z/OS 3.1 IBM Education Assistant

Solution Name: AT-TLS Currency – Support for x25519 and x448 KEX under TLSv1.2

Solution Name: AT-TLS Currency with System SSL

Solution Element(s): z/OS Communications Server

July 2023

Agenda

- Trademarks
- Objectives
- For each function:
  - Overview
  - Usage & Invocation
  - Diagnosis
  - Interactions & Dependencies
  - Upgrade & Coexistence Considerations
  - Installation & Configuration
  - Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- AT-TLS Currency – Support for x25519 and x448 KEX under TLSv1.2 (ZRM-648) provides the ability to negotiate x25519/x448 elliptic curves key exchange for TLS1.0-TLSv.2 protocol. This initiative also enhances security by allowing TLS server the ability to limit the elliptic curves used for TLSv1.0-TLSv1.2 key exchanges

- AT-TLS Currency with System SSL (ZRM-9856) - Optimized TLSv1.3 Sysplex Session Ticket Caching allows like-server applications using AT-TLS to benefit from sysplex-wide TLSv1.3 session resumption

Overview - Background: Application Transparent TLS (AT-TLS)

Policy-based TLS in the TCP/IP stack

- TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
- AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
  - Local address, port
  - Remote address, port
  - Connection direction
  - z/OS userid, jobname
  - Time, day, week, month
- The policy also specifies how to protect the traffic – TLS version, cipher suites, all kinds of TLS-specific settings

Application transparency

- Can be fully transparent to application
- An optional API allows applications to inspect or control certain aspects of AT-TLS processing – “application-aware” and “application- controlled” AT-TLS, respectively

Available to almost all TCP applications

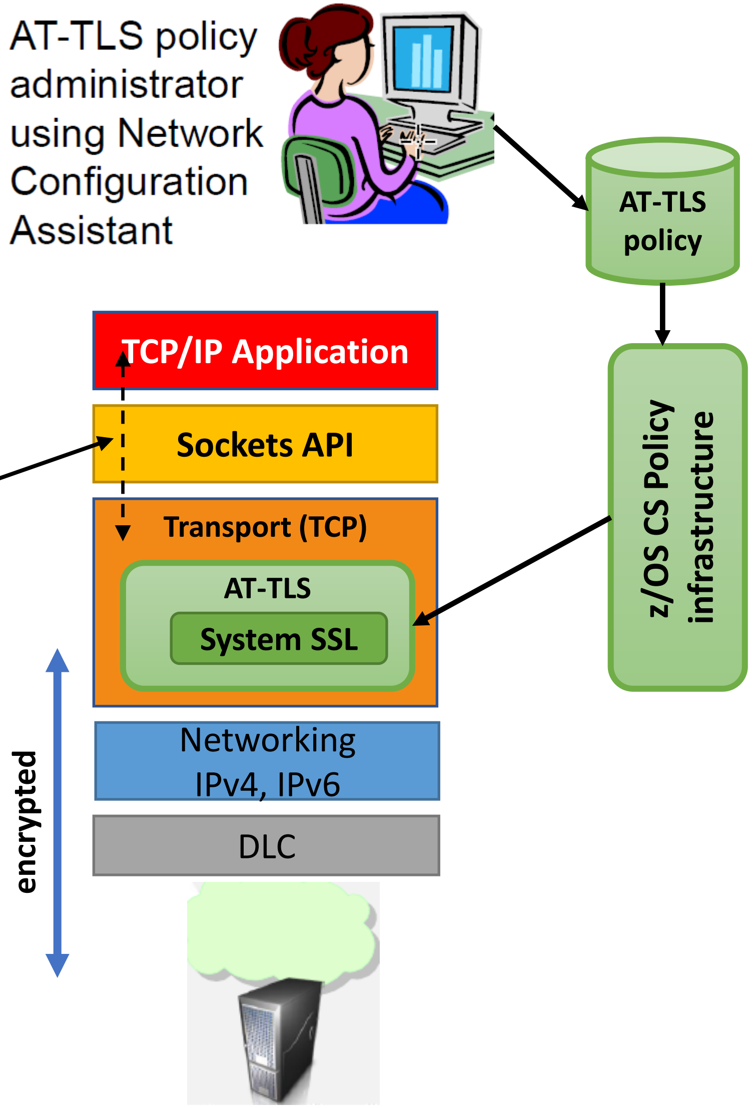
- Support all programming languages except PASCAL

