook Security Profile Update

9.2.2.1 Profile Selection and Conditions for Security Profile Update

When *Turn off setup email certificates in Microsoft Outlook on card insertion* is not configured or disabled (default setting), ActivClient updates the profile at card insertion if the following conditions are met:

- Certificate propagation is enabled (Microsoft certificate propagation).
- A default Microsoft Outlook profile is defined, and an Exchange account is set for this profile (for example POP accounts are ignored).).
- A signature certificate on the smart card inserted meets the conditions listed below. If several certificates meet the conditions, the most recent one (Valid From date) is selected:
  - Validity – current date being between 'Valid From' and 'Valid To'.
  - Key usage – the certificate key usage must contain the value 'Digital Signature'.
  - The Intended Key Usage includes CERT_KEY_DIGITAL_SIGNATURE_USAGE for the signature certificate or this is the CAC Signature Certificate or the PIV Digital Signature Key.
- An encryption certificate on the smart card inserted meets the conditions listed below. If several certificates meet the conditions, the most recent one (Valid From date) is selected:
  - Validity – current date being between 'Valid From' and 'Valid To'.
  - Key usage – the certificate key usage must contain the value 'Key Encipherment' or 'Data Encipherment'.

    The Intended Key Usage includes CERT_KEY_ENCIPHERMENT_KEY_USAGE for the encryption certificate or this is the CAC Encryption Certificate or the PIV Key Management Key.

Depending on configuration settings, additional checks are performed on the two selected certificates:

- Email address should be the same as the one configured in the Microsoft Exchange account (this check can be disabled using the setting Allow different email addresses in smart card certificate and Exchange account). The email address is retrieved from the certificate RFC822 Subject alternate name attribute or, if missing, in the E= of the subject and is checked against the Active Directory if online. If not, this check is by passed even if the setting is enabled.
  - If this setting is set to No, the name check is performed:
    - If the email addresses match, ActivClient updates the Outlook profile/publish to GAL.
    - If they do not match, then ActivClient does not update the Outlook profile/does not publish to GAL.
  - If this setting is configured to Yes, the name check is performed:
    - If the email addresses match, ActivClient updates the Outlook profile/publishes to GAL.
    - If they do not match, then ActivClient continues to check if Outlook/the GAL needs to be updated.

      – If no update is needed (that is, the card certificates are already used to configure Outlook/publish to the GAL), then no action is performed.

– If an update is needed, then ActivClient prompts the user by presenting the email addresses configured in Microsoft Exchange and the email address used in the smart card certificate. The user then makes an informed decision on whether to proceed with updating the Outlook profile/publishing to GAL.

This last configuration is only applicable to customers who configure Microsoft Outlook with SuppressNameChecks (http://support.microsoft.com/kb/276597).

- CRL check (if the setting is enabled):
  - If CRL check is enabled and enforced, and if CRL check is not OK (certificate is revoked or on hold, or CRL times out), the certificate is ignored and the operation (automatically configure email certificates in Microsoft Outlook and/or automatically publish certificates to the GAL) is not performed.
  - If CRL check is enabled and not enforced, and if CRL check is not OK certificate is revoked or on hold, or CRL times out), the certificate is accepted and the operation (automatically configure email certificates in Microsoft Outlook and/or automatically publish certificates to the GAL) is performed but the certificate is marked as not CRL valid and an event warning is added in the Microsoft Windows event log.
  - If CRL check is enabled (and enforced or non-enforced) and if CRL check is OK, the certificate is marked as CRL valid.
  - If CRL check is disabled, the operation (automatically configure email certificates in Outlook and/or automatically publish certificates to the GAL) is performed regardless of the CRL check status.

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).
- If an OCSP provider is installed and configured on the Windows client, ActivClient will check the certificate status with OCSP instead of CRL.

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 Microsoft Outlook is running or not, yet Microsoft Outlook needs to be restarted to see the updates in effect.

The Outlook security profile may be updated if new policies are configured (for example, changing the hashing algorithm from SHA-1 to SHA-256), even if certificates are not updated.

Note: The created profile might be altered if the ActivClient setting *Remove certificate from Microsoft 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.

9.2.2.2 Security Profile Updated Values

The values updated by the ActivClient configuration are retrieved either from the smart card (certificates) or from the configured policies (ActivClient policies or Microsoft policies).

The following table lists the configured value for each setting when the profile is created or updated.

Table 5: Security Profile Configured Values

Setting	Value
Security settings name *Default Setting* field	*ActivClient Certificates* (always – not configurable)
Encrypt contents and attachment for outgoing message	Same value as configured in Microsoft Outlook Cryptography Options Encrypt all e-mail messages.
Add digital signature to outgoing message	Same value as configured in Microsoft Outlook Cryptography Options Sign all e-mail messages.
Send clear text signed message when sending signed message	Same value as configured in Microsoft Outlook Cryptography Options Send all signed messages as clear signed messages.
Request S/MIME receipt for all S/MIME signed message	Same value as configured in Microsoft Outlook Cryptography Options Request an S/MIME receipt for all S/MIME signed messages.
Cryptography format	S/MIME (always – not configurable through ActivClient)

Setting	Value
'Default security settings for this cryptographic message format' check box	Checked (always – not configurable through ActivClient)
'Default security settings for all cryptographic message messages' check box	Checked (always – not configurable through ActivClient)
Signing certificate selected	The selected certificate is the most recent certificate (the most recent Valid From date) on the smart card that meets the following conditions: • Validity – current date being between Valid From and Valid To date. • User account – If workstation is online, the certificate email address corresponds to the email address configured for the Microsoft 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 Microsoft Exchange side, the comparison is performed by checking all email addresses defined in the Microsoft Exchange account (prefixed by 'SMTP:' or 'smtp:'). This allows supporting email aliases. If workstation is offline, no email address is checked. • Key usage: the certificate key usage must contain the value *Digital Signature*. • The certificate is valid. The certificate status is verified via CRL checking, only if workstation is online. This CRL check can be configured through an ActivClient policy.
Signing certificate displayed name	Certificate friendly name.
Hash algorithm	Same value as configured in ActivClient Outlook Enhancements setting Hash algorithm configured in Security Profile on card insertion. **Note:** The MD5 algorithm is not supported in Microsoft Outlook 2010. The selected algorithm cannot be updated in the Microsoft Outlook profile. It can only be updated through GPO settings. Default is SHA-1.
Encryption certificate selected	The selected certificate is the most recent certificate (the most recent Valid From date) on the smart card that meets the following conditions:

Setting	Value
	• Validity – current date being between Valid From and Valid To date. • User account – If workstation is online, the certificate email address corresponds to the email address configured for the Microsoft 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 Microsoft Exchange side, the comparison is performed by checking all email addresses defined in the Microsoft Exchange account (prefixed by 'SMTP:' or 'smtp:'). This allows supporting email aliases. If workstation is offline, no email address is checked. • Key usage – the certificate key usage must contain the value *Key Encipherment*. • The certificate is valid. The certificate status is verified via CRL checking, only if workstation is online. This CRL check can be configured through an ActivClient policy.
Encryption certificate displayed name	Certificate friendly name.
Encryption algorithm	Same value as configured in the ActivClient Outlook Enhancements setting Encryption algorithm configured in Security Profile on card insertion. The selected algorithm cannot be updated in the Microsoft Outlook profile. It can only be updated through GPO settings. Default 3DES.
'Send these certificates with signed message' check box	Checked (always – not configurable)

For further information about the Microsoft policies that control these settings, see section 4.16 Microsoft Policies Relevant to ActivClient on page 67.

9.2.3 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 Microsoft Exchange users using Microsoft 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 in the Trust Center (Outlook 2007).

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.

9.2.3.1 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).

9.2.3.2 Configuration

The setting Turn on automatic publication of certificates to the Global Address List is applicable only if the setting *Turn off setup email certificates in Outlook on card insertion* is not configured or disabled (the setting is disabled by default).

9.2.3.3 Workflow

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

If the smart card content is appropriate, the Microsoft Outlook security profile is updated (see section 9.2.2.2 Security Profile Updated Values on page 130), 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.
- 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 might 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 section 9.2.4 Audit on page 135.

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; refer to the Microsoft documentation for details.

9.2.3.4 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.

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

- 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.

9.2.4 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, it is recommended that you filter the audited information using the Event Viewer filters.

By default, the ActivClient auditing function is enabled. To disable the option, see section 4.5.4 Disable audit for Microsoft Outlook security profile creation and Publish to GAL on page 43.

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

- Logged in the HID Global 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 Table 6: Audited Event ID Codes on page 136.
- 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, go to 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, refer to the Microsoft documentation.

Table 6: Audited Event ID Codes

Event 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 applicable update
514	Warning	Publish to GAL	No applicable update
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

Event ID	Event Type	Category	Description
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 CAPI error code

9.3 Auto-Contact

When the *Turn off automatic sender's certificates addition to Outlook contacts* setting is not configured or disabled (see page 45), ActivClient enables saving a contact certificate to a Microsoft 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 the *Outlook Auto-Contact Destination Folder* (see page 45).

