citrix

ICA settings reference

Table of Contents

About this document

This document provides information on:

- Sections were each of the ICA setting parameters belongs to
- Information on each of the ICA setting parameters

Please note that the information in this document is updated gradually. The remaining parameters of the ICA settings will be updated in the coming days.

ICA settings reference – section

Server

- ClientAudio
- AudioBandwidthLimit
- EnableAudioInput
- EnableUDPAudio
- UDPAudioPortLow
- UDPAudioPortHigh
- EnableUDPThroughGateway
- AudioLatencyControlEnabled
- AudioMaxLatency
- AudioLatencyCorrectionInterval
- AudioTempLatencyBoost
- GSTAudioSrcName
- GSTAudioSinkName
- GSTSpeexBufferingLatency
- GSTVorbisBufferingLatency
- DesiredColor
- ScreenPercent
- FontSmoothingType
- EnableOSS
- PersistentCacheEnabled
- LocalDisplayNames
- ScreenPercent
- EnableOSS
- FontSmoothingType
- LocalDisplayNames
- EnableAtomicDisplay
- UserVisualID
- DesiredColor
- ApproximateColors
- DesiredHRES=640

- DesiredVRES=480
- UseFullScreen=false
- ResizeSession
- TWIDesiredIconColor
- TW2StopwatchMinimum
- WinSetting
- TwRedundantImageItems
- PrimaryMonitor
- PreferredLaunchMonitor
- NoWindowManager
- CGPSecurityTicket
- CGPAllowed
- Address
- UseAlternateAddress
- TransportDriver
- HDXoverUDP
- edtMSS
- edtRCVBUF
- edtSNDBUF
- edtIFlightFlagSize
- edtUDPRCVBUF
- edtUDPSNDBUF
- ProxyAutoConfigURL
- ProxyBypassList
- ProxyHost
- ProxyUsername
- ProxyPassword
- ProxyTimeout
- ProxyAuthenticationBasic
- AltProxyType
- AltProxyAutoConfigURL
- AltProxyBypassList
- AltProxyHost
- ICASOCKSProtocolVersion
- ICASOCKSProxyHost
- ProxyUseDefault
- ProxyFallback
- ProxyAuthenticationPrompt
- ProxyAuthenticationNTLM
- TransportReconnectOptions
- TCPSendBufferSize
- TCPRecvBufferSize
- TCPRecvBufferSizeNoFlow
- SSLEnable
- SSLProxyHost
- SSLCommonName

- SecureChannelProtocol
- SSLEnableCertificatePolicyVerification
- MinimumTLS
- MaximumTLS
- EnableClientSelectiveTrust
- EncryptionLevelSession

Wfclient

- AllowAudioInput
- HDXWebCamDevice
- HDXWebCamWidth
- HDXWebCamHeight
- HDXWebCamFramesPerSec
- HDXWebCamFramesPerSecDenominator
- HDXWebCamDebug
- HDXH264InputEnabled
- PersistentCacheMinBitmap
- PersistentCacheSize
- PersistentCachePath
- IdentificationController
- CGPAddress
- SessionReliabilityTTL
- UseAlternateAddress
- ProxyType
- ProxyAutoConfigURL
- ProxyHost
- ProxyPort
- ProxyPassword
- WpadHost
- AltProxyType
- AltProxyAutoConfigURL
- AltProxyBypassList
- AltProxyHost
- ICASOCKSProtocolVersion
- ICASOCKSProxyHost
- ProxyFallback
- ProxyAuthenticationPrompt
- ProxyAuthenticationNTLM
- TransportReconnectEnabled
- TransportReconnectRetries
- TransportReconnectDelay
- ICAKeepAliveEnabled
- ICAKeepAliveInterval

- SSLEnable
- SSLProxyHost
- SecureChannelProtocol
- SSLCiphers

Graphics

- TW2StopwatchMinimum

Thinwire 3.0

- DesiredColor
- TW2StopwatchMinimum
- PersistentCacheMinBitmap
- PersistentCacheSize
- LocalDisplayNames
- EnableAtomicDisplay
- UserVisualID
- DesiredColor
- ApproximateColors
- DesiredHRES=640
- DesiredVRES=480
- UseFullScreen=false
- ResizeSession
- TWIDesiredIconColor
- TW2StopwatchMinimum
- WinSetting
- TwRedundantImageItems
- PrimaryMonitor
- NoWindowManager
- PreferredLaunchMonitor

Dynamic

- Address
- UseAlternateAddress
- ProxyHost

TCP/IP

- ICAPortNumber

Network

- SSLNoCACerts
- SSLCACert1

ICA settings reference – parameters

Audio parameters

ClientAudio

Specifies whether to enable client audio mapping or not.

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.

Section	Server
Feature	Audio
Attribute Name	INI_CAM
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	Disables client audio mapping – Default
True	Enables client audio mapping

INI location

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

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.

