citrix

ICA Settings Reference

2015-04-19 05:22:07 UTC

© 2015 Citrix Systems, Inc. All rights reserved. Terms of Use | Trademarks | Privacy Statement

Contents

ICA Settings Reference

ChannelName

ChannelName

ClientAudio

AudioDevice	AudioHWSection	AudioInWakeOnInput	AudioOutWakeOnOutput
CommandAckThresh	ControlPollTime	ConverterSection	DataAckThresh
MaxDataBufferSize	MaxMicBufferSize	NumCommandBuffers	NumDataBuffers
PlaybackDelayThresh	VariantName		

ClientComm

COMAllowed	CommPollSize	CommPollWaitInc	CommPollWaitIncTime
CommPollWaitMax	CommPollWaitMin	CommWakeOnInput	MaxPort, WindowSize

ClientDrive

CDMReadOnly	DisableDrives	EnableAsyncWrites	EnableReadAhead
MaxOpenContext	MaxWindowSize	NativeDriveMapping	SFRAllowed

ClientPrinterPort

PrinterThreadPriority	PrintMaxRetry	WindowSize	WindowsPrinter

ClientPrinterQueue

PrinterResetTime	UnicodeEnabled	VSLAllowed	WindowSize
WindowsPrinter	WindowSize2		

Compress

DriverNameWin32

DefaultSerialConnection

DTR

Delegation

LockdownProfiles, RegionIdentification

Dynamic

AcceptURLType	Address	BUCC	Command
DesiredColor	DriverNameAlt	DriverNameAltWin32	DriverNameWin32
InitialProgram	LongCommandLine	Path	ProxyHost
RECD	RejectURLType	REWD	RtpAudioLowestPort
SessionSharingLaunchOnly	SSOnCredentialType	startIFDCD	startSCD
UseAlternateAddress	Username		

Encoding

InputEncoding

EncRC-5-0, EncRC-5-40, EncRC-5-56, and EncRC-5-128

DriverNameWin32

ICA 3.0

BufferLength	BufferLength2	DriverNameWin32	VirtualDriver
VirtualDriverEx			

Logging

LogConfigurationAccess, LogEvidence, LogFile

Ping

PingCount

PrelaunchApplication

State	Schedule	UserOverride

qwerty

LicenseType, startIFDCD

Server

Address	InitialProgram	ScalingWidth
AECD	IOBase	Schedule
AltProxyAutoConfigURL	KeyboardTimer	ScreenPercent
AltProxyBypassList	Launcher	SecureChannelProtocol
AltProxyHost	LaunchReference	SecurityTicket
AltProxyPassword	LocHttpBrowserAddress	SessionSharingKey
AltProxyType	LogFlush	SessionSharingName
AudioBandwidthLimit	LogonTicket	SmartcardRequired
AudioDuringDetach	LogonTicketType	SpeedScreenMMA
AUTHPassword	LongCommandLine	SpeedScreenMMAAudioEnabled
AUTHUserName	LPWD	SpeedScreenMMAMaxBufferThreshold
AutoLogonAllowed	LVBMode	SpeedScreenMMAMaximumBufferSize
BrowserProtocol	MouseTimer	SpeedScreenMMAMinBufferThreshold
BUCC	MSIEnabled	SpeedScreenMMASecondsToBuffer
CFDCD	NDS	SpeedScreenMMAVideoEnabled
ClearPassword	NRUserName	SSLCACert
ClientAudio	NRWD	SSLCertificateRevocationCheckPolicy
	Password	SSLCommonName
COCD	PersistentCacheEnabled	SSLEnable
ConnectionFriendlyName	pnStartSCD	SSLNoCACerts
DataBits	ProxyAuthenticationBasic	SSLProxyHost
DesiredColor	ProxyAuthenticationNTLM	SSOnCredentialType
DeviceName	ProxyAuthenticationPrompt	SSOnDetected
DisableCtrlAltDel	ProxyAutoConfigURL	startIFDCD
DisableMMMaximizeSupport	ProxyBypassList	startSCD
Domain	ProxyFallback	TRWD
DoNotUseDefaultCSL	ProxyFavorIEConnectionSetting	TWIEmulateSystray
EnableAudioInput	ProxyHost	TWIMode
EnableClientSelectiveTrust	ProxyPassword	TWISuppressZZEcho
EnableOSS	ProxyTimeout	TWITaskbarGroupingMode
EnableRtpAudio	ProxyUseDefault	UseAlternateAddress
EnableSessionSharing	ProxyUseFQDN	UseDefaultEncryption
EnableSessionSharingClient	ProxyUsername	UseLocalUserAndPassword
EnableSessionSharingHost	RECD	UseMRUBrowserPrefs
EncryptionLevelSession	REWD	Username

endIFDCD	RtpAudioHighestPort	VirtualChannels
FONTSMOOTHINGTYPE		WorkDirectory
FriendlyName	ScalingHeight	ZLAutoHiLimit
ICASOCKSProtocolVersion	ScalingHeight	ZLAutoLowLimit
ICASOCKSProxyHost	ScalingMode	ZLKeyboardMode
ICASOCKSProxyPortNumber	ScalingPercent	ZLMouseMode
InitialProgram		

Smartcard

BypassSmartcardDomain	BypassSmartcardPassword	BypassSmartcardUsername	PCSCCodePage
PCSCLibraryName	SmartcardRequired	Username	

TCP/IP

DefaultHttpBrowserAddress, DriverNameWin32, ICAPortNumber

Thinwire 3.0

DesiredColor	InstallColormap	PersistentCacheMinBitmap	PersistentCacheSize
Tw2CachePower	TW2StopwatchMinimum	TW2StopwatchScale	TWIFullScreenMode
WindowManagerMoveIgnored	WindowManagerMoveTimeout	WindowsCache	

Transport

BrowserRetry	BrowserTimeout	HttpBrowserAddress	OutBufCountClient
OutBufCountClient2	OutBufCountHost	OutBufCountHost2	OutBufLength

WFClient

AllowAudioInput	Hotkey1Shift	PNPDeviceAllowed
AllowVirtualDriverEx	Hotkey2Char	Port1
AllowVirtualDriverExLegacy	Hotkey2Shift	Port2
AltProxyAutoConfigURL	Hotkey3Char	POSDeviceAllowed
AltProxyBypassList	Hotkey3Shift	PrinterFlowControl
AltProxyHost	Hotkey4Char	ProxyAuthenticationBasic
AltProxyPassword	Hotkey4Shift	ProxyAuthenticationKerberos
AltProxyType	Hotkey5Char	ProxyAuthenticationNTLM
AlwaysSendPrintScreen	Hotkey5Shift	ProxyAuthenticationPrompt
AppendUsername	Hotkey6Char	ProxyAutoConfigURL
BrowserRetry	Hotkey6Shift	ProxyBypassList
BrowserTimeout	Hotkey7Char	ProxyFallback
CbChainInterval	Hotkey7Shift	ProxyFavorIEConnectionSetting
CDMAllowed	Hotkey8Char	ProxyHost
CGPAddress	Hotkey8Shift	ProxyPassword
ClientName	Hotkey9Char	ProxyPort
ClipboardAllowed	Hotkey9Shift	ProxyType
ColorMismatchPrompt_Have16_Want256	HotkeyJPN%dChar	ProxyUseFQDN
ColorMismatchPrompt_Have16M_Want256	HowManySkipRedrawPerPaletteChange	ReadersStatusPollPeriod
ColorMismatchPrompt_Have64K_Want256	ICAHttpBrowserAddress	RemoveICAFile
COMAllowed	ICAKeepAliveEnabled	ResMngrRunningPollPeriod
ContentRedirectionScheme	ICAKeepAliveInterval	SecureChannelProtocol
CPMAllowed	ICAPrntScrnKey	SessionReliabilityTTL
CRBrowserAcceptURLtype	ICASOCKSProtocolVersion	SkipRedrawPerPaletteChange
CRBrowserCommand	ICASOCKSProxyHost	SmartCardAllowed
CRBrowserPath	ICASOCKSProxyPortNumber	SSLCertificateRevocationCheckPolicy
CRBrowserPercentS	KeyboardLayout	SSLCiphers
CRBrowserRejectURLtype	KeyboardSendLocale	SSLNoCACerts
CREnabled	KeyboardType	SSLProxyHost
CRPlayerAcceptURLtype	KeyboardTimer	SSOnCredentialType
CRPlayerCommand	LocalIME	SSOnUserSetting
CRPlayerPath	LogAppend	SSPIEnabled
CRPlayerPercentS	LogConnect	SucConnTimeout
CRPlayerRejectURLtype	LogErrors	SwapButtons
CustomConnectionsIconOff	LogFileGlobalPath	TransparentKeyPassthrough

DeferredUpdateMode	LogFileWin32	TransportReconnectDelay
DesiredColor	Lpt1	TransportReconnectEnabled
DisableSound	Lpt2	TransportReconnectRetries
DisableUPDOptimizationFlag	Lpt3	TransportSilentDisconnect
DynamicCDM	LVBMode	TwainAllowed
EmulateMiddleMouseButton	MinimizeOwnedWindows	TWIIgnoreWorkArea
EmulateMiddleMouseButtonDelay	MissedKeepaliveWarningMsg	TWISeamlessFlag
EnableInputLanguageToggle	MissedKeepaliveWarningTime	TWIShrinkWorkArea
EnableSessionSharingHost	MouseWheelMapping	UseAlternateAddress
EnableSSOnThruICAFile	PassThroughLogoff	UsersShareIniFiles
FastIdlePollDelay	PercentS	VirtualCOMPortEmulation
ForceLVBMode	PersistentCacheGlobalPath	VSLAllowed
FullScreenBehindLocalTaskbar	PersistentCacheMinBitmap	Win32FavorRetainedPrinterSettings
FullScreenOnly	PersistentCachePath	WpadHost
Hotkey10Char	PersistentCachePercent	XmlAddressResolutionType
Hotkey10Shift	PersistentCacheSize	ZLDiskCacheSize
Hotkey1Char	PersistentCacheUsrRelPath	ZLFntMemCacheSize

AcceptURLType

Specifies the acceptable URL types for the Content Redirection scheme.

Section	Dynamic
Feature	ContentRedirection
Attribute Name	INI_CR_ACCEPT_URL_TYPE
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	None rejected - Default
http	
https	

INI Location

N/A

Registry Location

N/A

Address(2)

Address of the target server.

Gives application server host name. It is also used to check whether it is a dialup or lan connection. For TCP/IP connections, this can be the DNS name of a XenApp server, the IP address of a XenApp server, or the name of a published application.

Section	Server,dynamic
Feature	Misc
Attribute Name	INI_ADDRESS
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	DNS name or IP Address of a Citrix server - Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	
Module.ini	TCP/IP - FTP	
Module.ini	TCP/IP - Novell Lan WorkPlace	
Module.ini	TCP/IP - Microsoft	
Module.ini	TCP/IP - VSL	
All_Regions.ini	Network\Protocols	
canonicalization.ini	TCP/IP	Address

Registry Location

This key must be specified for .ica files.

Registry Key	Value

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\TCP/IP	Address
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - FTP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Microsoft	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Novell Lan WorkPlace	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - VSL	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	

AECD

End User Experience Monitoring APPLICATION_ENUM_CLIENT (AECD).

End User Experience Monitoring (EUEM) startup data. The time it takes to get the list of applications.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_AECD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

AllowAudioInput

Allows the audio input for client audio.

Gives a boolean value specifying whether audio input is allowed or not.

Note: UNIX specific implemenation.

Section	WFClient
Feature	Audio
Attribute Name	INI_ALLOWAUDIOINPUT
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
False	Client audio input is not allowed - Default
True	Client audio input is allowed

INI Location

N/A

Registry Location

N/A

AllowVirtualDriverEx

Allows third party virtual Driver Extention.

Used to check whether virtual driver extension is allowed and if yes, appends third party virtual channels.

To append a third-party virtual channel list to current virtual drivers, set AllowVirtualDriverEx to TRUE.

Section	WFClient
Feature	Core
Attribute Name	INI_ALLOW_VIRTUALDRIVER_THIRDPARTY
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Allows third-party virtual Driver Extention - Default
FALSE	Does not allow third-party virtual driver extention

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Third Party	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Third Party	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Third Party	*

AllowVirtualDriverExLegacy

Allows legacy third-party virtual drivers.

Specifies whether (TRUE) or not (FALSE) to load legacy third-party virtual driver.

If this is set, the client parses the INI_ICA30 section for value INI_VIRTUALDRIVER, which is a list of Virtual Drivers separated by commas; ICA client attempts to load each Virtual Driver in this list. In order to successfully load, the .ini file must contain a section name that matches the Virtual Driver, and has correct Virtual Driver entries in the section.

Section	WFClient
Feature	Core
Attribute Name	INI_ALLOW_VIRTUALDRIVER_THIRDPARTY_LEGACY
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Allow third-party legacy virtual drivers - Default
FALSE	Do not allow third-party legacy virtual drivers

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Third Party	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Third Party	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Third Party	*

AltProxyAutoConfigURL(2)

URLs for proxy auto detection script. Gives the URL (location) of proxy auto detection(.pac) script. Automatic Proxy Configuration is a proxy mode where the proxy configuration is described in a file, called a PAC (.pac) file.

It must be set if the value of "AltProxyType" is Script; otherwise, it is ignored.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client failover proxy settings > Proxy script URLs

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_ALTPROXYAUTOCONFIGURL
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	URL for proxy auto detection script - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	3
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

AltProxyBypassList(2)

List of servers that do not traverse the failover proxy.

Specifies a list of hosts for which to bypass proxy connections. For any proxy type, you can provide a list of servers that do not traverse the proxy. These should be placed in the "Bypass server list."

An asterisk (*) included in a host name acts as a wildcard (for example, *.widgets.com). Multiple hosts must be separated by a semicolon (;) or comma (,).

The bypass list can be up to 4096 characters. This parameter is ignored if the value of ProxyType is None or Auto.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client failover proxy settings > Bypass server list.

Section	WFClient, Server
Feature	Proxy
Attribute Name	INI_ALTPROXYBYPASSLIST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	List of hosts, seperated by semi-colon (;) or comma (,) - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

AltProxyHost(2)

Address of alternate (failover) proxy server.

Specifies the address of the proxy server. It is required if the value of ProxyType is any of the following: Socks, SocksV4, SocksV5, Tunnel(Secure); otherwise, ProxyHost is ignored.

To indicate a port number other than 1080 (default for SOCKS) or 8080 (default for Secure), append the appropriate port number to the value after a colon (:).

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client failover proxy settings > Proxy host names

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_ALTPROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Proxy Server Address - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

AltProxyPassword(2)

Failover proxy server password for user. Holds the clear text password to be used to automatically authenticate the client to the failover proxy.

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_ALTPROXYPASSWORD
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Prompt the user for the proxy password - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

AltProxyType(2)

Failover proxy type requested for connection.

Specifies what type of failover proxy server a host session uses. When AltProxyType = "Secure", the client contacts the proxy identified by the "AltProxyHost" and "AltProxyPort" settings. The negotiation protocol uses an "HTTP CONNECT" header request specifying the desired destination.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client failover proxy settings > Proxy types

Section	Server, WFClient
Feature	Proxy
Attribute Name	INI_ALTPROXYTYPE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
None	Use Direct Connection - Default
Auto	Auto Detect from Web browser
Tunnel (Secure)	
Wpad	
Socks	
Socks v4	
Socks v5	
Script	Interpret proxy auto-configuration script

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	
Trusted_Region.ini	Network\Proxy	Auto
Untrusted_Region.ini	Network\Proxy	Auto

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\Trusted Region\Lockdown\Network\Proxy	Auto
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\Untrusted Region\Lockdown\Network\Proxy	Auto
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

AlwaysSendPrintScreen

Turns on or off the " AlwaysSendPrintScreen" attrtibute in seamless application. By enabling the key, user can use the " Print Screen" key on the keyboard while an ICA session is running with seamless application.

Section	WFClient
Feature	Seamless
Attribute Name	INI_ALWAYSSENDPRNTSCRN
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Print Screen key cannot be used - Default
On	Print Screen key can be used

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Keyboard	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\	

AppendUsername

Specifies whether or not user can append user name to the window title bar. If the attribute is non zero, user can concatenate the user name with the regular text for the window title bar (very long window titles will be truncated).

Section	WFClient
Feature	CoreUI
Attribute Name	INI_APPEND_USERNAME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Do not append the username - Default
1	Add the username to the window title

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\GUI	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\GUI	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\GUI	

AudioBandwidthLimit

Specifies the audio bandwidth limit and, by extension, the audio quality for the connection. Higher audio quality requires more bandwidth. The bandwidth requirements for high quality audio might make this setting unsuitable for many deployments.

Corresponding UI Element:

For applicationsetname: SETTINGS dialog box > DEFALUT OPTION tab > SOUND QUALITY menu

For applicationservername: PROPERTIES dialog box > OPTIONS tab > SOUND QUALITY menu

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client audio settings.

Section	Server
Feature	Audio
Attribute Name	INI_AUDIOBANDWIDTHLIMIT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
1	Medium: 64 kilobits per second (network Connection) - Default
2	Low: 4 Kbps (serial Connection)
0	High : 1.4 megabits per second (Mbps)

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*

AudioDevice(2)

Specifies the output device when there is more than one audio device available. It should default to the name that is standard for each UNIX variant.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_AUDIODEVICE
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
/dev/dsp	For Linux, LinuxArm, or UCLinux - Default
/dev/audio	For Solaris, SolarisX86, or netbsd - Default
<none>	For any other platform - Default

INI Location

N/A

Registry Location

N/A

AudioDuringDetach

Specifies audio behavior when the ICO is detached from the page. Controls the audio behavior when a user navigates to a page with an ICA session, starts playing a wave file, and then navigates away.

If AudioDuringDetach is false and the ICO is detached from the page, the audio stops. If it is true, the audio continues even after the detach.

Section	Server
Feature	Audio
Attribute Name	INI_AUDIODURINGDETACH
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	The audio will stop when ICO is detached - Default
True	Audio will continue even after ICO is detached

INI Location

N/A

Registry Location

N/A

AudioHWSection

Used to locate the driver module in the [AudioConverter] section.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_AUDHW_SECTIONNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
AudioConverter	Default

INI Location

INI File	Section	Value
Module.ini	AudioConverter	AudioHardware
Module.ini	ClientAudio	AudioConverter

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\AudioConverter	AudioHardware
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	AudioConverter

AudioInWakeOnInput

Enable/Disable audio input. Audio is on when audio is detected on input channel.

Linux only platform.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_AUDIOIN_WAKE_ON_INPUT
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Enable audio input - Default
0	Disable audio input

INI Location

N/A

Registry Location

N/A

AudioOutWakeOnOutput

Enable/Disable audio output. Audio is enabled when audio is detected on output channel.

Linux only platform.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_AUDIOOUT_WAKE_ON_OUTPUT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Enable audio input - Default
0	Disable audio input

INI Location

N/A

Registry Location

N/A

AUTHPassword

Specifies SSL authorization password.

Section	Server
Feature	SSL
Attribute Name	INI_AUTHPASSWORD
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present, any valid string representing password for authentication - Default

INI Location

N/A

Registry Location

N/A

AUTHUserName

Specifies the SSL authorization username.

Section	Server
Feature	SSL
Attribute Name	INI_AUTHUSERNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present, the valid string representing username for authentication - Default

INI Location

N/A

Registry Location

N/A

AutoLogonAllowed

Specifies whether or not autologon is allowed for Secure ICA client; specifies whether (Off) or not (On) to require users to enter their user name, domain name, and password when connecting using encryption levels greater than Basic. By default, users are required to enter this information, even if it is present in appsrv.ini.

Section	Server
Feature	SSL
Attribute Name	AUTOLOGON
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Does not allow autologon for secure ICA client - Default
TRUE	Allows autologon for secure ICA client

INI Location

INI File	Section	Value
All_Regions.ini	Login	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon	*

BrowserProtocol

Specifies the network protocol used for ICA browsing.

Value contains the borwser-s protocol to use of either HTTP on TCP or UDP.

Note: IPX, SPX, and NetBIOS are no longer supported.

Section	Server
Feature	EnumRes
Attribute Name	INI_BROWSEPROTOCOL
Data Type	String
Access Type	Read/Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
UDP	Default
HTTPonTCP	

INI Location

INI File	Section	Value
All_Regions.ini	Application Browsing	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	

BrowserRetry(2)

Specifies the number of times the ICA Client device will resubmit an ICA Master Browser request that has timed out.

Section	Transport,WFClient
Feature	EnumRes
Attribute Name	INI_BROWSERRETRY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3	Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	3
All_Regions.ini	Application Browsing	*
appsrv.ini	WFClient	3

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	3
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	*

BrowserTimeout(2)

Specifies the number of milliseconds the ICA Client will wait for a response after making a request to the ICA Master Browser.

Section	Transport,WFClient
Feature	EnumRes
Attribute Name	INI_BROWSERTIMEOUT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1000	Timeout (ms) - Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	1000
All_Regions.ini	Application Browsing	*
appsrv.ini	WFClient	1000

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	1000
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	*

BUCC(2)

The number of backup URL retries before success. This is one of the Session Client startup data while End User Experience Monitoring (EUEM) metrics are stored.

Note: This is the only start-up metric that is a count of attempts, rather than a duration.

Section	Server, Dynamic
Feature	EUEM
Attribute Name	INI_EUEM_BUCC
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Number of backup URL retries before success - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

BufferLength

Specifies the input buffer length in bytes for connections to MetaFrame XP, Feature Release 1 or earlier servers.

Section	ICA 3.0
Feature	Core
Attribute Name	INI_BUFFERLENGTH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
2048	Buffer Length (Bytes) - Default

INI Location

INI File	Section	Value
Module.ini	ICA 3.0	2048

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	2048

BufferLength2

Specifies the input buffer length in bytes for connections to MetaFrame XP, Feature Release 2 or later servers.

Section	ICA 3.0
Feature	Core
Attribute Name	INI_BUFFERLENGTH2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
5000	Buffer Length (Bytes) - Default

INI Location

INI File	Section	Value
Module.ini	ICA 3.0	5000

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	5000

BypassSmartcardDomain

Enable/Disable bypass switch for domain name. Specifies whether (FALSE) or not (TRUE) to use smartcard to get the domain name or get it from appsrv.ini file.

Section	Smartcard
Feature	Smartcard
Attribute Name	INI_DOMAINBYPASS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Does not bypass smartcard to get domain information - Default
True	Bypass smartcard for domain information

INI Location

N/A

Registry Location

N/A

BypassSmartcardPassword

Specifies whether (FALSE) or not (TRUE) to get password from smartcard.

Section	Smartcard
Feature	Smartcard
Attribute Name	INI_DOMAINBYPASS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Does not bypass smartcard to get user information - Default
True	Bypass smartcard for user information

INI Location

N/A

Registry Location

N/A

BypassSmartcardUsername

Specifies whether (FALSE) or not (TRUE) to use smartcard to get username or get it from appsrv.ini file.

Section	Server
Feature	Smartcard
Attribute Name	INI_USERNAMEBYPASS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Does not bypass smartcard to get user information - Default
True	Bypass smartcard for user information

INI Location

N/A

Registry Location

N/A

CbChainInterval

Specifies the number of milliseconds before testing if clipboard viewer chain is broken. Set to a positive number or to 0 to disable testing.

Copying content from the user device and pasting it in a published application failed. This issue was caused by a third party application that prevented the client from receiving notification when new content was copied to the local clipboard. This attribute introduces support for a mechanism to check at periodic intervals the client`s ability to receive clipboard change notifications. If the mechanism finds the client cannot receive the notifications, the client attempts to register itself to receive future notifications. To enable this functionality, add in appsrv.ini files as follows:

[WFClient]

CbChainInterval=<value>, where value is the interval, in milliseconds, at which checks are to be performed.