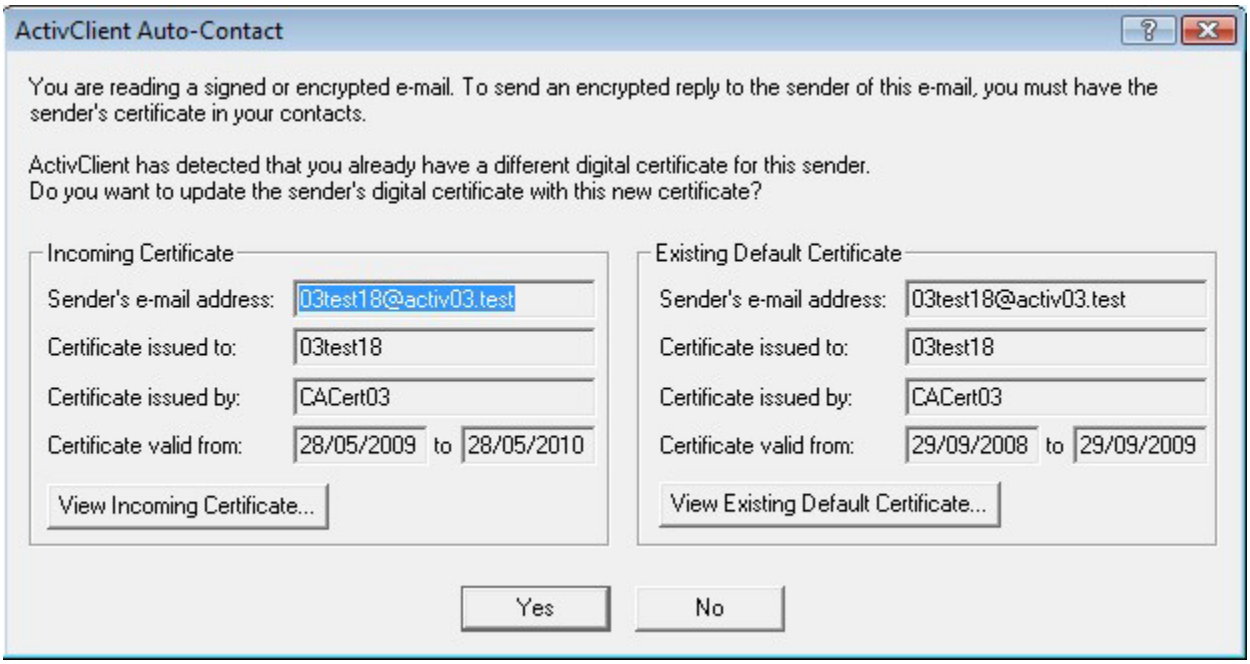
Depending on the scenario, ActivClient asks the user to confirm the operation:

- **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.

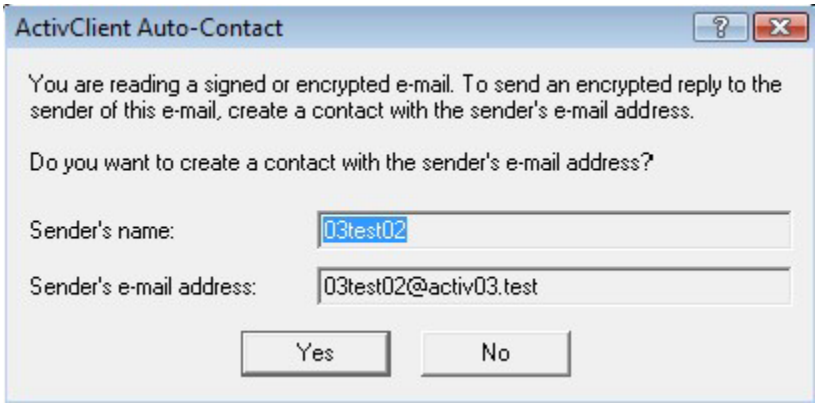
- **Scenario 2** – If a Contact already exists in the Contacts folder with the same email address but has a default certificate that is different from the received email encryption certificate, the following window is displayed.



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

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.

9.4 Auto-Decrypt

When the *Turn on automatic decryption of encrypted emails* is enabled (see page 45), 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.

10.0 PIN Caching Service

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.

Section 3.0 Defining the ActivClient Policies provides a list of the policies relevant to PIN Cache configuration (starting on page 46). This section provides more in-depth information about this ActivClient component.

10.1 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 (such as, 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.

The following sections provide more detailed information on the PIN Caching Service policy, compared to the corresponding section 4.6 PIN Caching on page 46.

10.2 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).

10.2.1 Policy Name: Allow per-process PIN caching

Description: Defines if the PIN cache is shared between Microsoft Windows processes.

If this setting is not configured or disabled, then all processes running in the same session share the same PIN cache.

10.2.2 Example 1: Per Process Mode

The following steps are an example of processes running on a workstation:

1. Set the policy to **Enabled**.
2. Open Microsoft Outlook with your smart card inserted.
3. Send a signed email, and enter your PIN when prompted.
4. Send a second signed email. You are not prompted for the PIN because it is already cached.
5. Close and re-open Microsoft Outlook.
6. 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 Microsoft Outlook and the other was Internet Explorer (running simultaneously), or if two Internet Explorer processes were running simultaneously.

10.2.3 Example 2: Per Session Mode

The following steps are an example of processes running on a workstation:

1. Set the policy to **Disabled**.
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 and re-open Microsoft Outlook.
6. Send a signed email. You are not prompted for the PIN because it is cached and shared between processes.

10.2.4 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 the policy to **Disabled**.
2. Open Microsoft Outlook on the workstation, with your smart card inserted.
3. Send a signed email, and enter your PIN when prompted.
4. Send a second signed email. You are not prompted for the PIN because it is already cached.
5. Close Microsoft 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.

10.3 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: The timer is reset each time a PIN protected operation occurs.

10.3.1 Policy Name: Number of minutes before PIN cache is cleared

Description: Defines the number of minutes before the PIN cache is cleared. The default value is 15.

If this value is set to 9999, the PIN cache timeout is infinite. This means that PIN cache is cleared at log off or shutdown or session disconnect or card removal or workstation lock (depending on the Disable PIN cache clearance on workstation lock setting)

Possible Values:

- Not Configured
- Enabled – displays the default value, 15, and can be updated
- Disabled

10.3.2 Exceptions

- Number of minutes before PIN cache is cleared set to 0

  When the policy 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.

- Number of minutes before PIN cache is cleared set to 9999

  When the policy is set to 9999, the maximum PIN inactivity period is considered infinite. In this case, no timer is maintained: the PIN cache is cleared at workstation lock, log off, shutdown, session disconnect, card removal and explicit card logout.

10.3.3 Example: PIN Cache Timeout of One Hour

1. Set the policy to **60**.
2. Open Outlook with your smart card inserted.
3. Send a signed email, and enter your PIN when prompted.
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.

10.4 PIN Caching for "PIN Always" Private Keys

Some smart cards are configured to enforce a PIN prompt for every key operation; the most common example is the Personal Identity Verification (PIV) card, where the Signature Key is configured for "PIN Always", as defined in FIPS 201 and NIST Special Publication 800-73.

The intent of the PIN Always policy is to provide non-repudiation services. To improve ease of use while preserving the need for an explicit user action, required to meet the non-repudiation requirements, ActivClient includes an option where the user can ‘confirm’ the operation, without needing to re-enter their PIN code if the PIN has already been provided previously and is present in the middleware cache.

This behavior complies with NISTIR 7863.

10.4.1 Policy Name: Enable PIN caching for "PIN Always" private keys

Description: Defines if the PIN cache is applicable for operations with a private key configured for "PIN Always".

If enabled, a confirmation dialog guarantees non-repudiation for these operations.

If this setting is not configured or disabled, then PIN entry is required for all operations with a private key configured for "PIN Always".

Note: If this setting is enabled, per-process PIN caching is recommended for improved security, and is required for FIPS 201 compliance.

Organizations can select the middleware behavior for private keys configured for PIN Always based on their own security and usability policies. You can configure ActivClient to display either a:

- PIN prompt (default policy – same behavior as with ActivClient 6.x and 7.0 earlier than 7.0.0.51).
- Confirmation dialog (new option available with ActivClient 7.0.0.51 and later).

  When the "You are about to digitally sign a file or message. Please confirm that you want to use your smart card for this operation." message is displayed, users can either click:

  - Confirm to proceed with the operation.
  - Cancel to end the operation.

This behavior can be combined with other PIN cache policies, and applies to all applications that use the PIV Digital Signature key, such as:

- Microsoft Outlook
- Outlook Web Access / Outlook Web App (a Microsoft Exchange feature, using Internet Explorer as interface)
- IBM Lotus Notes
- Mozilla Thunderbird
- Adobe Acrobat
- And many more off-the-shelf or custom applications

10.4.2 Example

The following example uses a configuration with:

- PIN cache set to 'per process'
- PIN cache timeout set to 15 minutes
- PIN caching for "PIN Always" private keys set to *enabled*

1. Insert your smart card into the reader and open Microsoft Outlook.
2. Compose and digitally sign an email, enter your PIN when prompted, and then send the email.
3. Five (5) minutes later, send a second signed email.

   The signature confirmation dialog displays.

   Confirm the operation.

   ActivClient sends the previously cached PIN code to the smart card.
4. Five (5) minutes later, you receive and attempt to open an encrypted email.

   Outlook decrypts it without prompting for the PIN, because the PIN is cached, and the Key Management key can access the PIN cache.

   Twenty (20) minutes later, you receive and attempt to open another encrypted email.

   As the PIN cache timeout has been reached, Outlook prompts you for the PIN in order to decrypt it.
5. Enter the correct PIN to decrypt the email.
6. Five (5) minutes later, open Adobe Acrobat and sign a document.