Section	Server
Feature	Audio
Attribute Name	INI_AUDIOBANDWIDTHLIMIT
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
1	Medium quality audio
2	Low quality audio
0	High quality audio – Default

INI location

INI File	Section
All_Regions.ini	Virtual Channels

EnableAudioInput

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

Section	Server
Feature	Audio
Attribute Name	INI_AUDIOINPUTENABLE
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

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

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

EnableUDPAudio

Specifies whether to enable UDP audio or not.

UDP audio can improve the quality of phone calls made over the Internet. It uses User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP).

Section	Server
Feature	Audio
Attribute Name	INI_AUDIOENABLEUDP
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
True	Enables UDP audio.
False	Disables UDP audio. This is the default value set.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

UDPAudioPortLow

Specifies the minimum port numbers for UDP audio traffic.

By default, ports 16500–16509 are used.

Section	Server
Feature	Audio
Attribute Name	INI_UDPAUDIOPORTLOW
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
Port value	By default, port 16500 is used

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

UDPAudioPortHigh

Specify the maximum port numbers for UDP audio traffic. By default, ports 16500–16509 are used.

Section	Server
Feature	Audio
Attribute Name	INI_UDPAUDIOPORTHIGH
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
Port value	By default, port 16509 is used

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

EnableUDPThroughGateway

Specifies whether to enable or disable UDP audio through Citrix Gateway.

Section	Server
Feature	Audio
Attribute Name	INI_UDPTHROUGHGATEWAYENABLE
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
True	Enables UDP audio through Citrix Gateway.
False	Disable UDP audio through Citrix Gateway. Default value.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

AudioLatencyControlEnabled

Enables latency control.

Section	Server
Feature	Audio
Attribute Name	INI_AUDIO_LATENCY_CONTROL_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
True	Reduces audio latency – default value.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

AudioMaxLatency

Sets the maximum latency in milliseconds(ms) before trying to discard audio data. Default=300 ms

Section	Server
Feature	Audio
Attribute Name	INI_AUDIO_MAX_LATENCY
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
300 ms	Maximum audio latency in audio. By default, the value is 300 ms.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

AudioLatencyCorrectionInterval

Defines how often to correct the latency (in ms). Default=300 ms

Section	Server
Feature	Audio
Attribute Name	INI_AUDIO_LATENCY_CORRECTION_INTERVAL
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
300 ms	Define audio latency correction interval. By default, the value is 300 ms.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

AudioTempLatencyBoost

Sets the higher latency band (in ms) above the lower PlaybackDelayThresh band. Default=300 ms.

Section	Server
Feature	Audio
Attribute Name	INI_AUDIO_TEMP_LATENCY_BOOST
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
300 ms	Audio latency boost interval. By default, the value is 300 ms.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

GSTAudioSrcName

Defines audio source name of Gstreamer.

Section	Server
Feature	Audio
Attribute Name	INI_CAM_AUDIOSRC_NAME
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
autoaudiosrc	Gstreamer audio source name. By default, the value is “autoaudiosrc”.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

GSTAudioSinkName

Defines audio sink name of Gstreamer.

Section	Server
Feature	Audio
Attribute Name	INI_CAM_AUDIOSINK_NAME
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
autoaudiosink	Gstreamer audio sink name. By default, the value is “autoaudiosink”.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

GSTSpeexBufferingLatency

Defines Gstreamer buffering latency for speex.

Section	Server
Feature	Audio
Attribute Name	INI_GST_SPEEX_BUFFERING_LATENCY
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
50 ms	Gstreamer buffering latency for speex. By default, the value is 50 ms.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

GSTVorbisBufferingLatency

Defines Gstreamer buffering latency for Vorbis.

Section	Server
Feature	Audio
Attribute Name	INI_GST_VORBIS_BUFFERING_LATENCY
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
150 ms	Gstreamer buffering latency for Vorbis. By default, the value is 150 ms.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\Audio

Webcam parameters

AllowAudioInput

Enables webcam redirection.

Section	wfclient
Feature	Webcam redirection
Attribute Name	INI_AUDIOINPUTENABLE
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes

Values

Value	
False	Disables webcam redirection.
True	Enables webcam redirection. Default value.

INI location

INI File	Section
Wfclient.ini	~./ICAClient/wfclient.ini

HDXWebCamDevice

Selects the default webcam. You can also use it to set another capture video as default.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_DEVICE
Data Type	String
Access Type	Read
UNIX Specific	Yes

Values

Value	
HDXWebCamDevice=<path to a different device path>. ex. HDXWebCamDevice=/dev/video2. For example, add HDXWebCamDevice=/dev/video2 to set the webcam mapped to /dev/video2 in a system.	

