

ActivIdentity CAC Troubleshooting FAQ's

Which versions of Windows are supported by ActivClient 6.1?

Product	ActivClient
Version	6.1
Platform/directory	Windows
Author	Jean-Luc Azou
Last reviewed	June 18, 2008

Question

Which versions of Windows are supported by ActivClient 6.1?

Answer

ActivClient 6.1 is supported on the following Windows versions:

Windows 2000 SP4

Windows XP Professional SP1, SP2 and SP3

Windows XP Home Edition SP2 and SP3

Windows Vista and Windows Vista SP1 (all 32- and 64-bit editions)

Windows Server 2003 SP1, R2 and SP2 (all 32- and 64-bit editions)

Windows Server 2008 (all 32- and 64-bit editions) with the following limitations, that ActivIdentity intends to address in the next ActivClient version

No support for the new templates available in the Certificate Server included in Windows Server 2008 ("Enrollment Agent (User)", "Kerberos Authentication", "OCSP Response Signing" and "Smartcard User On Behalf Of Another User").

No support for Server Core.

Note: Terminal Server included in Windows Server 2008 is supported with ActivClient 6.1 Service Pack 2.

Device manager sees reader but ActivClient does not

Product	ActivClient
Version	ActivClient 6.x ActivClient 5.4 ActivClient 5.4 - PKI Only ActivClient for CAC 5.4 Gold 2.3.1 Service Pack 2 (SP2) Gold for CAC 2.2 Gold for CAC 2.2 Service Pack 1 (SP1) Gold for CAC 2.2 Service Pack 2 (SP2) Gold for CAC - PKI 3.0 Gold for CAC - PKI 3.0 Feature Pack 1 (FP1) Gold for CAC - PKI 3.0 Feature Pack 2 (FP2)
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Question

Device manager sees reader but ActivClient does not

Answer

Best way to ensure a correct installation of the reader driver for ActivClient is to follow these steps:

unplug the reader

uninstall the driver

remove it from device manager
 reboot
 install the driver
 reboot
 plug in the reader
 At which point the middleware should "see" the reader

Error: Your Digital ID name can not be found by the underlying security

Product	ActivClient
Version	ActivClient 6.x ActivClient 5.4 ActivClient 5.4 - PKI Only ActivClient for CAC 5.4 Gold 2.3.1 Service Pack 2 (SP2) Gold for CAC 2.2 Gold for CAC 2.2 Service Pack 1 (SP1) Gold for CAC 2.2 Service Pack 2 (SP2) Gold for CAC - PKI 3.0 Gold for CAC - PKI 3.0 Feature Pack 1 (FP1) Gold for CAC - PKI 3.0 Feature Pack 2 (FP2)
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Question

Error: Your Digital ID name can not be found by the underlying security

Answer

Confirm that the certificates have been made available to window-check the Certificate store of the machine using Internet Explorer/Tools/Internet Options/Content/Certificates.
 If the certificates are not there, use ActivClient to put them in place by going to Tools/Advanced/Make Certificates Available to Windows.

How can I restore fast user switching in ActivClient Gold?

Product	ActivClient
Version	Gold 2.2j Gold 2.3.1 Service Pack 2 (SP2) Gold for CAC 2.2 Gold for CAC 2.2 Service Pack 1 (SP1) Gold for CAC 2.2 Service Pack 2 (SP2) Gold for CAC - PKI 3.0 Gold for CAC - PKI 3.0 Feature Pack 1 (FP1) Gold for CAC - PKI 3.0 Feature Pack 2 (FP2)
Platform/directory	N.A.
Author	Hari Veladanda
Last reviewed	February 5, 2008

Question

How can I restore fast user switching in ActivClient Gold?

Answer

When Gold is installed, it replaces the Microsoft Gina. When that happens, Fast user Switching capabilities are lost on XP systems. If the user needs to do local login (Gina based login) then they can not use the switching. If, however, they use it only for applications or web authentication, then they can remove the following registry key and reboot the machine to restore the Fast user Switching.

Back this key to the desktop as a precaution, then remove it from the registry and reboot:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL

How do I check which features are installed in ActivClient?