   You are prompted for the PIN again because it is a different Microsoft Windows process.
7. Five (5) minutes later, in the same Adobe Acrobat session, sign another document.

   The signature confirmation dialog displays.

   Confirm the operation.

   ActivClient sends the previously cached PIN code to the smart card.

10.5 PIN Cache Clearance on Workstation Lock

10.5.1 Policy Name: Disable PIN cache clearance on workstation lock

Description: Disables the clearance of the PIN cache when the workstation is locked.

If this setting is not configured or disabled, then the PIN is cleared from the cache when the workstation is locked.

Note: Disabling PIN cache clearance when the workstation is locked lowers the smart card deployment security.

ActivClient default behavior (when this policy is not configured or disabled) is to clear the PIN from the PIN cache when the workstation is locked, in order to guarantee the highest level of security. This requires users to enter their PIN again when they unlock the workstation.

When this policy is enabled, then the PIN is maintained in the PIN cache, when the workstation is locked and the card is maintained inserted in the card reader (the PIN is cleared from the cache if the card is removed from the reader).

The benefit of this approach is that when users unlock the screen, they are not required to enter their PIN again – if their card has remained inserted in the reader during the period the workstation was locked. This provides improved usability.

However, this approach lowers the security, as any user could unlock the screen and gain access to the user's desktop, if a user locked his screen and forgot to remove the card.

It is recommended that you consider the security implications before enabling this policy.

11.0 Auto-Update with ActivID CMS

The purpose of ActivClient Smart Card Auto-Update feature is to automate updating the smart card content, for cards managed by ActivID Credential 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 ActivID CMS self-help portal.

11.1 Overview

ActivClient Smart Card Auto-Update is a component providing a high-level of integration with ActivID CMS version 4.2 and later. When card updates are available in ActivID CMS (for example, a replacement certificate for a soon-to-expire certificate, or the addition of new certificates on the card), administrators would typically need to inform users to access ActivID 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 ActivID 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 ActivID 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 ActivID CMS to check for card updates without waiting for the recurrent (weekly) automatic check. This capability is mostly designed for troubleshooting purposes.

11.2 Configuration

If you intend to use the card auto-update feature:

1. Configure ActivID CMS to enable the card auto-update (refer to the ActivID 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 sections 11.3 Client Card Auto-Update Configuration on page 148 and 11.4 ActivID CMS Connection Configuration on page 151.
4. Configure the user workstations to support ActivID CMS self-help portal (My Digital ID Card). Refer to the ActivID CMS documentation for details for the following steps:
   a. Install the ActivID CMS root certificates on the user workstations.

b. Install the ActivID 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 ActivID 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 might 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).

The following sections provide detailed information on the Smart Card Auto Update policy.

For additional information, see section 4.10 Smart Card Auto-Update on page 51.

Prerequisite

The Smart Card Auto-Update is only available if 4.9.2 Disable smart card discovery information caching on page 51 is not configured or disabled.

(That is, if smart card discovery information caching is enabled.)

11.3 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 section 4.13.6 Hide Check for Card Update menu on page 60).

However, card auto-update is operational only after you configure the ActivID CMS connection information with the data specific to your environment.

11.3.1 Policy Name: Enable Card Auto-Update

Description: Defines if ActivClient will automatically check if inserted smart cards can be updated with card content updates available in the ActivID CMS. The smart card update process starts if updates are available.

If this card auto-update is enabled, then the ActivID CMS server URL must be specified for ActivClient to perform the Auto-update check.

Possible Values:

- Not Configured
- Enabled
- Disabled

11.3.2 Policy Name: CMS Server URL

Description: Defines the connection URL for the ActivID CMS server (see the ActivID CMS documentation). The port number must be included in the URL.

Example: http://cms.mycompany.com:89898

If this setting is not configured or disabled, then no automatic update check is performed on card insertion.

Possible Values:

- Not Configured
- Enabled – enter the ActivID CMS server URL
- Disabled

The ActivClient card auto-update feature contacts ActivID 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 ActivID CMS by a few minutes. Also, to avoid overloading ActivID CMS with too many simultaneous connections, ActivClient automatically spreads the load: ActivClient will contact ActivID 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 ActivID CMS between 0 and 120 minutes after Windows Logon.

It is recommended that you select 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 ActivID 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.

11.3.3 Policy Name: Maximum delay for card update check after Windows Logon

Description: Defines how long (in minutes) ActivClient waits after Microsoft Windows logon before it contacts ActivID CMS to determine if smart card updates are available.

To spread the requests received by ActivID CMS, this delay is a random value – between 0 and the maximum delay defined in this setting (in minutes).

Recommended values are between 5 and 120.

If this setting is not configured, then the delay is set to 120 minutes.

Possible Values:

- Not Configured

- Enabled – displays the default value, 120, and can be updated
- Disabled

Note: This policy also includes the case of a card used for Windows screen unlock.

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 ActivID 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 ActivID CMS between 0 and five minutes after card insertion.

It is recommended that you select 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 ActivID 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.

11.3.4 Policy Name: Maximum delay for card update check after card insertion

Description: Defines how long (in minutes) ActivClient waits after card insertion before it contacts ActivID CMS to determine if smart card updates are available. This delay is a random value – between 0 and the maximum delay defined in this setting (in minutes).

Recommended values are between 1 and 10.

If this setting is not configured, then the delay is set to 5 minutes.

Possible Values:

- Not Configured
- Enabled – displays the default value, 5, and can be updated
- Disabled

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 ActivID 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 ActivID CMS is not available, or if the user cancels the card update request, then ActivClient will contact ActivID CMS again at the next card insertion (after the usual delay).

- If ActivClient manages to contact ActivID 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 ActivID 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 ActivID 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).

11.3.5 Policy Name: Frequency of update (in days)

Description: Defines the interval (in days) between checks for smart card updates.

If this setting is not configured, then the update frequency is set to 7 days.

Possible Values:
- Not Configured
- Enabled – displays the default value, 7, and can be updated
- Disabled

11.4 ActivID 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.

The URL is defined in the Enable Card Auto-Update policy (see page 148).

The following policies configure additional ActivID CMS connection parameters. The default values apply to most configurations. For further information, see the ActivID CMS technical documentation.

If ActivID 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.

11.4.1 Policy Name: CMS Synchronization Manager timeout

Description: Defines the maximum time (in seconds) allocated to check with ActivID CMS if smart card updates are available.

If this setting is not configured, then the timeout is set to 5 seconds.

A value of zero (0) means there is no client timeout, in which case the client timeout is determined by the server settings.

Possible Values:
- Not Configured

- Enabled – displays the default value, 5, and can be updated
- Disabled

11.4.2 Policy Name: CMS Synchronization Manager retry

Description: Defines the maximum number of attempts to connect to the CMS Synchronization Manager after timeout.

If this setting is not configured, the number of attempts is set to 2.

Possible Values:

- Not Configured
- Enabled – displays the default value, 2, and can be updated
- Disabled

If ActivClient manages to contact ActivID CMS, and identifies that a card update request is available, ActivClient opens a window connecting to ActivID 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 performed. There is no repeated attempt performed that would disrupt the user. The next attempt will be performed at the next card insertion.

11.4.3 Policy Name: CMS MDIDC timeout

Description: Defines the maximum time (in seconds) allocated to perform a smart card update using CMS My Digital ID Card. When this timeout is reached, the process running the browser is terminated.

If this setting is not configured, then the timeout is set to 600 seconds.

Possible Values:

- Not Configured
- Enabled – displays the default value, 600, and can be updated
- Disabled

11.5 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 ActivID 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.

12.0 Security Guidelines

The section provides guidelines for ensuring the secure deployment of ActivClient.

It is limited to recommendations for securing the environment assets that have an impact on the ActivClient product and environment. Standard best IT security practices should also be considered as part of a secure deployment.

The section is organized by recommendations.

12.1 FIPS Compliance

This section applies to customers who want to achieve FIPS compliance for their Microsoft Windows environments.

12.1.1 Microsoft CNG Versions

ActivClient relies on Microsoft Cryptographic Next Generation (CNG) for all its internal cryptographic needs. The Microsoft CNG library is a FIPS 140-2 Level 1 approved cryptographic library. Detailed references to Microsoft FIPS 140 evaluation can be found at http://technet.microsoft.com/en-us/library/cc750357.aspx.

Per Microsoft Security Policy, an approved mode of operations of the library requires verification that the correct version of a number of OS components be verified to insure the use of the module under the approved FIPS policy, per http://technet.microsoft.com/en-us/library/cc750357.aspx:

"Systems Integrators must ensure that all cryptographic modules installed are, in fact, FIPS 140 validated. This can be accomplished by cross-checking the version number of the installed library with the list of validated binaries."

ActivClient does not verify the versions of the cryptographic modules installed on the platform; it is the customer's responsibility to make sure that the versions are correct. However, to ease configuration troubleshooting, the ActivClient diagnostic includes the version of the relevant modules. This information can be used to verify that the proper versions of the modules are installed on the end users' platforms.

It is recommended that customers regularly check for availability of newer FIPS approved CNG versions from NIST or Microsoft's web sites.

- For a list of currently validated FIPS 140 modules, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.
- For more information about FIPS 140 and NIST, go to the NIST web site at http://csrc.nist.gov/groups/STM/cmvp/index.html.

12.1.2 FIPS Policy Flag

The Windows operating system supports a security policy (System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing) which enforces various Microsoft applications to operate in FIPS mode.

The ActivClient installation or administrative template does not act on this Microsoft policy. It is the customer's responsibility to make sure that this policy is enabled to achieve FIPS compliance.