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXWebCamWidth

Sets the width value of the resolution for the webcam.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAMP_WIDTH
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	
Width value. HDXWebCamWidth=<width value>. ex. HDXWebCamWidth=480	

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXWebCamHeight

Sets the height value of the resolution for the webcam.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_HEIGHT
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	
Height value. HDXWebCamHeight=<height value> ex. HDXWebCamHeight=720	

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXWebCamFramesPerSec

Sets the numerator value of the frame rate for the webcam.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_ FRAMEPERSEC
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	
Frames per second – numerator value HDXWebCamFramesPerSec=<numerator value>. ex. HDXWebCamFramesPerSec=30	

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXWebCamFramesPerSecDenominator

Sets the denominator value of the frame rate for the webcam.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_FRAMEPERSECDENOMINATOR
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	
Frames per second denominator value. HDXWebCamFramesPerSecDenominator=<denominator value>. ex. HDXWebCamFramesPerSecDenominator=1	

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXWebCamDebug

Debug mode creates the following files that contains the encoded frames depending on the encoder used:

- /tmp/file_mode_buffers.h264
- /tmp/file_mode_buffers.theora

This file allows comparison between the video rendering on the VDA side and the actual buffers that the encoder produces on the client side. It allows to test the entire pipeline.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_ DEBUG
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes

Values

Value	
False	Disables the debug mode. Default value.
True	Sets the debug mode.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

HDXH264InputEnabled

Enables H264 encoder configuration.

Section	Wfclient
Feature	Webcam redirection
Attribute Name	INI_WEBCAM_H264_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes

Values

Value	
False	Disables H264 encoder. Default value.
True	Enables H264 encoder.

INI location

INI File	Section
All_Regions.ini	Virtual Channels\HDXRealTime

Graphics parameters

LocalDisplayNames

Specifies whether to use X server shared memory or not.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	LocalDisplayNames
Data Type	String
Access Type	Read
UNIX Specific	Yes

Values

Value	Description
:unix	Use the default unix socket.
:0	Use X server shared memory extension.

INI location

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

EnableAtomicDisplay

Enables atomic display. This parameter is only effective if you are using Presentation server 4.5 or later.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	EnableAtomicDisplay
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	Disabled atomic display.
True	Enables atomic display. This is the default value.

INI location

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

UserVisualID

Specifies a visual ID. If not specified, use the default from X11 API DefaultVisual.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	UserVisualID
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
-1	Use default from X11 API DefaultVisual.
<Number>	Specify a visual ID.

INI location

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

DesiredColor

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 might 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 Linux clients.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	INI_DESIREDCOLOR
Data Type	String
Access Type	Read
UNIX Specific	No

Values

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

INI location

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

ApproximateColors

Specifies whether to use color approximation or not. If not present, the default value from [Thinwire3.0] is used.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	ApprixmateColors
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	Do not use color approximation. This is the default value.
True	Use the color approximation.

INI location

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

DesiredHRES=640

Specifies the default value of horizontal window size. The default value is 640.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	DesiredHRES
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
640	The default value is number 640.

INI location

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

DesiredVRES=480

Specifies the default value of vertical window size. The default value is 480.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	DesiredVRES
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
480	The default value is 480.

INI location

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

UseFullScreen=false

Specifies whether to start a session as full screen or not.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	UseFullScreen
Data Type	Boolean
Access Type	READ
UNIX Specific	No

Values

Value	Description
False	Do not start session in full screen.
True	Starts session in full screen.

INI location

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

NoWindowManager

Disables scroll bars around client and window manager frame is removed.

Section	Server and Thinwire 3.0	
Feature	Graphics	
Attribute Name	NoWindowManager	
Data Type	Boolean	
Access Type	READ	
UNIX Specific	No	

Values

Value	Description
False	Disables scroll bars around client and window manager frame is removed. This is the default value.
True	Enables scroll bars around client and window manager frame is present.

INI location

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

ResizeSession

Specifies whether to use resizable session or to use scroll bars.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	ResizeSession
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	The session window is not resizable. It is recommended to use the scroll bar.
True	The session window is resizable. This is the default value.

INI location

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

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.

Section	Server
Feature	Core
Attribute Name	INI_SCREENPERCENT
Data Type	Integer
Access Type	Read and Write
UNIX Specific	No

Values

Value	Description
75	Default screen size when the setting is enabled.
0	Disables the setting.

INI location

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

TWIDesiredIconColor

Specifies icon color depth in bitsPerPixel. The values are: 4, 8, 16, 24, 32.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	TWIDesiredIconColor
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
Number	normal values: 4, 8, 16, 24, 32

INI location

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

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 is 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

Values

Value	Description
0	This is the default value.

INI location

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

EnableOSS

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

Reduces bandwidth in 15-bit 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

Values

Value	Description	
False	Enable OSS. This is the default value.	
True	Disable OSS.	