Section	WFClient
Feature	Clipboard
Attribute Name	INI_VCLIPBOARD_VIEWER_CHAIN_TEST_INTERVAL
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Disable testing - Default
2000	Minimum (ms)

INI Location

N/A

Registry Location

N/A

CDMAllowed

Specifies whether Client Drive Mapping is allowed or not.

ADM UI Element : Citrix Components > Citrix Receiver > Remoting client devices > Client drive mapping > Enable client drive mapping

Section	WFClient
Feature	CDM
Attribute Name	INI_CDMALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Allow Client Drive Mapping - Default
False	Do not allow Client Drive Mapping

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Drives	*
appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*

CDMReadOnly

Specifies that the CDM virtual channel permits read-only access to client drives.

ADM UI Element : Citrix Components > Citrix Receiver > Remoting client devices > Client drive mapping > Read-only client drives

Section	ClientDrive
Feature	CDM
Attribute Name	INI_CDMREADONLY
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
False	CDM is not read-only - Default
True	CDM is read-only

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Drives	*
Module.ini	ClientDrive	False
canonicalization.ini	ClientDrive	CDMReadOnly

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\ClientDrive	CDMRead Only
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	False
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*

CFDCD

Configuration File Download Client Duration (CFDCD) is the time it takes to get the configuration file from the XML server.

This is one of the Session Client startup data while End User Experience Monitoring (EUEM) metrics are stored.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_CFDCD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

CGPAddress

Specifies the CGP address. It is in "hostname:port" form. Rather than specifying the hostname, you can type an asterisk (*) to use the Address parameter value as the host (session reliability server).

The port value is optional. If you do not specify a port value, the default 2598 is used. If a connection on port 2598 fails, the client tries to establish a standard (non-session reliability) connection on port 1494.

Section	WFClient
Feature	CGP
Attribute Name	INI_CGPADDRESS
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present, some valid CGP address - Default
0.0.0.0	Bad CGP Address, use it as a marker for testing

INI Location

N/A

Registry Location

N/A

CGPSecurityTicket

Specifies whether (On) or not (Off) CGP security ticket is turned on. When CGPSecurityTicket is turned on, use CGP through SG.

Section	Server
Feature	CPG
Attribute Name	INI_CGPSECURITYTICKET
Data Type	inc\cgpini.h
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	CGP security ticket is turned off - Default
On	CGP security ticket is on

INI Location

INI File	Section	Value
All_Regions.ini	Network\CGP	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGPHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	*

ChannelName

Specifies a name for the static virtual channel to use for a specific DVC plug-in. By default the static channel name is automatically generated using the module file name of the DVC plug-in. To ensure that a unique name is generated, upon collision one or two digits can be used at the end of the name to make it unique while keeping the name length at a maximum of seven characters.

Section	ChannelName
Feature	DVC
Attribute Name	INI_DVC_PLUGIN_<DVC plugin name>
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
	Static virtual channel name

INI Location

INI File	Section	Value
Module.ini	[DVC_Plugin_<DVC plugin name>]	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\DVC_Plugin_<DVC plugin name>	*

ClearPassword

Specifies the clear password to automatically authenticate the client. It is a plain text password. It overrides the Password parameter, but it only overrides the Password parameter if the EncryptionLevel of Password is basic or the AutoLogonAllowed = On in the INI file.

Legacy Web Interface ticketing was implemented by passing a single-use authentication cookie to the server in the Clear Text password field.

ADM UI Element : Citirix Components > Citrix Receiver > User authentication > Web Interface authentication ticket > Legacy ticket handling

Section	Server
Feature	Core
Attribute Name	INI_CLEAR_PASSWORD
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Clear Password - Default

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Saved Credentials	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	

ClientAudio

Specifies whether (On) or not (Off) to enable client audio mapping.

Use this policy to control how sound effects and music produced by remote applications or desktops are directed to the client computer. When this policy is enabled, the "Enable audio" check box can be used to completely disable client audio mapping. This does not affect the client to server audio data, which is controlled through the "Remoting client devices" policy. It is also possible to control the audio quality.

Three quality levels are supported: low, medium, and high. This setting affects both server to client and client to server audio quality. Note that the bandwidth requirements for high quality audio could make this setting unsuitable for many deployments.

ADM UI Element : Citrix Components > Citrix Receiver > User experience > Client audio settings > Enable audio

Section	Server
Feature	Audio
Attribute Name	INI_CAM
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Off	Disables client audio mapping - Default
On	Enables client audio mapping

INI Location

INI File	Section	Value
Module.ini	VirtualDriver	
All_Regions.ini	Virtual Channels\Audio	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\VirtualDriver	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*

ClientName

Specifies the client name used to get serial number.

Clients prior to Version 6.30 store the client name in the [WFClient] section of wfcname.ini. As of Version 6.30, clients retrieve the client name from the system registry. As of Version 6.03 or later, any ClientName setting in wfcname.ini is used only for migrating the client name to the registry during client install; for example, when upgrading from or auto-updating a pre-Version 6.30 client.

The ClientName setting in the .ica file overrides the default way of retrieving the client name as described in Default Value.

Section	WFClient
Feature	Core
Attribute Name	INI_CLIENTNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Client name - Default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine	

ClipboardAllowed

Enable or disable access to the client clipboard. Use this policy to enable and restrict the remote application or desktop`s access to the client clipboard contents.

ADM UI Element: Citrix Components > Citrix Receiver > Remoting client devices > Clipboard > Enable/Disable

Section	WFClient
Feature	Clipboard
Attribute Name	INI_CLIPBOARDALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Enable access to clipboard - default
False	Disable access to clipboard

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Clipboard	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Clipboard	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Clipboard	*

COCD

End User Experience Monitoring (EUEM) COCD - CREDENTIALS_OBTENTION_CLIENT

The time it takes to get the user credentials. COCD is measured only when credentials are entered manually by the user.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_COCD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value - default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

ColorMismatchPrompt_Have16M_Want256

Specifies whether or not to display a warning if the client device's color depth is high color (16-bit) and the connection configuration is for 256 colors.

Section	WFClient
Feature	Core
Attribute Name	INI_HAVE16M_WANT256
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Enable device color depth warning display - default
Off	Disable device color depth warning display

INI Location

INI File	Section	Value
appsrv.ini	WFClient	On

Registry Location

N/A

ColorMismatchPrompt_Have16_Want256

Specifies whether or not to display a warning if the client device's color depth is 16 colors and the connection configuration is for 256 colors.

Not implemented in Program Neighborhood Client.

Section	WFClient
Feature	Core
Attribute Name	INI_HAVE16_WANT256
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Displays a warning message in case of color depth error - default
Off	Does not display a warning message in case of color depth error

INI Location

INI File	Section	Value
appsrv.ini	WFClient	On

Registry Location

N/A

ColorMismatchPrompt_Have64k_Want256

Specifies whether or not to display a warning if the client device's color depth is true color (32-bit) and the connection configuration is for 256 colors.

Not implemented in Program Neighborhood Client.

Section	WFClient
Feature	Core
Attribute Name	INI_HAVE64K_WANT256
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Displays a warning message in case of low color depth error - default
Off	Does not display a warning message in case of color depth error

INI Location

INI File	Section	Value
appsrv.ini	WFClient	On

Registry Location

N/A

COMAllowed(2)

Specifies whether or not COM port mapping is permitted.

Use this policy to enable and restrict the remote application or desktop`s access to the client’s serial ports. This allows the server to use locally attached hardware.

Troubleshooting: Remote PDA synchronization uses "virtual COM ports." These are serial port connections that are routed through USB connections. For this reason, it is necessary to enable serial port access to use PDA synchronization.

ADM UI Element: Citrix Components > Citrix Receiver > Remoting client devices > Client Hardware Access > Map Serial Ports

Section	WFClient,ClientComm
Feature	COMPortMapping
Attribute Name	INI_COMALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	COM Port mapping is permitted - default
Off	COM Port mapping is disabled

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Serial Port	*
appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Serial Port	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Serial Port	*

Command

Specify the command for Content Redirection.

This is the command that runs the executable used for server to client redirection. There is no default value for this attribute.

Section	dynamic
Feature	ContentRedirection
Attribute Name	INI_CR_CMD
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	Content Redirection Command - default

INI Location

N/A

Registry Location

N/A

CommandAckThresh

Command ACKs sent - threshold; the number of outstanding ACKs queued before a Command ACK is sent.

ACKs are sent in the following situations:

- The time since the last ACK was sent is at or above the delay threshold (time in milliseconds), OR
- The number of outstanding ACKs to be sent is at or above the threshold (Number of Command ACKs).

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_CMDACK_THRESH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Number of command ACKs sent threshold - default

INI Location

INI File	Section	Value
Module.ini	ClientAudio	1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	1

CommPollSize

Turns On or Off COM (communication) port polling for CCM (Citrix Client port Mapping).

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCMCOMMPOLLSIZE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Enable Com port polling (for wince) - default
Off	Disable com port polling (for any other

INI Location

INI File	Section	Value
Module.ini	ClientComm	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	On

CommPollWaitInc

Amount of time to slow down rate of COM polling. This setting is used to slow down the rate for polling of the COM port by the specified number of milliseconds.

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCMCOMMPOLLWAITINC
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	default

INI Location

INI File	Section	Value
Module.ini	ClientComm	1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	1

CommPollWaitIncTime

Specifies the number of times to poll the COM port at the current poll rate before slowing the poll rate by "CommPollWaitInc" milliseconds.

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCMCOMMPOLLWAITINCTIME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
20	default

INI Location

INI File	Section	Value
Module.ini	ClientComm	20

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	20

CommPollWaitMax

Specifies the maximum wait time (in milliseconds) for COM polling.

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCMCOMMPOLLWAITMAX
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
500	default

INI Location

INI File	Section	Value
Module.ini	ClientComm	500

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	500

CommPollWaitMin

Specifies the minimum wait time (in milliseconds) for COM polling.

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCMCOMMPOLLWAITMIN
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	1 millisecond timeout
0	No delay - default

INI Location

INI File	Section	Value
Module.ini	ClientComm	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	

CommWakeOnInput

This setting is used to wake the client upon COM port activity. Only used if pooling is allowed. These settings configure the client to be a bit more responsive to incoming serial port data and information.

Setting this parameter causes the Unix clients (Linux and Solaris) to wake-up immediately when the system receives a byte on a serial port.

Section	ClientComm
Feature	COMPortmapping
Attribute Name	INI_CCM_WAKE_ON_INPUT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Allows wake on input from a serial line - default
FALSE	Does not allow wake on input form a serial line

INI Location

N/A

Registry Location

N/A

ConnectionFriendlyName

Specifies the connection friendly name string for the server. This is the user-defined server name.

Section	Server
Feature	Core
Attribute Name	INI_CONNECTIONFRIENDLYNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Friendly name string for the server - default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\GUI	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\GUI	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\GUI	

ContentRedirectionScheme

Specifies the list of new schemes. Each scheme is added as new scheme.

This is done as a part of setting up Content Redirection for a Unix client.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_SCHEME
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	default

INI Location

N/A

Registry Location

N/A

ControlPollTime

This setting is used as a timer, in milliseconds, to poll client audio control values. If any control value changes, the new value is sent to the server.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_CONTROLPOLLTIME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1000	1 sec (1000 msec) - default

INI Location

N/A

Registry Location

N/A

ConverterSection

Audio converter list. Used to get the [AudioConverterList] section

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_AUDCVT_LIST_SECTIONNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
AudioConverterList	default

INI Location

INI File	Section	Value
Module.ini	AudioConverter	AudioConverterList

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\AudioConverter	AudioConverterList

CPMAllowed

Specifies whether (On) or not (Off) parallel port mapping is allowed. Enable and restrict the remote application or desktop`s access to the client's parallel ports. This allows the server to use locally attached hardware.

ADM UI Element: Citrix Component > Citrix Receiver > Remoting client devices > Client hardware access > Map parallel ports

Section	WFClient
Feature	ParallelPortMapping
Attribute Name	INI_CPMALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
true	Enable parallel port mapping - default
false	Disable parallel port mapping

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Printing	*
appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*

CRBrowserAcceptURLtype

Specify the acceptable browser URL types. Provides acceptable browser URL types for specific content redirection scheme.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_BROWSER_ACCEPT_URL
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
http, https	default
Browser	

INI Location

N/A

Registry Location

N/A

CRBrowserCommand

Name of the browser executable used to handle redirected browser URLs and it is appended with %s (for example, netscape %s).

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_BROWSER_CMD
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value			Description
$ICAROOT/util/nslaunch %s	${BROWSER:=netscape}%s	mozilla %s	default

INI Location

N/A

Registry Location

N/A

CRBrowserPath

Server to client content redirection browser path, that is, the directory where the browser executable is located.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_BROWSER_PATH
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	Browser path - default

INI Location

N/A

Registry Location

N/A

CRBrowserPercentS

The number of occurrences of %s in the CRBrowserCommand setting

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_N_BROWSER_PERCENT_S
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
3	default

INI Location

N/A

Registry Location

N/A

CRBrowserRejectURLtype

Specifies the browser URL types that should be rejected for the specific content redirection scheme.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_BROWSER_REJECT_URL
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	Browser URL to reject - default

INI Location

N/A

Registry Location

N/A

CREnabled

Specifies whether server to client content redirection is enabled.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
TRUE	Enable Content redirection - default
FALSE	Disable content redirection

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Control	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Control	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Control	*

CRPlayerAcceptURLtype

Specifies which types of strings are acceptable for RealPlayer Schemes for content redirection setting of the Unix client.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_PLAYER_ACCEPT_URL
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
"rtsp,rtspu,pnm"	default

INI Location

N/A

Registry Location

N/A

CRPlayerCommand

Specifies the name of the executable used to handle the redirected multimedia URLs, appended with %s during RealPlayer content redirection for the Unix client.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_PLAYER_CMD
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
realplay %s	default

INI Location

N/A

Registry Location

N/A

CRPlayerPath

Specifies the directory where the RealPlayer executable is located during content redirection for the Unix client.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_PLAYER_PATH
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	

INI Location

N/A

Registry Location

N/A

CRPlayerPercentS

The number of occurrences of %s in the CRPlayerCommand setting

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_N_PLAYER_PERCENT_S
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
1	default

INI Location

N/A

Registry Location

N/A

CRPlayerRejectURLtype

Specifies which type of strings will be rejected for RealPlayer Schemes for content redirection setting of the UNIX client.

The reason there is both an accept and reject is that the code that tests them matches just to the length of the definition. So if you accept HTTP, it also means that HTTPS will be accepted. In case you wanted only HTTP, there is the option to explicitly reject HTTPS.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_PLAYER_REJECT_URL
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
*	The type of string to reject for content redirection - No default value.

INI Location

N/A

Registry Location

N/A

DataAckThresh

Data acknowledgment threshold value, which represents the maximum number of command acknowledgments that can accumulate before sending an acknowledgment (purging the queue).

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_DATAACK_THRESH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Do not send any other command until you get the ack - default

INI Location

INI File	Section	Value
Module.ini	ClientAudio	1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	1

DataBits

Specifies the number of data bits used for serial connections.

Section	Server
Feature	SerialPort
Attribute Name	INI_DATA
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
8	Number of data bits for serial connection - default

INI Location

N/A

Registry Location

N/A

DefaultHttpBrowserAddress

Default HTTP browser address for TCP.

Section	TCP/IP
Feature	EnumRes
Attribute Name	INI_DEFHTTPBROWSERADDRESS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Default HTTP browser address - default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	

DeferredUpdateMode

Enables or disables deferred screen update mode.

Add this value and the ForceLVBMode value to the [WFClient] section of the Appsrv.ini file located in the user's profile directory to address repaint issues due to a poor refresh rate. This may occur with some applications when running the application in seamless mode while utilizing the pass-through client on the server.

Section	WFClient
Feature	Graphics
Attribute Name	INI_DEFERRED_UPDATE_MODE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Disable deferred screen updates - default
True	Enable deferred screen updates

INI Location

N/A

Registry Location

N/A

DesiredColor(5)

Specifies the preferred color depth for a session. In general, low color depths give better performance over low bandwidth; however some of the compression technologies available can only be used with full color, so the effective performance depends on the individual application and usage pattern. The server may choose not to honor the color depth setting chosen because higher color depths result in heavy memory usage on the servers.

256 or greater colors are supported only for Windows clients.

The value of 8 is treated as "true color" which is 32-bit, unless the administrator explicitly prohibits a server from supporting a 32-bit session. In that case, the session is downgraded to 24-bit.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client graphics settings > Color depth

Interface Element:

- For applicationsetname: Settings dialog box > Default Options tab > Window Properties > Window Colors menu
- For applicationservername: Properties dialog box > Options tab > Window Properties > Window Colors menu

Section	dynamic,WFClient,Thinwire3.0,Thinwire3.0,Server
Feature	Graphics
Attribute Name	INI_DESIREDCOLOR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
1	16 colors - default
2	256 colors
4	high color
8	true color

INI Location

INI File	Section	Value
Module.ini	Thinwire3.0	8
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
canonicalization.ini	Thinwire3.0	DesiredColor
wfclient.ini	Thinwire3.0	0x0002
appsrv.ini	WFClient	2

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	DesiredColor
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	8
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

DeviceName

Specifies the device name for serial connections (COM1, COM2, etc). If this value is not NULL, it is assumed that a serial port connection is being used. If this value is NULL (empty string), the network transport driver is used.

Section	Server
Feature	SerialPort
Attribute Name	INI_DEVICE
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
COM1	Name of COM port

INI Location

N/A

Registry Location

N/A

DisableCtrlAltDel

Enables (Off) or disables (On) the Ctrl+Alt+Del key combination within the ICA session to prevent users from shutting down the Citrix server.

ADM UI element: Citrix Components -> Presentation Server Client -> User Authentication -> Smartcard Authentication-> Passthrough Authentication for PIN

Section	Server
Feature	Keyboard
Attribute Name	INI_CTRLALTDEL
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	Disables the Ctrl+Alt+Del key combination - default
Off	Enables the Ctrl+Alt+Del key combination

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Smartcard	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	*

DisableDrives

Gives the list of the client drives that should not be mapped to the server.

Access to Windows drives can be disabled by entering the relevant drive letter in the "Do not map drives" box. This is a concatenation of all drives that should not be mapped when connecting to a published application or desktop, for example "ABFK" disables the drives A, B, F and K. (DisableDrives = "A,B,F,K")

ADM UI Element : Citrix Components > Citrix Receiver > Remoting client devices > Client drive mapping > Do not map drives

Section	ClientDrive
Feature	CDM
Attribute Name	INI_DISABLEDRIVES
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Client drives to map - default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Drives	
Module.ini	ClientDrive	
canonicalization.ini	ClientDrive	DisableDrives

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\ClientDrive	DisableDrives
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\VirtualChannels\Drives	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\VirtualChannels\Drives	

DisableMMMaximizeSupport

Enable/disable desktop maximize capability. This setting is used by monitor layout to disable maximize capability. MonitorLayout is the data that is sent to the server to describe the layout of the client`s desktop in a multi-monitor environment.

Section	Server
Feature	MultiMonitor
Attribute Name	INI_DISABLE_MAXIMIZE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Enables maximize capability - default
True	Disables maximize capability

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Seamless Windows	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*

DisableSound

Disables Windows alert sounds (the Windows "Asterisk" event). If client audio mapping is disabled with the ClientAudio parameter, this setting has no effect.

Section	WFClient
Feature	Audio
Attribute Name	INI_SOUND
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Enable windows alert sounds - default
On	Disable windows alert sounds

INI Location

INI File	Section	Value
appsrv.ini	WFClient	Off

Registry Location

N/A

DisableUPDOptimizationFlag

Disables the universal printer driver (UPD) bitmap compression (only) or both the compression and optimization.

When printing to certain printers using the UPD, letters might be printed faded and barely legible. The issue occurs because certain print drivers do not work well with XenApp UPD optimization, which compresses the bitmap to use fewer bits whenever possible.

To disable this optimization, modify the user's appsrv.ini file using a text editor and insert this parameter in the [WFClient] section.

Section	WFClient
Feature	Printing
Attribute Name	INI_UPD_OPTIMIZATION_DISABLE_FLAG
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Do not disable UPD compression and optimization - default
1	Disables bitmap compression, which attempts to use fewer bits to encode the bitmap
2	Disables optimization that skips spaces; it also disables bitmap compression

INI Location

N/A

Registry Location

N/A

Domain

XenApp domain name.

This is the domain name that appears in the Domain text box if the user selects the user-specified credentials option for the associated custom ICA connection.

"Domain" can be used to restrict or override which users can be automatically authenticated to servers. These can be specified as comma-separated lists.

Corresponding UI Element Properties dialog box > Logon Information tab > Userspecified credentials option > Domain text box

ADM UI Element: Citrix Components > Citrix Receiver > User Authentication > Locally Stored Credentials > Domain

Section	Server
Feature	Core
Attribute Name	INI_DOMAIN
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Domain name - default

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Saved Credentials	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	

DriverNameAlt

Specifies the name of the Unix/Mac alternate virtual driver.

Section	dynamic
Feature	Core
Attribute Name	INI_DRIVERNAMEALT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
DriverName	default

INI Location

N/A

Registry Location

N/A

DriverNameAltWin32

Specifies the name of the Win32 alternate virtual driver.

Section	dynamic
Feature	Core
Attribute Name	INI_DRIVERNAMEALT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
DriverNameWin32	default

INI Location

N/A

Registry Location

N/A

DriverNameWin32(12)

Specifies the name of the Win32 driver file to load for the specified driver. The driver could be one of the following. depending on the section name from where this attribute is being read.

- ClientAudio HW driver
- Transport driver
- TCP/IP transport driver
- ICA 3.0 Winstation driver
- ClientAudio driver
- Compress driver
- EncRC5-0 driver
- EncRC5-128 driver
- EncRC5-40 driver
- EncRC5-56 driver
- EncryptionLevelSession driver

Section	Compress,dynamic,EncRC5-56,EncRC5-40,EncRC5-128, EncRC5-0,dynamic,ICA 3.0,TCP/IP,dynamic,dynamic,dynamic
Feature	Core
Attribute Name	INI_DRIVERNAMEWIN32
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	For ClientAudio HW, Transport, TCP/IP, ICA 3.0, ClientAudio, EncryptionLevelSession drivers - default
pdcompn.dll	For Compress driver - default
pdc0n.dll	For EncRC5-0 driver - default
pdc128n.dll	For EncRC5-128 driver - default
pdc40n.dll	For EncRC5-40 driver - default
pdc56n.dll	For EncRC5-56 driver - default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	TDWSTCPN.DLL
Module.ini	ICA 3.0	WDICA30N.DLL
Module.ini	RFrame	PDRFRAMN.DLL
Module.ini	Frame	PDFRAMEN.DLL
Module.ini	Reliable	PDRELIN.DLL
Module.ini	EncRC5-0	PDC0N.DLL
Module.ini	Encrypt	PDCRYPTN.DLL
Module.ini	EncRC5-40	PDC40N.DLL
Module.ini	EncRC5-56	PDC56N.DLL
Module.ini	EncRC5-128	PDC128N.DLL
Module.ini	Thinwire3.0	VDTW30N.DLL
Module.ini	ClientDrive	VDCDM30N.DLL
Module.ini	ClientPrinterQueue	VDSPL30N.DLL
Module.ini	ClientPrinterPort	VDCPM30N.DLL
Module.ini	ClientComm	VDCOM30N.DLL
Module.ini	Clipboard	VDCLIPN.DLL
Module.ini	TWI	VDTWIN.DLL
Module.ini	ZL_FONT	VDFON30N.DLL
Module.ini	ZLC	VDZLCN.DLL
Module.ini	ICACTL	VDCTLN.DLL
Module.ini	LicenseHandler	VDLICN.DLL
Module.ini	ClientAudio	VDCAMN.DLL
Module.ini	AudioConverter	AUDCVTN.DLL
Module.ini	AudioHardware	AUDHALN.DLL
Module.ini	ConverterADPCM	ADPCM.DLL
Module.ini	SmartCard	VDSCARDN.DLL
Module.ini	Multimedia	VDMMN.DLL
Module.ini	SpeechMike	VDSPMIKE.DLL
Module.ini	TwainRdr	VDTWN.DLL
Module.ini	SSPI	VDSSPIN.DLL
Module.ini	UserExperience	VDEUEMN.DLL
Module.ini	Compress	PDCOMPN.DLL

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\AudioConverter	AUDCVTN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\AudioHardware	AUDHALN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	VDCAMN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	VDCOM30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	VDCDM30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	VDCPM30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	VDSPL30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Clipboard	VDCLIPN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Compress	PDCOMPN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ConverterADPCM	ADPCM.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\EncRC5-0	PDC0N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\EncRC5-128	PDC128N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\EncRC5-40	PDC40N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\EncRC5-56	PDC56N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Encrypt	PDCRYPTN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Frame	PDFRAMEN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	WDICA30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICACTL	VDCTLN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LicenseHandler	VDLICN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Multimedia	VDMMN.DLL

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Reliable	PDRELIN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\RFrame	PDRFRAMN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\SmartCard	VDSCARDN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\SpeechMike	VDSPMIKE.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\SSPI	VDSSPIN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	TDWSTCPN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	VDTW30N.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TwainRdr	VDTWN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI	VDTWIN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\UserExperience	VDEUEMN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ZLC	VDZLCN.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ZL_FONT	VDFON30N.DLL

DTR

Set the Default state of the COM port DTR.