ActivClient has been tested for compliance with supported Microsoft applications with this flag set.

It has to be noted that:

- Neither the Operating System nor ActivClient modify their behavior when this flag is configured; it is the customer's responsibility to verify that proper (that is, FIPS-compliant) versions of the module are installed, according to the previous section. It is also the responsibility of the calling applications to make sure that only FIPS approved algorithms and key sizes are used.
- Setting the FIPS flag might impact the use of some Microsoft products and components (see http://technet.microsoft.com/en-us/library/cc750357.aspx (Effects of Setting FIPS policy flag) and knowledge base http://support.microsoft.com/kb/811833). It is therefore strongly recommended that you make sure there is no functional impact on the ActivClient-enabled applications deployed in the organization.

It is also recommended that you refer to the following Microsoft article on the effect of setting the FIPS policy flag – https://blogs.technet.microsoft.com/secguide/2014/04/07/why-were-not-recommending-fips-mode-anymore/

12.1.3 ActivClient Compatibility with FIPS Approved Cryptographic Algorithms, Modes, and Key Sizes

ActivClient only relies on FIPS approved cryptographic algorithms, modes and keys size for its internal use. This encompasses:

- Use of RSA, AES, 3DES, SHA approved algorithms.
- Use of approved key generation for AES and 3DES keys.
- Use of approved random generator.

12.1.4 FIPS Compliance for Firefox

Firefox can be configured so that it only uses FIPS approved algorithms and cryptographic modules. Refer to this link for detailed configuration steps required, http://support.mozilla.com/en-US/kb/Configuring%20Firefox%20for%20FIPS%20140-2

12.1.5 FIPS Compliance for PKCS#11

ActivClient supports new mechanisms through its PKCS#11 library, permitting custom applications to use FIPS approved algorithms (AES, SHA-2) in FIPS approved mode of operation.

Internally the ActivClient PKCS#11 library relies on the CNG FIPS approved library for implementation. It is therefore important that proper conditions of use of the CNG library as defined in section 12.1.1 Microsoft CNG Versions on page 154 are also met when custom applications integrate with the ActivClient PKCS#11 library and use the new mechanisms.

12.1.6 FIPS Compliance for Terminal Services

ActivClient supports remote sessions in Microsoft Remote Desktop Service and Citrix XenApp environments.

Due to the smart card redirection supported by the RDP and ICA protocols, all card interactions established by ActivClient installed on the server are redirected to the client. It is therefore very important that you protect the RDP connection properly to guarantee that card commands and responses cannot be intercepted or eavesdropped by an attacker.

12.1.6.1 Microsoft Remote Desktop Sessions

Starting with Windows Vista, it is possible to configure Windows Terminal Services to leverage the TLS protocol, including host certificate authentication and usage of FIPS approved cryptography. This configuration is recommended over the standard RPC encryption method, which is considered weaker and does not provide host authentication.

This requires configuration of the RDP connection to use the following RDP group policy settings:

- Encryption Level to FIPS compliant
- Require Secure RPC Communication to Enabled
- Require Use Of Specific Security Layer For Remote (RDP) Connections to SSL (TLS 1.0)

In this configuration, the RDP connection is protected by the TLS session, the host is authenticated and uses only FIPS approved cipher suites.

Note: This configuration requires RDP Client v6.0 or later.

In addition, RDP connections can be configured with Network Level authentication. In this configuration, user authentication completes before the RDP session is established, reducing resource consumption and risk of denial of service.

Reference to RDP security configuration can be found in:

- Server authentication and encryption levels – http://technet.microsoft.com/en-us/library/cc770833.aspx
- Network level authentication – http://technet.microsoft.com/en-us/library/cc732713.aspx

12.1.6.2 Citrix XenApp Sessions

Similarly to Microsoft remote desktop sessions, Citrix also supports the use of the TLS 1.0 protocol to protect access to a Citrix XenApp server through the ICA protocol.

Citrix recommends using the SSL/TLS protocol over the SecureICA protocol, especially when the RDP server is configured to be accessible from outside LAN areas.

SSL is supported through different Citrix components, depending on the deployment requirements and topology:

- Through SSL gateway

- Through SSL relay

Citrix also enables configuring the cipher suite; you can select it as a subset of FIPS approved cipher suites.

Internally, Citrix relies on Microsoft CAPI to implement cryptography. The Citrix products do not provide a specific handling of the FIPS policy flag. It is therefore important that proper conditions of use of the CAPI library are met when Citrix products are used.

Refer to Citrix documentation for further information http://docs.citrix.com/.

12.2 SHA-2 Compliance

As part of a security improvement, organizations are transitioning from the SHA-1 hashing algorithm to a SHA-2 (usually SHA-256) hashing algorithm. This change is usually driven by compliance requirements:

- NIST SP 800-78 requires that the content of a PIV card (digital certificates, CHUID, biometric information) is signed with the SHA-256 hashing algorithm.
- NIST SP 800-131 provides guidance specifying that SHA-2 (SHA-224, SHA-256, SHA-384 or SHA-512) should be used as a hashing algorithm for digital signature generation and verification (SHA-1 remains acceptable for non-digital signature generation operations).

This change has a big impact on many applications. This section describes the impact of these changes on ActivClient and various applications. Support for SHA-2 for other use cases (non-digital signature operations) is not covered in this section.

12.2.1 Card Content Signed with SHA-2

ActivClient supports smart cards whose content (digital certificates, CHUID, biometric information) is signed with a SHA-2 hashing algorithm.

This change might have an impact on some applications, as indicated in the table below.

Note: The table focuses on the ActivClient 7-supported environments (Windows Vista and later).

Service	Product and versions	Notes
Windows PKI Logon	• Supported Clients – Windows Vista and later • Supported Servers – Windows Server 2003 and later	Windows Server 2003 requires two Microsoft hot fixes not available on Windows Update – KB 938397 and 968730
Remote access	Windows, Check Point, Cisco, Juniper, etc.	

Service	Product and versions	Notes
	Check with your vendor	
Secure web access	• Supported browsers – Microsoft Internet Explorer 7 and later, Microsoft Edge, Firefox 3.0 and later, Google Chrome 11 and later. Browsers have limited impact on SHA-2 certificates. • Supported server – IIS 6 and later, Apache 2.2 and later Check with your vendor for other web servers	IIS 6 on Windows Server 2003 requires two Microsoft hot fixes not available on Windows Update – KB 938397 and 968730.
Secure email	Supported applications: • Microsoft Outlook 2003 and later, • Outlook Web Access (with Exchange 2003 and later) • Mozilla Thunderbird	Email signature is configured for SHA-1. See next section for SHA-2 configuration.
Document signing	Supported applications: • Office 2003 and later (e.g. Word, Excel) • Adobe Acrobat Professional 9 and later • Windows XPS Viewer	Document signature is configured for SHA-1. See next section for SHA-2 configuration
Document encryption	Supported applications: • Windows EFS on Windows Vista and later • BitLocker To Go on Windows 7 and later	

12.2.2 Using SHA-2 for Digital Signature Operations

ActivClient includes several middleware libraries that enable applications to use SHA-2 for digital signature operations:

- A Mini Driver, required to support SHA-2 for digital signature operations with the latest Microsoft applications.
- A PKCS#11 library v2.2, this latest version is required to support SHA-2.

The fact that ActivClient middleware exposes some SHA-2 services to applications is usually not enough. Applications usually have to be updated as well in order to support SHA-2, as software vendors have started supporting this algorithm very recently. The table below provides information available by HID Global at the time of publication. It is recommended that you check with your software provider for the latest compatibility information.

Note: The table focuses on the ActivClient 7-supported environments (Windows Vista and later).

Service	Product and versions	Notes
Email signature	Supported applications: • Microsoft Outlook 2007 and later with Exchange 2003 and later • Outlook Web Access with Exchange 2007 and later	Outlook information: • Requires Windows Vista or later. • Sender and recipient both need to comply with these Windows, Outlook and Exchange system requirements (otherwise, they cannot read the SHA-256 signed email). • You can use an ActivClient policy to configure SHA-2 as the default hashing algorithm (see section 12.2 SHA-2 Compliance on page 157). Outlook Web Access information: • Requires Windows Vista or later. • Sender and recipient both need to comply with these Windows, Outlook and Exchange system requirements (otherwise, they cannot read the SHA-256 signed email). • Exchange requires a specific registry-based configuration. See details at http://technet.microsoft.com/en-us/library/bb738151(EXCHG.80).aspx, set the *S/MIME Default Signing Algorithm* to SHA 256. **Note:** Mozilla Thunderbird does not support for SHA-2 in S/MIME at this point.
Document signature	Supported applications: • Office 2010 and later (e.g. Word, Excel) • Adobe Acrobat Professional 9.1 and later	Office information: • Requires a specific policy configuration: *Select digital signature hashing algorithm*. See http://technet.microsoft.com/en-us/library/cc545900.aspx for details.

Service	Product and versions	Notes
		Acrobat information: • Requires a specific policy configuration. See details at http://learn.adobe.com/wiki/download/attachments/52658564/acrobat_reader_security_9x.pdf?version=1 (pages 16 and 124). **Note:** The Windows 7 XPS Viewer does not support SHA 256 at this point.

12.3 PIN Policies

ActivClient can accommodate different PIN policies:

- To meet FIPS security objectives (1/1,000,000 probability of detection) it is recommended to use a minimum PIN length of 6 Digits.
- For CAC and PIV cards, ActivClient enforces that the PIN length is 6 to 8 digit, as specified in the relevant standards.

