

GENESYS

This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Platform SDK Developer's Guide

Configuring TLS Parameters in Configuration Manager

Contents

- 1 Configuring TLS Parameters in Configuration Manager
 - 1.1 Introduction
 - 1.2 Application Objects
 - 1.3 List of TLS Parameters
 - 1.4 Notes and Issues

Configuring TLS Parameters in Configuration Manager

Introduction

As described earlier, the Platform SDK Application Template Application Block allows both client and server applications to read TLS parameters from configuration objects. This page describes how to set TLS parameters correctly in those configuration objects.

Configuration objects that will be used, and their relations, are shown in the diagram below:



To edit TLS-related parameters for these objects, you will need to have access to the Annex tab in Configuration Manager.

Precedence of Configuration Objects

Platform SDK uses different sets of configuration objects to configure client- and server-side TLS settings. For TLS parameters, these objects are searched from the most specific object to the most general one. Parameters found in specific objects take precedence over those in more general objects.

Note: This search occurs independently for each supported TLS parameter.

Location of specific TLS parameters can differ for each object, but is detailed in the appropriate section on this page.

Configuration Object Precedence

Application type	Configuration Objects Used, in Order of Precedence
Client	 Connection from the client application to the server.

Application type	Configuration Objects Used, in Order of Precedence
	 Application of the client. Host where client application resides. Port of the target server that client connects to.^[1]
Server	 Port of the server application. Application of the server. Host where the server application resides.

 If the tls parameter is not set to 1 in both the client Application and Connection objects, then the client application will look to the Port object for the target server to determine if TLS should be turned on. Configuration Manager does not automatically add the tls=1 parameter to Connection Transport parameters when it is linked to a server's secure Port. This is the only case when a client application considers settings in the server's configuration objects.

Displaying the Annex Tab in Configuration Manager

By default, Configuration Manager does not show Annex tab in Object Properties windows. This tab can contain TLS parameters for Host and Application objects.

To show the Annex tab, select *View > Options...* from the main menu and ensure the *Show Annex tab in object properties* and *Show Advanced Security Information* options are selected.

Options 🔀
General Warnings
Connection Parameters Timeout: 300 🗢 sec.
Reconnect options Disconnect notification
Auto reconnect 60 C Reconnect timeout (sec)
New Objects Make New in Properties Make New in Properties of existing objects
Server Ports Assignment
Auto From: 7000 🗢
Auto For Backup To: 8000 🤤
✓ Include description bar for right and left panes
Show Annex tab in object properties
Show Last Name first in Person object properties
✓ Exclude bytecode from Script objects
Case insensitive objects find. Show advanced security information
OK Cancel Apply Help

Application Objects

Host Object

The properties window for a Host object includes most common TLS parameters on the General tab:

- Certificate
- Certificate Key
- Trusted CA

These fields allow copy/paste operations, so they can be set manually by copying and pasting the "Thumbprint" field values from certificates in Windows Certificate Services (WCS) into the related field in Configuration Manager.

🛓 xpigors [192.168.	83.109:6000] Properties	\mathbf{X}
General Annex Securit	by Dependency	
<u>N</u> ame:	xpigors 🗸	
<u>I</u> P Address:	192 . 168 . 83 . 60	
<u>O</u> S Type:	Windows XP 💌	
Version:	~	
LCA Port:	4999	
Solution <u>C</u> ontrol Server:	💭 [None] 🖌 🛃	
<u>C</u> ertificate:	A4 7E A6 E4 7D 45 6A A6 2F 1	
Description:		
Certificate <u>K</u> ey:	A4 7E A6 E4 7D 45 6A A6 2F 15 BE	
<u>T</u> rusted CA:	A4 7E A6 E4 7D 45 6A A6 2F 15 BE	
	✓ <u>S</u> tate Enabled	
ОК	Cancel <u>A</u> pply Help	

To select a certificate, use the button next to *Certificate* field. This opens the *Select certificate* window, displaying a list of certificates installed in WCS under the Local Computer account for the local machine.

Select certificate on host "xpigors"				
Select the certificate you want to use.				
Issued to	Issued by	Intended	P Friendly na	Expiration
🕮 xpigors	xpigors	<all></all>	None	11.08.2022
1				
		ок	Cancel	<u>V</u> iew Certificate

The Annex tab contains a security section that holds TLS settings for this object. Any change made to TLS-related fields on the General tab are mirrored between the Annex tab automatically. You can also specify additional TLS parameters here that aren't reflected on the General tab.