Section	Default Serial Connection
Feature	COMPortMapping
Attribute Name	INI_DTR
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Set DTR ON by default - default
Off	Set DTR OFF by default

INI Location

INI File	Section	Value
Module.ini	Hardware Receive Flow Control	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Hardware Receive Flow Control	

DynamicCDM

Specifies whether Dynamic Client Drive Mapping is allowed or not. This setting enables or disables PnP support for USB thumb drives.

Section	WFClient
Feature	USB Thumb Drive Support
Attribute Name	INI_DYNAMIC_CDM
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
true	Dynamic Client Drive Mapping is allowed - default
false	Dynamic Client Drive Mapping is not allowed

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Drives	*
Appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*

EmulateMiddleMouseButton

Emulate middle mouse button on a system with a two-button mouse. This setting is used with EmulateMiddleMouseButtonDelay.

Section	WFClient
Feature	Mouse
Attribute Name	INI_EMULATE_MIDDLE_MOUSE_BUTTON
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Emulate middle mouse button - default
FALSE	Do not emulate middle mouse button (default for Win16)

INI Location

N/A

Registry Location

N/A

EmulateMiddleMouseButtonDelay

Specifies timer used in middle mouse button emulation. When middle-mouse button emulation is enabled (EmulateMiddleMouseButton set to True), holding left and right mouse buttons down together for the specified timeout emulates the pressing of the middle button.

Section	WFClient
Feature	Mouse
Attribute Name	INI_EMULATE_MIDDLE_MOUSE_BUTTON_DELAY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
100	Time in milliseconds.

INI Location

INI File	Section	Value
n/a		

Registry Location

Registry Key	Value
n/a	

EnableAsyncWrites

Section	ClientDrive
Feature	CDM
Attribute Name	INI_ENABLE_ASYNCWRITES
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Enable async disk write.
Off	Disable disk write.

INI Location

INI File	Section	Value
n/a		

Registry Location

Registry Key	Value
n/a	

EnableAudioInput

Enable access to audio capture devices. Use this policy to enable and restrict the remote application or desktop access to local audio capture devices (microphones).

ADM Interface Element: Remoting Client Devices->Client Microphone->Enable Client Microphone

Section	Server
Feature	Audio
Attribute Name	INI_AUDIOINPUTENABLE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Allow use of audio capture devices (microphone).
False	Disallow use of audio capture devices (microphone).

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Audio	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*

EnableClientSelectiveTrust

Enables Trusted Server Configuration.

Use this policy to control how the client identifies the published application or desktop to which it is connecting. The client determines a trust level, known as a trust region with a connection. The trust region then determines how the client is configured for the connection.

When this policy is enabled, the client can perform region identification by using the Enforce trusted server configuration option.

By default, region identification is based on the address of the server the client is connecting to. To be a member of the trusted region, the server must be a member of the Windows Trusted Sites zone. You can configure this using the Windows Internet Explorer > Internet Options > Trusted sites setting.

Alternatively, for compatibility with non-Windows clients, the server address can be specifically trusted using the Address setting. This is a comma-separated list of servers, which also supports the use of wildcards; for example, cps*.citrix.com.

ADM UI Element : Citrix Components > Citrix Receiver > Network Routing > Configure Trusted Server Configuration > Enforce Trusted Server Configuration

Section	Server
Feature	CST
Attribute Name	INI_CLIENTSELECTIVETRUST_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0	Default
1	

INI Location

INI File	Section	Value
All_Regions.ini	Network\ClientSelectiveTrust	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\ClientSelective	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\ClientSelectiveTrust	*

Troubleshooting

In the default configuration, when trusted server configuration prevents the client from connecting, the following error message is displayed:

```
<Server> ERROR: Cannot connect to the Citrix XenApp Server. The
server (xxx) is not trusted for ICA connections. Connections to the
(Untrusted Region) Region are not allowed by lockdown settings.
Please contact your administrator.
```

The server identified in the "xxx" must be added to the Windows Trusted Sites zone (as either http:// or https:// for SSL connections) for the connection to succeed.

For the SSL connections, add the certificate common name to the Windows Trusted Sites zone. For non-SSL connections, all servers that are contacted must be individually trusted. When using application browsing, include both the XML Service and the server it redirects to in the Windows Trusted Sites zone.

EnableInputLanguageToggle

Allows users to define and use hotkeys, such as the grave accent or the Ctrl + Shift key combination to switch between allowed input languages.

For Win32 only.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_INPUTLANGUAGETOGGLE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Disabled - Default
TRUE	Enabled

INI Location

N/A

Registry Location

N/A

EnableOSS

Specifies whether or not to enable Off Screen Surface (OSS). Enables the server to command the creation and use of X pixmaps for off-screen drawing.

Reduces bandwidth in 15 and 24-bit color at the expense of X server memory and processor time.

Section	Server
Feature	Graphics
Attribute Name	INI_ENABLE_OSS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Enable OSS - Default
FALSE	Disable OSS

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	

EnableReadAhead

Enables read-ahead for processing the request.

Memory-constrained clients may allocate less memory for this purpose. This attribute indicates whether drive mapping acceleration is supported or not.

Section	ClientDrive
Feature	CDM
Attribute Name	INI_ENABLE_READAHEAD
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Enable read-ahead - Default
FALSE	Disable read-ahead

INI Location

N/A

Registry Location

N/A

EnableRtpAudio

Enables or disables the real-time transport of audio over UDP.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client audio settings

Section	Server
Feature	Audio
Attribute Name	INI_RTPAUDIOENABLE
Definition Location	inc\icaini.h
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description	
TRUE	Enables Rtp Audio	Default
FALSE	Disables Rtp Audio	

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Audio	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	*

EnableSessionSharing

Use this policy to configure the client handling of remote applications. When enabled, this policy uses the list in the "Application" box to determine which published applications can be directly launched by the client.

You can request that remote applications share sessions (run in a single ICA connection). This provides a better user experience, but is sometimes not desirable. The session sharing feature can be disabled by clearing the "Session sharing" check box.

ADM UI Element : Citrix Components > Citrix Receiver > User experience > Remote applications

Section	Server
Feature	SessionSharing
Attribute Name	INI_ENABLE_SESSIONSHARING
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	Enable session sharing - Default
Off	Disable session sharing

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	*

Troubleshooting

Published applications are denoted by a # in front of the application name. Omitting the # symbol attempts to launch a particular program or desktop. A computer running XenApp will not allow this by default, and rejects the connection, displaying: "You do not have access to this session."

Session sharing is controlled by the SessionSharingKey that prevents applications launched from different Web Interface servers from sharing sessions. In addition, applications with different graphics or security settings are prevented from sharing sessions.

EnableSessionSharingClient

Enables or disables seamless applications to operate using the same session on the same terminal server.

Section	Server
Feature	SessionSharing
Attribute Name	INI_SESSION_SHARING_CLIENT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Disable session sharing - Default
TRUE	Enable session sharing

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	*

EnableSessionSharingHost(2)

Specifies whether or not to accept the session sharing requests from other ICA sessions on the same X display.

Section	WFClient, Server
Feature	SessionSharing
Attribute Name	INI_SESSION_SHARING_HOST
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Does not accept session sharing requests from other ICA session - Default
TRUE	Accepts session sharing requests from other ICA session

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	

EnableSSOThruICAFile

Specifies whether or not to use the same user name and password the user used to log on to the client device for authentication through .ica files. For security reasons, users cannot be authenticated to the server unless this parameter is present and its value set to On, even if UseLocalUserAndPassword and SSOnUserSetting are specified in the .ica file.

The EnableSSOnThruICAFile entry should be present in the APPSRV.INI file to respect the other SSON entries in the ICA File.

Used in three User Authentication policies in ADM file.

Smart card authentication: Use this policy to control how the client uses smart cards attached to the client device.

When enabled, this policy allows the remote server to access smart cards attached to the client device for authentication and other purposes. When disabled, the server cannot access smart cards attached to the client device.

ADM UI Element : Citrix Components > Citrix Receiver > User authentication > Smart card authentication > Use pass-through authentication for PIN

Kerberos authentication: Use this policy to control how the client uses Kerberos to authenticate the user to the remote application or desktop. When enabled, this policy allows the client to authenticate the user using the Kerberos protocol. Kerberos is a Domain Controller authorised authentication transaction that avoids the need to transmit the real user credential data to the server. When disabled, the client will not attempt Kerberos authentication.

ADM UI Element : Citrix Components > Citrix Receiver > User authentication > Kerberos authentication

Local user name and password: Use this policy to instruct the client to use the same logon credentials (pass-through authentication) for the XenApp server as the client machine. When this policy is enabled, the client can be prevented from using the current user's logon credentials to authenticate to the remote server by clearing the "Enable pass-through authentication" check box.

ADM UI Element : Citrix Components > Citrix Receiver > User authentication > Local user name and password

Section	WFClient
Feature	SSON
Attribute Name	INI_ENABLE_SSON_THRU_ICA_FILE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
FALSE	Do not use same user name and password - Default
TRUE	Use same user name and password
Off	Do not use same user name and password
On	Use same user name and password
0	Do not use same user name and password
1	Use same user name and password
no	Do not use same user name and password
yes	Use same user name and password

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Local Credentials	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*

EncryptionLevelSession

Specifies the encryption level of the ICA connection.

Section	Server
Feature	SecureICA
Attribute Name	INI_ENCRYPTIONLEVELSESSION
Data Type	String
Access Type	Read and write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Basic	Encryption level - Default
RC5 (128 bit - Logon Only)	Encryption level
RC5 (40-bit)	Encryption level
RC5 (56-bit)	Encryption level
RC5 (128 bit)	Encryption level

INI Location

INI File	Section	Value
All_Regions.ini	Network\Encryption	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Encryption	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Encryption	

endIFDCD

End User Experience Monitoring EUEM ENDIFDCD ICA File download.

ENDIFDCD the time at which the ICA file download was finished.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_ENDIFDCD
Data Type	Integer
Access Type	Read and write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Initial time value - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

FONTSMOOTHINGTYPE

Specifies the font smoothing type for the session. The value is only set at connection time whether it's a new connection or for a reconnect.

The Web plug-in and Receiver only set the value to client default or none.

Section	Server
Feature	FontSmoothing
Attribute Name	INI_FONTSMOOTHINGTYPE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Client default uses the user profile setting for font smoothing - Default
1	None

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
appsvr.ini	application/server	value

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

ForceLVBMode

Address repaint issues due to a poor refresh rate.

Add this value and the DeferredUpdateMode value to the [WFClient] section of the Appsrv.ini file located in the user's profile directory to address repaint issues due to a poor refresh rate. This may happen with some applications when running an application in seamless mode while utilizing the pass-through client on the server.

Section	WFClient
Feature	Graphics
Attribute Name	INI_FORCELVB_MODE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Do not force LVBMode - Default
1	Force LVBMode

INI Location

N/A

Registry Location

N/A

FriendlyName

Specifies user native language type (friendly name) for communication.

Section	Server
Feature	Core
Attribute Name	INI_FRIENDLYNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	User's language setting - Default

INI Location

N/A

Registry Location

N/A

FullScreenBehindLocalTaskbar

Allows you to enable true full screen mode for a WBT session. Used on WINCE platform.

Section	WFClient
Feature	Core
Attribute Name	INI_FULL_SCREEN_BEHIND_LOCAL_TASKBAR
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	ICA session is sized according to the size of the local taskbar - Default
TRUE	Full screen mode is enabled and the ICA session is behind the local taskbar

INI Location

N/A

Registry Location

N/A

FullScreenOnly

Specifies the default value for TransparentKeyPassthrough attribute.

When no TransparentKeyPassthrough setting in the ICA file is passed to the ICA Engine, the keyboard transparent feature behaves as if FullScreenOnly is set.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_TPKEYPASSTHRU_FULLSCRNONLY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3	Full Screen (default). Key combinations apply to non-seamless ICA sessions in full-screen mode.
2	Remote. Key combinations apply to seamless and non-seamless ICA sessions when their windows have the keyboard focus.
1	Local. Key combinations apply to the local desktop.

INI Location

INI File	Section	Value
Module.ini	TransparentKeyPassthrough	3

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TransparentKeyPassthrough	3

HotKey10Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey10 - Toggle Latency Reduction.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY10_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F10	Mac and UNIX platforms default
F5	Win32 platform default
1	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F5

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey10Shift

Specifies the keys to use for mapping hotkey sequence.

Along with Hotkey10Char, specifies the key combinations to use for the various hotkey sequences.

Hotkey10 is used for Toggle Latency Reduction action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY10_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Ctrl	Win32 platform default
Alt	WinCE platform default
Shift	
none	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Ctrl

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey1Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey1 is used for "Task List" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY1_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F1	Mac, UNIX, and Win32 platforms default
6	WinCE platform default
(none)	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
ESC	
minus	
plus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey1Shift

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey1 is used for "Task List" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY1_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Shift	Win32 platform default
Ctrl	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Shift

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey2Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey2 is used for Close Remote Application action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY2_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F2	Mac and UNIX platforms default
F3	Win32 platform default
2	WinCE platform default
(none)	
F1	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
ESC	
minus	
plus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F3

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey2Shift

Along with Hotkey2Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey2 is "Close Remote Application" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY2_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Shift	Win32 platform default
Ctrl	WinCE platform default
(none)	
Alt	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Shift

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey3Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey10 - Toggle Title Bar.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY3_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F3	Mac and UNIX platforms default
F2	Win32 platform default
3	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F2

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey3Shift

Along with Hotkey3Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey3 is "Toggle Title Bar" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY3_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Shift	Win32 platform default
Ctrl	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Shift

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey4Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey4 is "CTRL-ALT-DEL" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY4_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F4	Mac and UNIX platforms default
F1	Win32 platform default
4	WinCE platform default
(none)	
F2	
F3	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
ESC	
minus	
plus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey4Shift

Along with Hotkey4Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey4 is used for "CTRL-ALT-DEL" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY4_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Ctrl	Win32 and WinCE platforms default
Shift	
(none)	
Alt	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Ctrl

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey5Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey5 - CTRL-ESC.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY5_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F5	Mac and UNIX platforms default
F2	Win32 platform default
5	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F2

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey5Shift

Along with Hotkey5Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey5 is used for "CTRL-ESC" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY5_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Ctrl	Win32 and WinCE platforms default
Shift	
(none)	
Alt	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Ctrl

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey6Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey6 is used for "ALT-ESC" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY6_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F6	Mac and UNIX platforms default
F2	Win32 platform default
7	WinCE platform default
(none)	
F1	
F3	
F4	
F5	
F7	
F8	
F9	
F10	
F11	
F12	
ESC	
minus	
plus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F2

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey6Shift

Along with Hotkey6Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey6 - ALT-ESC

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY6_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Alt	Win32 platform default
Ctrl	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Alt

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey7Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey7 is used for "ALT-TAB" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY7_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F7	Mac and UNIX platforms default
plus	Win32 platform default
8	WinCE platform default
(none)	
F1	
F2	
F3	
F4	
F5	
F6	
F8	
F9	
F10	
F11	
F12	
ESC	
minus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	plus

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey7Shift

Along with Hotkey7Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey7 is used for "ALT-TAB" action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY7_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Alt	Win32 platform default
Ctrl	WinCE platform default
(none)	
Shift	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Alt

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey8Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey8 is used for ALT-BACKTAB action.

Corresponding UI element ICA Settings dialog box > Hotkeys tab > right menu column

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY8_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F8	Mac and UNIX platforms default
minus	Win32 platform default
9	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	minus

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey8Shift

Along with Hotkey8Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey8 is used for ALT-BACKTAB action.

Corresponding UI element ICA Settings dialog box > Hotkeys tab > right menu column

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY8_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Alt	Win32 platform default
Ctrl	WinCE platform default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Alt

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey9Char

Specifies the keys to use for mapping hotkey sequence.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey9 is used for CTRL-SHIFT-ESC action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY9_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
F9	Mac and UNIX platforms default
F3	Win32 platform default
1	WinCE platform default
(none)	
F1	
F2	
F4	
F5	
F6	
F7	
F8	
F10	
F11	
F12	
ESC	
minus	
plus	
star	
tab	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	F3

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKey9Shift

Along with Hotkey9Char, specifies the key combinations to use for the various hotkey sequences.

Each action is defined by a combination of a character and a shift state. To disable a particular hotkey, set both its character and shift state parameters to (none).

Hotkey9 is used for CTRL-SHIFT-ESC action.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEY9_SHIFT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Alt+Ctrl	Mac and UNIX platforms default
Ctrl	Win32 and WinCE platforms default
(none)	
Shift	
Alt	

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Hot Keys	
appsrv.ini	WFClient	Ctrl

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys	

HotKeyJPN%dChar

Specifies the hotkeyJPN I key.

Used to form a strings like HotkeyJPN1Char, HotkeyJPN2Char, HotkeyJPN3Char.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_HOTKEYJPN_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

N/A

INI Location

N/A

Registry Location

N/A

HowManySkipRedrawPerPaletteChange

Specifies the number of consecutive redraw requests to skip before redrawing the screen. See SkipRedrawPerPaletteChange for more information.

Section	WFClient
Feature	Graphics
Attribute Name	INI_NUMSKIPREDRAWPERPALETTECHANGE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
9	Number of times to skip redraw request - Default

INI Location

N/A

Registry Location

N/A

HttpBrowserAddress

Specifies the location of the browser used in conjunction with the particular network protocol specified for browsing in BrowserProtocol. If BrowserProtocol value is HTTPonTCP, then parameter used to locate the browser is HttpBrowserAddress or LocHttpBrowserAddress

Whether [Protocol]BrowserAddress or Loc[Protocol]BrowserAddress is used depends on the value of DoNotUseDefaultCSL.

- If DoNotUseDefaultCSL value is FALSE (default) then parameter used to locate the browser is [Protocol]BrowserAddress.
- If DoNotUseDefaultCSL value is TRUE then parameter used to locate the browser is Loc[Protocol]BrowserAddress (overriding any existing [Protocol]BrowserAddress settings).

Section : All [Protocol]BrowserAddress settings:

WFClient for all custom ICA connections unless otherwise overridden

Section : applicationsetname for each applicable published applicationset

Corresponding UI Element For applicationsetname:

Settings dialog box > Connection tab > Server Location >Network Protocol

Published application sets do not use Loc[Protocol]BrowserAddress

Section : All Loc[Protocol]BrowserAddress settings:

applicationservername for each custom ICA connection

Corresponding UI Element For applicationservername:

Properties dialog box > Connection tab > Server Location >Network Protocol

Section	Transport
Feature	EnumRes
Attribute Name	INI_HTTPBROWSERADDRESS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Any valid server name or address - Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	
All_Regions.ini	Application Browsing\HTTP Addresses	
canonicalization.ini	TCP/IP	HttpBrowser Address

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\TCP/IP	HttpBrowser Address
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing\HTTP Addresses	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing\HTTP Addresses	

ICAHttpBrowserAddress

Specifies the browser address. Used for HTTP or HTTPS browsing (BrowserProtocol=HTTPonTCP) if the browser address is not set through the HttpBrowserAddress or the Loc[Protocol]BrowserAddress parameters.

Section	Transport
Feature	EnumRes
Attribute Name	INI_ICADOMAINNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
ica	Any valid server name or address - Default

INI Location

INI File	Section	Value
All_Regions.ini	Application Browsing	
appsrv.ini	WFClient	ica

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing	

ICAKeepAliveEnabled

Use this parameter to notify users when inactive seamless applications are disconnected from the server under the following scenarios:

- Users are using a published application that displays dynamic information
- The client auto-reconnect feature is disabled
- Applications for users of multi-monitors are out of focus

If ICAKeepAliveEnabled is set to On, it enables a timer in the ICA Client Engine. This timer checks every N milliseconds (where N is set by ICAKeepAliveInterval) to determine if any data was sent by the server. If no data was sent, the timer pings the server, to which it expects a response after N milliseconds. If the server responds, the connection is still present. If there is no response or the ping request fails, the client displays an error message and the connection is terminated.

To enable this enhancement, add the following two values to the [WFClient] section of the Appsrv.ini file:

- ICAKeepAliveEnabled=On
- ICAKeepAliveInterval =<time in milliseconds for an ICA ping>

If the connection to the server goes down and these values were added to the Appsrv.ini file, the user receives an error message and the session terminates. The user must reconnect manually to the session.

Section	WFClient
Feature	Core
Attribute Name	INI_PING_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Disable ICA Keep Alive - Default
On	Enable ICA Keep Alive

INI Location

N/A

Registry Location

N/A

ICAKeepAliveInterval

Specifies the interval that is used for the ICAKeepAliveEnabled setting.

Section	WFClient
Feature	Core
Attribute Name	INI_PING_RETRY_INTERVAL
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
180000	milliseconds - Default
10000	milliseconds - UNIX platform default

INI Location

N/A

Registry Location

N/A

ICAPortNumber

Specifies the TCP port used for the ICA protocol. Change the port on all Citrix servers in the farm using the ICAPORT command-line utility before you change this parameter on clients.

Section	TCP/IP
Feature	Core
Attribute Name	INI_ICAPORTNUMBER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1494	TCP network port number - Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP - FTP	
Module.ini	TCP/IP - Novell Lan WorkPlace	
Module.ini	TCP/IP - Microsoft	
Module.ini	TCP/IP - VSL	
All_Regions.ini	Network\Protocols	
Module.ini	TCP/IP	1494
canonicalization.ini	TCP/IP	ICAPortNumber

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\TCP/IP	ICAPortNumber
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	1494
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - FTP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Microsoft	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Novell Lan WorkPlace	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - VSL	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	

ICAPrntScrnKey

Key mapping for the hotkey for PrntScrn.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_VK_PRNTSCRN_CHAR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Default

INI Location

N/A

Registry Location

N/A

ICASOCKSProtocolVersion(2)

Specifies which version of the SOCKS protocol to use for the connection.

If ICASOCKSProtocolVersion is set, the following parameters are used to specify SOCKS proxy settings:

- ICASOCKSProxyHost
- ICASOCKSPortNumber
- ICASOCKSrfc1929Password
- ICASOCKSrfc1929UserName
- ICASOCKSTimeout

Used only if ProxyType = ProxySocks.