12.4 Log Handling

ActivClient provides diagnostics and troubleshooting capabilities. Through ActivClient utilities, it is possible to collect ActivClient logs so that they are subsequently sent to a remote IT department or HID Global support for diagnostics and troubleshooting.

ActivClient logs do not contain any sensitive data or personally identifiable information according to HID Global internal security policies.

By default, ActivClient logs are not signed or encrypted. As such, as an additional precautionary measure, it is recommended that you protect ActivClient logs for confidentiality and integrity during transport to a remote IT group.

Usage of such capabilities as signed and encrypted email or secure FTP shall be used to exchange ActivClient log files with a remote IT department or the HID Global support organization.

12.5 ActivClient Policies

ActivClient includes policies that have bearing on the security of the solution. For example, the choice of PIN caching policies or the choice of the S/MIME cryptographic algorithms.

By default, ActivClient relies on Microsoft Group Policy mechanisms for enforcement of these policies:

- By leveraging group policy push mechanisms, it is possible to make sure that ActivClient configuration is always up to date and automatically configured across all machines and / or users (pushed at logon and regular interval).
- Write/modify access to the policy is a privileged operation reserved to administrators. As a consequence, end users cannot tamper with policies without the corresponding Windows privileges.

ActivClient recommends leveraging the group policy infrastructure to centrally manage the security of the solution configuration according to Microsoft best practices: http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx

12.6 Code Integrity

According to industry best practices, all ActivClient components are digitally signed (installer, executables, libraries). The signature relies on Authenticode technology from Microsoft.

The fact that all ActivClient components are signed permits a deployment to leverage the Microsoft Software Restriction Policies (http://technet.microsoft.com/en-us/library/cc507878.aspx) for Windows Vista and its successor AppLocker (http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx) for Microsoft Windows 7 and later.

These technologies enable enforcing that only approved software is installed on computers:

- It enables to define a collection of rules for enforcing only certain software to run on the machine.
- The rules can be based on: trust of code signature, hash of files or file path location.
- Rules can be applied to executables (.exe), Windows Installer files (*.msi* and *.msp*), scripts (*.bat, .cmd, .js, .ps1*, and *.vbs*), and DLLs (*.dll* and *.ocx*)
- Rules can then be assigned to users or group of users.
- Rules can be denied or accepted. Rules can have exceptions.
- Rules can be managed and pushed centrally via GPO mechanisms.

Of particular interest is the possibility to define publisher condition rules. These conditions are the most secure ones, and permit to define rules for files that are digitally signed. Additional conditions can be added including: publisher, product name, files version and name. This type of rules can be defined for all ActivClient components.

It is recommended that you leverage these technologies to make sure that only genuine ActivClient signed components are deployed on end user machines.

12.7 Hardening Desktop Security

ActivClient is compliant with the United States Federal Desktop Core Configuration (FDCC) and its successor USGC (United States Government Configuration Baseline):

- NIST provides Mandatory FDCC SCAP Content checklist for Windows XP, Windows Vista and Internet Explorer 7. However per FAQ, it is possible to use other security checklists from other sources. With the following priorities: NIST, NSA or DISA, Vendor-Provided when available.

- FDCC has now been replaced by USGCB. Windows 7 and Internet Explorer 8 are covered by USGCB. Per FAQ, FDCC Mandatory content shall still be used when available for a given platform or product.
- Outlook 2007 has a DISA checklist. No checklist exists for Outlook 2010 but the Outlook 2007 settings are also relevant to Outlook 2010.
- ActivClient has been tested with the following configurations:
  - Windows Vista – Mandatory OMB checklist.
  - Internet Explorer 7 – Mandatory OMB Checklist (same as Windows Vista)
  - Windows 7 – USGCB checklist.
  - Internet Explorer 8 – USGCB checklist (same as Windows 7)
  - Outlook 2007 – DISA checklist

It is recommended that you apply the above FDCC / USGCB configurations to desktops where ActivClient is installed.

12.8 Additional Recommendations

The following are generic recommendations that will enable to further increase the security of the ActivClient solution and smart card usage:

- Make sure anti-virus and anti-malware software on the users' workstations remain in use, up to date, and that Windows remains up to date on all security patches.
- Consider installing anti-key logger software; select software options that cover all desktop applications.
- Consider configuring Windows to only allow authorized software using technologies such as Software Restriction Policies and AppLocker as described in section 12.6 Code Integrity on page 161.
- Consider locking down the security of the browsers according to industry best practices – for government customers, leveraging FDCC-approved configurations.
- Consider locking down the security of email clients according to best practices, especially to guarantee that attachments are handled securely – for government customers, leveraging FDCC-approved configurations.
- Consider locking down the platform configuration according to best practices – for government customers, leveraging FDCC-approved configurations.
- Train users on social engineering risks, and best practices to handle their PIN and interacting with applications.

13.0 Troubleshooting

The section describes the ActivClient troubleshooting tools and suggested strategies.

13.1 ActivClient Troubleshooting Tools

13.1.1 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 information
- Smart card content information
- List of installed ActivClient files and registry entries

The output of the diagnostics can be viewed on the screen, 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, the Start menu, or the Microsoft Windows 8 'modern' interface.

For more information, see the *ActivID ActivClient for Windows User Guide*.

13.1.2 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 then **Enable Logging**.
- Using an Administrative Policy, configure the **Logging** settings (see section 4.15 Logging on page 65).

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.

13.2 Troubleshooting Strategies

To troubleshoot a problem in ActivClient, follow these basic steps:

- 13.2.1 Check Common Issues and Known Problems on page 164.
- 13.2.2 Analyze Symptoms and Factors on page 164.
- 13.2.3 Isolate the Error Condition and Reproduce the Error on page 164.
- 13.2.4 Ask for Technical Support Resources on page 164.

13.2.1 Check Common Issues and Known Problems

To check common issues and known problems, consider the following:

- Check if your problem was reported in the *ActivClient ReadMe.htm* of your original ActivClient distribution.
- Check the HID Global web site for the latest support information.

13.2.2 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?

13.2.3 Isolate the Error Condition and Reproduce the Error

To isolate and, if possible, reproduce the error, consider the following checklist:

- Run the Advanced Diagnostics wizard, save the result file, and compare the same output with a reference identical working platform.
- Restore the default policy settings and try again.
- Replace the smart card reader.
- Try another smart card.
- Consider removal and reinstallation of ActivClient and try again.

13.2.4 Ask for Technical Support Resources

Run the Advanced Diagnostics Wizard, save the result file, and contact your reseller's technical support organization for analysis.

Appendix A: ActivClient Files and Processes

This appendix describes the files installed and used by ActivClient.

The installed files are listed by ActivClient feature and edition:

- Table 7 lists the files in the ActivClient 7.1 32-bit edition.
- Table 8 lists the files in the ActivClient 7.1 64-bit edition.

Note: Only the installation directory can be customized (by default, it is **%ProgramFiles%\HID Global\ActivClient**).

In the following tables, the directory is represented by *%INSTALLDIR%.*

A.1. ActivClient 7.1 Installed Files (32-bit Edition)

Table 7: ActivClient 7.1 32-bit Edition

Feature	Filename	Location
BSI	acbsi21.dll	%INSTALLDIR%
	JNIBSI21.dll	%INSTALLDIR%
	acbsi21rc.dll	%INSTALLDIR%\Resources
	bsi21classes.jar	%INSTALLDIR%
	bsi21inter.jar	%INSTALLDIR%
PIV	acpivapi.dll	%INSTALLDIR%
	aijnipiv.dll	%INSTALLDIR%
	aijnipiv.jar	%INSTALLDIR%
ActivClient	ac.activclient.gui.pin.dll	%INSTALLDIR%
	ac.activclient.gui.pinrc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.scagent.exe	%INSTALLDIR%
	ac.activclient.gui.scagentrc.dll	%INSTALLDIR%\Resources

Feature	Filename	Location
ActivClient (continued)	ac.activclient.scardactions.exe	%INSTALLDIR%
	ac.activclient.syslog.dll	%INSTALLDIR%
	ac.cardsync.dll	%INSTALLDIR%\Smart Card Auto Update
	ac.cext.dll	%INSTALLDIR%
	ac.crypto.parser.dll	%INSTALLDIR%
	ac.evtbroadcast.dll	%INSTALLDIR%
	ac.evtmon.certstore.dll	%INSTALLDIR%
	ac.evtmon.dll	%INSTALLDIR%
	ac.evtmon.scard.dll	%INSTALLDIR%
	ac.evtmon.sys.dll	%INSTALLDIR%
	ac.evtproc.cachelifecycle.dll	%INSTALLDIR%
	ac.evtproc.certstore.dll	%INSTALLDIR%
	ac.evtproc.dll	%INSTALLDIR%
	ac.evtproc.scard.dll	%INSTALLDIR%
	ac.evtsessionstate.dll	%INSTALLDIR%
	ac.mscredprov.pincache.dll	%INSTALLDIR%
	ac.msgbox.dll	%INSTALLDIR%
	ac.msgboxrc.dll	%INSTALLDIR%\Resources
	ac.scardmon.dll	%INSTALLDIR%
	ac.scmwdiag.dll	%INSTALLDIR%
	ac.scmwdiagrc.dll	%INSTALLDIR%\Resources