Support all standard configurations

- z/OS as a client or as a server
- Server authentication (server identifies self to client)
- Client authentication (both ends identify selves to other)

Relies on Systems SSL for TLS protocol processing

- Remote endpoint sees an RFC-compliant implementation
- Interoperates with other compliant implementations



AT-TLS Currency – Support for x25519 and x448 KEX under TLSv1.2 (ZRM-648)

Overview

- Who
  - z/OS network security administrator with responsibility for protecting applications with AT-TLS
- What (Solution)
  - AT-TLS Currency – Support for x25519 and x448 KEX under TLSv1.2
- Wow (Benefit / Value, Need Addressed)
  - You can use x25519/x448 key exchange curves for TLSv1.0 – TLSv1.2 AT-TLS connections
  - AT-TLS servers can ensure stronger elliptic curves by limiting the list of curves used for key exchange negotiations

Overview - Background – Elliptic Curve Configuration

- Designations for different **elliptic curves** that are allowed for use in Elliptic Curve Diffie Hellman (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA) operations
- Separate **ECurve** configuration for TLS client vs. TLS server
- Like cipher suites, the client proposes a list of **ECurves** to the server (in order of preference) and then the server selects one that it is willing to use

The key exchange mechanism is indicated through TLS configuration and negotiated early in the TLS handshake process:

- Cipher suites up through TLSv1.2 – groupings of cryptographic algorithms and strengths:

  Example: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

  - Key exchange algorithm (the method by which both endpoints derive the secret session keys)
  - The type of asymmetric key in the server certificate
  - Bulk encryption algorithm (including secret key length)
  - Hashing algorithm (often used for message authentication/integrity protection)

Overview – AT-TLS Solution

System SSL has provided support for:

- ❖ x25519 and x448 ecurves key exchange for TLSv1.2 and earlier protocols
- ❖ option to limit the TLS server’s allowable ecurves

AT-TLS is exposing this functionality through AT-TLS configuration parameters

- ➢ To use x25519 and x448 key exchange curves for TLSv1.0, TLSv1.1, or TLSv1.2 negotiation, you must configure:
  - **ClientECurves** parameter on the TTLSSignatureParms statement with the proposed curves on the AT-TLS client rule
  - Specify the curves on the server side using the new **ServerKexECurves** parameter on the TTLSSignatureParms statement
- ➢ To allow AT-TLS server to limit the key exchange curves that can be used for TLSv1.0, TLSv1.1, and TLSv1.2:
  - Use the new AT-TLS parameter, **ServerKexECurves**, to limit the curves that a TLS server supports. Parameter can be specified on the TTLSSignatureParms statement associated with the TTLSEnvironmentAction or TTLSConnectionAction statements