🛃 xpigors [192.168.83.109:6000] Properties	×
General Annex Security Dependency	
🏷 security 🕑 🎓 🗋 🗙 🔂 🎓	
Name 🔶 Value	
Enter text here	
abc certificate "A4 7E A6 E4 7D 45 6A A6 2F 15 BE	
be certificate-key "A4 7E A6 E4 7D 45 6A A6 2F 15 BE	
abetts-cri "C:\certs\cri.pem"	
Cancel Apply Help	, <u> </u>

Server Application Object

For the server Application object, TLS-related fields are located on the *Server Info* tab of the properties window. Note the *Certificate View* controls group, where the server can be set to use Host TLS parameters (generally recommended for Genesys Framework) or application-specific ones.

Discription TLSServer [192.168.83.109:6000] Properties
Connections Options Annex Security Dependency General Tenants Server Info Start Info
Host: Tentants Contract and Con
ID Listening port Secured C.
secure 7001 Yes
Add <u>Port</u> Edit Port Delete Port
Certificate View O Host O Application
Certificate: "C:\certs\server-cert-3-cert.pem" Description:"" Key: "C:\certs\server-cert-3-key.pem"
Backup Server: 💭 TLSServer Backup 🔽 🧭
Redundancy Type: Warm Standby
Reconnect Timeout: 10
Reconnect Attempts: 1
OK Cancel Apply Help

If using application-specific TLS parameters, use the button next to the certificate information field to open a certificate selection window where you can choose from a list of certificates installed for the Local Computer account or manually enter certificate information:

192.1	68.83.109:6000)] Properties
Certificate		
	<u>C</u> ertificate:	C:\certs\server-cert-3-cert.pem
	Description:	
	Certificate <u>K</u> ey:	C:\certs\server-cert-3-key.pem
	Trusted CA:	C:\certs\ca.pem
	(OK Cancel Help

Port Object

For port objects, TLS-related fields are located on the *Server Info* tab of the properties window. You can see here whether a port is secured (TLS-enabled) or not, and have the option to edit existing ports to update TLS parameters or to add new ports.

Discription TLSServer [192.168.83.109:6000] Properties
Connections Options Annex Security Dependency General Tenants Server Info Start Info
Host: Noise Venter and And
Ports
efault 7000 Secure 7001 Yes
Add Port Edit Port Delete Port
Certificate View O Host O Application
Certificate: "C:\certs\server-cert-3-cert.pem" Description:"" Key: "C:\certs\server-cert-3-key.pem"
Backup Server: 💭 TLSServer Backup 💌 🧭
Redundancy Type: Warm Standby
Reconnect Timeout: 10
Reconnect Attempts: 1
OK Cancel Apply Help

When adding or editing a port, TLS parameters are specified on the following tabs:

- *Port Info* Turn on *Secured* listening mode for the port (the same as adding the *t*/*s*=1 string to transport parameters).
- *Certificate* Show certificate information, open a certificate selection window, or delete the current certificate information.
- Advanced Manually edit the Transport Protocol Parameters field. TLS parameters not reflected on the *Certificate* tab can be added here.

🖫 secure [192.168.83.109:6000] Properties 💦 🔀
Port Info Certificate Advanced
Port ID: secure
Communication Port: 7001
Connection Protocol:
HA sync:
Listening <u>M</u> ode: <u>U</u> nsecured
_
🖷 secure [192.168.83.109:6000] Properties 🛛 🔀
Secure [192.168.83.109:6000] Properties Port Info Certificate Advanced Reat Certificate
Secure [192.168.83.109:6000] Properties Port Info Certificate Port Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5
Secure [192.168.83.109:6000] Properties Port Info Certificate Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 A7 6E AA 96 B8 D8 0D 34 28" Description: "xpigors, xpigors, exp: August 11, X
Secure [192.168.83.109:6000] Properties Port Info Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 A7 6E AA 96 B8 D8 0D 34 28" Description: "xpigors, xpigors, exp: August 11, 2022" Key: "" CA: ""
Port Info Certificate Advanced Port Certificate Certificate Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 Image: Certificate Certificate: "89 F1 4A 60 01 A 28" Image: Certificate Description: "xpigors, xpigors, exp: August 11, 2022" Image: Certificate Key: " Certificate Image: Certificate
Secure [192.168.83.109:6000] Properties Port Info Certificate Advanced Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 A7 6E AA 96 B8 D8 0D 34 28" Description: "xpigors, xpigors, exp: August 11, 2022" Key: ""
Secure [192.168.83.109:6000] Properties Pott Info Certificate Advanced Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 A7 6E AA 96 B8 D8 0D 34 28" Description: "xpigors, xpigors, exp: August 11, 2022" Key: "" CA: ""
Port Info Certificate Advanced Port Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 Image: Certificate Certificate: "89 F1 4A 60 01 D9 99 EA 4A 37 F5 Image: Certificate Image: Certificate Description: "xpigors, xpigors, exp: August 11, 2022" Image: Certificate Image: Certificate Key: "" Image: Certificate Image: Certificate Image: Certificate Image: Certificate Cat: " Image: Certificate Image: Certificate Image: Certificate Image: Certificate Image: Certificate Cat: " Image: Certificate Image: Certific

secure [192.168.83.109:6000] Properties	X
Port Info Certificate Advanced	
Transport Protocol Parameters:	
tls=1;tls-crl=C:\certs\crl.pem	^
Application Parameters:	
	^
OK Cancel Hel	