Configure SOCKS proxy settings: Use to configure the use of additional SOCKS proxies required for some advanced network topologies.

When enabled, the client examines the "SOCKS protocol version" setting. If connection via SOCKS is not disabled, the client connects using the SOCKS proxy specified by the "Proxy host names" and "Proxy ports" settings.

The client supports connections using either SOCKS v4 or SOCKS v5 proxy servers. Alternatively, it can automatically detect the version being used by the proxy server.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure SOCKS proxy settings > SOCKS protocol version

Section	Server, WFClient
Feature	Proxy
Attribute Name	INI_SOCKSPROTOCOLVERSION
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
5	Use SOCKS version 5
5	Use SOCKS version 5
5	Use SOCKS version 5
5	Use SOCKS version 5

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	
appsrv.ini	WFClient	-1

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

Troubleshooting

The SOCKS proxy settings are designed for traversing a proxy in addition to the primary or alternative proxy server. When traversing only a single proxy, these SOCKS proxy settings should be disabled.

ICASOCKSProxyHost(2)

Specifies the DNS name or IP address of the SOCKS proxy to use.

Configure SOCKS proxy settings : Use this policy to configure the use of additional SOCKS proxies required for some advanced network topologies.

When enabled, the client examines the "SOCKS protocol version" setting. If connection via SOCKS is not disabled, the client connects using the SOCKS proxy specified by the "Proxy host names" and "Proxy ports" settings.

The client supports connections using either SOCKS v4 or SOCKS v5 proxy servers. Alternatively, it can automatically detect the version being used by the proxy server.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy > Configure SOCKS proxy settings > Proxy host names

Section	Server, WFClient
Feature	Proxy
Attribute Name	INI_SOCKSPROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	DNS name or IP address of proxy host

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	
appsrv.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

Troubleshooting

The SOCKS proxy settings are designed for traversing a proxy in addition to the primary or alternative proxy server. When traversing only a single proxy, these SOCKS proxy settings should be disabled.

ICASOCKSProxyPortNumber(2)

Specifies the port number of the SOCKS proxy server.

This parameter is deprecated by ProxyType, but maintained to ensure backward compatibility with older .ini/.ica files that do not contain ProxyType.

Use this policy to configure the use of additional SOCKS proxies that are required for some advanced network topologies.

When enabled, the client will examine the "SOCKS protocol version" setting. If connection via SOCKS is not disabled, the client will attempt to connect using the SOCKS proxy specified by the "Proxy host names" and "Proxy ports" settings.

The client supports connections using either SOCKS v4 or SOCKS v5 proxy servers. Alternatively, it can attempt to automatically detect the version being used by the proxy server.

ADM UI Element : Citrix Components > Citrix Receiver > Network routing > Proxy

Section	Server, WFClient
Feature	Proxy
Attribute Name	INI_SOCKSPROXYPORTNUMBER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
1080	Port number - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*
appsrv.ini	WFClient	1080

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

Troubleshooting

The SOCKS proxy settings are designed for traversing a proxy in addition to the primary or alternative proxy server. When traversing only a single proxy, these SOCKS proxy settings should be disabled.

InitialProgram

Specifies the initial program to start after establishing the associated custom ICA connection. For server connections, this is the full path and file name. For published applications, this is the name of the published application preceded by the pound (#) symbol. Omitting the # symbol attempts to launch a particular program or desktop. A computer running Citrix XenApp will not allow this by default, and rejects the connection, displaying: "You do not have access to this session."

This key must be specified for .ica files. InitialProgram takes initial app and also some parameters up to the length of a single INI line length.

Syntax: InitialProgram=#<AppName> <parameters> For example: InitialProgram=#Notepad “\\Client\V:\folder\file.txt”

If longer parameters have to be passed, then the following should be used:

- LongCommandLine=”…first part..” LongCommandLine000=”continuation”

In this case anything passed after InitialProgram is ignored.

Related Parameters: LongCommandLine

Corresponding UI Element: Properties dialog box > Application tab > Application text box

ADM UI Element: Citrix Receiver > User Experience > Remote Applications > Application

Section	Server
Feature	Core
Attribute Name	INI_INITIALPROGRAM
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Initial Program - Default

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Application Launching	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	

InitialProgram(2)

Specifies the initial program to start after establishing the associated custom ICA connection. For server connections, this is the full path and file name. For published applications, this is the name of the published application preceded by the pound (#) symbol. Omitting the # symbol attempts to launch a particular program or desktop. A computer running Citrix XenApp will not allow this by default, and rejects the connection, displaying: "You do not have access to this session."

This key must be specified for .ica files.

Related Parameters: LongCommandLine

Corresponding UI Element: Properties dialog box > Application tab > Application text box

ADM UI Element: Citrix Receiver > User Experience > Remote Applications > Application

Section	dynamic,Server
Feature	Core
Attribute Name	INI_INITIALPROGRAM
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Default	Initial program

INI Location

INI File	Section	Value
All_regions.ini	Client Engine\Application Launching	Not applicable

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	

InputEncoding

Describes the character encoding type of the .ica file. This information is used by the client to convert and understand the .ica file if the Web server that created it used an encoding type that is different from that of the the client.

Section	Encoding
Feature	Core
Attribute Name	INI_INPUT_ENCODING
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
ISO8859_1	Default
SJIS	
EUC-JP	
UTF8	

INI Location

Not applicable.

Registry Location

Not applicable.

InstallColormap

Force colormap installation on UNIX or AIX operating systems if the window has the override_redirect attribute. On UNIX or AIX operating systems, window managers install colormaps rather than having the client device do it. This does not occur if the window has the override_redirect attribute set. In this case installation of the colormap is explicitly forced.

Section	Thinwire3.0
Feature	Core
Attribute Name	INI_INSTALL_COLORMAP
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
TRUE	Default - Window colormap is forced
FALSE	Window colormap is not forced

INI Location

Not applicable.

Registry Location

Not applicable.

IOBase

Specifies the standard COM port I/O base address.

Section	Server
Feature	COMPortMapping
Attribute Name	INI_IOADDR
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Default	Default

INI Location

Not applicable.

Registry Location

Not applicable.

KeyboardLayout

Specifies the keyboard layout of the client device. The Citrix XenApp server uses the keyboard layout information to configure the ICA session for the client's keyboard layout. The default value causes the keyboard layout specified in the user profile to be used.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_KEYBOARDLAYOUT
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Default is user profile

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Keyboard	
wfclient.ini	WFClient	(User Profile)
appsrv.ini	WFClient	(User Profile)

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

KeyboardSendLocale

Send keyboard locale setting. Specifies whether to make the default input locale in an ICA session the same as the default input locale on the client operating system (Control Panel > Keyboard > Input Locales).

Section	WFClient
Feature	Keyboard
Attribute Name	INI_KEYBOARDSENDLOCALE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Default - Disable using the client operating system locale
On	Use the client operating system locale

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Keyboard	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

KeyboardTimer(2)

Specifies the amount of time, in milliseconds, the client queues keystrokes before passing them to the server. Use keystroke queueing if bandwidth limitations require a reduction of network traffic. Queuing reduces the number of network packets sent from the client to the server, but also reduces keyboard responsiveness during the session. Higher values improve performance when connecting over a RAS connection.

Section	Server, WFClient
Feature	Keyboard
Attribute Name	INI_KEYBOARDTIMER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - no delay
50	50 milliseconds (default for WinCE)

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Keyboard	
appsrv.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

KeyboardType

Specifies the keyboard type of the client device. The Citrix XenApp server uses this information to configure the ICA session for the client's keyboard type. Use the default value for most English and European keyboards. When using a Japanese keyboard, specifying the default auto-detects the correct keyboard type.

Section	Server, WFClient
Feature	Keyboard
Attribute Name	INI_KEYBRDTYPESECTION
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default - Auto-detect
IBM PC/XT or compatible keyboard	
101 Keyboard (Japanese)	
106 Keyboard (Japanese)	
NEC PC-9800 on PC98-NX (Japanese)	
NEC PC-9800 on PC98-NX 2 (Japanese)	
NEC PC-9800 Windows 95 and 98 (Japanese)	
NEC PC-9800 Windows NT (Japanese)	
Japanese Keyboard for 106n (Japanese)	
DEC LK411-JJ Keyboard (Japanese)	

DEC LK411-AJ Keyboard (Japanese)	

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Keyboard	
wfclient.ini	WFClient	(Default)
appsrv.ini	WFClient	(Default)

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

Launcher

Specifies the name of launch mechanism (that is, the client launcher name). This parameter is used to launch multiple ICA windows from the startup folder at logon time.

Section	Server
Feature	Core
Attribute Name	INI_LAUNCHER
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
ICA Client	Default - launch by using the ICA client
WI	Launch through the Web Interface
PN	Launch through Program Neighborhood client
PNAgent	Launch through Program Neighborhood agent
MSAM	Launch through the Metaframe Secure Access Manager
Custom	Launch through a custom client

INI Location

INI File	Section	Value
All_regions.ini	Client Engine\ICA File	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\ICA File	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\ICA File	

LaunchReference

Reference token for a specific session on a Citrix XenApp server.

Section	Server
Feature	Core
Attribute Name	INI_LAUNCHREFERENCE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default - Session Launch Token

INI Location

INI File	Section	Value
All_regions.ini	Client Engine\Application Launching	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	

LicenseType

Specifies the license type. If the user is an offline plug-in user but the requested application is an online application, then add "LicenseType=offline" to the file so that the Citrix XenApp server will request an offline license.

Section	qwerty
Feature	Core
Attribute Name	<LicenseType>
Data Type	String
Access Type	Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
offline	Default - an offline application license is requested
online	an online application license is requested

INI Location

Not applicable.

Registry Location

Not applicable.

LocalIME

Specifies if Local IME (Input Method Editor) is enabled. When local IME is enabled, keyevents that were processed by IME should be ignored.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_USE_LOCAL_IME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - disable local IME
1	Enable local IME

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Keyboard	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

LocHttpBrowserAddress

Specify the location of the browser used in conjunction with the HTTP specified for browsing in BrowserProtocol. If the value of DoNotUseDefaultCSL is = False (default) then the parameter used to locate the browser is HttpBrowserAddress. If DoNotUseDefaultCSL is = true then the parameter used to locate the browser is LocHttpBrowserAddress (overriding any existing HttpBrowserAddress settings).

For applicationsetname: Settings dialog box > Connection tab > Server Location > Network Protocol

For applicationservername: Properties dialog box > Connection tab > Server Location > Network Protocol

Section	Server
Feature	EnumRes
Attribute Name	INI_LOCHTTPBROWSERADDRESS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default - Location of HTTP Browser

INI Location

INI File	Section	Value
All_regions.ini	Application Browsing\HTTP Addresses	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing\HTTP Addresses	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing\HTTP Addresses	

LockdownProfiles

Specifies whether lockdown profiles should be read from the administrator location or user location. This is ignored if there is no administrator configuration. By default lockdown profiles are read from both locations, administrator and user.

Section	Delegation
Feature	ClientLockdown
Attribute Name	INI_DELEGATION_LOCKDOWNPROFILES
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
administrator	Read lockdown profiles from the administrator location
user	Read lockdown profiles from the user location
grouppolicy_machine	
grouppolicy_user	

INI Location

INI File	Section	Value
Module.ini	Delegation	administrator, user, grouppolicy_machine, grouppolicy_user

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Delegation	administrator, user, grouppolicy_machine, grouppolicy_user

LogAppend

Specifies file open mode for logs. Switches between appending new log file entries to the end of the existing log file (On) and creating a new file (Off). For 16-bit DOS client the existing log file is the value of "LogFile" attribute and for Win32 the existing log file is the value of "LogFileWin32" attribute. Applies only at start of session.

Section	WFClient
Feature	Core
Attribute Name	INI_LOGAPPEND
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Default - Creates a new log file and writes new log entries to it
TRUE	Append new log file entries to the end of the existing log file

INI Location

INI File	Section	Value
appsrv.ini	WFClient	Off

Registry Location

Not applicable.

LogConfigurationAccess

Enable or disable logging of configuration access.

Section	Logging
Feature	ConfigMgr
Attribute Name	INI_LOG_CONFIGURATION_ACCESS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Default
TRUE	

INI Location

INI File	Section	Value
Module.ini	Logging	False

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging	false

LogConnect

Enables or disables the logging of Citrix XenApp server connection status changes (connection and disconnection).

Section	WFClient
Feature	Core
Attribute Name	INI_LOGCONNECT
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Default - Logs connections to and disconnections from Citrix servers
FALSE	Does not log connections to and disconnections from Citrix servers

INI Location

INI File	Section	Value
appsrv.ini	WFClient	On

Registry Location

Not applicable.

LogErrors

Enables (On) or disables (Off) the logging of Citrix XenApp server connection errors.

Section	WFClient
Feature	Core
Attribute Name	INI_LOGERRORS
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
On	Default - Enables Citrix XenApp server connection error log
Off	Disables Citrix XenApp server connection error log

INI Location

INI File	Section	Value
appsrv.ini	WFClient	On

Registry Location

Not applicable.

LogEvidence

Specifies whether to return a location suitable for writing log entries. This is a log type, not an attribute for itself.

Section	Logging
Feature	Core
Attribute Name	INI_LOG_EVIDENCE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Default - No file to write log information.
TRUE	File location found to write log information

INI Location

INI File	Section	Value
Module.ini	Logging	False

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging	false

LogFile

Specifies the name of the Citrix XenApp plug-in log file. The log file is generated by the plug-in at run-time and is saved in the ICA Client directory. The types of details logged depends on the values of the LogConnect, LogErrors, LogReceive, and LogTransmit parameters.

Section	Logging
Feature	Core
Attribute Name	INI_LOG_File
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default - If present, then any valid file name.

INI Location

INI File	Section	Value
Module.ini	Logging	
appsrv.ini	WFClient	C:\Program Files\Citrix\ICA Client\wfclient.log

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging	

LogFileGlobalPath

Specifies how log files are created. If On, a single log file is used for all users of a given client device. LogFileWin32 must specify the entire directory path to the log file, including the file name. If Off, a separate log file is created for each user and stored in the user's profile directory. In this case, LogFileWin32 specifies the file name only.

Section	WFClient
Feature	Core
Attribute Name	INI_LOGFILEGLOBALPATH
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
off	Default - LogWinFile32 specifies the log file name only
on	LogFileWin32 specifies the entire directory path to the log file

INI Location

Not applicable.

Registry Location

Not applicable.

LogFileWin32

Specifiy the name of the log file. The types of details logged depends on the values of the LogConnect, LogErrors, LogReceive, and LogTransmit parameters. Log data can alternately be sent to standard out or standard error by specifying stdout or stderr instead of a file name.

If LogFileGlobalPath=On, a single log file is used for all users of a given client device. LogFileWin32 must specify the entire directory path to the log file, including the file name. If LogFileGlobalPath=Off, a separate log file is created for each user and stored in the user's profile directory. In this case, LogFileWin32 specifies the file name only.

Section	WFClient
Feature	Core
Attribute Name	INI_LOGFILE32
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Log file name.

INI Location

INI File	Section	Value
appsrv.ini	WFClient	

Registry Location

N/A

LogFlush

Specifies whether to flush out log results for each write. All the log data is written out as quickly as possible instead of being cached in memory. This ensures that the log file is completely up to date at any given moment.

When set to True, the system writes each log record as it is generated. When set to False, the system buffers log records and writes them periodically for optimal performance.

The log file location is specified in the registry at HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData.

Section	Server
Feature	Core
Attribute Name	INI_LOGFLUSH
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Default - Does not flush the log result
True	Flush out the log result

INI Location

Not applicable.

Registry Location

Not applicable.

LogonTicket

Specifies client authentication token for web interface. The client handles an authentication token in the form of an opaque LogonTicket with an associated interpretation defined by the LogonTicketType. This functionality can be disabled by clearing the Web Interface 4.5 and above check box.

ADM UI Element: Citrix Receiver > User Authentication > Web Interface Authentication ticket > Web interface 4.5 and above

Section	Server
Feature	Core
Attribute Name	INI_LOGONTICKET
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
" "	Default.

INI Location

INI File	Section	Value
All_regions.ini	Logon\Ticket	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Ticket	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Ticket	

LogonTicketType

Specifies the logon ticket type for "Web interface authentication ticket". Use this policy to control the ticketing infrastructure used when authenticating through the Web Interface. The client handles an authentication token in the form of an opaque LogonTicket with an associated interpretation defined by the LogonTicketType.

Section	Server
Feature	Core
Attribute Name	INI_LOGONTICKETTYPE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - no ticket
1	For Secure Ticketing Authority (STA) version 1 ticket
2	For STA version 4 ticket

INI Location

INI File	Section	Value
All_regions.ini	Logon\Ticket	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Ticket	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Ticket	

LongCommandLine

Allows passing of a very long string of parameters to the program specified in InitialProgram. The value of LongCommandLine replaces any command-line parameters specified at the end of InitialProgram.

To provide LongCommandLine support without breaking compatibility with older XenApp plug-ins, all lines in the .ica/.ini file must be limited to 255 characters. To support longer command lines, use a series of LongCommandLine parameters as follows:

LongCommandLine="The beginning of my long command line"

LongCommandLine000="continuation of my long command line"

LongCommandLine001="the rest of my long command line"

Each value must be in quotation marks ("") and must not exceed 224 characters. The ICA Client engine concatenates the values to create a single long command line parameter. You can include as many LongCommandLine parameters as necessary.

Section	dynamic, Server
Feature	Core
Attribute Name	INI_LONGPARAMETERS
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default

INI Location

INI File	Section	Value
All_regions.ini	Client Engine\Application Launching	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	

Lpt1

Specifies the mappping information between host lpt and client port. Both Lpt1 and Port1 together specify the mapping information between host lpt and client port. Connect this (1=lpt1...8=lpt8) host lpt to the client port specified by Port1. For example, Lpt1=4 means connect host lpt4 to client port specified by Port1. Lpt1=0 means no mapping information is specified by this attribute but some other attributes like Lpt2-Port2, Lpt3-Port3 may have this information.

Section	WFClient
Feature	ParallelportMapping
Attribute Name	INI_LPT1
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - No mapping is specified by this attribute.
1 through 8	Connect this host lpt to the client device port specified by Port11 entry

INI Location

Not applicable.

Registry Location

Not applicable.

Lpt2

Specifies the mappping information between host lpt and client port. Both Lpt2 and Port2 together specify the mapping information between host lpt and client port. Connect this (1=lpt1...8=lpt8) host lpt to the client port specified by Port2. For example, Lpt2=4 means connect host lpt4 to client port specified by Port2. Lpt2=0 means no mapping information is specified by this attribute but some other attributes like Lpt1-Port1, Lpt3-Port3 may have this information.

Section	WFClient
Feature	ParallelportMapping
Attribute Name	INI_LPT2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - No mapping is specified by this attribute.
1 through 8	Connect this host lpt to the client device port specified by Port2 entry

INI Location

Not applicable.

Registry Location

Not applicable.

Lpt3

Specifies the mappping information between host lpt and client port. Both Lpt3 and Port3 together specify the mapping information between host lpt and client port. Connect this (1=lpt1...8=lpt8) host lpt to the client port specified by Port3. For example, Lpt3=4 means connect host lpt4 to client port specified by Port3. Lpt3=0 means no mapping information is specified by this attribute but some other attributes like Lpt1-Port1, Lpt2-Port2 may have this information.

Section	WFClient
Feature	ParallelportMapping
Attribute Name	INI_LPT3
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - No mapping is specified by this attribute.
1 through 8	Connect this host lpt to the client device port specified by Port3 entry

INI Location

Not applicable.

Registry Location

Not applicable.

LPWD

End User Experience Monitoring EUEM LPWD - LAUNCH_PAGE_WEB_SERVER. The time it takes to process the launch page (launch.aspx) on the Web Interface server.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_LPWD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

LvbMode2

Enables or disables local video buffer (LVB) mode. For WINCE, the attribute is read from Server section.

Section	Server, WFClient
Feature	Graphics
Attribute Name	INI_LVB_MODE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Default - Turns LVB mode off
True	Turns LVB mode on

INI Location

Not applicable.

Registry Location

Not applicable.

MaxDataBufferSize

Set the maximum client audio data buffer size (that is, the size of the maximum client audio data packet the client can accept and/or send).

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_MAXDATABUFFERSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
2048	Default - value for maximum data buffer size for initial

INI Location

INI File	Section	Value
Module.ini	ClientAudio	2048

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	

MaxMicBufferSize

Set the maximum data buffer size for audio input (that is, the size of the maximum client audio input packet the client can accept and/or send).

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_MAXMICBUFFERSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
256	Default - value for maximum input buffer size
128-256	Value for maximum input buffer size

INI Location

INI File	Section	Value
Module.ini	ClientAudio	256

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	

MaxOpenContext

Specifies the number of files that can be opened on a client-mapped drive. "Out of file handles" message might be encountered when an application running on the server opens too many files on a client mapped drive and causes the ICA session to run out of file handles. The operating system does not provide the ICA Client engine sufficient file handles on request. This can be solved by increasing the number of initial file handles available to the Client by adding the MaxOpenContext parameter to the [ClientDrive] section in the MODULE.INI file . If the user needs to open a large number of files, increase the number of initial file handles to 50 or greater. The default value for MaxOpenContext is 20.

Section	ClientDrive
Feature	CDM
Attribute Name	INI_MAXOPENCONTEXT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
20	Default - Number of initial file handles available to the client

INI Location

Not applicable.

Registry Location

Not applicable.

MaxPort

Specify the maximum number of COM ports supported by the client platform.

Section	ClientComm
Feature	COMPortMapping
Attribute Name	INI_CCMMAXPORT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
5	Default

INI Location

Not applicable.

Registry Location

Not applicable.

MaxWindowSize

Set the maximum write window size (in bytes) for flow management (that is, the maximum number of bytes writeable for the ClientDrive section).

Section	ClientDrive
Feature	CDM
Attribute Name	INI_MAXWINDOWSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
6276	Default - value for maximum write window size

INI Location

INI File	Section	Value
Module.ini	ClientDrive	8650
Module.ini	ClientPrinterPort	2048
Module.ini	ClientPrinterQueue	8650

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	8650
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	2048
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	8650

MinimizeOwnedWindows

Specify whether all child windows are minimized when the parent window is minimized.

Section	WFClient
Feature	Core
Attribute Name	INI_MINIMIZE_OWNED_WINDOWS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - disable minimize
1	Enable minimize

INI Location

Not applicable.

Registry Location

Not applicable.

MissedKeepaliveWarningMsg

Specify the message displayed when the keep-alive time has expired. It will display according to the amount of time in seconds defined in MissedKeepaliveWarningTime.

Section	WFClient
Feature	CGP
Attribute Name	INI_CGP_WARNMESSAGE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default - Keep Alive Expiration Message

INI Location

INI File	Section	Value
All_regions.ini	Network\CGP	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	

MissedKeepaliveWarningTime

Specify the number of seconds to display the message defined in MissedKeepaliveWarningMsg after the keep-alive time has expired.

Section	WFClient
Feature	CGP
Attribute Name	INI_CGP_WARNTIME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - off.
1 through 60	Amount of time in seconds to display the message. Maximum value is 60.

INI Location

INI File	Section	Value
All_regions.ini	Network\CGP	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	

MouseTimer

Specifies the amount of time, in milliseconds, the client queues mouse events before passing them to the server. Use mouse event queueing if bandwidth limitations require a reduction of network traffic. Queuing reduces the number of network packets sent from the client to the server, but also reduces responsiveness to mouse movements during the session. Higher values improve performance when connecting over a RAS connection.