INI location

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

WinSetting

Decides which display settings must be used for a window.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	WinSetting
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	Prefer full screen.
1	Prefer fixed width and height window.
2	Prefer percentage window.

INI location

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

TwRedundantImageItems

Conditionally compiled mechanism for eliminating redundant bitmap drawing. The value is the number of screen rectangles to track. The number zero means disable the parameter.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	TwRedundantImageItems
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
Number	Number of screen rectangles to track. The number zero means disable.

INI location

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

PrimaryMonitor

Defines the primary monitor. Default value is zero, meaning the first monitor is the primary monitor.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	PrimaryMonitor
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
<Number>	Default value is zero, meaning the first monitor is the primary monitor.

INI location

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

PreferredLaunchMonitor

Prefer to launch session into which monitor.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	PreferredLaunchMonitor
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
<number>	0=Primary Monitor, 1=Secondary Monitor

INI location

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

FontSmoothingType

Improves the quality of displayed fonts beyond the available quality through traditional font smoothing or anti-aliasing.

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

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

Values

Value	Description
0	The local preference on the device is used. The **FontSmoothingTypePref** setting defines this value.
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing
Note: Both standard smoothing and ClearType smoothing can increase Citrix Workspace app's bandwidth requirements.	

INI location

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

H264Enabled

Enables or disables H.264-based compression codec support.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	H264Enabled
Data Type	Boolean
Access Type	Read
UNIX Specific	Yes

Values

Value	Description
False	Disables H.264-based compression codec support.
True	Enables H.264-based compression codec support. This is the default value.

INI location

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

TextTrackingEnabled

Enables or disables deep compression codec support and text tracking.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	TextTrackingEnabled
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	Disables deep compression codec support and text tracking.
True	Enables deep compression codec support and text tracking. This is the default value.

INI location

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

SmallFramesEnabled

Enables or disables small frames in full H.264 mode.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	SmallFramesEnabled
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
False	Disables small frames in full H.264 mode. This is the default value.
True	Enables small frames in full H.264 mode.

INI location

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

FontSmoothingTypePref

Determines the local preference. This parameter is used to express client font-smoothing preference.

Section	Server and Thinwire 3.0
Feature	Graphics
Attribute Name	FontSmoothingTypePref
Data Type	Number
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	No smoothing
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal subpixel) smoothing. This is the default value.

INI location

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

Network parameters

IdentificationController

This setting handles network topology, security, and routing. This setting specifies the preferred LAN device for getting host identity. There is no default value.

Section	WFClient
Feature	Network
Attribute Name	IdentificationController
Data Type	String
Access Type	Read
UNIX Specific	Yes

Values

Value	Description
"ln0", "tra0" and so on.	The name of the network interface.

INI Location

INI File	Section	Value
All_Regions.ini	[Network]	<Network Interface>

CGPAddress

Specifies address and port for CGP connection. The address is usually `*` to indicate that the same address must be used as if CGP is not used. For example,`*:1111` sets the port to 1111. Default="*:2598"

Section	WFClient
Feature	CGP
Attribute Name	INI_CGPADDRESS
Data Type	String
Access Type	Read and Write
UNIX Specific	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

INI File	Section	Value
All_Regions.ini	[Network\CGP]	The IP Address and port value.

CGPSecurityTicket

Specifies whether the CGP security ticket is to be used, when traversing a Secure Gateway. Default=Off

Section	Server
Feature	CGP
Attribute Name	INI_CGPSECURITYTICKET
Data Type	inc\cgpini.h
Access Type	Read
UNIX Specific	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	*

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

Values

Value	Description
180	Seconds – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\CGP	*
Module.ini	WFClient	*

CGPAllowed

Enables or disables the Common Gateway Protocol (CGP), the underlying mechanism that provides HDX Broadcast session reliability. Disabling CGP can be useful when debugging this feature. Do not use this setting to configure the feature permanently for users. Use server policies instead.

Section	Server
Feature	Network\CGP
Attribute Name	CGPAllowed
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
On	Enables Common Gateway Protocol (CGP).
Off	Disables Common Gateway Protocol (CGP).

INI Location

INI File	Section	Value
All_Regions.ini	[Network\CGP]	On or Off

Address

Specifies the 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 name 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 and dynamic
Feature	Network
Attribute Name	INI_ADDRESS
Data Type	String
Access Type	Read and Write

UNIX Specific	No

Values

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

INI Location

INI File	Section	Value
All_Regions.ini	Network\Protocols	IP address

UseAlternateAddress

Selects (1) or clears (0) the **Use alternate address for firewall connection** option.

Used to do 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're 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 main browser. When the client connects by server or published application name, the ICA main 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 the ICA file (specified by *ipaddress*) access. 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.

Section	WFClient, dynamic, and Server
Feature	Network
Attribute Name	INI_USEALTERNATEADDRESS
Data Type	String
Access Type	Read
UNIX Specific	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	

TransportDriver

Specifies which transport layer to use.