Product	ActivClient
Version	ActivClient 5.4, ActivClient 5.4 - PKI Only, ActivClient for CAC 5.4, ActivClient for CAC with CoreStreet OCSP 5.4
Platform/directory	N.A.
Author	Hari Veladanda
Last reviewed	February 5, 2008

Question

How do I check which features are installed in ActivClient?

Answer

For a high-level point of view, Control Panel, Add/Remove Programs, Modify and check which feature is selected or not.

For a very detailed view, use the Advanced Diagnostics Tool (available on menu Start/Programs/ActivCard ActivClient/Advanced Diagnostic) report. In this report, check for "Product #xxx (installed)".

IOCTL SET_PROTOCOL error in Event Log

Product	ActivClient
Version	ActivClient 5.4 ActivClient 6.0
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Issue

Smart Card Reader 'ActivCard ActivCard USB Reader C2 0' rejected IOCTL SET_PROTOCOL: The request is not supported.

Solution:

This error is the result of a new process in ActivClient 6.0, where in order to support both card protocols, we have to try one before the other.

So, in the case where the card is using a t=1 protocol, this error will occur as a result of the t=0 protocol attempt failing.

This error can be safely ignored.

Product	ActivClient
Version	ActivClient 5.4

	ActivClient 5.4 - PKI Only ActivClient for CAC 5.4
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Issue

Use Case:

Disabled PIN Caching (Restart machine)

Compose and send signed message

Enter PIN when prompted

Compose and send second signed message

PIN wasn't prompted (PIN should be prompted)

Roaming user profile is not working correctly with ActivClient

Product	ActivClient
Version	ActivClient v6.X
Platform/directory	PC Blades/ Thin clients/ RDP/ Domain users
Author	Gurjeet Mann
Last reviewed	April 15, 2008

Issue

When a PC blade user is logged into a PC blade and attempts to access a website that requires a PKI certificate, Internet Explorer will hang. Also sending a digitally signed or encrypted email will hang Outlook.

Cause

ActivClient opens and closes transactions to the scard service when needed. During Microsoft certificate propagation, ActivClient is not able to complete transactions to the scard service because it stops and restarts (0x8010001e: The Smart card resource manager is shut down). At this time is not possible for ActivClient to shut down the transaction to the scard service. The scard service starts again after a few seconds.

As a transaction is opened and cannot be closed, all future communications with the card are blocked.

Solution

Potential workaround: Disable MS cert propagation: Disable Microsoft automatic certificate registration by setting the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ScCertProp, Enabled = 0 then restart your computer.

The system could not log you on. (error 0xC00000BB)

Product	ActivClient
Version	ActivClient 6.x ActivClient 5.4 ActivClient 5.4 - PKI Only ActivClient for CAC 5.4 Gold 2.3.1 Service Pack 2 (SP2) Gold for CAC 2.2 Gold for CAC 2.2 Service Pack 1 (SP1) Gold for CAC 2.2 Service Pack 2 (SP2) Gold for CAC - PKI 3.0 Gold for CAC - PKI 3.0 Feature Pack 1 (FP1) Gold for CAC - PKI 3.0 Feature Pack 2 (FP2)

Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Question

The system could not log you on. (error 0xC00000BB)

Answer

<http://support.microsoft.com/default.aspx?scid=kb:en-us:891849>

This problem may occur when the user name portion of the your User Principal Name (RFC822 name) does not match your downlevel logon name (sAMAccountName).

For example, if you log on with the following attributes, you will not experience the problem:

sAMAccountName: johnsmith

userPrincipalName: johnsmith@contoso.com

However, if you log on with the following attributes after you install Windows XP SP2, you will experience the problem:

sAMAccountName: johnsmith

userPrincipalName: jsmith@contoso.com

Note This problem may not occur until after you install Windows XP Service Pack 2 (SP2).

A supported hotfix is now available from Microsoft, but it is only intended to correct the problem that is described in this article. Only apply it to systems that are experiencing this specific problem. This hotfix may receive additional testing. Therefore, if you are not severely affected by this problem, we recommend that you wait for the next Windows XP service pack that contains this hotfix.