Feature	Filename	Location
ActivClient (continued)	ac.sharedstore.dll	%INSTALLDIR%
	ac.sharedstorecl.dll	%INSTALLDIR%
	ac.sharedstoreps.dll	%INSTALLDIR%
	ac.smmw.common.dll	%INSTALLDIR%
	ac.smmw.common.srvctl.dll	%INSTALLDIR%
	ac.smmw.common.srvprov.dll	%INSTALLDIR%
	ac.smmw.mwctl.dll	%INSTALLDIR%
	ac.smmw.srvctl.cache.dll	%INSTALLDIR%
	ac.smmw.srvctl.sm.dll	%INSTALLDIR%
	ac.smmw.srvprov.authcach.dll	%INSTALLDIR%
	ac.smmw.srvprov.datacach.dll	%INSTALLDIR%
	ac.smmw.srvprov.disco.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.cac.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.cacv1.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.cacv2.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.gp.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.piv.ai.ep.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.piv.ai.wrap.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.piv.std.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.v1.common.dll	%INSTALLDIR%

Feature	Filename	Location
ActivClient (continued)	ac.smmw.srvprov.dm.v1.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.v1.standalone.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.v2.common.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.v2.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.v2.standalone.dll	%INSTALLDIR%
	ac.smmw.srvprov.dm.virtualMD.dll	%INSTALLDIR%
	ac.smmw.srvprov.info.javacard.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.piv.ai.262.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.piv.ai.27.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.piv.std.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.soft.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.v1.dll	%INSTALLDIR%
	ac.smmw.srvprov.sm.v2.dll	%INSTALLDIR%
	ac.smmw.srvprov.sma.v1.dll	%INSTALLDIR%
	ac.smmw.srvprov.sma.v3.dll	%INSTALLDIR%
	ac.winext.settings.dll	%INSTALLDIR%
	ac.winext.winrt.dll	%INSTALLDIR%
	AcBcgProu.dll	%INSTALLDIR%
	acCobAPIlrc.dll	%INSTALLDIR%\Resources
	acCobAPIrc.dll	%INSTALLDIR%\Resources

Feature	Filename	Location
ActivClient (continued)	accryptou.dll	%INSTALLDIR%
	acevents.exe	%INSTALLDIR%
	acevtsub.dll	%INSTALLDIR%
	acispcard.dll	%INSTALLDIR%
	aclogu.dll	%INSTALLDIR%
	acomx.dll	%INSTALLDIR%
	acregcrt.exe	%INSTALLDIR%
	ActivClient_EULA.pdf	%INSTALLDIR%\Documentation
	ReleaseNotes.html	%INSTALLDIR%\Documentation
	actsinit.exe	%INSTALLDIR%
	ai.ccm.apiU.dll	%INSTALLDIR%
	ai.interfacesU.dll	%INSTALLDIR%
	ai.localizationU.dll	%INSTALLDIR%
	aiwinextu.dll	%INSTALLDIR%
	Windows_Toast_Info.png	%INSTALLDIR%\Resources
MiniDriver	ac.scapi.scmd.dll	%INSTALLDIR%
	ac.scapi.scmd.x86.cat	%INSTALLDIR%\Smart Card Minidriver
	ac.scapi.scmd.x86.inf	%INSTALLDIR%\Smart Card Minidriver
	ac.scmd.kerbauth.dll	%INSTALLDIR%
Outlook	ac.activclient.oladdin.dll	%INSTALLDIR%
	ac.activclient.oladdin.rc.dll	%INSTALLDIR%\Resources

Feature	Filename	Location
PKCS	acpkcs211.dll	%INSTALLDIR%
MozillaSupport	chrome.manifest	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	install.rdf	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	overlay.js	%INSTALLDIR%\Mozilla Extensions ActivClient PKCS #11 Security Module \chrome\content
	overlay.xul	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module \chrome\content
	manifest.mf	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF
	mozilla.rsa	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF
	mozilla.sf	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF
UserConsole	ac.activclient.gui.usrcons.exe	%INSTALLDIR%
	ac.activclient.gui.usrcons.helper.dll	%INSTALLDIR%
	ac.activclient.gui.usrcons.helperrc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrcons.pdata.dll	%INSTALLDIR%
	ac.activclient.gui.usrcons.pdatarc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrcons.ski.dll	%INSTALLDIR%
	ac.activclient.gui.usrcons.skirc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrconsrc.dll	%INSTALLDIR%\Resources

Feature	Filename	Location
	ActivClient.msc	%INSTALLDIR%
PIN Initialization Tool	ac.activclient.gui.scinitwiz.dll	%INSTALLDIR%
	ac.activclient.gui.scinitwiz.exe	%INSTALLDIR%
	ac.activclient.gui.scinitwizrc.dll	%INSTALLDIR%\Resources
	ac.aspcom.wrapper.dll	%INSTALLDIR%
	ac.sharedstore.wrapper.dll	%INSTALLDIR%
	accuvoplite.dll	%INSTALLDIR%
	acvop.dll	%INSTALLDIR%
	acvopsm.cfg	%INSTALLDIR%
	acvopsm.dll	%INSTALLDIR%
	acvopsvr.dll	%INSTALLDIR%
	apduengine.dll	%INSTALLDIR%
	*.ini	%INSTALLDIR%\Profiles
Troubleshooting	ac.activclient.gui.diagtool.exe	%COMMONFILES%\HID Global
	ac.activclient.gui.diagtoolrc.dll	%COMMONFILES%\HID Global\Resources
	ac.cext.dll	%COMMONFILES%\HID Global
	ac.diag.activclient.dll	%INSTALLDIR%
	ac.diag.activclientrc.dll	%INSTALLDIR%\Resources
	ac.diag.hidproducts.dll	%COMMONFILES%\HID Global
	ac.diag.hidproductsrc.dll	%COMMONFILES%\HID Global\Resources
	ac.diag.system.dll	%COMMONFILES%\HID Global

Feature	Filename	Location
	ac.diag.systemrc.dll	%COMMONFILES%\HID Global\Resources
	ac.winext.settings.dll	%COMMONFILES%\HID Global
	aclogu.dll	%COMMONFILES%\HID Global
	aiwinextu.dll	%COMMONFILES%\HID Global
SoftwareAutoUpdate	ac.autoupdate.exe	%INSTALLDIR%
	ac.autoupdaterc.dll	%INSTALLDIR%\Resources
	ai-cms-ccm-syncU.dll	%INSTALLDIR%\Smart Card Auto Update
	ai-cms-ccmU.dll	%INSTALLDIR%\Smart Card Auto Update
	SyncManagerU.ini	%INSTALLDIR%\Smart Card Auto Update
SettingsManagement	HIDGlobal.ActivClient.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.ActivClient.admx	%SystemRoot%\PolicyDefinitions
	HIDGlobal.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.admx	%SystemRoot%\PolicyDefinitions
	HIDGlobal.AdvancedDiagnostics.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.AdvancedDiagnostics.admx	%SystemRoot%\PolicyDefinitions
	HIDGlobal.Logging.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.Logging.admx	%SystemRoot%\PolicyDefinitions
Help	ActivClient.chm	%INSTALLDIR%\Documentation\
Merge Module	Visual Studio 2015 Redistributables	Please refer to Microsoft documentation

A.2. ActivClient 7.1 Installed Files (64-bit Edition)

Table 8: ActivClient 7.1 64-bit Edition

Feature	Filename	Location
BSI	acbsi21.dll	%INSTALLDIR%;%INSTALLDIRX86%
	JNIBSI21.dll	%INSTALLDIR%;%INSTALLDIRX86%
	acbsi21rc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	bsi21classes.jar	%INSTALLDIR%
	bsi21inter.jar	%INSTALLDIR%
PIV	acpivapi.dll	%INSTALLDIR%;%INSTALLDIRX86%
	aijnipiv.dll	%INSTALLDIR%;%INSTALLDIRX86%
	aijnipiv.jar	%INSTALLDIR%
ActivClient	ac.activclient.gui.pin.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.activclient.gui.pinrc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	ac.activclient.gui.scagent.exe	%INSTALLDIR%
	ac.activclient.gui.scagentrc.dll	%INSTALLDIR%\Resources
	ac.activclient.scardactions.exe	%INSTALLDIR%
	ac.activclient.syslog.dll	%INSTALLDIR%
	ac.cardsync.dll	%INSTALLDIR%\Smart Card Auto Update
	ac.cext.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.crypto.parser.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtbroadcast.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtmon.certstore.dll	%INSTALLDIR%;%INSTALLDIRX86%

Feature	Filename	Location
ActivClient (continued)	ac.evtmon.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtmon.scard.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtmon.sys.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtproc.cachelifecycle.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtproc.certstore.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtproc.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtproc.scard.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.evtsessionstate.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.mscredprov.pincache.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.msgbox.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.msgboxrc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	ac.scardmon.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.scmwdiag.dll	%INSTALLDIR%
	ac.scmwdiagrc.dll	%INSTALLDIR%\Resources
	ac.sharedstore.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.sharedstorecl.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.sharedstoreps.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.common.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.common.srvctl.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.common.srvprov.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.mwctl.dll	%INSTALLDIR%;%INSTALLDIRX86%

Feature	Filename	Location
ActivClient (continued)	ac.smmw.srvctl.cache.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvctl.sm.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.authcach.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.comm.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.datacach.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.disco.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.cac.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.cacv1.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.cacv2.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.gp.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.piv.ai.ep.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.piv.ai.wrap.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.piv.std.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v1.common.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v1.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v1.standalone.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v2.common.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v2.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.v2.standalone.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.dm.virtualMD.dll	%INSTALLDIR%;%INSTALLDIRX86%