Usage & Invocation - AT-TLS Policy Configuration

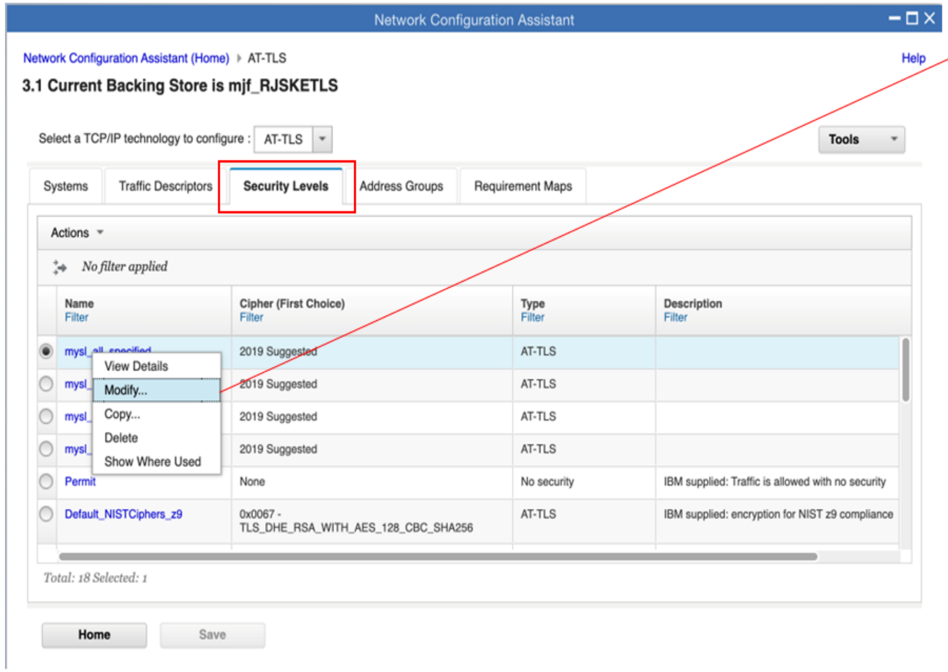
TTLSSignatureParms configuration for AT-TLS

```
TTLSSignatureParms Parameters

  .-ClientECurves default_client_ecurves-.
   |                                      |
|--+--------------------------------------+----------------------------->
   +-ClientECurves-Any--------------------+
   '-+-----------------------------+------'
   | .---------------------------. |
   | V                           | |
   '---ClientECurves-curves----- +-'

   .-ServerKexECurves 00230024002500210019---.
   |                                         |
|--+-----------------------------------------+--------------------------->
   | .-------------------------------------. |
   | V                                     | |
   '---ServerKexECurves -curves------------+-'
```

- TTLSSignatureParms can be specified for an environment and connection action
- Default on environment action: 0023(secp256r1),0024(secp384r1),0025(secp521r1),0021(secp224r1),0019(secp192r1)
- No default for connection action
- Values specified on the environment action will be used when none are specified on the connection action

Usage & Invocation – Navigating to the client and server ecurve configuration

Signature and key share controls… locating them in the NCA panels



Network Configuration Assistant

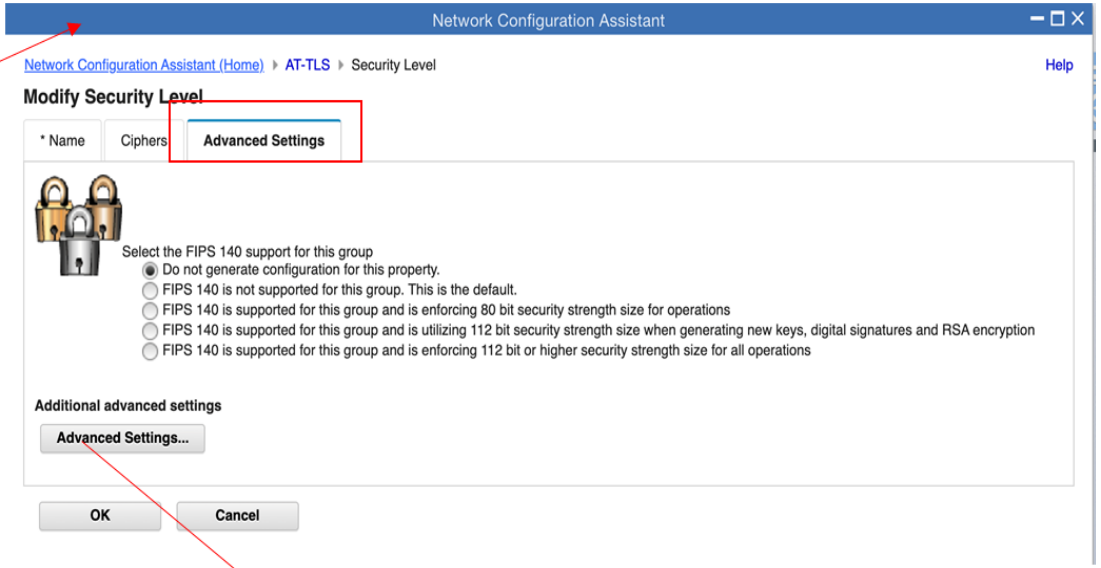
Network Configuration Assistant (Home) ▸ AT-TLS