It is also read from the following sections:

- Thinwire 3.0 (if the operating environment is WinCE). In WinCE, the setting for queuing the mouse events is not in the UI, so it mustbe set in module.ini. As an internet client, it does not have access to the WFClient section of the module.ini file and is loaded it from the Thinwire section.
- WFClient (if the operating environment is other than WinCE)

Section	Server
Feature	Mouse
Attribute Name	INI_MOUSETIMER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default - off.
1 through 900	Amount of time in milliseconds to queue mouse events. Maximum value is 900.

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Mouse	
appsrv.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Mouse	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Mouse	

MouseWheelMapping

Specifies the mouse buttons whose down events are processed as mouse wheel motion. This attribute is considered as specific for MacIntosh/UNIX.

Section	WFClient
Feature	Mouse
Attribute Name	INI_MOUSEWHEELMAPPING
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
4,5	Default. mousewheelupmapping is assigned to button 4, mousewheeldownmapping is assigned to button 5.

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Mouse	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Mouse	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Mouse	

MSIEnabled

Allows Multi-Stream ICA connections. Use this setting to enable or disable the Multi-Stream ICA feature on the client.

Section	WFClient
Feature	Multi-Stream ICA
Attribute Name	INI_MSIENABLED
Definition Location	Client_Ini.h
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description	
TRUE	Allows Multi-Stream ICA connections.	Default
FALSE	Does not allow Multi-Stream ICA connections.	

INI Location

INI File	Section	Value
All_Regions.ini	NetWork\Multi-Stream	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Multi-Stream	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Multi-Stream	*

NativeDriveMapping

Specify the pass-through support for the network drive. Local or network drives configured on the server running Citrix XenApp can now be mapped by the pass-through client in a pass-through session by adding the following line to the [ClientDrive] section of the Module.ini file: NativeDriveMapping=TRUE.

When TRUE, the client drives on the client device are not mapped and are not available. The drives configured on the server are mapped and are available to the pass-through client.

Section	ClientDrive
Feature	CDM
Attribute Name	INI_CDMINCLUDENETWORKDRIVEINPASSTHRU
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Default. Native drive mapping is disabled.
TRUE	Native drive mapping is enabled.

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\Drives	*
Module.ini	ClientDrive	True
canonicalization.ini	ClientDrive	NativeDriveMapping

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\ClientDrive	NativeDriveMapping
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	TRUE
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*

NDS

Specifies a string representing the single sign-on credential type of NDS (for Novell Directory Service). Other credential types are NT and Any.

Section	Server
Feature	SSON
Attribute Name	INI_SSON_CREDENTIAL_NDS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
NDS	Default

INI Location

Not applicable.

Registry Location

Not applicable.

NRUserName

Indicates a string representing the user name for a XenApp farm connection. If Username or INI_USERNAME for custom connections is not found, NRUserName is retrieved.

Section	Server
Feature	Core
Attribute Name	INI_NR_USERNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
" "	Default

INI Location

Not applicable.

Registry Location

Not applicable.

NRWD

Name Resolution Web server Duration (NRWD) is the time it takes the XML Service to resolve the name of a published application to an IP address. This metric is only collected for new sessions, and only if the ICA file does not specify a connection to a Citrix XenApp server with the IP address already provided. This is one of the Session Client startup data while End User Experience Monitoring (EUEM) metrics are stored.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_NWRD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Default.

INI Location

INI File	Section	Value
All_regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	*

NumCommandBuffers

Set the maximum number of client audio command buffers.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_NUMCOMMANDBUFFERS
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
64	Default. Number of command buffers.

INI Location

INI File	Section	Value
Module.ini	ClientAudio	64

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	64

NumDataBuffers

Set the maximum number of client audio data buffers created.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_NUMDATABUFFERS
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
32	Default. Number of data buffers.

INI Location

INI File	Section	Value
Module.ini	ClientAudio	32

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	32

OutBufCountClient

Number of outbuffers allocated on client.

Section	Transport
Feature	Core
Attribute Name	INI_OUTBUFCOUNTCLIENT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
6	Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	6
Module.ini	TCP/IP – FTP	6
Module.ini	TCP/IP – Novell Lan WorkPlace	6
Module.ini	TCP/IP – Microsoft	6
Module.ini	TCP/IP – VSL	6

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Microsoft	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Novell Lan WorkPlace	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – VSL	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	6

OutBufCountClient2

Number of outbuffers on client for high throughput.

Used only when PD drivers (Protocol Drivers) supports any high-throughput in the server.

If high throughput is supported then certain drivers should switch to large sizing. For that, OutBufCountClient2 is used.

Section	Transport
Feature	Core
Attribute Name	INI_OUTBUFCOUNTCLIENT2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
42	Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	44
Module.ini	TCP/IP – FTP	44
Module.ini	TCP/IP – Novell Lan WorkPlace	44
Module.ini	TCP/IP – Microsoft	44
Module.ini	TCP/IP – VSL	44

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Microsoft	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Novell Lan WorkPlace	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – VSL	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	44

OutBufCountHost

Specifies the number of server output buffers to allocate.

Section	Transport
Feature	Core
Attribute Name	INI_OUTBUFCOUNTHOST
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
6	Default
12	

INI Location

INI File	Section	Value
Module.ini	TCP/IP	6
Module.ini	TCP/IP – FTP	6
Module.ini	TCP/IP – Novell Lan WorkPlace	6
Module.ini	TCP/IP – Microsoft	6
Module.ini	TCP/IP – VSL	6

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Microsoft	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Novell Lan WorkPlace	6
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – VSL	6

OutBufCountHost2

Specifies high performance server buffer count.

Used only when PD drivers (Protocol Drivers) supports any high-throughput in the server. If high throughput is supported then certain drivers should switch to large sizings. For that, OutBufCountHost2 is used.

Section	Transport
Feature	Core
Attribute Name	INI_OUTBUFCOUNTHOST2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
42	Default

INI Location

INI File	Section	Value
Module.ini	TCP/IP	44
Module.ini	TCP/IP – FTP	44
Module.ini	TCP/IP – Novell Lan WorkPlace	44
Module.ini	TCP/IP – Microsoft	44
Module.ini	TCP/IP – VSL	44

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Microsoft	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Novell Lan WorkPlace	44
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – VSL	44

OutBufLength

Specifies the size (in bytes) of the output buffer for transport driver.

Section	Transport
Feature	Core
Attribute Name	INI_OUTBUFLENGTH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1460	Default for WinCE
530	Default for Wany other platform

INI Location

INI File	Section	Value
Module.ini	TCP/IP	1460
Module.ini	TCP/IP – FTP	1460
Module.ini	TCP/IP – Novell Lan WorkPlace	1460
Module.ini	TCP/IP – Microsoft	1460
Module.ini	TCP/IP – VSL	1460

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	1460
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – FTP	1460
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Microsoft	1460
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – Novell Lan WorkPlace	1460
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP – VSL	1460

PassThroughLogoff

Enables and disables the posting of a logoff message.

Section	WFClient
Feature	Core
Attribute Name	INI_PASSTHROUGHLOGOFF
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

N/A

INI Location

INI File	Section	Value
All_Regions.ini		

Registry Location

N/A

Password

Specifies the encrypted password that appears in the Password text box if the user selects the User- specified credentials option for the associated custom ICA connection. Use "Locally stored credentials" policy to control how user credential data stored on user machines or placed in ICA files is used to authenticate the user to the remote published application or desktop. When this policy is enabled, you can prevent locally stored passwords from being automatically sent to remote servers by clearing the Allow authentication using locally stored credentials check box. This causes any password fields to be replaced with dummy data.

ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Locally stored credentials > Allow authentication using locally stored credentials

Section	Server
Feature	Core
Attribute Name	INI_PASSWORD
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
" "	Default - Any string representing a password

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Saved Credentials	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	
KEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	

Path

Specify the content redirection path for the executable used for server to client redirection.

Section	dynamic
Feature	FeatureRedirection
Attribute Name	INI_CR_PATH
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
" "	Content Redirection Path (no default path for this attribute)

INI Location

N/A

Registry Location

N/A

PCSCCodePage

Specifies smart card code-page identifier for an ANSI-based String encoding system.

Section	SmartCard
Feature	SmartCard
Attribute Name	INI_PCSC_CODEPAGE
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
0	Default. Code-page identifier value

INI Location

N/A

Registry Location

N/A

PCSCLibraryName

Specifies name of smart card`s dynamic link library name.

Section	SmartCard
Feature	SmartCard
Attribute Name	INI_PCSC_LIBRARY_NAME
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
libpcsclite .so	Default. Dynamic link library name.

INI Location

N/A

Registry Location

N/A

PercentS

Number of occurrences of % (percent signs) in the UNIX command settings used to handle redirected browser URLs.

Section	WFClient
Feature	ContentRedirection
Attribute Name	INI_CR_PERCENT_S
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
0	Default number of percent signs.

INI Location

N/A

Registry Location

N/A

PersistentCacheEnabled

Enables (On) or disables (Off) the persistent disk cache. The persistent disk cache stores commonly used graphical objects such as bitmaps on the hard disk of the client device. Using persistent disk cache increases performance across low-bandwidth connections but reduces the amount of available client disk space. For clients on high-speed LANs, using persistent disk cache is, therefore, not warranted. Disk caching is enabled by default for dial-in connections.

ADM UI Element : Citrix Components > Citrix Receiver > User experience > Client graphics settings > Disk-based caching

Interface Element

For published application sets: Settings dialog box > Default Options tab > Use disk cache for bitmaps option

For custom ICA connections: Properties dialog box > Options tab > Use disk cache for bitmaps option

For client devices with limited RAM, better compression rates can be achieved by saving temporary graphics objects to the disk cache.

Section	Server
Feature	Graphics
Attribute Name	INI_DIMCACHEENABLED
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0 or OFF	Default. Does not use persistent disk cache
1 or ON	Uses the persistent disk cache

INI Location

INI File	Section	Value
Module.ini	Thinwire3.0	OFF
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
appsrv.ini	WFClient	OFF
canonicalization.ini	Thinwire3.0	PersistentCacheEnabled

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	OFF
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	PersistentCacheEnabled

PersistentCacheGlobalPath

Specify the type of cache directory to use.

If On, a single cache directory is used for all users of a given client device. PersistentCachePath must specify the entire directory path to the cache directory, including the cache directory name.

If Off, a separate cache directory is created for each user and stored in the user`s profile directory. In this case, PersistentCachePath specifies the cache directory name only.

Note: This is a case sensitive string. Only the On string is verified; if the PersistentCacheEnabled value is "on" or "ON" then the "Off" value is the assumed default.

Section	WFClient
Feature	Graphics
Attribute Name	INI_DIMCACHEPATHGLOBAL
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Default. Disable single cache directory.
On	Enable single cache directory.

INI Location

N/A

Registry Location

N/A

PersistentCacheMinBitmap(2)

Sets the minimum size, in bytes, of a bitmap that is added to the persistent disk cache. Bitmaps that are too small will not be cached.

The persistent disk cache stores commonly used graphical objects such as bitmaps on the hard disk of the client device. Using persistent disk cache increases performance across low bandwidth connections but reduces the amount of available client disk space.

Section	WFClient,Thinwire3.0
Feature	Graphics
Attribute Name	INI_DIMMINBITMAP
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Size in bytes - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
Module.ini	Thinwire3.0	
canonicalization.ini	Thinwire3.0	PersistentCacheMinBitmap
appsrv.ini	WFClient	8192

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	PersistentCacheMinBitmap
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

PersistentCachePath

Specifies the location of the local directory containing the cached image data.

The PersistentCachePath entry specifies where the Cache folder will be created. Create the Cache folder under the user's profile under the hidden folder \Application Data\ICAClient\.

Section	WFClient
Feature	Graphics
Attribute Name	INI_DIMCACHEPATH
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Location of Persistent Disk Cache - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	
Module.ini	Thinwire3.0	
canonicalization.ini	Thinwire3.0	PersistentCachePath
appsrv.ini	WFClient	C:\Documents and Settings*userprofile name*\Application Data\ICAClient\Cache

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	PersistentCachePath
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	

PersistentCachePercent

Determines what percentage of disk drive to use for persistent cache.

Functionality is obsolete.

Section	WFClient
Feature	Graphics
Attribute Name	INI_DIMCACHEPERCENT_UI
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3	Percentage to use. (3%) - Default

INI Location

INI File	Section	Value
appsrv.ini	WFClient	

Registry Location

Registry information not found.

PersistentCacheSize(2)

Specifies the size of the persistent disk cache in bytes.

Section	WFClient,Thinwire3.0
Feature	Graphics
Attribute Name	INI_DIMCACHESIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Disk cache size in bytes. - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
Module.ini	Thinwire3.0	
canonicalization.ini	Thinwire3.0	PersistentCacheSize
appsrv.ini	WFClient	30000000

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	PersistentCacheSize
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

PersistentCacheUsrRelPath

Specifies the location of the persistent disk cache.

Used only if PersistentCacheGlobalPath = Off, a separate cache directory is created for each user and stored in the user's profile directory, and PersistentCachePath (location of the persistent disk cache) specifies the cache directory name only.

Section	WFClient
Feature	Graphics
Attribute Name	INI_DIMCACHEUSRPATH
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Cache Location - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

PingCount

Specifies the number of times to ping. It is a tunable parameter used by the Ping virtual channel.

CTXPING sends PingCount separate pings. Each ping consists of a BEGIN packet and an END packet.

Section	Ping
Feature	Ping
Attribute Name	INI_PING_PINGCOUNT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3	Pings - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

PlaybackDelayThresh

Delay, in milliseconds, between being asked to open audio device and actually opening it in order to build up a backlog of sound.

Section	ClientAudio
Feature	Audio
Attribute Name	INI_CAM_PLAYDELAY_THRESH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
250	Milliseconds - Default
0	Disable audio input

INI Location

INI File	Section	Value
Module.ini	ClientAudio	250

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio	250

PNPDeviceAllowed

Use this policy to enable and restrict the remote application or desktop's access to the client USB PNP devices.

ADM UI Element: Citrix Components > Citrix Receiver > Remoting client devices > USB PNP Devices

Section	WFClient
Feature	PlugNPlaySupport
Attribute Name	INI_DVC_PNPDEVICE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Allows USB PnP device redirection - Default
False	Does not allow USB PnP device redirection

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\PNPDeviceAllowed	*

Registry Location

Registry Key	Value
HKLM\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\DVC_PlugAndPlay\PNPDeviceAllowed	*

pnStartSCD

New session creation time, from the moment wfica32.exe is launched to when the connection is established.

This is one of the Session Client startup data while End User Experience Monitoring (EUEM) metrics are captured.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_PNSTARTSCD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

Port1

Specifies the mappping information between the host LPT and client port.

Both Port1 and Lpt1 together specify the mapping information between the host LPT and client port. Connect the host LPT specified by Lpt1 to this (1=lpt1,...,8=com4) client port. For example, if Port1=2, this means the host LPT specified by Lpt1 is connected to client port Lpt2. If Port1=0, this means no mapping information is specified by this attribute but some other attributes like Lpt2-Port2, Lpt3-Port3 may have this information.

Section	WFClient
Feature	ParallelPortMapping
Attribute Name	INI_PORT1
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	No mapping information specified by this attribute - Default
1-8	Connect the host lpt specified by Lpt1 to this client port

INI Location

INI information not found.

Registry Location

Registry information not found.

Port2

Specifies the mapping information between the host LPT and client port.

Both Port2 and Lpt2 together specify the mapping information between the host LPT and client port. Connect the host LPT specified by Lpt2 to this (1=lpt1,...,8=com4) client port. For example, if Port2=1, this means the host LPT specified by Lpt2 is connected to client port Lpt1. If Port2=0, this means no mapping information is specified by this attribute but some other attributes like Lpt1-Port1, Lpt3-Port3 may have this information.

Section	WFClient
Feature	ParallelPortMapping
Attribute Name	INI_PORT2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	No mapping information specified by this attribute - Default
1-8	Connect the host LPT specified by Lpt2 to this client port

INI Location

INI information not found.

Registry Location

Registry information not found.

POSDeviceAllowed

Use this policy to enable and restrict the remote application or desktop's access to the client USB POS devices. For this setting to work PNPDeviceAllowed should be set to allowed.

If PNPDeviceAllowed is set to disallowed, POS devices won't be available in the session, regardless of the POSDeviceAllowed value.

ADM UI Element : Citrix Components > Citrix Receiver > Remoting client devices > POS USB Devices

Section	WFClient
Feature	PlugNPlaySupport
Attribute Name	INI_DVC_POSDEVICE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Allows USB POS device redirection - Default
False	Does not allow USB POS device redirection

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\POSDeviceAllowed	*

Registry Location

Registry Key	Value
HKLM\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\DVC_PlugAndPlay\POSDeviceAllowed	*

PrinterFlowControl

Specifies whether flow control on a printer virtual channel is allowed.

Section	WFClient
Feature	Printing
Attribute Name	INI_CPM_FLOW_CONTROL
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Disables flow control - Default
True	Enable flow control

INI Location

INI information not found.

Registry Location

Registry information not found.

PrinterResetTime

Gives the amount of time (in milliseconds) that the client will wait for a printer to reset.

Section	ClientPrinterQueue
Feature	Printing
Attribute Name	INI_VSLPRINTERRESETTIME
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1100	Wait time (ms) - Default

INI Location

INI File	Section	Value
Module.ini	ClientPrinterPort	1100
Module.ini	ClientPrinterQueue	1100

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	1100
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	1100

PrinterThreadPriority

Specify the printer thread priority for CPM. Can be adjusted for performance.

Section	ClientPrinterPort
Feature	Printing
Attribute Name	INI_CPMPRINTERTHREADPRIORITY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Normal - Default
1	Above Normal
2	Highest
3	Time-critical

INI Location

INI information not found.

Registry Location

Registry information not found.

PrintMaxRetry

Specify the maximum number of times to retry printing.

The number of times to retry sending data to the printer when writing data to the printer fails and elicits an ambigous LastError. Attempts that result in specific errors, such as "Out of Paper," will not be retried.

Section	ClientPrinterPort
Feature	Printing
Attribute Name	INI_CPMPRINTMAXRETRY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default
1000	PrintMaxRetry variable

INI Location

INI information not found.

Registry Location

Registry information not found.

ProxyAuthenticationBasic(2)

Specifies whether or not the Basic authentication mechanism is allowed.

Configure proxy authentication: Use this policy to control the authentication mechanisms that the client uses when connecting to a proxy server. Authenticating proxy servers can be used to monitor data traffic in large network deployments.

In general, authentication is handled by the operating system but in some scenarios, the user may be provided with a specific user name and password. To prevent the user from being specifically prompted for these credentials, clear the Prompt user for credentials check box. This will force the client to attempt an anonymous connection. Alternatively, you can configure the client to connect using credentials passed to it by the Web Interface server, or these can be explicitly specified via Group Policy using the Explicit user name and Explicit password options.

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYAUTHBASIC
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Basic authentication mechanism is allowed - Default
False	Basic authentication mechanism is not enabled

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

Troubleshooting

In general, NTLM proxy authentication will be performed under the control of the domain controller and cannot be controlled by the client. Both client and proxy will need to be configured with the appropriate domain level trust relations.

Proxy authentication cannot be linked to the pass-through authentication feature of the client. In general, the proxy password will be unrelated to users' passwords.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure proxy authentication

ProxyAuthenticationKerberos

Specifies whether or not Kerberos authentication is allowed.

This is one of the authentication mechanisms that the client uses when connecting to a proxy server. Authenticating proxy servers can be used to monitor data traffic in large network deployments.

Kerberos is a domain controller authorized authentication transaction that avoids the need to transmit the real user credential data to the server.

Section	WFClient
Feature	Proxy
Attribute Name	INI_PROXYAUTHKERBEROS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Does not allow Kerberos authentication - Default
True	Allows Kerberos authentication

INI Location

INI information not found.

Registry Location

Registry information not found.

ProxyAuthenticationNTLM(2)

NT Lan Manager (NTLM) proxy authentication option.

NTLM proxy authentication will be performed under the control of the domain controller and cannot be controlled by the client. Both client and proxy will need to be configured with the appropriate domain level trust relations.

ADM UI Element: Citrix Components > Citrix Receiver > Network Routing > Proxy > Configure proxy authentication

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYAUTHNTLM
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	NTLM proxy authentication option is enabled - Default
False	NTLM proxy authentication option is not enabled

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyAuthenticationPrompt(2)

Specifies whether or not the Prompt proxy authentication mechanism is used.

Configure proxy authentication: Use this policy to control the authentication mechanisms that the client uses when connecting to a proxy server. Authenticating proxy servers can be used to monitor data traffic in large network deployments.

In general, authentication is handled by the operating system but in some scenarios, the user may be provided with a specific user name and password. To prevent the user from being specifically prompted for these credentials, clear the Prompt user for credentials check box. This will force the client to attempt an anonymous connection. Alternatively, you can configure the client to connect using credentials passed to it by the Web Interface server, or these can be explicitly specified via Group Policy using the Explicit user name and Explicit password options.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure proxy authentication > Prompt user for credentials

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYAUTHPROMPT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
True	Prompt proxy authentication mechanism is used - Default
False	Prompt proxy authentication mechanism is not used

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyAutoConfigURL(2)

Specifies the location of a proxy auto-detection (.pac) script. It must be set if the value of ProxyType is Script. Otherwise, it is ignored.

When ProxyType=*Script* is selected, the client will retrieve a JavaScript based .pac file from the URL specified in the Proxy script URLs policy option. The .pac file is executed to identify which proxy server should be used for the connection.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client proxy settings > Proxy script URLs

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYAUTOCONFIGURL
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	If present then any string giving location of a .pac script - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

ProxyBypassList

Specifies a list of hosts for which to bypass proxy connections. An asterisk (*) included in a host name acts as a wildcard (for example, *.widgets.com). Multiple hosts must be separated by a semicolon (;) or comma (,). This parameter is ignored if the value of ProxyType is None or Auto.

Configure client proxy settings: Use this policy to configure the primary network proxies that the client can use when connecting to a remote application or desktop.

When this policy is not configured, the client will use its own settings to decide whether to connect through a proxy server. When this policy is enabled, the client will use the proxy configured based on the proxy type selected. For any proxy type, you can provide a list of servers that do not traverse the proxy. These should be placed in the Bypass server list.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client proxy settings > Bypass server list

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYBYPASSLIST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Lists of hosts, separated by ";" or ","

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

ProxyFallback(2)

Allows clients to bypass the proxy to connect to servers.

If a Proxy Auto Configuration (PAC) file is used and the client is unable to download the PAC file, for example, due to the client's location, the client cannot connect to servers. Support for a proxy fallback has been added that allows clients to bypass the proxy to connect to servers.

To enable the fallback:

1. Open the Appsrv.ini file in a text editor.
2. Locate the DoNotUseDefaultCSL entry.
3. Perform one of the following actions:
   - If set to True, add the following parameter to the [applicationservername] and, if applicable, the [applicationsetname] sections:

     ProxyFallback=yes
   - If set to False, add the following parameter to the [WFClient] section:

     ProxyFallback=yes
4. Save your changes and close the file.

If both the primary and alternative proxy fail to service the connection, selecting the Failover to direct check box instructs the client to attempt a final direct connection with no proxies.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client failover proxy settings > Failover to direct

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYFALLBACK
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0	Not set - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyFavorIEConnectionSetting(2)

Specifies from where the client checks the proxy settings.

Use this setting when the client is used to connect to the Internet and has a proxy server setting set up for a LAN connection.

By default, the client checks the proxy settings for LAN connections. Setting this value to On causes the client to check the Internet Explorer connection settings for the proxy server information.

For the Windows CE platform, it will not be read from ini file and its value will be set to True. Otherwise, it will be read form the WFClient section. It is used when ProxyType is set to Auto.