Section	Server
Feature	Network
Attribute Name	TransportDriver
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
TCP/IP	Use TCP/IP as the transport layer.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\Protocols]	TCP/IP

ICAPortNumber

Specifies the TCP port used for the ICA protocol. Change the port on all Citrix servers 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

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	ICA port number

HDXoverUDP

Specifies which Transport protocol to use.

Section	Server
Feature	Network
Attribute Name	HDXoverUDP
Data Type	Boolean
Access Type	Read and Write
UNIX Specific	No

Values

Value	Description
On	Use UDP and do not fall back to TCP on failure.
Off	Use TCP. This value is the default value.
Preferred	Try UDP first and fall back to TCP on failure

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	On/Off/Preferred

edtMSS

Specifies the maximum segment size in bytes for EDT. Default = 1500

Section	Server
Feature	Network\UDT
Attribute Name	edtMSS
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
1500	Maximum segment size in bytes for EDT. This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	Any number

edtRCVBUF

Receive flow window * (edtMSS-28) in bytes. Default = 0.

Section	Server
Feature	Network\UDT
Attribute Name	edtRCVBuf
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	Description
0	This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	0

edtSNDBUF

Send flow window * (edtMSS-28) in bytes. Default = 0.

Section	Server
Feature	Network\UDT
Attribute Name	edtSNDBUF
Data Type	Integer
Access Type	Read
UNIX Specific	Yes

Values

Value	Description
0	This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	<Number>

edtIFlightFlagSize

Buffer count related to in-flight data. Default = 0.

Section	Server
Feature	Network\UDT
Attribute Name	edtIFlightFlagSize
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	0

edtUDPRCVBUF

SO_RCVBUF value passed to underlying UDP socket. Default = 0

Section	Server
Feature	Network\UDT
Attribute Name	edtUDPRCVBUF
Data Type	Boolean
Access Type	Integer
UNIX Specific	No

Values

Value	Description
0	This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	0

edtUDPSNDBUF

SO_SNDBUF value passed to underlying UDP socket. Default = 0.

Section	Server
Feature	Network\UDT
Attribute Name	edtUDPSNDBUF
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	This value is the default value.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\UDT]	0

ProxyType

Identifies the proxy type requested for the connection.

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 wanted destination.

Proxy type: None

When None is selected, the client tries to connect to the server directly without traversing a proxy server.

Proxy type: Auto

When Auto is selected, the client uses the local machine settings to determine which proxy server to use for a connection. This setting is usually the settings used by the Web browser installed on the machine.

Proxy type: Script

When Script is selected, the client retrieves a JavaScript based on the .pac file from the URL specified in the Proxy script URLs policy option. The .pac file is run to identify which proxy server must be used for the connection.

Proxy type: Secure

When Secure is selected, the client contacts the proxy identified by the Proxy host names and Proxy ports settings. The negotiation protocol uses an 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 performs a SOCKS V4 or SOCKS V5 handshake to the proxy identified by the Proxy host names and Proxy ports settings. The SOCKS option detects and uses the correct version of SOCKS.

Section	WFClient
Feature	Server
Attribute Name	INI_PROXYTYPE
Data Type	String
Access Type	Read and Write
UNIX Specific	No

Values

Value	Description
None	Use Direct connection – Default
Tunnel (Secure)	Use secure (HTTPS) proxy
Wpad	Web Proxy AutoDiscovery Protocol
Auto	Auto detect from Web browser
SOCKS V4	SOCKS version 4
SOCKS V5	SOCKS version 5
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

ProxyAutoConfigURL

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 retrieves a JavaScript based .pac file from the URL specified in the Proxy script URLs policy option. The .pac file is run to identify which proxy server must be used for the connection.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_PROXYAUTOCONFIGURL
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	If present then any string giving the location of a .pac script – Default

INI Location

INI File	Section	Value
All_Regions.ini	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). Separate multiple hosts with 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 uses its own settings to decide whether to connect through a proxy server. When this policy is enabled, the client uses 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 servers must be placed in the Bypass server list.

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYBYPASSLIST
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	Lists of hosts, separated by ";" or ","

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

ProxyHost

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 (:).

Section	WFClient, dynamic, and Server
Feature	Proxy
Attribute Name	INI_PROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	Proxy Server Address – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

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.

Section	WFClient
Feature	Proxy
Attribute Name	INI_PROXYPORTNUMBER
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	Default
65536	Maximum Port Value

INI Location

INI File	Section	Value
All_Regions.ini	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, operating system handles authentication. However, in some scenarios, the user might be provided with a specific user name and password. To prevent the user from being prompted for these credentials, clear the **Prompt user for credentials** check box. This action forces 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 credentials can be explicitly specified through 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 is unrelated to users' passwords.