3.1 Current Backing Store is mjf_RJSKETLS

Select a TCP/IP technology to configure : AT-TLS

Name	Cipher (First Choice)	Type	Description
● mysl_all_specified	2019 Suggested	AT-TLS	
○ mysl_	2019 Suggested	AT-TLS	
○ mysl_	2019 Suggested	AT-TLS	
○ mysl_	2019 Suggested	AT-TLS	
○ Permit	None	No security	IBM supplied: Traffic is allowed with no security
○ Default_NISTCiphers_z9	0x0067 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z9 compliance

Total: 18 Selected: 1



Network Configuration Assistant

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level

Modify Security Level

Select the FIPS 140 support for this group

● Do not generate configuration for this property.
○ FIPS 140 is not supported for this group. This is the default.
○ FIPS 140 is supported for this group and is enforcing 80 bit security strength size for operations
○ FIPS 140 is supported for this group and is utilizing 112 bit security strength size when generating new keys, digital signatures and RSA encryption
○ FIPS 140 is supported for this group and is enforcing 112 bit or higher security strength size for all operations

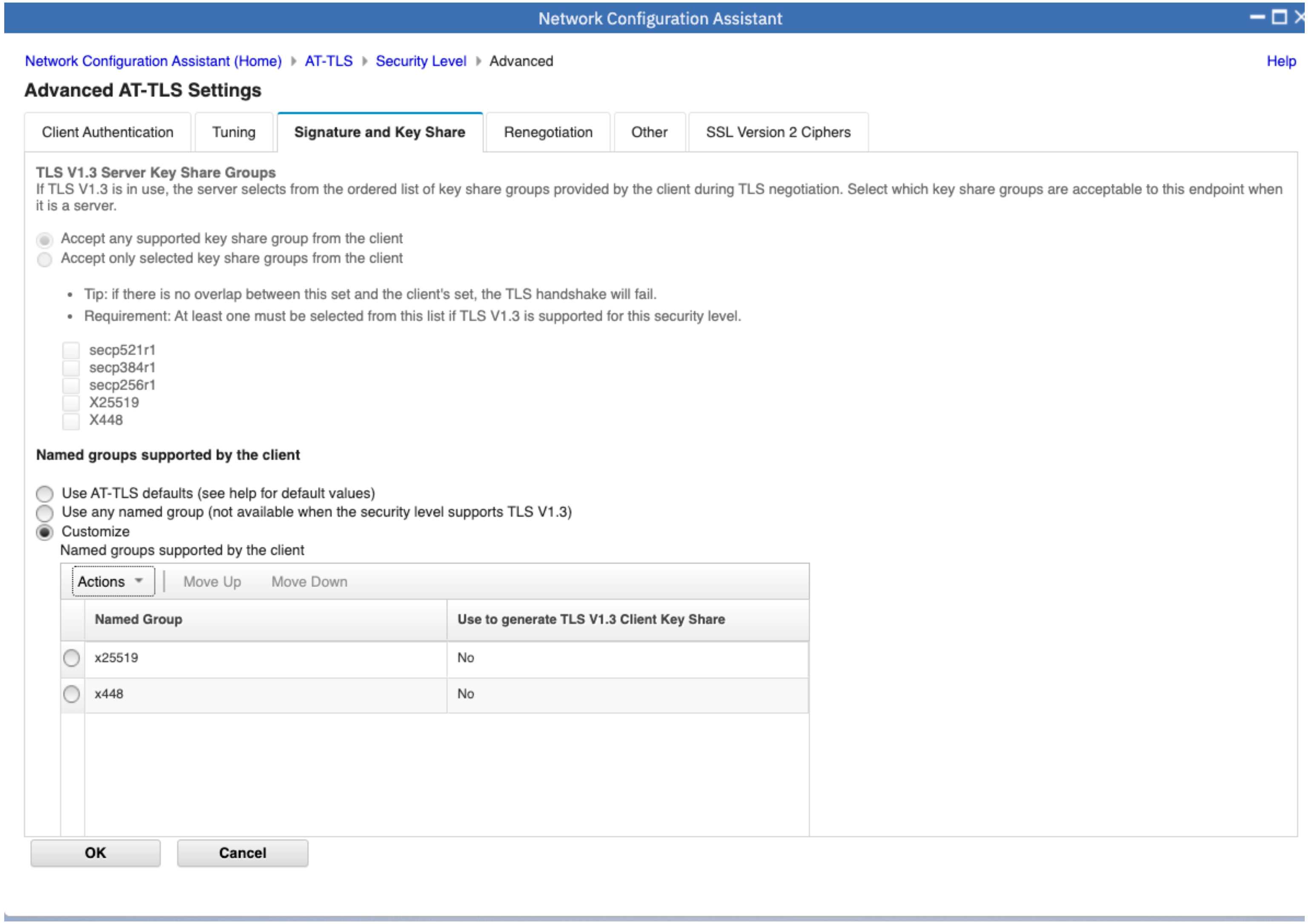
Additional advanced settings

Signature and Key Share settings are in the advanced settings for an AT-TLS security level