Client Application Object

For client Application objects, TLS-related fields are located under the *security* sections of both the *Options* and *Annex* tabs. There is no certificate selection window provided, but TLS parameters can be configured manually in either section.

Configuring TLS Parameters in Configuration Manager

🕻 TLSClient [192.168.83.109:6000] Properties 💦 🚺	<
General Connections Options Annex Security Dependency	
🗞 security 🔤 🎓 🔛 🔁	
Name 🔶 Value	
Enter text here 🍸 Enter text here	
dec certificate "C:\certs\client-cert-3-cert.pem"	
abc certificate-key "C:\certs\client-cert-3-key.pem"	
dbctrusted-ca "C:\certs\ca.pem"	
<	
	1
Cancel Apply Help	J

Configuring TLS Parameters in Configuration Manager

🔀 TLSClient [192.168.83.109:6000] Properties 💦 🔀
General Connections Options Annex Security Dependency
💱 security 🕑 🏂 🗋 🗙 🛃 🕸 🎼
Name 🔷 Value
Enter text here Tenter text here
Cancel Apply Help

When processing a client Application object, Platform SDK looks at parameters from both sections. If any parameters are specified in both places, then the values from the *Options* tab take precedence.

Connection Object

The properties window for all Application objects includes a *Connection* tab where connections to servers can be added or edited. Each connection determines if TLS mode should be enabled based on port settings for the target server.

Discrimination The Science of the Sc	68.83.109:6000] Prop	erties 🛛 🔀
General Connections	Options Annex Security	Dependency
Server 🔺	Sec Conn	ectio
Confserv		Т
TLSServer	Yes	U
	A <u>d</u> d <u>E</u> dit	Delete
ОК	Cancel Apply	Help

😹 TLSServer [192.168.83.109:6000] Properties 🛛 🛛 🔀
General Certificate Advanced
Server: TLSServer V
Connection Protocol:
Local Timeout: 0
Remote Timeout: 0
Trace Mode: [Unknown Trace Mode]
Connection Mode: Unsecured
(<u>S</u> ecured
OK Cancel Help

Similar to the *Port* properties window, the *Certificate* tab allows you to select from a list of certificates or manually edit certificate properties. You can also use the *Advanced* tab to edit TLS settings not included with the certificate. However, the *Transport Protocol Parameters* field behaves differently for this object — which may result in lost or incorrect settings in some cases. See the Notes and Issues section for details.

🐱 TLSServer [192.168.83.109:6000] Properties 🛛 🛛 🔀
General Certificate Advanced
Certificate: "C:\certs\client-cert-3-cert.pem" Description:"" Key: "C:\certs\client-cert-3-key.pem" CA: "C:\certs\ca.pem"
OK Cancel Help

Configuring TLS Parameters in Configuration Manager

👪 TLSServer [192.168.83.109:6000] Properties 🛛 🛛 🔀
General Certificate Advanced
Transport Protocol Parameters:
certificate=C:\certs\client-cert-3-cert.pem;certificate-key=C:\certs \client-cert-3-key.pem;trusted-ca=C:\certs\ca.pem
Application Parameters:
OK Cancel Help

List of TLS Parameters

The following table lists all TLS parameters supported by Platform SDK, with their valid value ranges and purpose:

Parameter Name	Acceptable Values	Purpose
tls	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "tls=1"	Client: 1 - perform TLS handshake immediately after connecting to server. 0 - do not turn on TLS immediately but autodetect can still work.
provider	"PEM", "MSCAPI", "PKCS11" Not case-sensitive. Example: • "provider=MSCAPI"	Explicit selection of security provider to be used. For example, MSCAPI and PKCS11 providers can contain all other parameters in their internal database. This parameter allow configuration of TLS through security provider tools.