Feature	Filename	Location
ActivClient (continued)	ac.smmw.srvprov.info.javacard.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.piv.ai.262.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.piv.ai.27.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.piv.std.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.soft.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.v1.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sm.v2.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sma.v1.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.smmw.srvprov.sma.v3.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.winext.settings.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.winext.winrt.dll	%INSTALLDIR%;%INSTALLDIRX86%
	AcBcgProu.dll	%INSTALLDIR%
	acCobAPIlrc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	acCobAPIrc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	accryptou.dll	%INSTALLDIR%
	acevents.exe	%INSTALLDIR%
	acevtsub.dll	%INSTALLDIR%;%INSTALLDIRX86%
	acispcard.dll	%INSTALLDIR%
	aclogu64.dll	%INSTALLDIR%
	aclogu.dll	%INSTALLDIRX86%

Feature	Filename	Location
ActivClient (continued)	acomx.dll	%INSTALLDIR%;%INSTALLDIRX86%
	acregcrt.exe	%INSTALLDIR%
	ActivClient_EULA.pdf	%INSTALLDIR%\Documentation
	ReleaseNotes.html	%INSTALLDIR%\Documentation
	actsinit.exe	%INSTALLDIR%
	ai.ccm.apiU.dll	%INSTALLDIR%
	ai.interfacesU.dll	%INSTALLDIR%
	ai.localizationU.dll	%INSTALLDIR%
	aiwinextu.dll	%INSTALLDIR%;%INSTALLDIRX86%
	Windows_Toast_Info.png	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
MiniDriver	ac.scapi.scmd.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.scapi.scmd.x86.cat	%INSTALLDIR%\Smart Card Minidriver
	ac.scapi.scmd.x86.inf	%INSTALLDIR%\Smart Card Minidriver
	ac.scmd.kerbauth.dll	%INSTALLDIR%;%INSTALLDIRX86%
Outlook	ac.activclient.oladdin.dll	%INSTALLDIR%;%INSTALLDIRX86%
	ac.activclient.oladdin.rc.dll	%INSTALLDIR%\Resources;%INSTALLDIRX86%\Resources
	aiCOMMAPI.dll	%INSTALLDIR%
	aiCOMMAPI.exe	%INSTALLDIRX86%
	aiCOMMAPIPS.dll	%INSTALLDIR%
	aiCOMMAPIPS.dll	%INSTALLDIRX86%
PKCS	acpkcs211.dll	%INSTALLDIR%;%INSTALLDIRX86%

Feature	Filename	Location
MozillaSupport	chrome.manifest	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module;%INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	install.rdf	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module;%INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	overlay.js	%INSTALLDIR%\Mozilla Extensions ActivClient PKCS #11 Security Module \chrome\content; %INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	overlay.xul	%INSTALLDIR%\Mozilla Extensions\ ActivClient PKCS #11 Security Module \chrome\content; %INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	manifest.mf	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF; %INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	mozilla.rsa	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF; %INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
	mozilla.sf	%INSTALLDIR%\Mozilla Extensions\ActivClient PKCS #11 Security Module\META-INF; %INSTALLDIRX86%\Mozilla Extensions\ ActivClient PKCS #11 Security Module
UserConsole	ac.activclient.gui.usrcons.exe	%INSTALLDIR%
	ac.activclient.gui.usrcons.helper.dll	%INSTALLDIR%

Feature	Filename	Location
	ac.activclient.gui.usrcons.helperrc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrcons.pdata.dll	%INSTALLDIR%
	ac.activclient.gui.usrcons.pdatarc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrcons.ski.dll	%INSTALLDIR%
	ac.activclient.gui.usrcons.skirc.dll	%INSTALLDIR%\Resources
	ac.activclient.gui.usrconsrc.dll	%INSTALLDIR%\Resources
	ActivClient.msc	%INSTALLDIR%
PIN Initialization Tool	ac.activclient.gui.scinitwiz.dll	%INSTALLDIR%
	ac.activclient.gui.scinitwiz.exe	%INSTALLDIR%
	ac.activclient.gui.scinitwizrc.dll	%INSTALLDIR%\Resources
	ac.aspcom.wrapper.dll	%INSTALLDIR%
	ac.sharedstore.wrapper.dll	%INSTALLDIR%
	accuvoplite.dll	%INSTALLDIR%
	acvop.dll	%INSTALLDIR%
	acvopsm.cfg	%INSTALLDIR%
	acvopsm.dll	%INSTALLDIR%
	acvopsvr.dll	%INSTALLDIR%
	apduengine.dll	%INSTALLDIR%
	*.ini	%INSTALLDIR%\Profiles
Troubleshooting	ac.activclient.gui.diagtool.exe	%COMMONFILES%\HID Global
	ac.activclient.gui.diagtoolrc.dll	%COMMONFILES%\HID Global\Resources

Feature	Filename	Location
	ac.cext.dll	%COMMONFILES%\HID Global
	ac.diag.activclient.dll	%INSTALLDIR%
	ac.diag.activclientrc.dll	%INSTALLDIR%\Resources
	ac.diag.hidproducts.dll	%COMMONFILES%\HID Global
	ac.diag.hidproductsrc.dll	%COMMONFILES%\HID Global\Resources
	ac.diag.system.dll	%COMMONFILES%\HID Global
	ac.diag.systemrc.dll	%COMMONFILES%\HID Global\Resources
	ac.winext.settings.dll	%COMMONFILES%\HID Global
	aclogu.dll	%COMMONFILES%\HID Global
	aiwinextu.dll	%COMMONFILES%\HID Global
SoftwareAutoUpdate	ac.autoupdate.exe	%INSTALLDIR%
	ac.autoupdaterc.dll	%INSTALLDIR%\Resources
	ai-cms-ccm-syncU.dll	%INSTALLDIR%\Smart Card Auto Update
	ai-cms-ccmU.dll	%INSTALLDIR%\Smart Card Auto Update
	SyncManagerU.ini	%INSTALLDIR%\Smart Card Auto Update
SettingsManagement	HIDGlobal.ActivClient.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.ActivClient.admx	%SystemRoot%\PolicyDefinitions
	HIDGlobal.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.admx	%SystemRoot%\PolicyDefinitions

Feature	Filename	Location
	HIDGlobal.AdvancedDiagnostics.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.AdvancedDiagnostics.admx	%SystemRoot%\PolicyDefinitions
	HIDGlobal.Logging.adml	%SystemRoot%\PolicyDefinitions\en-US
	HIDGlobal.Logging.admx	%SystemRoot%\PolicyDefinitions
Help	ActivClient.chm	%INSTALLDIR%\Documentation\
Merge Module	Visual Studio 2015 Redistributables x86	Please refer to Microsoft documentation
	Visual Studio 2015 Redistributables x64	Please refer to Microsoft documentation

A.3. 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\HID Global\ActivClient\Downloads**.

This folder is used to store downloaded hot-fixes if the ActivClient Auto-Update feature is used.

Appendix B: Registry Keys

This appendix describes all the Microsoft Windows registry keys used (for read or write) by ActivClient. They are listed by feature and edition:

- B.1 Registry Keys Installed by ActivClient 7.1 (32-bit Edition) on page 182.
- B.2 Registry Keys Installed by ActivClient 7.1 (64-bit Edition) on page 185.

Note: These registry keys are not used for ActivClient configuration; use the ActivClient policies described in section 4.0 ActivClient Policy Settings on page 27 instead. These 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.

B.1. Registry Keys Installed by ActivClient 7.1 (32-bit Edition)

Table 9: Registry Keys Installed by ActivClient 7.1 (32-bit Edition)

Feature	Registry key name
ActivClient	[HKEY_CLASSES_ROOT\CLSID\{05A69B2E-F05A-426b-BB43-7895A67B1A56}]
	[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}]
	[HKEY_CLASSES_ROOT\CLSID\{F7928249-E288-4332-9412-3ED9BFB71D20}]
	[HKEY_CLASSES_ROOT\CLSID\{22123996-E0B7-485B-86C7-D6A926117B5F}]
	[HKEY_CLASSES_ROOT\CLSID\{DF2B2E0E-8406-44E5-AFB1-21A485C78ABE}]
	[HKEY_CLASSES_ROOT\CLSID\{78414097-B22E-4846-AD3F-63A60E225034}]
	[HKEY_CLASSES_ROOT\CLSID\{AD91587E-C288-4C07-830F-1C61DBFAC1B4}]
	[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}]
	[HKEY_CLASSES_ROOT\AppID\acevents.EXE]

Feature	Registry key name
ActivClient (continued)	[HKEY_CLASSES_ROOT\AppID\{CFDD1051-06E1-4446-BFA1-3D63B5CB2B5A}]
	[HKEY_CLASSES_ROOT\Interface\{ED32AB06-3E5C-4BBF-A04B-0FAFA88CFCCB}]
	[HKEY_CLASSES_ROOT\Interface\{0A0F91AF-02F5-4291-B06E-79F88EDD1118}]
	[HKEY_CLASSES_ROOT\Interface\{AF00C046-74DB-4045-A9DE-71B1B561ECD4}]
	[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}]
	[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}]
	[HKEY_CLASSES_ROOT\Interface\{DF2B2E0E-8406-44E5-AFB1-21A485C78ABE}]
	[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}]
	[HKEY_CLASSES_ROOT\TypeLib\{E042663E-CDC5-406F-9AAC-1982E7EF0D68}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SecurityModuleMW]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Logging]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SharedStore]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SnapIns\EventService]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