Next slide

Usage & Invocation – Configuring Client Ecurves (ClientECurves parameter)

NCA for the new x25519 and x448 support - client



Network Configuration Assistant

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced

Help

Advanced AT-TLS Settings

TLS V1.3 Server Key Share Groups

If TLS V1.3 is in use, the server selects from the ordered list of key share groups provided by the client during TLS negotiation. Select which key share groups are acceptable to this endpoint when it is a server.

● Accept any supported key share group from the client
○ Accept only selected key share groups from the client

- Tip: if there is no overlap between this set and the client's set, the TLS handshake will fail.
- Requirement: At least one must be selected from this list if TLS V1.3 is supported for this security level.

□ secp521r1
□ secp384r1
□ secp256r1
□ X25519
□ X448

Named groups supported by the client

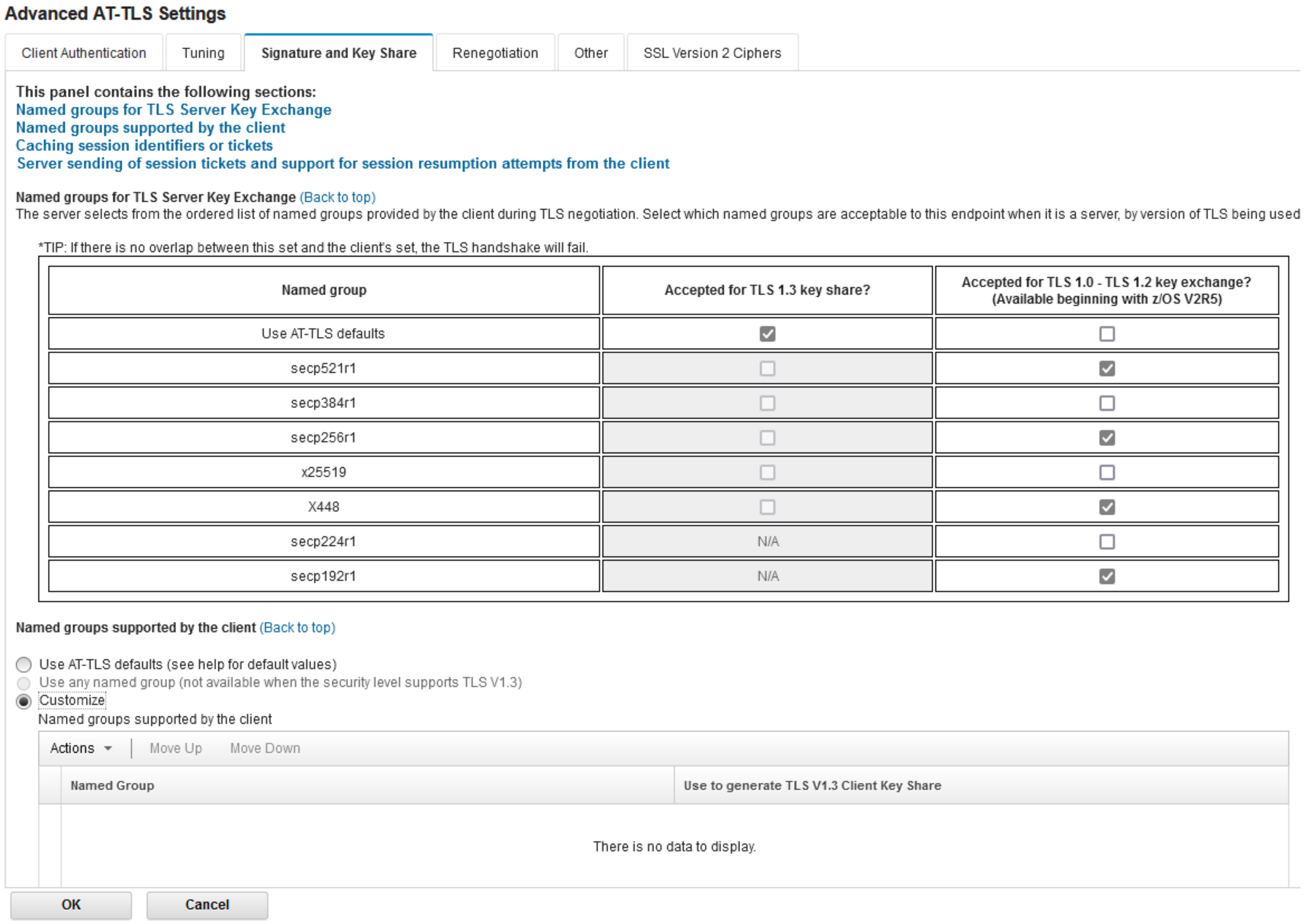
○ Use AT-TLS defaults (see help for default values)
○ Use any named group (not available when the security level supports TLS V1.3)
● Customize