Section	Server,WFClient
Feature	Proxy
Attribute Name	INI_PROXYFAVORIECONNECTIONSETTING
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
False	Client checks the Internet Explorer connection settings for the proxy server information - Default
True	Causes the client to check the Internet Explorer connection settings for

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyHost(3)

Specifies the address of the proxy server. It is required if ProxyType contains any of the following values:

- SOCKS
- SOCKS V4
- SOCKS V5
- Secure

ProxyHost is otherwise ignored.

To indicate a port number other than 1080 (default for SOCKS) or 8080 (default for Secure), append the appropriate port number to the value after a colon (:).

ADM UI Element: Citrix XenApp > Network Routing > Proxy > Configure client proxy settings

Section	WFClient,dynamic,Server
Feature	Proxy
Attribute Name	INI_PROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Proxy Server Address - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

ProxyPassword(2)

Holds the clear text password to be used to automatically authenticate the client to the proxy.

Use this policy to control the authentication mechanisms that the client uses when connecting to a proxy server. Authenticating proxy servers can be used to monitor data traffic in large network deployments.

In general, authentication is handled by the operating system but in some scenarios, the user may be provided with a specific user name and password. To prevent the user from being specifically prompted for these credentials, clear the Prompt user for credentials check box. This will force the client to attempt an anonymous connection. Alternatively, you can configure the client to connect using credentials passed to it by the Web Interface server, or these can be explicitly specified via Group Policy using the Explicit user name and Explicit password options.

Section	WFClient,Server
Feature	Proxy
Attribute Name	INI_PROXYPASSWORD
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Password - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

Troubleshooting

In general NTLM proxy authentication will be performed under the control of the domain controller and cannot be controlled by the client. Both client and proxy will need to be configured with the appropriate domain level trust relations.

Proxy authentication cannot be linked to the pass-through authentication feature of the client. In general, the proxy password will be unrelated to users' passwords.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure proxy authentication > Explicit password

ProxyPort

Identifies the port number for proxy support. The proxy port number must be a positive integer less than 65536. The port number depends on the proxy type.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client proxy settings > Proxy ports

Section	WFClient
Feature	Proxy
Attribute Name	INI_PROXYPORTNUMBER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0	Default
65536	Maximum Port Value

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyTimeout

Specifies the time, in milliseconds (ms), to wait for browsing requests through a proxy server to be satisfied.

Uses the value of BrowserTimeout, if specified. Otherwise, it uses the Web browser default timeout (2,000 ms).

Note: This value is ignored if it is less than the Web browser default timeout.

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYTIMEOUT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3000	Proxy timeout (ms) - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyType

Identifies the proxy type requested for the connection.

When AltProxyType = Secure, the client will contact the proxy identified by the AltProxyHost and AltProxyPort settings. The negotiation protocol will use a HTTP CONNECT header request specifying the desired destination.

Proxy type: None

When None is selected, the client will attempt to connect to the server directly without traversing a proxy server.

Proxy type: Auto

When Auto is selected, the client will use the local machine settings to determine which proxy server to use for a connection. This is usually the settings used by the Web browser installed on the machine.

Proxy type: Script

When Script is selected, the client will retrieve a JavaScript based .pac file from the URL specified in the Proxy script URLs policy option. The .pac file is executed to identify which proxy server should be used for the connection.

Proxy type: Secure

When Secure is selected, the client will contact the proxy identified by the Proxy host names and Proxy ports settings. The negotiation protocol will use a HTTP CONNECT header request specifying the desired destination address. This proxy protocol is commonly used for HTTP based traffic, and supports GSSAPI proxy authentication.

Proxy Type: SOCKS/SOCKS V4/SOCKS V5

When a SOCKS proxy is selected, the client will perform a SOCKS V4 or SOCKS V5 handshake to the proxy identified by the Proxy hostnames and Proxy ports settings. The SOCKS option will detect and use the correct version of SOCKS.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure client proxy settings > Proxy types

Section	WFClient
Feature	Proxy
Attribute Name	INI_PROXYTYPE
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
None	Use Direct connection - Default
Tunnel (Secure)	Use secure (HTTPS) proxy
Wpad	
Auto	Auto detect from Web browser
SOCKS	
SOCKS V4	
SOCKS V5	
Script	Interpret proxy auto-configuration script

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	
Trusted_Region.ini	Network\Proxy	Auto
Untrusted_Region.ini	Network\Proxy	Auto

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\Trusted Region\Lockdown\Network\Proxy	Auto
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\Untrusted Region\Lockdown\Network\Proxy	Auto
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

ProxyUseDefault

For UNIX and Macintosh, this parameter determines from which section the default proxy is chosen.

If set to True, the section is [WFClient]; otherwise, [serversection].

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYUSEDEFAULT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
True	Default proxy is chosen from WFClient - Default
False	Default proxy is chosen from serversection

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyUseFQDN

This setting is used in an environment that is set up to connect to applications through a proxy and Secure Gateway. If the proxy is configured to allow only FQDNs, when the client tries to connect to the applications, the proxy may reject the request.

This happens because the client resolves the Secure Gateway server name to the IP address before trying to connect to the server.

Setting this value to on ensures that the client does not try to resolve the Secure Gateway server name to an address but will instead send the name to the proxy. The client should be able to resolve the address and then connect to the Secure Gateway server through the proxy.

Section	Server,WFClient
Feature	Proxy
Attribute Name	INI_PROXYUSEFQDN
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
off	Client resolves the Secure Gateway server name to an address - Default
on	Client sends the server name to the proxy, which resolves the address

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	*

ProxyUsername

Holds the user name to be used to automatically authenticate the client to the proxy.

Use this policy to control the authentication mechanisms that the client uses when connecting to a proxy server. Authenticating proxy servers can be used to monitor data traffic in large network deployments.

In general, authentication is handled by the operating system but in some scenarios, the user may be provided with a specific user name and password. To prevent the user from being specifically prompted for these credentials, clear the Prompt user for credentials check box. This will force the client to attempt an anonymous connection. Alternatively, you can configure the client to connect using credentials passed to it by the Web Interface server, or these can be explicitly specified via Group Policy using the Explicit user name and Explicit password options.

Proxy authentication cannot be linked to the pass-through authentication feature of the client. In general, the proxy password will be unrelated to users' passwords.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Proxy > Configure proxy authentication >Explicit user name

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYUSERNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	User Name (prompt given) - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

ReadersStatusPollPeriod

Specifies the delay, in milliseconds, for reading information from a smart card after the card is inserted or removed, or a reader is disconnected, etc.

When inserting a smart card into the reader there is a two- to five-second delay before the information from the card is read. This delay occurs by design, but it is configurable. The client polls the card for events and the default value for this is five seconds.

Section	WFClient
Feature	SmartCard
Attribute Name	INI_READERS_STATUS_POLL_PERIOD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
500	For WinCE only - Default
5000	For any other platforms

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Smartcard	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	

RECD(2)

Reconnection Enumeration Client Duration (RECD) is the time it takes a client to get a list of reconnections.

This is one of the Session Client startup data while End User Experience Monitoring (EUEM) metrics are stored.

Section	Server,dynamic
Feature	EUEM
Attribute Name	INI_EUEM_RECD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

RegionIdentification

Specifies whether regions.ini should be read from the administrator location or user location. This is ignored if there is no administrator configuration. Regions.ini is used to perform region identification of client connections to servers.

Section	Delegation
Feature	ClientLockdown
Attribute Name	INI_DELEGATION_REGIONIDENTIFICATION
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
administrator	Default
user	

INI Location

INI File	Section	Value
All_Regions.ini	Delegation	administrator

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Delegation	administrator

Troubleshooting

Not applicable.

RejectURLType

Specifies URLs that are explicitly rejected for content redirection.

The reason there is both an accepturltype and a rejecturltype setting is that the code that tests them matches just to the length of the definition. So if you accept HTTP, it also means that HTTPS will also be accepted. In case you wanted only HTTP, there is the option to explicitly reject HTTPS.

Section	dynamic
Feature	ContentRedirection
Attribute Name	INI_CR_REJECT_URL_TYPE
Data Type	String
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
""	Reject URL

INI Location

INI information not found.

Registry Location

Registry information not found.

RemoveICAFile

Specifies whether or not the ICA file should be deleted after the session is finished.

Section	WFClient
Feature	Core
Attribute Name	INI_REMOVEICAFILE
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Does not remove ICA file - Default
On	Removes ICA file
True	Removes ICA file
False	Does not remove ICA file
yes	Removes ICA file
no	Does not remove ICA file
1	Removes ICA file
0	Does not remove ICA file

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\ICA File	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\ICA File	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\ICA File	*

ResMngrRunningPollPeriod

Specifies the time, in milliseconds, of polling for a restart of the Smart Card Resource Manager. Used only when there is an outstanding query for that Smart Card Resource Manager availability.

Used to create a timer for polling for a restart of the Smart Card Resource Manager.

Section	WFClient
Feature	SmartCard
Attribute Name	INI_RES_MNGR_RUNNING_POLL_PERIOD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
10000	Time in milliseconds - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Smartcard	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Smartcard	

REWD(2)

Specifies the time it takes Web Interface to get the list of reconnections from the XML Service. REWD stands for Reconnection Enumeration Web server Duration.

Section	dynamic,Server
Feature	EUEM
Attribute Name	INI_EUEM_REWD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

RtpAudioHighestPort

Specifies the highest UDP port that the client can attempt to use for transmission of Real-time Transport Protocol (RTP) audio.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client audio settings

Section	Server
Feature	Audio
Attribute Name	INI_RTPAUDIOHIGHESTPORT
Definition Location	inc\icaini.h
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
16509	Default Value

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Audio	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	RtpAudioHighestPort
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	RtpAudioHighestPort

RtpAudioLowestPort

Specifies the lowest UDP port that the client can attempt to use for transmission of Real-time Transport Protocol (RTP) audio.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client audio settings

Section	Dynamic, Server
Feature	Audio
Attribute Name	INI_RTPAUDIOLOWESTPORT
Definition Location	inc\icaini.h
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
16500	Default Value

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Audio	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	RtpAudioLowestPort
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Audio	RtpAudioLowestPort

ScalingHeight

Specifies the height of scaled window. This is one of the scaling properties (ScalingMode, ScalingPercent, ScalingHeight, and ScalingWidth) which is used to determine the initial "scaled"state of the session.

Only used when ScalingMode=2. ScalingMode=2 setting instructs ICO (ICA Client Object) to use the ScalingHeight and ScalingWidth properties. It ignores the ScalingPercent property. The width and height of the scaling area are checked against the size of the control window. The size cannot be bigger than the control window area. If the width and height is not less than the session size it means that scaling should not be enabled.

This property is the initial settings. Changes made to property during a connected session will not have any effect. When the session is established, use scaling methods to change the scaling attributes of the session.

Section	Server
Feature	Core
Attribute Name	INI_SCALING_HEIGHT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	No scaling - Default

INI Location

N/A

Registry Location

N/A

ScalingMode

Specifies the scaling mode that will be used for the initial connection. ScalingMode can be set to one of four possible initial states.

- 0 (Disabled): This is the default setting and means that scaling is not enabled at initialization.
- 1 (Percent): This setting instructs ICO to use the ScalingPercent property to determine the size of the scaling area. It ignores ScalingWidth and ScalingHeight. One hundred percent means that the area of the scaling is the same as the area of the control window. Fifty percent means that the scaling area is fifty percent of the control window.
- 2 (Size): This setting instructs ICO to use the ScalingHeight and ScalingWidth properties. It ignores the ScalingPercent property. The width and height of the scaling area are checked against the size of the control window. The size cannot be bigger than the control window area.
- 3 (To fit Window): This setting instructs ICO to fit the session into the existing control window. This is the easiest to do for a script because it forces the session to show its complete yet scaled area inside the control window.

This mode ignores the three other properties ScalingPercent, ScalingWidth, and ScalingHeight.

This property is the initial settings. Changes made to property during a connected session will not have any effect. When the session is established, use scaling methods to change the scaling attributes of the session.

Section	Server
Feature	Core
Attribute Name	INI_SCALING_MODE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Disabled - Default
1	Percent
2	Size
3	To fit window (autosize)

INI Location

N/A

Registry Location

N/A

ScalingPercent

Specifies scaling percentage to calculate the width and height of the ICA client`s window.

This setting instructs ICO to use the ScalingPercent property to determine the size of the scaling area. It ignores ScalingWidth and ScalingHeight. One hundred percent means that the area of the scaling is the same as the area of the control window. Fifty percent means that the scaling area is fifty percent of the control window.

This percentage should be between the minimum scaling percentage (10) and maximum scaling percentage (100).

Section	Server
Feature	Core
Attribute Name	INI_SCALING_PERCENT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
100	Maximum scaling (percent) - Default
10-99	Scaling (percent)

INI Location

N/A

Registry Location

N/A

ScalingWidth

Specifies the scaling factor to adjust Client window width. The purpose is to adjust the dimensions to fit the client LVB model. This is used only when ScalingMode=2.

It ignores the ScalingPercent property. The width and height of the scaling area are checked against the size of the control window. The size cannot be bigger than the control window area. So if the width and height is not less than the session size, scaling should not be enabled.

Section	Server
Feature	Core
Attribute Name	INI_SCALING_WIDTH
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
)	No scaling is done - Default
>= 0	Disable audio input

INI Location

N/A

Registry Location

N/A

Schedule

If the value for the application pre-launch setting State is 2 (pre-launch scheduled), use this setting to schedule the application session to prelaunch on specific days and times.

Section	PrelaunchApplication
Feature	Pre-Launch
Attribute Name	PRELAUNCH_TIME
Definition Location	prelaunch.h
Data Type	String
Access Type	Read/Write
UNIX Specific	No
Present in ADM	No

Values

The value specifies the time (in 24-hour format) and the days of the week for the application session to prelaunch.

HH:MM|M:T:W:Th:F:S:Su

HH:MM - Hours and Minutes in 24 hour format

M:T:W:Th:F:S:Su - Days of the week. A value of 1 to enable and 0 to disable.

Example:

08:30|1:1:1:1:1:0:0:0 - Enables Pre-Launch Monday through Thursday at 8:30 AM

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Prelaunch	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Prelaunch	

ScreenPercent

Specifies the size of the ICA session as a percentage of total screen size.

If DesiredWinType is set to 5, this parameter is used to specify the size of the ICA session as a percentage of total screen size.

Client Display Setting: Use this policy to control how the client presents remote applications and desktops to the end user. Remote applications can be seamlessly integrated with local applications, or the entire local environment can be replaced with a remote desktop.

Window Percent can be used as an alternative to manually choosing the width and height. It selects a window size as a fixed percentage of the entire screen. The server may choose to ignore this value. This setting is ignored when seamless windows is in use.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client display settings > Window percent

Section	Server
Feature	Core
Attribute Name	INI_SCREENPERCENT
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
75	Default screen size when the setting is enabled.
0	Disables the setting.
1-100	

INI Location

INI File	Section	Value
Module.ini	Thinwire3.0	
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
canonicalization.ini	Thinwire3.0	ScreenPercent
appsrv.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	ScreenPercent
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

SecureChannelProtocol(2)

Specifies which secure channel protocol to use.

Use this policy to configure the TLS/SSL options that help to ensure that the client connects to genuine remote applications and desktops. TLS and SSL encrypt the transferred data to prevent third-parties viewing or modifying the data traffic. Citrix recommends that any connections over untrusted networks use TLS/SSL or another encryption solution with at least the same level of protection.

When this policy is enabled, the client will apply these settings to all TLS/SSL connections performed by the client. The Require SSL for all connections check box can be used to force the client to use the TLS or SSL protocol for all connections that it performs.

TLS and SSL identify remote servers by the common name on the security certificate sent by the server during connection negotiation. Usually the common name is the DNS name of the server, for example www.citrix.com. It is possible to restrict the common names to which the client will connect by specifying a comma-separated list in the "Allowed SSL servers" setting. Note that a wildcard address, for example *.citrix.com:443 will match all common names that end with .citrix.com. The information contained in a certificate is guaranteed to be correct by the certificate`s issuer.

Some security policies have requirements related to the exact choice of cryptography used for a connection. By default the client will automatically select either TLS v1.0 or SSL v3.0 (with preference for TLS v1.0) depending on what the server supports. This can be restricted to only TLS v1.0 or SSL v3.0 using the "SSL/TLS version" setting.

Similarly, certain security policies have requirements relating to the cryptographic ciphersuites used for a connection. By default the client will automatically negotiate a suitable ciphersuite from the five listed below. If necessary, it is possible to restrict to just the ciphersuites in one of the two lists.

- Government Ciphersuites:
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- Commercial Ciphersuites:
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_RC4_128_MD5

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows security certificates to be revoked (invalidated before their expiry date) in the case of cryptographic compromise of the certificate private key, or simply an unexpected change in DNS name.

Valid CRLs must be downloaded periodically from the certificate issuer and stored locally. This can be controlled through the selection made in "CRL verification."

- Disabled: When selected, no CRL checking will be performed.
- Only check locally stored CRLs: When selected, any CRLs that have been previously installed or downloaded will be used in certificate validation. If a certificate is found to be revoked, the connection will fail.
- Retrieve CRLs from network: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail.
- Require CRLs for connection: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail. If the client is unable to retrieve a valid CRL, the connection will fail.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing

Section	WFClient,Server
Feature	SSL
Attribute Name	INI_SSLPROTOCOLS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Detect	Protocol value - Default
TLS	Protocol value
SSL	Protocol value

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	

Troubleshooting

Error Message: "SSL Error 61: You have not chosen to trust "<xxx>" the issuer of the server`s security certificate". The common name and other information on a security certificate is guaranteed to be accurate by the certificate`s issuer. For a connection to be successful, the client must trust the certificate`s issuer to make that guarantee.

Error Message: "SSL Error 59: The server sent a security certificate identifying `xxx`. The SSL connection was to `yyy`". The common name did not match the server the client was expecting to connect to.

SessionReliabilityTTL

Specifies the session reliability timeout in number of seconds. This attribute allows you to configure Session Reliability Time To Live (TTL).

Section	WFClient
Feature	SessionReliability
Attribute Name	INI_SESSIONRELIABILITY_TTL
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
180	Seconds - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\CGP	*
Module.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	3
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\CGP	*

SessionSharingKey

Specifies the session sharing key.

Session sharing key takes priority over all other checks. If it matches you share, if it does not you do not. It is up to the server to set the session sharing key correctly. Session sharing key is created from (Neighborhood Name, Color Depth, Username/Domain, Encryption Level, Audio BandWidth). If the key is not present, go through the old checks.

Section	Server
Feature	SessionSharing
Attribute Name	INI_SESSIONKEY_NAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
oLdWaY	Default
Off	Launch failed because session key is set to Off

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	

SessionSharingLaunchOnly

Specifies the name of the session to be shared.

Section	Server
Feature	SessionSharing
Attribute Name	INI_SESSION_SHARING_NAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present then any string representing the name of the session

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	

SFRAllowed

Specifies whether Special folder direction is allowed or not. If it is enabled, client sends the Desktop and Documents folder paths to the server side SFR as part of CDM VC data. SFR redirects the logged on user's document and desktop folders to client's document and desktop folders respectively.

Section	ClientDrive
Feature	SFR
Attribute Name	INI_SFRALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Off	Disables SFR - Default
On	Enables SFR

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\ Drives	*
Canonicalization.ini	ClientDrive	SFRAllowed
Module.ini	ClientDrive	FALSE

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive	FALSE
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Drives	*
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\ClientDrive	SFRALLOWED

SkipRedrawPerPaletteChange

Specifies whether (On) or not (Off) to skip redrawing the screen after a palette change. If this parameter is enabled, HowManySkipRedrawPerPaletteChange specifies how many palette changes are skipped before each redraw. Use this only as directed by Citrix Technical Support.

Section	WFClient
Feature	Graphics
Attribute Name	INI_SKIPREDRAWPERPALETTECHANGE
Data Type	Boolean
Access Type	Reed
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Does not skip redrawing the screen after a palette change - Default
1	Skips redrawing the screen after a palette change

INI Location

N/A

Registry Location

N/A

SmartCardAllowed

Specifies whether or not Smartcard virtual channel has been enabled.

When enabled, this policy allows the remote server to access smart cards attached to the client device for authentication and other purposes.

When disabled, the server cannot access smart cards attached to the client device.

ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Smart card authentication > Allow smart card authentication

Section	Smartcard,Server
Feature	SmartCard
Attribute Name	INI_SMARTCARDSWITCH
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Disable the requirement for a smart card. - Default
NO	Enable the requirement for a smart card.

INI Location

N/A

Registry Location

N/A

SpeedScreenMMA

Specifies whether(On) or not(Off) to enable the HDX MediaStream Multimedia Acceleration.

It is used to decide the default value of Tw2CachePower. If SpeedScreenMMA = On then Tw2CachePower = 19 else Tw2CachePower = 22.

Remote Video: The remote video option allows the server to directly stream certain video data to the client. This provides better performance than decompressing and recompressing video data on the computer running Citrix XenApp.

ADM UI Element : Citrix Components > Citrix Receiver > User experience > Client graphics settings

Section	Server
Feature	RAVE
Attribute Name	INI_MM
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
oLdWaY	Default
Off	Launch failed because session key is set to Off

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Session Sharing	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Session Sharing	

SpeedScreenMMAAudioEnabled

Specifies whether (True) or not (False) audio playback will occur through HDX MediaStream Multimedia Acceleration.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_AUDIO_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Audio playback will occur through HDX MediaStream Multimedia Acceleration - Default
FALSE	Audio playback will not occur through HDX MediaStream Multimedia Acceleration

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SpeedScreenMMAMaxBufferThreshold

Specifies (as a percentage) the amount of data in the media queue before the client requests that the server stops sending data until the data in the queue levels off.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_MAX_THRESHOLD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
90	Percent - Default
85-90	Percent

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SpeedScreenMMAMaximumBufferSize

Specifies the maximum size in kilobytes of the media queue that the client can create. This is per stream, so the client could create a 30240KB queue for audio and a 30240 queue for video.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_MAX_BUFFER_SIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
30240	Size in KB - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SpeedScreenMMAMinBufferThreshold

Specifies what percent value the data in the media queue will be when the client requests a burst from the server to replenish its media queue.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_MIN_THRESHOLD
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
10	Default
5-15	

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SpeedScreenMMASecondsToBuffer

Specifies the number of seconds of MMA data to buffer. The value is set on both the server and client and the connection is set up with the smaller of these values.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_SECONDS_TO_BUFFER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Default
10	(wince default)
1-10	

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SpeedScreenMMAVideoEnabled

Specifies whether (True) or not (False) video playback will occur through HDX MediaStream Multimedia Acceleration.

Section	Server
Feature	RAVE
Attribute Name	INI_MM_VIDEO_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Video playback will occur through HDX MediaStream Multimedia Acceleration - Default
FALSE	Video playback will not occur through HDX MediaStream Multimedia Acceleration

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Multimedia	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Multimedia	*

SSLCACert

Specifies a Certificate Authority Certificates count and a string.

The attribute CACerts (Certificate Authority Certificates) is stored and read with the current CACerts count and string containing the certificate name. Specific to SSL (Secure Sockets Layer).

Only present if there are any Certificate Authority Certificates to store.

Section	Server
Feature	SSL
Attribute Name	INI_SSLCACERT
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

INI Location

INI information not found.

Registry Location

Registry information not found.

SSLCertificateRevocationCheckPolicy(2)

Governs how a given trusted root certificate authority is treated during an attempt to open a remote session through SSL when using the client for 32-bit Windows.

When certificate revocation list checking is enabled, the client checks whether or not the server's certificate is revoked. This feature improves the cryptographic authentication of the Citrix server and improves the overall security of the SSL/TLS connections between a client and a server. There are several levels of certificate revocation list checking. For example, the client can be configured to check only its local certificate list, or to check the local and network certificate lists. In addition, certificate checking can be configured to allow users to log on only if all Certificate Revocation lists are verified.