Feature	Registry key name
ActivClient (continued)	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{05A69B2E-F05A-426b-BB43-7895A67B1A56}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{F7928249-E288-4332-9412-3ED9BFB71D20}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{23560575-A750-499E-82F1-671681F54906}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{EDAD57CE-8470-4B9A-8236-0C6B4B4EEDA9}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{82F2CE02-F655-43E9-A6BF-C98FD7E0C7F6}]
	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\HID Global\ActivClient]
BSI	[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1\ActivIdentity]
DeptOfDefenseConfiguration	[HKEY_LOCAL_MACHINE\SOFTWARE\ActivClient\Notifications]
MozillaSupport	[HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\extensions]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Thunderbird\extensions]
Outlook	[HKEY_CLASSES_ROOT\CLSID\{78414097-B22E-4846-AD3F-63A60E225034}]
	[HKEY_CLASSES_ROOT\CLSID\{AD91587E-C288-4C07-830F-1C61DBFAC1B4}]
	[HKEY_CLASSES_ROOT\Interface\{ED32AB06-3E5C-4BBF-A04B-0FAFA88CFCCB}]
	[HKEY_CLASSES_ROOT\Interface\{22123996-E0B7-485B-86C7-D6A926117B5F}]
	[HKEY_CLASSES_ROOT\TypeLib\{2AA0E6DD-00CA-42C1-B513-1567A15B7E4A}]
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\ac.activclient.oladdin]

Feature	Registry key name
PKCS	[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\ActivIdentity]
SoftwareAutoUpdate	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient\AutoUpdate]
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Autoupdate\ActivClient]
Troubleshooting	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SnapIns\AdvancedDiagnostics]
UserConsole	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient\Snapins]

B.2. Registry Keys Installed by ActivClient 7.1 (64-bit Edition)

This section provides information on the registry keys installed on 64-bit platforms and specifies in which registry (32-bit and/or 64-bit):

Table 10: Registry Keys Installed by ActivClient 7.1 (64-bit Edition)

Feature	Registry key name	Registry location
ActivClient	[HKEY_CLASSES_ROOT\CLSID\{05A69B2E-F05A-426b-BB43-7895A67B1A56}]	x86 and x64
	[HKEY_CLASSES_ROOT\CLSID\{5E248397-8614-4EC5-8926-BD242DC9830A}]	x64
	[HKEY_CLASSES_ROOT\CLSID\{F7928249-E288-4332-9412-3ED9BFB71D20}]	x86 and x64
	[HKEY_CLASSES_ROOT\CLSID\{DF2B2E0E-8406-44E5-AFB1-21A485C78ABE}]	x86 and x64
	[HKEY_CLASSES_ROOT\CLSID\{F7C82795-14F3-47D2-ADA4-3183AD6ED9D9}]	x86 and x64
	[HKEY_CLASSES_ROOT\AppID\acevents.EXE]	x64
	[HKEY_CLASSES_ROOT\AppID\{CFDD1051-06E1-4446-BFA1-3D63B5CB2B5A}]	x64

Feature	Registry key name	Registry location
ActivClient (continued)	[HKEY_CLASSES_ROOT\Interface\{0A0F91AF-02F5-4291-B06E-79F88EDD1118}]	x86 and x64
	[HKEY_CLASSES_ROOT\Interface\{AF00C046-74DB-4045-A9DE-71B1B561ECD4}]	x86 and x64
	[HKEY_CLASSES_ROOT\Interface\{F2255E01-7804-42D2-AB6F-F3DC4B17875C}]	x86 and x64
	[HKEY_CLASSES_ROOT\Interface\{3D9C1CF1-7AA4-4ED7-9B8A-EC57B4F76DD8}]	x64
	[HKEY_CLASSES_ROOT\Interface\{DF2B2E0E-8406-44E5-AFB1-21A485C78ABE}]	x86 and x64
	[HKEY_CLASSES_ROOT\TypeLib\{C89A2418-4FB7-47BE-A1A6-206379EE0449}]	x64
	[HKEY_CLASSES_ROOT\TypeLib\{E042663E-CDC5-406F-9AAC-1982E7EF0D68}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SecurityModuleMW]	x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Logging]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SharedStore]	x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SnapIns\EventService]	x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]	x64

Feature	Registry key name	Registry location
ActivClient (continued)	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{05A69B2E-F05A-426b-BB43-7895A67B1A56}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{F7928249-E288-4332-9412-3ED9BFB71D20}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{23560575-A750-499E-82F1-671681F54906}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{EDAD57CE-8470-4B9A-8236-0C6B4B4EEDA9}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{82F2CE02-F655-43E9-A6BF-C98FD7E0C7F6}]	x86 and x64
	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\HID Global\ActivClient]	x64
BSI	[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\BSI\2.1\ActivIdentity]	x86 and x64
DeptOfDefenseConfiguration	[HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\ActivClient\Notifications]	x64
MozillaSupport	[HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\extensions]	x86 and x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Thunderbird\extensions]	x86 and x64
Outlook	[HKEY_CLASSES_ROOT\CLSID\{22123996-E0B7-485B-86C7-D6A926117B5F}]	x64
	[HKEY_CLASSES_ROOT\CLSID\{78414097-B22E-4846-AD3F-63A60E225034}]	x86 and x64
	[HKEY_CLASSES_ROOT\CLSID\{AD91587E-C288-4C07-830F-1C61DBFAC1B4}]	x86 and x64

Feature	Registry key name	Registry location
	[HKEY_CLASSES_ROOT\CLSID\{BAE2936A-20CA-449F-AC00-82E36FE7A3A4}]	x86
	[HKEY_CLASSES_ROOT\AppID\{E56BFAC1-9567-49EA-AB6C-AB545B3A2C29}]	x86
	[HKEY_CLASSES_ROOT\AppID\aiCOMMAPI.EXE]	x86
	[HKEY_CLASSES_ROOT\Interface\{ED32AB06-3E5C-4BBF-A04B-0FAFA88CFCCB}]	x86 and x64
	[HKEY_CLASSES_ROOT\Interface\{22123996-E0B7-485B-86C7-D6A926117B5F}]	x86 and x64
	[HKEY_CLASSES_ROOT\TypeLib\{2AA0E6DD-00CA-42C1-B513-1567A15B7E4A}]	x86 and x64
	[HKEY_CLASSES_ROOT\TypeLib\{93287305-D3F7-4FB5-8871-E2A9007C08C9}]	x86
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\ac.activclient.oladdin]	x86 and x64
PKCS	[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\ActivIdentity]	x86 and x64
SoftwareAutoUpdate	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient\AutoUpdate]	x64
	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Autoupdate\ActivClient]	x64
Troubleshooting	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\SnapIns\AdvancedDiagnostics]	x64
UserConsole	[HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\ActivClient\Snapins]	x64

B.3. 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\HID Global\SharedStore\RemanentDataStore – used for performance optimization
- HKEY_LOCAL_MACHINE\SOFTWARE\HID Global\Logging – used for logging
- HKEY_LOCAL_MACHINE\SOFTWARE\ActivIdentity\Diagnostic – used for diagnostics

Appendix C: Terms and Acronyms

This appendix lists terms and acronyms used throughout the full set of the set of technical publications for this product. Not all terms and acronyms appear in all documents in the set.

C.1. 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 Credential Management System (CMS)	Formally known as ActivID Card Management System, ActivID CMS is a web-based, smart card, credential and application lifecycle management system. ActivID CMS augments and works in concert with an enterprise's primary identity management infrastructure components, including popular directory, database, and PKI components.
Challenge	Random number generated by the server API for authentication of a user in the asynchronous (challenge/response) mode.
Cryptographic Service Provider (CSP)	An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.
Discovery mode	Discovery mode enables a calling application to find out the size of the data that will be returned to by making a preliminary discovery call and then making a second call after it allocates a buffer large enough to accommodate the data that will be returned.
End-point card	The PIV standard defines two interfaces for communicating with PIV cards: • The PIV transitional interface. • The PIV end-point interface. A PIV end-point card is a card that implements the second of these interfaces. **Note:** The PIV transitional interface is not supported by the PIV API.
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.
Force change PIN flag	Flag which indicates whether the user must change the PIN on first use of the card.

Integrated circuit chip (ICC)	The chip on the smart card.
Mini Driver	Smart card middleware for the Microsoft platform that works with the Microsoft Base Smart Card CSP (Cryptographic Service Provider). The ActivClient Mini Driver replaces the ActivClient CSP available in previous versions. The Mini Driver architecture provides stronger cryptographic services.
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)	The Personal Identification Number (PIN) code used to access an HID Global device's services such as Windows PKI logon, remote access and email signature. HID Global devices can only be used after a correct PIN is entered.
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.
Unlock code	Value that the card holder needs to provide in order to unlock a locked smart card. Depending upon the smart card unlock mechanism, the unlock code may or may not be different from the unlock key.
Verification	Process in which a signature that was produced by the signing operation is verified.
Weak PIN	A weak PIN is a PIN in which: • The length is less than three characters or digits, or • The difference between each character or digit, and the following one is a constant. For example, a PIN that is a sequence of the same number (1111) or an increasing/decreasing sequence of numbers (1234, 4321) is a weak PIN.

C.2. Acronyms

CA Certificate Authority

CAC Common Access Card (for the United States Department of Defense)

CSP Cryptographic Service Provider

CUID Card Unique Identifier

CUID is a number that uniquely identifies a card.

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