Named groups supported by the client

	Named Group	Use to generate TLS V1.3 Client Key Share
○	x25519	No
○	x448	No

Usage & Invocation – Configuring server allowed ecurves (ServerKexECurves parameter)

Update to NCA for TLS 1.0-1.2 server acceptable key shares



Advanced AT-TLS Settings

This panel contains the following sections:
Named groups for TLS Server Key Exchange
Named groups supported by the client
Caching session identifiers or tickets
Server sending of session tickets and support for session resumption attempts from the client

Named groups for TLS Server Key Exchange (Back to top)
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☑	☐
secp521r1	☐	☑
secp384r1	☐	☐
secp256r1	☐	☑
x25519	☐	☐
X448	☐	☑
secp224r1	N/A	☐
secp192r1	N/A	☑

Named groups supported by the client (Back to top)

○ Use AT-TLS defaults (see help for default values)
○ Use any named group (not available when the security level supports TLS V1.3)
● Customize

Named groups supported by the client

Named Group	Use to generate TLS V1.3 Client Key Share

There is no data to display.

The first table in the Security Level Advanced settings, **Signature and Key Share** tab, contains controls for this new function.

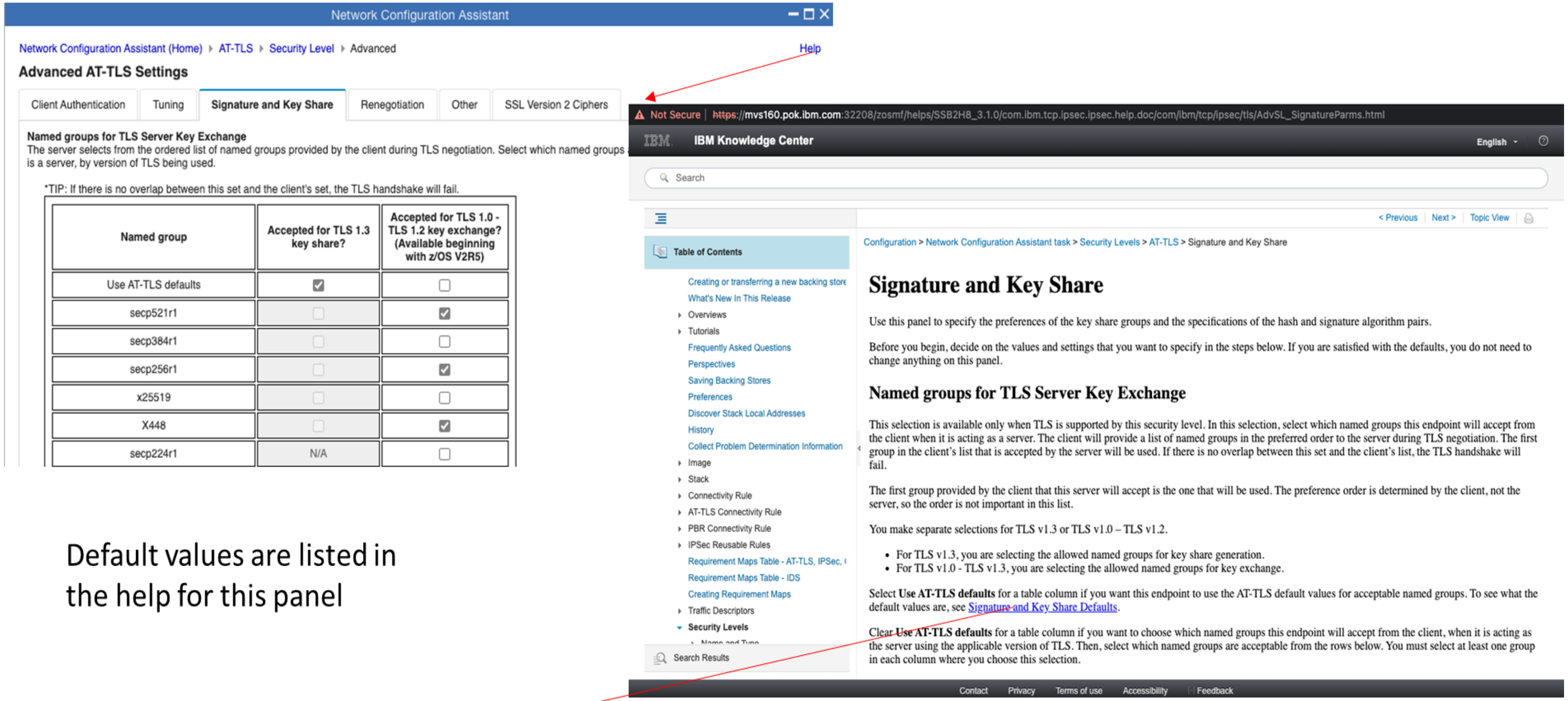
The first column in the table controls which named groups are accepted for TLS 1.3 key share.