Parameter Name	Acceptable Values	Purpose
certificate	 PEM provider: path to a X.509 certificate file in PEM format. Path can use both forward and backward slash characters. MSCAPI provider: thumbprint of a certificate - string with hexadecimal SHA-1 hash code of the certificate. Whitespace characters are allowed anywhere within the string. PKCS11 provider: this parameter is ignored. Examples: "certificate = C:\certs\client-cert-3-cert.pem" "certificate = A4 7E A6 E4 7D 45 6A A6 2F 15 BE 89 FD 46 F0 EE 82 1A 58 B9" 	Specifies location of X.509 certificate to be used by application. MSCAPI provider keeps certificates in internal database and can identify them by hash code; so called thumbprint. In Java, PKCS#11 provider does not allow selection of the certificate; it must be configured using provider tools. Note: When using autodetect (upgrade) TLS connection, this option MUST be specified in application configuration, otherwise Configuration Server would return empty TLS parameters even if other options are set.
certificate-key	 PEM provider: path to a PKCS#8 private key file without password protection in PEM format. Path can use both forward and backward slash characters. MSCAPI provider: this parameter is ignored; key is taken from the entry identified by "certificate" field. PKCS11 provider: this parameter is ignored. Examples: "certificate-key= C:\certs\ client-cert-3-key.pem" 	Specifies location of PKCS#8 private key to be used in pair with the certificate by application. MSCAPI provider keeps private keys paired with certificates in internal database. In Java, PKCS#11 provider does not allow selection of the private key; it must be configured using provider tools.
trusted-ca	 PEM provider: path to a X.509 certificate file in PEM format. Path can use both forward and backward slash characters. MSCAPI provider: thumbprint of a certificate - string with hexadecimal SHA-1 hash code of the certificate. Whitespace characters are allowed anywhere within the string. PKCS11 provider: this parameter is ignored. Examples: "trusted-ca= C:\certs\ ca.pem" "trusted-ca=A4 7E A6 E4 7D 	Specifies location of a X.509 certificate to be used by application to validate remote party certificates. The certificate is designated as Trusted Certification Authority certificate and application will only trust remote party certificates signed with the CA certificate. MSCAPI provider keeps CA certificates in internal database and can identify them by hash code; so called thumbprint. In Java, PKCS#11 provider does not allow selection of the CA certificate; it must be configured using provider tools.

Parameter Name	Acceptable Values	Purpose
	45 6A A6 2F 15 BE 89 FD 46 F0 EE 82 1A 58 B9"	
tls-mutual	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "tls-mutual=1"	Has meaning only for server application. Client applications ignore this value. When turned on, server will require connecting clients to present their certificates and validate the certificates the same way as client applications do.
tls-crl	All providers: path to a Certificate Revocation List file in PEM format. Path can use both forward and backward slash characters. Example: • "tls-crl= C:\certs\crl.pem"	Applications will use CRL during certificate validation process to check if the (seemingly valid) certificate was revoked by CA. This option is useful to stop usage of leaked certificates by unauthorized parties.
tls-target-name-check	"host" or none. Not case- sensitive. Example: • "tls-target-name-check=host"	When set to "host", enables matching of certificate's Alternative Subject Name or Subject fields against expected host name. PSDK supports DNS names and IP addresses as expected host names.
cipher-list	String consisting of space- separated cipher suit names. Information on cipher names can be found online. Example: • "cipher-list= TLS_ECDHE_RSA_WITH_AES_25 TLS_ECDHE_RSA_WITH_AES_12 TLS_ECDH_RSA_WITH_3DES_ED	Used to calculate enabled cipher suites. Only ciphers present in both the cipher suites supported by security provider and the cipher-list parameter will be 6 CBC_SHA 8 CBC_SHA DE_CBC_SHA"
fips140-enabled	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "fips140-enabled=1"	PSDK Java: when set to true, effectively is the same as setting "provider=PKCS11" since only PKCS11 provider can support FIPS-140. If set to true while using other provider type, PSDK will throw exception.

Notes and Issues

- Key/value pairs in *Transport Protocol Parameters* fields should be separated only with a single semicolon character. Adding space characters to improve readability can cause applications, including those based on Platform SDK, unable to parse these parameters correctly.
- *Transport Protocol Parameters* fields in Configuration Manager are limited to 256 characters in length. Be sure to keep your parameter list as short as possible. For example: certificate thumbprints for MSCAPI provider take 40 characters without spaces and 49 characters with them, and long paths to certificate files can easily eat up all available space.
- The Connection properties window behaves differently from the Port properties window, as described below. Be sure to double-check TLS settings for Connection objects.
 - It does not save content of the *Transport Protocol Parameters* field unless a certificate was selected using UI controls on the *Certificate* tab.
 - If certificate information is deleted from the *Certificate* tab, then all transport protocol parameters are also erased (including those entered manually).
 - In some cases it does not save additional TLS parameters that were entered manually.
- Configuration Server reads its own TLS parameters from Application or from Host object only during startup. If you use an Application or Host object as a source of TLS parameters for Configuration Server, be sure to restart the server after any changes to the parameters.