Unable to start a DCOM server error in Event Viewer

Product	ActivClient
Version	ActivClient 5.4 ActivClient 5.4 - PKI Only ActivClient for CAC 5.4 ActivClient for CAC with CoreStreet OCSP 5.4 ActivClient 6.x
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Question

Unable to start a DCOM server error in Event Viewer

Answer

When running ActivClient in a TSE environment, it may happen that the following message is logged in the TSE server event log:

"Unable to start a DCOM Server: {5E248397-8614-4EC5-8926-BD242DC9830A}. The error: "No process is on the other end of the pipe."

Happened while starting this command: C:\PROGRA~1\ACTIVC~1\ACTIVC~1\acevents.exe - Embedding"

Explanation

This is a design limitation of ActivClient on TSE (Terminal Server) due to a Microsoft issue.

Each time a user remote logs on the server, acevents tries to instantiate a COM object. The instantiation failed as no user is logged: this engender an error in Event Viewer logs. This Microsoft issue is bypassed in ActivClient code thanks to a workaround and does not alter ActivClient behavior.

Using CAC with Mac OS X 10.4 (Tiger)

Product	ActivClient
---------	-------------

Version	ActivClient 5.4 ActivClient 5.4 - PKI Only ActivClient for CAC 5.4
Platform/directory	MacOS
Author	Hari Veladanda
Last reviewed	February 7, 2008

Issue

ActivCard Gold for Mac 1.2.1 does NOT support Mac OS 10.4.

Support for Mac OS 10.4 is planned for the next release - this next release is under definition; a scheduled release date is to be confirmed.

Solution:

Workaround

Uninstall ActivCard Gold for Mac 1.2.1.

Smart Cards in Mac OS 10.4.x (Tiger)

Smart Cards (CAC, GSCIS, PIV, JPKI, BELPIC, and others) are all abstracted as keychains for access by any application utilizing Mac OS X's built in Cert/Key & Keychain APIs (i.e. Entourage 2004). The architecture has changed, but largely from the abstraction layers on top of what was already there before. Users and Sys Admins have far less to do or worry about than they did with 10.3.x.

Smart Card Services Provided in "Tiger" -10.4.0

The Tiger installation includes a CCID Class Driver. This means that any USB-based Smart Card Reader that complies with the CCID standards will work out of the box with no need to load a reader-specific driver.

Cryptographic Login to local/network-based accounts (more info to follow below)

S/MIME -- Signing and Encrypting of Mail Messages

Leading Applications supporting this

- Mail.App (Apple)
- Entourage 2004 (Microsoft)
- Netscape/Mozilla/... software train still works as well...

Secure Web Access / Client Side Authentication

- Safari (Apple)
- Netscape/Mozilla/... software train still works as well...

VPN (PPTP, L2TP, 802.1X, ... VPN On Demand)

- Internet Connect (Apple)

Address Book

Now also displays the "signing" check symbol just left of email addresses that the user has corresponding Public Cert in their keychain. The Cert is NOT stored in the keychain, but represents a relationship with one in one of the currently active keychains.

"Common Access Card Viewer" functionality is largely now available since the Smart Cards appear as dynamic keychains. You can view the Certificate and Key information as well as change the PIN on the card by selecting the "Change Password for Keychain ...". If you still feel the need to run the Common Access Card Viewer Utility on Tiger, then you need to install it from the Tiger DVD.

The installer for the Common Access Card Viewer Utility is located at:

Mac OS X Install DVD /System/Installation/Packages/CommonAccessCard.pkg

I also placed it on my personal iDisk as well. (see end of message)

Tiger Smart Card Login Setup

*** PLEASE DO NOT COPY OVER OR USE PANTHER CONFIGURATIONS ON TO YOUR TIGER SYSTEMS!**

Many of you are anxious to enable Smart Card cryptographic login right now on your Tiger systems. I have posted a zipped folder on my iDisk as well labeled: "TigerSmartcardSetup.zip" which has a Text document with initial instructions and examples as well as a 'diff' file with the modification for /etc/authorization.

In short:

/etc/authorization is modified for system.login.console

Accounts are, by default, bound to Public Key Hash of the User's ID Private Key.