The second column in the table controls which named groups are accepted for TLS 1.0-1.2 key exchange. This is new for this function.

When "Accept AT-TLS defaults" is checked for a column, the rest of the column is greyed out as show in the middle column of this example.

Usage & Invocation – How to find AT-TLS default values

How to find the default values



Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced

Advanced AT-TLS Settings

Named groups for TLS Server Key Exchange

The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups
is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☑	☐
secp521r1	☐	☑
secp384r1	☐	☐
secp256r1	☐	☑
x25519	☐	☐
X448	☐	☑
secp224r1	N/A	☐

⚠ Not Secure | ~~https~~://mvs160.pok.ibm.com:32208/zosmf/helps/SSB2H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com/ibm/tcp/ipsec/tls/AdvSL_SignatureParms.html

Configuration > Network Configuration Assistant task > Security Levels > AT-TLS > Signature and Key Share

Signature and Key Share

Use this panel to specify the preferences of the key share groups and the specifications of the hash and signature algorithm pairs.

Before you begin, decide on the values and settings that you want to specify in the steps below. If you are satisfied with the defaults, you do not need to change anything on this panel.

Named groups for TLS Server Key Exchange

This selection is available only when TLS is supported by this security level. In this selection, select which named groups this endpoint will accept from the client when it is acting as a server. The client will provide a list of named groups in the preferred order to the server during TLS negotiation. The first group in the client's list that is accepted by the server will be used. If there is no overlap between this set and the client's list, the TLS handshake will fail.

The first group provided by the client that this server will accept is the one that will be used. The preference order is determined by the client, not the server, so the order is not important in this list.

You make separate selections for TLS v1.3 or TLS v1.0 – TLS v1.2.

- For TLS v1.3, you are selecting the allowed named groups for key share generation.
- For TLS v1.0 - TLS v1.3, you are selecting the allowed named groups for key exchange.

Select **Use AT-TLS defaults** for a table column if you want this endpoint to use the AT-TLS default values for acceptable named groups. To see what the default values are, see Signature and Key Share Defaults.