The client checks SSL certificate revocation only when the underlying operating system is Windows 2000 or later. When this setting is not configured in the Appsrv.ini and .ica files, NoCheck is used as the default value for Windows NT4/9x and CheckWithNoNetworkAccess is used as the default value for Windows 2000/XP. When the CertificateRevocationCheckPolicy setting is configured in the Appsrv.ini file of a user's profile and the .ica file, the value in the Appsrv.ini file takes precedence when attempting to launch a remote session using the .ica file.

This behavior is the reverse of that displayed with most other parameters shared between the two file types.

Possible values for the parameter SSLCertificateRevocationCheckPolicy in the Appsrv.ini/.ica file are as follows:

- NoCheck. No Certificate Revocation List check is performed.
- CheckWithNoNetworkAccess. Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- FullAccessCheck. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- FullAccessCheckAndCRLRequired. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows security certificates to be revoked (invalidated before their expiry date) in the case of cryptographic compromise of the certificate private key, or simply an unexpected change in DNS name.

Valid CRLs must be downloaded periodically from the certificate issuer and stored locally. This can be controlled through the selection made in "CRL verification":

- Disabled: When selected, no CRL checking will be performed.
- Only check locally stored CRLs: When selected, any CRLs that have been previously installed or downloaded will be used in certificate validation. If a certificate is found to be revoked, the connection will fail.
- Retrieve CRLs from network: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail.
- Require CRLs for connection: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail. If the client is unable to retrieve a valid CRL, the connection will fail.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing

Section	WFClient,Server
Feature	SSL
Attribute Name	INI_SSLCERTREVCHECKPOLICY
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	Policy value - Default
NoCheck	No Certificate Revocation List check is performed
CheckWithNoNetworkAccess	Only local certificate revocation list stores are used. All distribution points are ignored
FullAccessCheck	Local Certificate Revocation List stores and all distribution points are used
FullAccessCheckAndCRLRequired	Local Certificate Revocation List stores and all distribution points are used

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	

Troubleshooting

Error Message: "SSL Error 61: You have not chosen to trust "<xxx>" the issuer of the server`s security certificate". The common name and other information on a security certificate is guaranteed to be accurate by the certificate`s issuer. For a connection to be successful, the client must trust the certificate`s issuer to make that guarantee.

Error Message: "SSL Error 59: The server sent a security certificate identifying `xxx`. The SSL connection was to `yyy`". The common name did not match the server the client was expecting to connect to.

SSLCiphers

On platforms that support multiple SSL cipher suites (currently 32-bit editions of Windows only), this parameter determines which cipher suite(s) the client is permitted to use to establish an SSL connection. Non-32-bit Windows platforms are locked (hard-coded) to COM.

ADM UI: Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification > SSL ciphersuite

Section	WFClient
Feature	SSL
Attribute Name	INI_SSLCIPHERS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
ALL	Either - Default
RC4	COM
GOV	3DES

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	
appsrv.ini	WFClient	ALL

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	

SSLCommonName

Specifies the server name as it appears on the SSL certificate.

If the value of SSLProxyHost is not identical to that of the server name as it appears on the SSL certificate, this parameter is required, and its value must specify the server name as it appears on the SSL certificate.

Section name would be WFClient for all custom ICA connections unless otherwise overridden.

Section name would be applicationservername for each custom ICA connection where DoNotUseDefaultCSL=On.

Section	Server
Feature	SSL
Attribute Name	INI_SSLCOMMONNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Server name - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	

SSLEnable

Specifies whether or not SSL is enabled.

The value of this parameter must be On to enable SSL. This setting is ignored by network protocols other than TCP/IP.

Use this policy to configure the TLS/SSL options that help to ensure that the client connects to genuine remote applications and desktops. TLS and SSL encrypt the transferred data to prevent third-parties viewing or modifying the data traffic. Citrix recommends that any connections over untrusted networks use TLS/SSL or another encryption solution with at least the same level of protection.

When this policy is enabled, the client will apply these settings to all TLS/SSL connections performed by the client. The Require SSL for all connections check box can be used to force the client to use the TLS or SSL protocol for all connections that it performs.

TLS and SSL identify remote servers by the common name on the security certificate sent by the server during connection negotiation. Usually the common name is the DNS name of the server, for example www.citrix.com. It is possible to restrict the common names to which the client will connect by specifying a comma-separated list in the "Allowed SSL servers" setting. Note that a wildcard address, for example, *.citrix.com:443, will match all common names that end with .citrix.com. The information contained in a certificate is guaranteed to be correct by the certificate`s issuer.

Some security policies have requirements related to the exact choice of cryptography used for a connection. By default the client will automatically select either TLS v1.0 or SSL v3.0 (with preference for TLS v1.0) depending on what the server supports. This can be restricted to only TLS v1.0 or SSL v3.0 using the "SSL/TLS version" setting.

Similarly, certain security policies have requirements relating to the cryptographic ciphersuites used for a connection. By default the client will automatically negotiate a suitable ciphersuite from the five listed below. If necessary, it is possible to restrict to just the ciphersuites in one of the two lists.

- Government Ciphersuites:
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- Commercial Ciphersuites:
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_RC4_128_MD5

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows security certificates to be revoked (invalidated before their expiry date) in the case of cryptographic compromise of the certificate private key, or simply an unexpected change in DNS name.

Valid CRLs must be downloaded periodically from the certificate issuer and stored locally. This can be controlled through the selection made in "CRL verification."

- Disabled: When selected, no CRL checking will be performed.
- Only check locally stored CRLs: When selected, any CRLs that have been previously installed or downloaded will be used in certificate validation. If a certificate is found to be revoked, the connection will fail.
- Retrieve CRLs from network: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail.
- Require CRLs for connection: When selected, the client will attempt to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection will fail. If the client is unable to retrieve a valid CRL, the connection will fail.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing

Section	Server,WFClient
Feature	SSL
Attribute Name	INI_SSLNOCACERTS
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Number of CACerts. (Certificate Authority Certificates) - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	*
appsrv.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	*

Troubleshooting

Error Message: "SSL Error 61: You have not chosen to trust "<xxx>" the issuer of the server`s security certificate". The common name and other information on a security certificate is guaranteed to be accurate by the certificate`s issuer. For a connection to be successful, the client must trust the certificate`s issuer to make that guarantee.

Error Message: "SSL Error 59: The server sent a security certificate identifying `xxx`. The SSL connection was to `yyy`". The common name did not match the server the client was expecting to connect to.

SSLProxyHost(2)

Specifies the server name value.

By default, this parameter is not present, or, if present, the value is set to *:443.

Assuming that every Citrix server in a server farm has its own SSL relay, the asterisk means that the address of the SSL relay is the same as that of the Citrix server.

If not every Citrix server in a given server farm has its own relay, the value can specify an explicit server name in place of the asterisk. If the value is an explicit server name, SSL traffic enters the server farm through the server whose name is specified by the value. The server name value must match the server name in the server's SSL certificate; otherwise, SSL communications fail. For listening port numbers other than 443, the port number is appended to the server name following a colon (:):SSLProxyHost=*:SSL relay port number, where SSL relay port number is the number of the listening port. Related parameter: SSLCommonName.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing

Section	Server,WFClient
Feature	SSL
Attribute Name	INI_SSLPROXYHOST
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
*.443	SSL Proxy host string - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	
appsrv.ini	WFClient	*:443

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL	

SSOnCredentialType(3)

Specifies the credential type to used with pass-through authentication.

Allows particular credentials (Windows, NetWare, either) to be used with pass-through authentication on client devices that have the Novell Client installed.

Local user name and password: Use this policy to instruct the client to use the same logon credentials (pass-through authentication) for Citrix XenApp as the client machine.

When this policy is enabled, the client can be prevented from using the current user`s logon credentials to authenticate to the remote server by clearing the Enable pass-through authentication check box.

When run in a Novell Directory Server environment, selecting the Use Novell Directory Server credentials check box requests that the client uses the user's NDS credentials.

ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Local user name and password -> Use Novell Directory Server credentials

Section	WFClient,dynamic,Server
Feature	SSON
Attribute Name	INI_SSON_CREDENTIAL_TYPE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Any	Windows, NetWare, either - Default
NT	
NDS	

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Local Credentials	
appsrv.ini	WFClient	Any

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	

SSOnDetected

A boolean setting enabled when (Single Sign-On) is being used.

(Single Sign-On) setting handles authentication to servers.

SSOnDetected Citrix pass-through authentication (Single Sign-On) is being used.

Section	Server
Feature	SSON
Attribute Name	INI_SSON_DETECTED
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Disable single sign-on detected - Default
TRUE	Enable single sign-on detected

INI Location

INI File	Section	Value
All_Regions.ini	Logon	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon	*

SSOnUserSetting

Selects (On) or clears (Off) the Use local credentials to log on option. Choose use pass-through authentication when installing the ICA Client for this parameter to have an effect.

This attribute is used for 3 types of User authentications in ADM file: "Smart Card Authentication", "Kerberos authentication" and "Local user name and password".

- "Smart Card Authentication": Use Smart Card Authentication to control how the client uses smart cards attached to the client device. When enabled, this policy allows the remote server to access smart cards attached to the client device for authentication and other purposes. When disabled, the server cannot access smart cards attached to the client device.

  ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Smart card authentication > Use pass-through authentication for PIN

- "Kerberos authentication": Use this policy to control how the client uses Kerberos to authenticate the user to the remote application or desktop. When enabled, this policy allows the client to authenticate the user using the Kerberos protocol. Kerberos is a Domain Controller authorised authentication transaction that avoids the need to transmit the real user credential data to the server. When disabled, the client will not attempt Kerberos authentication.

  ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Kerberos authentication

- "Local user name and password": Use this policy to instruct the client to use the same logon credentials (pass-through authentication) for Citrix XenApp as the client machine. When this policy is enabled, the client can be prevented from using the current user`s logon credentials to authenticate to the remote server by clearing the Enable pass-through authentication check box.

  ADM UI Element: Citrix Components > Citrix Receiver > User authentication > Local user name and password

Section	WFClient
Feature	SSON
Attribute Name	INI_USER_SETTING_SINGLE_SIGN_ON
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
Off	Clear the user local credentials to log on option - Default
On	Selects the use local credentials to log on option

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Local Credentials	*
appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*

SSPIEnabled

Enables and disables Kerberos authentication protocol.

Use this policy to control how the client uses Kerberos to authenticate the user to the remote application or desktop.

When enabled, this policy allows the client to authenticate the user using the Kerberos protocol. Kerberos is a Domain Controller authorised authentication transaction that avoids the need to transmit the real user credential data to the server.

When disabled, the client will not attempt Kerberos authentication.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > User authentication

Section	WFClient
Feature	SSPI
Attribute Name	INI_SSPI_ENABLED
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	Enable Kerberos authentication protocol- Default
Off	Disable Kerberos authentication protocol

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Kerberos	*
wfclient.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client	0x1
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Kerberos	*
0x1 HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Kerberos	*

Troubleshooting

The machine running the client and the server running the remote application must be in domains that have a trust relationship. The Domain Controller must be aware that Citrix XenApp will be performing a full user logon (interactive logon) using Kerberos. This is configured using the "Trust for Delegated Authentication" settings on the Domain Controller.

When connecting using Web Interface, Web Interface server must be aware that the client will connect using Kerberos authentication. This is necessary because by default Web Interface server will use an IP address for the destination server whereas Kerberos authentication requires a Fully Qualified Domain Name.

Both client and server machines must have correctly registered DNS entries. This is necessary because endpoints will authenticate each other during connection.

startIFDCD(3)

This is an End User Experience Monitoring (EUEM) metric. This metric tracks the time it takes the client to download the ICA file from the Web server for Program Neighborhood Agent or Web Interface.

Section	qwerty,dynamic,Server
Feature	EUEM
Attribute Name	INI_EUEM_STARTIFDCD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

startSCD(2)

New session creation time (SCD), from the moment wfica32.exe is launched to when the connection is established

An ICA session may be started by different launchers, all of the launchers use the same engine wfica32.exe. This is specific to the ICA launcher when it is not Program Neighborhood Classic.

Section	dynamic,Server
Feature	EUEM
Attribute Name	INI_EUEM_STARTSCD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Session Creation Time (ms) - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

State

Specifies whether or not to launch a pre-launched application session at user logon. When set to 1 (default setting), the session is enabled at user logon. When set to 2, the pre-launched application session is launched at the

When set to 2, the pre-launched application session launches at the specified Schedule; if the schedule is not set, the session is disabled.

To enable users to override this administrator's configuration, enable the UserOverride setting.

Section	PrelaunchApplication
Feature	Pre-Launch
Attribute Name	PRELAUNCH_STATE
Definition Location	prelaunch.h
Data Type	string
Access Type	Read/Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description	
1	Pre-Launch enabled	default
0	Pre-Launch disabled	
2	Pre-Launch scheduled	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\PreLaunch	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\PreLaunch	

SucConnTimeout

Specifies the number of seconds to wait for a recently started session to become available for session sharing.

Multiple sessions can be opened if multiple configured seamless Window applications are started in rapid succession and the server has custom logon scripts that take longer than 20 seconds to complete. To extend this time-out value, enter this setting in the Appsrv.ini file under the [WFClient] section.

Section	WFClient
Feature	SessionSharing
Attribute Name	INI_SUCCONNTIMEOUT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
20	Wait for Session Sharing (seconds) - Default

INI Location

N/A

Registry Location

N/A

SwapButtons

Specifies whether (On) or not (Off) to swap the function of the client device's mouse buttons within the ICA session.

Section	WFClient
Feature	Mouse
Attribute Name	INI_SWAPBUTTONS
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Disable swap function - Default
On	Enable the swap function

INI Location

N/A

Registry Location

N/A

TransparentKeyPassthrough

Determines how the mapping of certain Windows key combinations are used when connecting to ICA sessions.

This setting appears in the Citrix Receiver user interface under Session Options page and in the Web Interface for Citrix XenApp Settings page.

- When Local is set, the key combinations apply to the local desktop.
- When Remote is set, the key combinations apply to seamless and non-seamless ICA sessions when their windows have the keyboard focus.
- When FullScreenOnly is set, the key combinations apply to the non-seamless ICA session in full screen mode.

The default value is FullScreenOnly. When no TransparentKeyPassthrough setting in the ICA file is passed to the ICA Engine, the keyboard transparent feature behaves as if FullScreenOnly is set.

Section	WFClient
Feature	Keyboard
Attribute Name	INI_TPKEYPASSTHRU
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FullScreen Only	Default
Local	
Remote	

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Keyboard	
wfclient.ini	WFClient	FullScreenOnly
appsrv.ini	WFClient	FullScreenOnly

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard	

TransportReconnectDelay

Specifies the number of seconds to wait before attempting to reconnect to the disconnected session.

When a network error occurs, the auto client reconnect feature normally displays a dialog box asking whether or not to try to reconnect. The TransportReconnectDelay=delay setting replaces this display with a delay (in seconds) followed by an automatic reconnection attempt.

Specifies the number of retries the client will attempt to reconnect to the disconnected session. If the TransportReconnectEnabled value is set to On or is not present in the .ini file, the number that is specified for this value is used.

Use "Session reliability and automatic reconnection" policy to control how the client behaves when a network failure causes the connection to be dropped.

When this policy is enabled, the client will attempt to reconnect to a server only if "Enable reconnection" is selected. By default three reconnection attempts are made, but this can be altered using the "Number of retries" setting. Similarly the delay between retries can be altered from the default of 30 seconds using the "Retry delay" setting.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Session reliability and automatic reconnection > Retry delay (seconds)

Section	WFClient
Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_DELAY
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
30	Seconds - Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*

Troubleshooting

Some proxy servers will automatically disconnect connections that are idle for a certain length of time. This can cause client sessions to be disconnected when not in use. A server-side option "ICA Keep-Alive" is available to send extra data packets during periods of inactivity that can be used prevent proxies from closing connections.

TransportReconnectEnabled

Specifies whether (On) or not (Off) the Auto Client Reconnect is enabled. By default if the client connects to a server that is enabled for AutoClientReconnect and a disconnection occurs, the client tries indefinitely to reconnect to the disconnected session until the user clicks the Cancel button in the AutoClientReconnect dialog box.

Session reliability and automatic reconnection: Use this policy to control how the client behaves when a network failure causes the connection to be dropped.

When this policy is enabled, the client will attempt to reconnect to a server only if "Enable reconnection" is selected. By default three reconnection attempts are made, but this can be altered using the "Number of retries" setting. Similarly the delay between retries can be altered from the default of 30 seconds using the "Retry delay" setting.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Session reliability and automatic reconnection > Enable reconnection

Section	WFClient
Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
1	Enables Auto Client Reconnect - Default
0	Disables Auto Client Reconnect
On	Enables Auto Client Reconnect
Off	Disables Auto Client Reconnect
true	Enables Auto Client Reconnect
false	Disables Auto Client Reconnect
yes	Enables Auto Client Reconnect
no	Disables Auto Client Reconnect

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*

TransportReconnectRetries

Specifies the number of times the client will attempt to reconnect to the disconnected session. If the TransportReconnectEnabled value is set to On or is not present in the .ini file, the number that is specified for this value is used.

Use the Session reliability and automatic reconnection policy settings to control how the client behaves when a network failure causes the connection to be dropped.

When these policy settings are enabled, the client will attempt to reconnect to a server only if Enable Reconnection is selected in the Citrix User policy setting for Auto Client Reconnect. By default three reconnection attempts are made, but this can be altered using the Number of retries setting. Similarly the delay between retries can be altered from the default of 30 seconds using the Retry delay setting. Retry delay is supported only on WinCE.

ADM UI Element: Citrix Components > Citrix Receiver > Network routing > Session reliability and automatic reconnection > Number of retries

Section	WFClient
Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_RETRIES
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0xFFFFFFFF	For Win32 (infinite) - Default
3	(default for non-windows)
1 - 0xFFFFFFFF	1 or higher

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Reconnection	*

Troubleshooting

Some proxy servers will automatically disconnect connections that are idle for a certain length of time. This can cause client sessions to be disconnected when not in use. The server-side policy setting for ICA Keep Alives is available to send extra data packets during periods of inactivity that can be used to prevent proxies from closing connections.

TRWD

EUEM: End User Experience Monitoring .

TRWD: TICKET_RESPONSE_WEB_SERVER

The time it takes to get a ticket (if required) from the STA server or XML Service. This metric is collected when the application is launched via the Citrix Receiver or Web Interface.

Section	Server
Feature	EUEM
Attribute Name	INI_EUEM_TRWD
Data Type	Integer
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Initial reset value - Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\End User Experience	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\End User Experience	

Tw2CachePower

Specifies, in powers of 2 bytes, the size of the ThinWire cache. For example, a TW2CachePower value of 23 creates an 8MB (2^23 bytes) ThinWire cache. Set it in the range of 19 to 25. Any value less than 19 is reset to 19; any value greater than 25 is reset to 25. If you do not specify a value, the ThinWire driver automatically computes the initial size based on connection resolution and color depth, applying a value in the range of 22 to 25. If the required memory space cannot be allocated, the value is gradually lowered until it matches the actual amount of available memory space. If memory space equivalent to a value of 19 (512KB) cannot be allocated, the connection is dropped.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_TW2_CACHE_POWER
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
19	Default
19-25	

INI Location

N/A

Registry Location

N/A

TW2StopwatchMinimum

Sets a minimum return value for TW2 stopwatch timers.

TW2`s stopwatch timers can return meaningless results when the underlying graphics system is not synchronous, for example X11 on Unix. This option allows an implementation to set a minimum value that will be returned for a stopwatch timer period. The minimum value used is taken from the configuration files and scaled by the size of the last image copy.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_TW2_STOPWATCH_MINIMUM
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
canonicalization.ini	Thinwire3.0	TW2StopwatchMinimum

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	TW2StopwatchMinimum
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

TW2StopwatchScale

Sets a scale factor to be applied to TW2 stopwatch timers.

TW2`s stopwatch timers can return over-optimistic results when there is a large disparity between the speed of different graphics operations; for example, some WinCE terminals can scroll quickly but draw relatively slowly. This option allows a scale factor to be applied to values returned by the stopwatch timers in an attempt to correct this.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_TW2_STOPWATCH_SCALE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1	Scale Factor - Default

INI Location

N/A

Registry Location

N/A

TwainAllowed

Specifies whether (TRUE) or not (FALSE) Image capture is enabled.

Image Capture: Use this policy to enable and restrict the remote application or desktop`s access to scanners, webcams, and other imaging devices on the client device (TWAIN).

ADM UI Element: Citrix Components > Citrix Receiver > Remoting client devices > Image capture

Section	WFClient
Feature	Twain
Attribute Name	INI_TWAINALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
TRUE	Enables Image capture (TWAIN) - Default
FALSE	Disables Image capture (TWAIN)

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Image Capture	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Image Capture	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Image Capture	*

TWIEmulateSystray

Specifies whether (TRUE) or not (FALSE) to do system tray emulation on non-windows clients.

Controls the creation of a system emulation window to display notification area icons when using seamless mode.

Section	Server
Feature	Seamless
Attribute Name	INI_TWI_SYSTRAY_EMULATION
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Do system tray emulation on non-Windows clients - Default
FALSE	Does not do system tray emulation on non-Windows clients

INI Location

N/A

Registry Location

N/A

TWIFullScreenMode

This setting switches the client to full screen mode.

The server display will completely cover the client display.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client display settings

Section	Thinwire3.0
Feature	Keyboard
Attribute Name	INI_FULLSCREENMODE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0	Disable client full screen mode - Default
1	Enable client full screen mode

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Thinwire Graphics	*
Module.ini	Thinwire3.0	
canonicalization.ini	Thinwire3.0	TWIFullScreenMode

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Canonicalization\Thinwire3.0	TWIFullScreenMode
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Thinwire Graphics	*

TWIIgnoreWorkArea

Enable/Disable sending only desktop work area.

Specifies whether (True) or not (False) the entire desktop area will be sent to the server. By default when the client connects to the server it sends the entire desktop area (including the taskbar) of the client display to the server. Setting this value to True sends only the desktop work area (area where shortcuts are placed, for example).

Section	WFClient
Feature	Seamless
Attribute Name	INI_OVERRIDE_WORKAREA_SETTING
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Disable sending only desktop work area.
1	Enable sending only desktop work area.

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Seamless Windows	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*

TWIMode

Specifies whether (On) or not (Off) to use seamless mode for all connections in the associated application set or for the associated custom ICA connection. Set the parameters DesiredVRES, DesiredHRES, and DesiredWinType accordingly.

Client display settings: Use this policy to control how the client presents remote applications and desktops to the end user. Remote applications can be seamlessly integrated with local applications, or the entire local environment can be replaced with a remote desktop.

Seamless windows: When set to False this setting allows the client to disable the use of seamless windows, instead displaying a fixed size window. When set to True it forces the client to request seamless windows, although the server may choose to reject this request.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client display settings > Seamless windows

Section	Server
Feature	Seamless
Attribute Name	INI_TWI_MODE
Data Type	Boolean
Access Type	Read & Write
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
FALSE	Disables the seamless mode for all connections - default
TRUE	Enables the seamless mode for all connections
Off	Disables seamless mode for all connections
On	Enables seamless mode for all connections

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Seamless Windows	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*

TWISeamlessFlag

Enable/Disable seamless applications launch.

Starting with Version 9.x of the Citrix Receiver for Windows, when an application launches seamlessly, if focus is shifted away from the Logon Status dialog boxes before the application is displayed, the application launches behind whichever window has focus.

By setting this value to 1, seamless applications launch in the foreground and have focus, even if the focus shifted away from the Logon Status dialog boxes.

Section	WFClient
Feature	Seamless
Attribute Name	INI_SEAMLESS_FLAG
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Disable seamless application launch - default
1	Enable seamless application launch.