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYUSERNAME
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	User Name (prompt given) – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	

ProxyPassword

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, operating system handles authentication. However, in some scenarios, the user might be provided with a specific user name and password. To prevent the user from being prompted for these credentials, clear the **Prompt user for credentials** check box. This setting forces 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 credentials can be explicitly specified through Group Policy using the Explicit user name and Explicit password options.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_PROXYPASSWORD
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	Password – Default

INI Location

INI File	Section	Value
All_Regions.ini	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

Values

Value	Description
3000	Proxy timeout (ms) – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

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

Values

Value	Description
http://wpad/wpad.Dat	Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

AltProxyType

Failover proxy type requested for connection.

Specifies what type of failover proxy server that 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.

Section	Server and WFClient
Feature	Proxy
Attribute Name	INI_ALTPROXYTYPE
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
None	Use Direct Connection – Default
Auto	Auto Detect from Web browser
Tunnel (Secure)	Secure Proxy
Wpad	Web Proxy AutoDiscovery Protocol
Socks	Can be removed
Socks v4	Socks version 4
Socks v5	Socks version 5
Script	Interpret proxy auto-configuration script

INI Location

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

AltProxyAutoConfigURL

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.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_ALTPROXYAUTOCONFIGURL
Data Type	String
Access Type	Read
UNIX Specific	No

Values

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

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

AltProxyBypassList

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 servers must be placed in the "Bypass server list."

An asterisk (*) included in a host name acts as a wildcard (for example, *.widgets.com). Separate multiple hosts with 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.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_ALTPROXYBYPASSLIST
Data Type	String
Access Type	Read
UNIX Specific	No

Values

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

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

AltProxyHost

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 (:).

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_ALTPROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
""	Proxy Server Address – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

ICASOCKSProtocolVersion

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 extra SOCKS proxies required for some advanced network topologies.

When enabled, the client examines the "SOCKS protocol version" setting. If connection via SOCKS isn't 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.

Section	Server and WFClient
Feature	Proxy
Attribute Name	INI_SOCKSPROTOCOLVERSION
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
5	Use SOCKS version 5

INI Location

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

ICASOCKSProxyHost

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 more SOCKS proxies required for some advanced network topologies.

When enabled, the client examines the "SOCKS protocol version" setting. If connection through SOCKS isn't 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.

Section	Server and WFClient
Feature	Proxy
Attribute Name	INI_SOCKSPROXYHOST
Data Type	String
Access Type	Read
UNIX Specific	No

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	

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, [server section].

Section	Server
Feature	Proxy
Attribute Name	INI_PROXYUSEDEFAULT
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
True	Default proxy is chosen from WFClient – Default
False	Default proxy is chosen from server section

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

ProxyFallback

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.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_PROXYFALLBACK
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	Not set – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Proxy	*

ProxyAuthenticationBasic

Specifies whether the Basic authentication mechanism is allowed or not.

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, operating system handles authentication. However, in some scenarios, the user might be provided with a specific user name and password. To prevent the user from being prompted for these credentials, clear the **Prompt user for credentials** check box. This setting forces 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 credentials can be explicitly specified through Group Policy using the Explicit user name and Explicit password options.

Section	Server
Feature	Proxy
Attribute Name	ProxyAuthenticationBasic
Data Type	Boolean
Access Type	Read and write
UNIX Specific	No

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	*

ProxyAuthenticationPrompt

Specifies whether 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, operating system handles authentication. However, in some scenarios, the user might be provided with a specific user name and password. To prevent the user from being prompted for these credentials, clear the Prompt user for credentials check box. This setting forces 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 credentials can be explicitly specified via Group Policy using the Explicit user name and Explicit password options.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_PROXYAUTHPROMPT
Data Type	Boolean
Access Type	Read
UNIX Specific	No

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	*

ProxyAuthenticationNTLM

NT LAN Manager (NTLM) proxy authentication option.

NTLM proxy authentication is done under the control of the domain controller and cannot be controlled by the client. Both client and proxy need to be configured with the appropriate domain level trust relations.

Section	WFClient and Server
Feature	Proxy
Attribute Name	INI_PROXYAUTHNTLM
Data Type	Boolean
Access Type	Read
UNIX Specific	No

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	*

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 attempts to reconnect to a server only if "Enable reconnection" is selected. By default, three reconnection attempts are made, but this value 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.

Section	WFClient
Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No

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	*

TransportReconnectOptions

Specifies options for automatic reconnection.

Section	Server
Feature	Network
Attribute Name	TransportReconnectOptions
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
1	Add 1 to show a dialog box during reconnection.
2	Add 2 to remove session windows when reconnection starts.
3	This value is the default value. This value implies that values 1 and 2 are enabled.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\Reconnection]	Integer (1, 2, or 3)

TransportReconnectRetries

Specifies the number of times the client attempts 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 attempts 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 setting 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.