As was the case in 10.3.x., those wanting/needing to use combination of other Card information (ie. UPN) can still configure the systems for your desired combination as well. With Tiger, you will need to setup and configure the file: /etc/cacloginconfig.plist

Mac OS X 10.3.x utilized the cac_setup, cac_addid, cac_anchors commands and these have been superseded by "sc_auth" located in /usr/sbin/sc_auth.

hostname# /usr/sbin/sc_auth -h Usage: sc_auth accept [-v] [-u user] [-k keyname] # by key on inserted card(s)
sc_auth accept [-v] [-u user] -h hash # by known pubkey hash
sc_auth remove [-v] [-u user] # remove all public keys for this user
sc_auth hash [-k keyname] # print hashes for keys on inserted card(s)
Once enabled, there is NO performance degradation if user's do not have or use Smart Cards. Many agency admins should probably consider, currently, making these mods to all systems and therefore enabling the use of Smart Cards on ALL systems.

If enabled on a system running Tiger:

User inserts a Smart Card (at Login Panel)

Login Panel momentarily disappears and then reappears with

- Smart Card User's Account Name

- PIN field empty and waiting for entry by user logging in

User enters PIN

Login Cryptographically validates and unlocks the card

User Account is looked for / found in one of any of the configured DS Servers.

User is logged in.

Outstanding Challenges for Federal Customers:

As of 10.4.0, the modifications for enabling Smart Card Login are not enabled by default

- A subsequent update to Mac OS X 10.4.x should include these by default

The DoD Intermediate CAs are not available to the Keychain List by default

- Federal Customers within DoD will need to add the "X509Certificates" to the list

1. Launch Keychain Access

2. Select "Edit -> Keychain List"

3. Select "Show: Mac OS X (System)"

4. Check "Shared" checkbox next to "X509Certificates" (/System/Library/Keychains)

X509Certificates will now appear in the Keychains List and will be available for Intermediates for the whole trust path validation.

As of 10.4.0, Smart Card Login does not currently support the unlocking of FileVault protected Home Directories. You can create Encrypted Images for your folders inside your Home Directory and unlock them manually at login.

"error : Unable to build pkgmap from prototype file, packaging wasn't successful" when tried to install ActivClient 6.1 for Solaris

Product	ActivClient
Version	ActivClient for Solaris 2.1
Platform/directory	Sparc
Author	Hari Veladanda
Last reviewed	February 7, 2008

Issue

error : Unable to build pkgmap from prototype file, packaging wasn't successful when tried to install ActivClient 6.1 for Solaris on the system

Cause

Older version of ActivClient for Solaris 2.0_30 was not removed from the system first.

Solution

Older version of Solaris 2.0_30 needs to be removed by running command :

Pkgrm ActivClient

before upgrading to Solaris 2.1_13.

Can we customize the ActivIdentity Device Installer(AIDI)?

Product	ActivClient
Version	All
Platform/directory	All
Author	Hari Veladanda
Last reviewed	February 7, 2008

Issue

Can we customize the ActivIdentity Device Installer(AIDI)?

Solution:

The ActivIdentity Device Installer (AIDI) can be customize so as to install for example only a given device and not the other ones.

This can be done by modifying the values of the properties inside the MSI file that are suffixed by “REQ” (with no underscore before “REQ”).

A value of 0 means the property will be visible but not installed,

1 means visible and installed,

-1 means invisible and not installed.

The modification can be done either by executing the standard ActivIdentity Device Installer.msi file with options in the command line or by modifying the values inside the ActivIdentity Device Installer.msi using ORCA and then execute that modified ActivIdentity Device Installer.msi.

For example, for installing only the ActivKey SIM driver:

```
msiexec /i "ActivIdentity Device Installer.msi" USBKEYV2REQ=-1 PCMCIAV2REQ=-1  
PCMCIAV1REQ=-1 SERIALREQ=-1 USBKEYSIMREQ=1 USBV3REQ=-1 ACTIVDIAGREQ=-1  
USBV2REQ=-1
```

OR

Edit "ActivIdentity Device Installer.msi" with ORCA and set USBKEYV2REQ, PCMCIAV2REQ, PCMCIAV1REQ, SERIALREQ, USBV3REQ, ACTIVDIAGREQ and USBV2REQ to -1, and USBKEYSIMREQ to 1 and then execute the modified MSI

Note: The properties inside the MSI file that are suffixed by “_REQ” (with an underscore before "REQ") are dynamically modified at the execution of the MSI file by an internal “apply typical property” script.

Changing the values of those "_REQ" properties will have no effect.