INI Location

INI information not found.

Registry Location

Registry information not found.

TWIShrinkWorkArea

Specifies the value that the work area will be minimized. By specifying this users can make work area for seamless windows smaller.

Seamless applications cover the local taskbar on Windows 2000, 2003, and XP workstation computers when Auto hide is selected in the taskbar and Start Menu Properties dialog box. If the user selects to auto hide the local taskbar and a seamless ICA session is run, the local taskbar may not be accessible. If the seamless application is minimized, the local taskbar can be accessed. To avoid this problem, set the setting to a value of 3 or more.

Section	WFClient
Feature	Seamless
Attribute Name	INI_WORKAREA_TOSHRINK
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Default
greater than 0	

INI Location

INI information not found.

Registry Location

Registry information not found.

TWISuppressZZEcho

Suppress post-move jiggle of seamless window.

By setting this property to True, any attempt by the server to move a seamless window to the top left corner of the screen is ignored after the window is moved locally. This affects Windows servers only.

Section	Server
Feature	Seamless
Attribute Name	INI_TWI_SUPPRESS_ZZ_ECHO
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Does not suppress post-move jiggle - default
TRUE	Suppress post move jiggle

INI Location

INI information not found.

Registry Location

Registry information not found.

TWITaskbarGroupingMode

Mode used for Seamless Taskbar Grouping of hosted, published applications.

Set this parameter to the desired value for Seamless Taskbar Grouping support. If GroupAll is specified, hosted, published app instances are grouped together on the Windows Taskbar by app. Likewise, these app instances are grouped together with corresponding local app instances. If GroupNone is specified, the Seamless Taskbar Grouping feature is disabled. As a result, all instances of all hosted apps are grouped together in the Windows Taskbar in the same group, and not with local apps.

Section	Server
Feature	Seamless
Attribute Name	INI_TWI_TASKBAR_GRP_MODE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
GroupAll	Specifies that published app instances should be grouped with corresponding local app instances on the Windows Taskbar - default
GroupNone	Disables taskbar button grouping support

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Seamless Windows	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows	*

Troubleshooting

Not applicable.

UnicodeEnabled

Enable UNICODE printer names.

Section	ClientPrinterQueue
Feature	Printing
Attribute Name	INI_CPMUNICODEENABLED
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
TRUE	Default
FALSE	

INI Location

INI information not found.

Registry Location

Registry information not found.

UseAlternateAddress(3)

Selects (1) or clears (0) the Use alternate address for firewall connection option.

Selects (1) or clears (0) the Use alternate address for firewall connection option. Used to perform Network Address Translation (NAT).

Firewalls use IP address translation to convert public (Internet) IP addresses into private (intranet) IP addresses. Public IP addresses are called external addresses because they are external to the firewall, while private IP addresses are called internal addresses. In this context, *alternate* means *external*.

A client configured to use the TCP/IP server location network protocol sends a directed UDP datagram to the server IP address, using TCP/IP port 1604. Any intervening firewall must be configured to allow UDP packets to pass port 1604 or client-server communication fails.

If a fixed server location address is specified, the client contacts that server to determine the address of the ICA master browser. When the client connects by server or published application name, the ICA master browser returns the address of the requested server or published application.

You can use UseAlternateAddress for TCP/IP connections only. To specify the server's IP address, you must include the following statement in the [WFClient] section of the ICA file:

TcpBrowserAddress=*ipaddress*, where *ipaddress* is the IP address of the Citrix server.

You must also use the ALTADDR command on the Citrix server with the IP address that is accessed by the ICA file (specified by*ipaddress*). See the *XenApp Administration* guide for more information about the ALTADDR command.

Note: WFClient is used as section for all custom ICA connections unless otherwise overridden.

Corresponding UI Element:

- For applicationsetname: Settings dialog box > Connection tab > Firewalls > Use alternate address for firewall connection option
- For applicationservername: Properties dialog box > Connection tab > Firewalls > Usealternate address for firewall connection option

Section	WFClient,dynamic,Server
Feature	NATSupport
Attribute Name	INI_USEALTERNATEADDRESS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
0	Do not use the alternate address for firewall connection option - default
1	Use alternate address for firewall connection option.

INI Location

INI File	Section	Value
Module.ini	TCP/IP	
Module.ini	TCP/IP - FTP	
Module.ini	TCP/IP - Novell Lan WorkPlace	
Module.ini	TCP/IP - Microsoft	
Module.ini	TCP/IP - VSL	
All_Regions.ini	Network\Protocols	*
Module.ini	WFClient	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - FTP	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Microsoft	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - Novell Lan WorkPlace	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP - VSL	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient	
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Protocols	*

UseDefaultEncryption

Specifies from where to use the default encryption setting.

In applicationsetname: Specifies whether to use the server-side default encryption setting (On) or the setting specified in applicationsetname (Off). EncryptionLevel must be specified in applicationsetname if the value of UseDefaultEncryption in applicationsetname is Off.

In applicationservername: Specifies whether to use the custom default encryption setting in WFClient (On) or the setting specified in applicationservername (Off). EncryptionLevel must be specified in applicationservername if the value of UseDefaultEncryption in applicationservername is Off.

Interface Element:

- For applicationsetname: Settings dialog box > Default Options tab > Encryption Level > Use Server Default option
- For applicationservername: Properties dialog box > Options tab > Encryption Level > Use Custom Default option

Section	Server
Feature	Misc
Attribute Name	INI_USEDEFENCRYPT
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Use the default encrypting setting from applicationsetname / applicationservername - default
TRUE	Use default encryption setting from server side or from WFClient

INI Location

INI information not found.

Registry Location

Registry information not found.

UseLocalUserAndPassword(2)

Specifies whether (On) or not (Off) to use the same user name and password the user used to log on to the client computer for authentication to the Citrix server.

SSOnUserSetting must be set to On.

Use the Local username and password policy to instruct the client to use the same logon credentials (pass-through authentication) for the XenApp server as the client machine. When this policy is enabled, the client can be prevented from using the current user`s logon credentials to authenticate to the remote server by clearing the Enable pass-through authentication check box.

ADM UI Element : Citrix Components > Citrix Receiver > User authentication > Local user name and password > Enable pass-through authentication

Section	Server,Server
Feature	SSON
Attribute Name	INI_USE_LOCAL_USER_AND_PASSWORD
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	Use pass-through authentication
Off	Does not use pass-through authentication

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Local Credentials	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Local Credentials	*

UseMRUBrowserPrefs

Specifies how it will be determined which browser's preferences will be used for the proxy settings.

It is used when the client finds more than one browser preferences file when processing the ProxyType=Auto setting to find network proxy settings. If this is set, it uses the one that changed most recently.

If the parameter is False the client uses its old method: it looks first for Firefox browser settings, then Mozilla, then Netscape, and uses the first one found.

Section	Server
Feature	Proxy
Attribute Name	INI_USEMRUBROWSERPREFS
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
True	Proxy setting is the one changed most recently - default
False	Uses old method: look first for Firefox browser settings, then Mozilla, the Netscape, and use the first one found

INI Location

INI information not found.

Registry Location

Registry information not found.

Username(3)

Specifies the user name that appears in the User name text box if the user selects the User-specified credentials option for the associated custom ICA connection.

Use this policy to control how user credentials data stored on users' machines or placed in ICA files is used to authenticate the user to the remote published application or desktop. When this policy is enabled, you can prevent locally stored passwords being automatically sent to remote servers by clearing the Allow authentication using locally stored credentials check box. This causes any password fields to be replaced with dummy data. In addition, the User name and Domain options can be used to restrict or override which users can be automatically authenticate to servers. These can be specified as comma-separated lists.

Properties dialog box > Logon Information tab > User-specified credentials option > User name text box

ADM UI Element : Citrix Component > Citrix Receiver > User Authentication > Locally stored credential > User name

Section	Smartcard,dynamic,Server
Feature	Core
Attribute Name	INI_USERNAME
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
""	User name - Default

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Saved Credentials	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Saved Credentials	

UserOverride

Specifies whether the users can override the Pre-Launch configuration set by the administrator (see settings State and Schedule). If enabled, but the user configuration setting is not present on the client, the Pre-Launch configuration specified by the administrator is enabled.

Section	PrelaunchApplication
Feature	Pre-Launch
Attribute Name	PRELAUNCH_USER_OVERRIDE
Definition Location	prelaunch.h
Data Type	string
Access Type	Read/Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description	
0	Disable users override	default
1	Enable users override	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\PreLaunch	

UsersShareIniFiles

Specifies whether (On) or not (Off) users shares .ini files or they have their own .ini files.

Section	WFClient
Feature	Core
Attribute Name	INI_USERS_SHAREINIFILES
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Off	Users have their own ini files - default
On	Users shares ini file

INI Location

INI information not found.

Registry Location

Registry information not found.

Troubleshooting

Not applicable.

UseSSPIOnly

Specifies whether to use only Kerberos authentication or to get credentials from the Single sign-on service. Authentication will fail if Kerberos authentication fails. This prevents fallback to using passthrough.

If set to True, only Kerberos authentication is used and credentials are not retrieved from the Single sign-on service.

Section	WFClient
Feature	SSPI
Attribute Name	INI_SSPI_ONLY
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
FALSE	Use Kerberos authentication or get credentials from Single sign-on service - Default
TRUE	Use only Kerberos authentication

INI Location

INI File	Section	Value
All_Regions.ini	Logon\Kerberos	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Kerberos	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Logon\Kerberos	*

VariantName

Identify that the client is a variant of the regular client.

If Module.ini or Appsrv.ini contain a line named "VariantName=[ ]" it designates the client is not a regular Win32 client (OEMs).

Section	ClientAudio
Feature	Core
Attribute Name	INI_CM_VARIANTNAME
Data Type	String
Access Type	Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Base	Default

INI Location

INI information not found.

Registry Location

Registry information not found.

VirtualChannels

List of virtual channel names to create.

Specifies the virtual channels to be opened on connection. You can specify multiple channel names as a comma separated list. Names must be restricted to seven characters or less.

Section	Server
Feature	Core
Attribute Name	INI_VIRTUALCHANNELS
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present then any possible virtual channel list

INI Location

INI information not found.

Registry Location

Registry information not found.

VirtualCOMPortEmulation

Specifies whether virtual COM ports are enabled or not.

Remote PDA synchronization uses virtual COM ports. These are serial port connections that are routed through USB connections. It is necessary to enable serial port access to use PDA synchronization for this reason.

ADM UI: Citrix Receiver > Remote Client Devices > Client hardware Access > Allow PDA Synchronizaton.

Section	WFClient
Feature	PDASync
Attribute Name	INI_VCOM_EMULATION
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
On	Virtual COM ports are enabled - Default
Off	Virtual COM ports are not enabled

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Serial Port	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Serial Port	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Serial Port	*

VirtualDriver

Specifies a list of virtual drivers to load, in sequence. The listed items correspond to section names containing parameters for each specific virtual driver. Individual features can be disabled by removing their drivers from this list (for example, remove ClientDrive to disable client drive mapping).

Section	ICA 3.0
Feature	Core
Attribute Name	INI_VIRTUALDRIVER
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
Thinwire3.0, ClientDrive, ClientPrinterQueue, ClientPrinterPort, Clipboard, ClientComm, ClientAudio, LicenseHandler, ProgramNeighborhood,TWI,ZL_FONT,ZLC,SmartCard,Multimedia,ICACTL,SpeechMike,SSPI,TwainRdr,UserExperience	Default

INI Location

INI File	Section	Value
Module.ini	ICA 3.0	Thinwire3.0, ClientDrive, ClientPrinterQueue, ClientPrinterPort, Clipboard, ClientComm, ClientAudio, LicenseHandler, ProgramNeighborhood,TWI,ZL_FONT,ZLC,SmartCard,Multimedia,ICACTL,SpeechMike,SSPI,TwainRdr,UserExperience

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	Thinwire3.0, ClientDrive, ClientPrinterQueue, ClientPrinterPort, Clipboard, ClientComm, ClientAudio, LicenseHandler, ProgramNeighborhood,TWI,ZL_FONT,ZLC,SmartCard,Multimedia,ICACTL,SpeechMike,SSPI,TwainRdr,UserExperience

VirtualDriverEx

Specifies the list of third party virtual channels.

Set AllowVirtualDriverEx to True to append the third party virtual channel list to the current virtual drivers.

Section	ICA 3.0
Feature	Core
Attribute Name	INI_VIRTUALDRIVER_THIRDPARTY
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	If present then any possible virtual channels

INI Location

INI File	Section	Value
Module.ini	ICA 3.0	

Registry Location

Registry Key	Value
On 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	
On 64-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0	

VSLAllowed(2)

Specifies whether or not client printer queue mapping has been enabled.

Enables (On) or disables (Off) client printer spooling by controlling whether (On) or not (Off) the client printer mapping virtual driver in ClientPrinterQueue is loaded.

Use this policy to enable and restrict the remote application or desktop`s access to client printers.

When this policy is disabled, the client prevents the server from accessing or printing to printers available to the client device.

ADM UI Element : Citrix Components > Citrix Receiver > Remoting client devices > Client printers

Section	WFClient,ClientPrinterQueue
Feature	Printing
Attribute Name	INI_VSLALLOWED
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
TRUE	Enables client printer queue mapping - Default
FALSE	Disable client printer queue mapping

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Printing	*
appsrv.ini	WFClient	On

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*

Win32FavorRetainedPrinterSettings

Specifies whether (False) or not (True) to prevent the system from retaining any changes to the properties store.

The Win32FavorRetainedPrinterSettings=Off setting in the client's appsrv.ini file (under the [WFClient] section) prevents the system from retaining any changes to the properties store.

For certain printer drivers, changes made to printer properties or advanced printer settings within a session do not persist between sessions. This is the server-side component of an enhancement that allows to modify the client-side appsrv.ini file to set the client to always use the printer settings from the actual printer rather than the retained settings in the properties store. This setting also forces the client to attempt to write settings modified within a client session to the client printer if the drivers are determined to be equivalent.

Win32FavorRetainedPrinterSettings = TRUE implies that the client shall service properties requests from the client's private printer properties store in the client-side user profile at HKCU\Software\Citrix\PrinterProperties. If there are no retained properties for the printer in question, real properties should be returned from the real Windows printer object instead. FALSE implies client shall service properties enumerations and saves to/from the real printer first. When client and server drivers are equivalent, all properties would be read from (written to) the real printer. When server and client driver are not equivalent, device dependent properties will still be serviced from retained settings since the device specific settings of the real printer are not useable.

Section	WFClient
Feature	Printing
Attribute Name	INI_VSLPROPSFROMPROFILE
Data Type	Boolean
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
TRUE	Client shall service properties requests from the clients private printer properties store - Default
FALSE	Prevents the system from retaining any changes to the properties store

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Printing	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Printing	*

WindowManagerMoveIgnored

Flag to indicate that the Window Manager's initial move should be ignored for the UNIX client.

If this flag is set to True, dubious window configuration messages from WM at start-up are acknowledged and Window Manager's initial move should be ignored.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_WINDOW_MANAGER_MOVE_IGNORED
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
False	Window Manager's initial move should be not be ignored - Default
True	Window Manager's initial move should be ignored.

INI Location

INI information not found.

Registry Location

Registry information not found.

WindowManagerMoveTimeout

Time period in milliseconds for WindowManagerMoveIgnored, which ignores local changes in window size and position for a short period after creation of a seamless window.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_WINDOW_MANAGER_MOVE_TIMEOUT
Data Type	Integer
Access Type	Read
UNIX Specific	Yes
Present in ADM	No

Values

Value	Description
500	Window Manager Timeout (ms) - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

WindowsCache

Specifies the size of the Receiver's Thinwire memory (in 1KB chunks). The maximum size of the Thinwire cache is 8192KB.

Section	Thinwire3.0
Feature	Graphics
Attribute Name	INI_LARGECACHE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
3072	KB - Default
8192	Maximum cache size (KB)

INI Location

INI File	Section	Value
Module.ini	Thinwire3.0	3072

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0	3072

WindowSize

Gives the write window size, in bytes, for flow management for ClientComm section.

Section	ClientComm
Feature	Printing
Attribute Name	INI_CCMWINDOWSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
1024	Write window size in bytes - Default
512	Write window size in bytes

INI Location

INI File	Section	Value
Module.ini	ClientPrinterQueue	1440
Module.ini	ClientPrinterPort	1024
Module.ini	ClientComm	1024

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	1440

WindowSize

Gives the maximum write window size (in bytes) for flow management; i.e., the maximum number bytes that can be written for the ClientPrinterQueue section.

Section	ClientPrinterPort
Feature	Printing
Attribute Name	INI_CPMWINDOWSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
512	Default
1024	

INI Location

INI File	Section	Value
Module.ini	ClientPrinterQueue	1440
Module.ini	ClientComm	1024
Module.ini	ClientPrinterPort	1024

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	1440

WindowSize

Specifies the write window size (in bytes) for flow management for the ClientPrinterQueue driver.

Section	ClientPrinterQueue
Feature	Graphics
Attribute Name	INI_VSLWINDOWSIZE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
512	Window Size (Bytes) - Default
1024	Window Size (Bytes)

INI Location

INI File	Section	Value
Module.ini	ClientPrinterPort	1024
Module.ini	ClientComm	1024
Module.ini	ClientPrinterQueue	1440

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientComm	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	1024
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	1440

WindowSize2

Specifies the larger window size for flow management for ClientPrinterQueue driver.

This virtual driver is responsible for providing client printer queue access to supplement the ICA 3.0 driver.

If this window size is not suitable, then smaller size (WindowSize) is used.

Section	ClientPrinterQueue
Feature	Printing
Attribute Name	INI_VSLWINDOWSIZE2
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
4102	Window Size (Bytes) - Default

INI Location

INI File	Section	Value
Module.ini	ClientPrinterQueue	4102

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterQueue	4102

WindowsPrinter

Specifies the queue name displayed for the available printer.

Section	ClientPrinterPort
Feature	Printing
Attribute Name	INI_CPMQUEUE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Default Windows Printer Name - Default

INI Location

INI File	Section	Value
Module.ini	ClientPrinterPort	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	

WindowsPrinter

Specifies a queue name to print to.

Section	ClientPrinterQueue
Feature	Printing
Attribute Name	INI_VSLQUEUE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Queue name - Default

INI Location

INI File	Section	Value
Module.ini	ClientPrinterPort	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientPrinterPort	

WorkDirectory

Specifies the working directory after logon.

Section	Server
Feature	Core
Attribute Name	INI_WORKDIRECTORY
Data Type	String
Access Type	Read & Write
UNIX Specific	No
Present in ADM	No

Values

Value	Description
""	Directory location of working directory

INI Location

INI File	Section	Value
All_Regions.ini	Client Engine\Application Launching	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Application Launching	

WpadHost

Specifies the URL to query for the automatic proxy detection configuration file to determine proxy settings.

Section	WFClient
Feature	Proxy
Attribute Name	INI_WPADHOST
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
http://wpad/wpad.dat	Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\Proxy	

XmlAddressResolutionType

Specifies the address resolution method used for XML requests. Address resolution is the process of resolving server and published application names to network addresses that the network driver can understand and use.

Section	WFClient
Feature	EnumRes
Attribute Name	INI_XMLADDRESSRESTYPE
Data Type	String
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
DNS-Port	Address name - Default
IPv4-Port	Address name

INI Location

INI File	Section	Value
appsrv.ini	WFClient	DNS-Port

Registry Location

Registry information not found.

ZLAutoHiLimit

Zero-Latency Mouse Threshold Upper Limit.

The Mouse Threshold Upper Limit is compared with the average response time of ICA to determine if the mouse zero latency feature playback is turned on.

The zero latency feature monitors the response time of keyboard and mouse inputs on the Receiver and enables playback features to make ICA seem more responsive to the user when necessary. This is determined by keeping track of ICA's average response time and comparing the average response time to the IZLAutoLowLimit and the ZLAutoHiLimit.

If the average response time is greater than or equal to ZLAutoHiLimit, then ICA is responding at an unacceptable speed and the zero latency feature turns on the mouse zero latency playback and the keyboard zero latency playback features.

Section	Server
Feature	ZLC
Attribute Name	INI_AUTO_ZLHILIMIT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
250	Mouse zero latency playback turns on if average response time is greater than this limit - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

ZLAutoLowLimit

Zero-latency Mouse Threshold Lower Limit.

Mouse Threshold Lower Limit that is compared with average response time of ICA to determine if the mouse zero latency playback feature is turned off.

The zero latency feature monitors the response time of keyboard and mouse inputs on the Receiver, and enables playback features to make ICA seem more responsive to the user when necessary. This is determined by keeping track of ICA's average response time and comparing the average response time to the IZLAutoLowLimit and the ZLAutoHiLimit.

If the average response time is less than ZLAutoLowLimit, then ICA is responding at an acceptable speed and the zero latency feature turns off the mouse zero latency playback feature and continues to monitor the average response time.

Section	Server
Feature	ZLC
Attribute Name	INI_AUTO_ZLLOWLIMIT
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
150	Lower limit threshold - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

ZLDiskCacheSize

Specifies the cache size, in bytes, on disk for latency reduction.

Section	WFClient
Feature	ZLC
Attribute Name	INI_ZLDISK_CACHE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
-1	Disk free space will be used - Default

INI Location

INI information not found.

Registry Location

Registry information not found.

ZLFntMemCacheSize

Specifies a memory size value to create a cache directory.

This attribute is for Zero Latency Window - Virtual Font driver interface.

Section	WFClient
Feature	ZLC
Attribute Name	INI_ZLMEM_CACHE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	No

Values

Value	Description
512000	Cache Directory Size (Bytes) - Default
0	Disable audio input

INI Location

INI information not found.

Registry Location

Registry information not found.

ZLKeyboardMode

Specifies whether or not to use local text echo.

For 2 (Auto), local text echo is used if the connection latency exceeds the high latency threshold set using the SpeedScreen Latency Reduction Manager. The Citrix server must support SpeedScreen Latency Reduction for this setting to take effect.

Corresponding UI Element:

- For applicationsetname: Settings dialog box > Default Options tab > SpeedScreen Latency Reduction menu; Local text echo option
- For applicationservername: Properties dialog box > Options tab > SpeedScreen Latency Reduction menu; Local Text Echo option

ADM UI Element: XenApp server > User Experience > Client graphic settings > Speed Screen Latency Reduction - keyboard Local echo

Section	Server
Feature	ZLC
Attribute Name	INI_ZLC_MODE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
0	Always off - Default
1	Always on
2	Auto

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Zero Latency	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Zero Latency	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Zero Latency	*

ZLMouseMode

Specifies whether or not to use mouse click feedback.

Set a value for mouse zero latency (mouse pointer prediction), 2, 1 or 0.

For ZLMouseMode=2 (Auto), mouse click feedback is used if the connection latency exceeds the high latency threshold set using the SpeedScreen Latency Reduction Manager. The Citrix server must support SpeedScreen Latency Reduction for this setting to take effect.

Interface Element:

- For applicationsetname: Settings dialog box > Default Options tab > SpeedScreen Latency Reduction menu; Mouse Click Feedback option

Enabling SpeedScreen Latency Reduction settings allows the client to predict how mouse movement and text entry will appear on the server. This results in the user getting immediate feedback when typing or moving the mouse pointer.

ADM UI Element: Citrix Components > Citrix Receiver > User experience > Client graphics settings > SpeedScreen Latency Reduction - mouse pointer prediction

Section	Server
Feature	ZLC
Attribute Name	INI_MOUSEZLMODE
Data Type	Integer
Access Type	Read
UNIX Specific	No
Present in ADM	Yes

Values

Value	Description
2	Auto - Default
0	Always Off
1	Always On

INI Location

INI File	Section	Value
All_Regions.ini	Virtual Channels\Zero Latency	*

Registry Location

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Zero Latency	*
HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Zero Latency	*