Section	WFClient

Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_RETRIES
Data Type	Integer
Access Type	Read
UNIX Specific	No

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	*

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 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 attempts to reconnect to the disconnected session. If the TransportReconnectEnabled value is set to On or isn't present in the .ini file, the number that is specified for this value is used.

Use the "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 attempts to reconnect to a server only if "Enable reconnection" is selected. By default, three reconnection attempts are made, but this setting 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.

Section	WFClient
Feature	ACR
Attribute Name	INI_TRANSPORT_RECONNECT_DELAY
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
30	Seconds – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

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 verifies every N millisecond (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

Values

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

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

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

Values

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

INI Location

INI File	Section	Value
All_Regions.ini	Network\Reconnection	*

TCPSendBufferSize

Sets the send buffer size. No default value.

Requested size of the TCP transmit buffer for the ICA connection in units of 1024 bytes. Negative values are used to specify a minimum and can never reduce the kernel default. Positive values are used unconditionally. Linux kernels might allocate twice the requested amount. Default = -63.

Section	Server
Feature	Network\TCP
Attribute Name	TCPSendBufferSize
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
<Integer>	Requested size of the TCP transmit buffer for the ICA connection in units of 1024 bytes. Negative values are used to specify a minimum and can never reduce the kernel default. Positive values are used unconditionally. Linux kernels might allocate twice the requested amount. default = -63.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\Reconnection]	

TCPRecvBufferSize

Sets the receive buffer size. No default

Section	Server
Feature	Network\TCP
Attribute Name	TCPRecvBufferSize
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
<Integer>	Similar to TCPRecvBufferSize except that it is used only when TCPRecvBufferSize is not set and the server does not support flow control. When flow control is supported and TCPRecvBufferSize is not set, the kernel is allowed to control the buffer size. Default = 60.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\Reconnection]	

TCPRecvBufferSizeNoFlow

Similar to `TCPRecvBufferSize` except that it is used only when `TCPRecvBufferSize` is not set and the server does not support flow control. When flow control is supported and `TCPRecvBufferSize` is not set, the kernel is allowed to control the buffer size. Default: 60

Section	Server
Feature	Network\TCP
Attribute Name	TCPRecvBufferSizeNoFlow
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
Number	Similar to `TCPRecvBufferSize` except that it is used only when `TCPRecvBufferSize` is not set and the server does not support flow control. When flow control is supported and `TCPRecvBufferSize` is not set, the kernel is allowed to control the buffer size. Default: 60

INI Location

INI File	Section	Value
All_Regions.ini	[Network\Reconnection]	<number>

SSLEnable

Specifies whether SSL is enabled or not.

The value of this parameter must be On to enable SSL. Th e network protocols other than TCP/IP. Ignores this setting.

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 as much protection.

When this policy is enabled, the client applies 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 connects by specifying a comma-separated list in the "Allowed SSL servers" setting. A wildcard address, for example, *.citrix.com:443, matches 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 automatically selects TLS v1.1, v1.2, or v1.3 depends on what the server supports. This value can be restricted 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 automatically negotiates a suitable cipher suite from the following list. If necessary, it is possible to restrict to just the cipher suites in one of the two lists.

Government cipher suites:

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA ·

Commercial cipher suites:s

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 the 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 verification is done.
- Only check locally stored CRLs: When selected, any CRLs that have been previously installed or downloaded is used in certificate validation. If a certificate is found to be revoked, the connection fails.
- Retrieve CRLs from network: When selected, the client attempts to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection fails.
- Require CRLs for connection: When selected, the client attempts to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection fails. If the client is unable to retrieve a valid CRL, the connection fails.

Section	Server and WFClient
Feature	SSL
Attribute Name	INI_SSLNOCACERTS
Data Type	Integer
Access Type	Read and Write
UNIX Specific	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	

SSLProxyHost

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 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 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 the SSL relay port number is the number of the listening port. Related parameter: SSLCommonName.

Section	Server and WFClient
Feature	SSL
Attribute Name	INI_SSLPROXYHOST
Data Type	String
Access Type	Read and Write
UNIX Specific	No

Values

Value	Description
*.443	SSL Proxy host string – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	
appsrv.ini	WFClient	*:443

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 must be WFClient for all custom ICA connections unless otherwise overridden.

Section name must 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

Values

Value	Description
""	Server name – Default

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	Any string

SSLNoCACerts

The number of CA certificates to read from config CACert. Default is 0.

Section	Network
Feature	Network\SSL
Attribute Name	SSLNoCACerts
Data Type	Integer
Access Type	Read
UNIX Specific	No

Values

Value	Description
Number	How many CA certificates to read

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

SSLCACert1

Specifies the SSL certificate name. 1 implies the first certificate. The number can be up to the value of SSLNoCACerts. For example, if SSLNoCACerts is 2, then set SSLCACert1 and SSLCACert2.

Section	Network
Feature	Network\SSL
Attribute Name	SSLCACert1
Data Type	String
Access Type	Read and Write
UNIX Specific	No

Values

Value	Description
<cert name>	The certificate name to read.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

SecureChannelProtocol

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 as much protection.

When this policy is enabled, the client applies 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 connects by specifying a comma-separated list in the "Allowed SSL servers" setting. A wildcard address, for example *.citrix.com:443 matches 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 automatically selects TLS v1.1, v1.2, or v1.3 depends on what the server supports. This value can be restricted using the “SSL/TLS version” setting.

Similarly, certain security policies have requirements relating to the cryptographic cipher suites used for a connection. By default, the client automatically negotiates a suitable cipher suite from the following five listed cipher suites. If necessary, it is possible to restrict to just the cipher suites in one of the two lists.

Government cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Commercial cipher suites:

- 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 the DNS name.

Valid CRLs must be downloaded periodically from the certificate issuer and stored locally. This setting can be controlled through the selection made in "CRL verification." SecureChannelProtocol(2)

- Disabled: When selected, no CRL checking is performed.
- Only check locally stored CRLs: When selected, any CRLs that have been previously installed or downloaded is used in certificate validation. If a certificate is found to be revoked, the connection fails.
- Retrieve CRLs from network: When selected, the client attempts to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection fails.

- Require CRLs for connection: When selected, the client attempts to retrieve CRLs from the relevant certificate issuers. If a certificate is found to be revoked, the connection fails. If the client is unable to retrieve a valid CRL, the connection fails.

Section	WFClient and Server
Feature	SSL
Attribute Name	INI_SSLPROTOCOLS
Data Type	String
Access Type	Read
UNIX Specific	No

Values

Value	Description
Detect	Protocol value – Default
TLS	Protocol value
SSL	Protocol value

INI Location

INI File	Section	Value
All_Regions.ini	Network\SSL	

SSLCiphers

On platforms that support multiple SSL cipher suites (currently 32-bit editions of Windows only), this parameter determines which cipher suite the client is permitted to use to establish an SSL connection. Non-32-bit Windows platforms are locked (hard-coded) to COM.

Section	WFClient
Feature	SSL
Attribute Name	INI_SSLCIPHERS
Data Type	String
Access Type	Read
UNIX Specific	No

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

SSLEnableCertificatePolicyVerification

Enable or disable the Certificate Policy Verification, default 0: disabled

Section	Server
Feature	Network\SSL
Attribute Name	SSLEnableCertificatePolicyVerification
Data Type	Boolean
Access Type	Read and write
UNIX Specific	No

Values

Value	Description
0	Default, disabled
1	Enabled

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

SSLInTitle

Controls whether the SSL strength indicator is shown in a session window's title bar or not.
Default=On

Section	Server
Feature	SSL
Attribute Name	SSLInTitle
Data Type	Boolean
Access Type	Read and write
UNIX Specific	No

Values

Value	Description
On	SSL strength indicator is shown in a session window's title bar. Default value.
Off	SSL strength indicator isn’t shown in a session window's title bar.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

MinimumTLS

The lowest version of the TLS protocol that can be used: 1.1, 1.2, or 1.3. The '.' might be omitted. Default=1.1

Section	Server
Feature	Network\SSL
Attribute Name	MinimumTLS
Data Type	String
Access Type	Read and write
UNIX Specific	No

Values

Value	Description
1.1	The version of the TLS protocol is 1.1. The default value of the lowest version of the Minimum TLS is 1.1.
1.2	The version of the TLS protocol is 1.2.
1.3	The version of the TLS protocol is 1.3.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

MaximumTLS

The highest version of the TLS protocol that can be used: 1.1, 1.2 or 1.3. The '.' might be omitted. Default=1.3.

Section	Server
Feature	Network\SSL
Attribute Name	MaximumTLS
Data Type	String
Access Type	Read and write
UNIX Specific	No

Values

Value	Description
1.1	The version of the TLS protocol is 1.1.
1.2	The version of the TLS protocol is 1.2.
1.3	The version of the TLS protocol is 1.3. The default value of the highest version of the MaximumTLS is 1.3.

INI Location

INI File	Section	Value
All_Regions.ini	[Network\SSL]	*

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 trusted using the Address setting. This setting is a comma-separated list of servers, which also supports the use of wildcards; for example, cps*.citrix.com.

Section	Server
Feature	CST
Attribute Name	INI_CLIENTSELECTIVETRUST_ENABLED
Data Type	Boolean
Access Type	Read
UNIX Specific	No

Values

Value	Description
0	Disable Default
1	Enable

INI Location

INI File	Section	Value
All_Regions.ini	Network\ClientSelectiveTrust	*

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

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	Basic and RC5