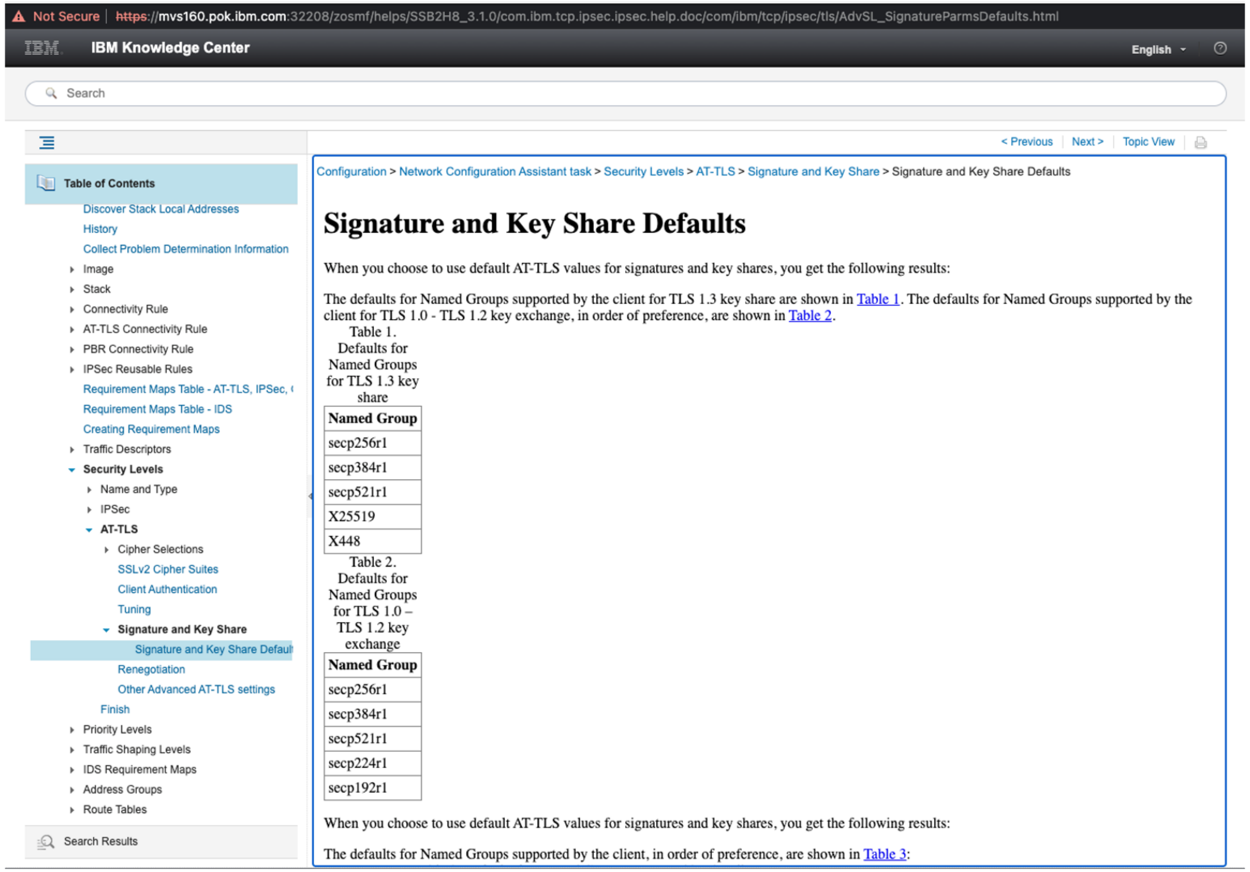
Clear **Use AT-TLS defaults** for a table column if you want to choose which named groups this endpoint will accept from the client, when it is acting as the server using the applicable version of TLS. Then, select which named groups are acceptable from the rows below. You must select at least one group in each column where you choose this selection.

Default values are listed in the help for this panel

Next slide

Usage & Invocation – AT-TLS default values for client and server ecurves

Signature and key share defaults


Not Secure
https://mvs160.pok.ibm.com:32208/zosmf/helps/SSB2H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com/ibm/tcp/ipsec/tls/AdvSL_SignatureParmsDefaults.html
IBM Knowledge Center
English
Search
< Previous
Next >
Topic View
Table of Contents
Discover Stack Local Addresses
History
Collect Problem Determination Information
Image
Stack
Connectivity Rule
AT-TLS Connectivity Rule
PBR Connectivity Rule
IPSec Reusable Rules
Requirement Maps Table - AT-TLS, IPSec,
Requirement Maps Table - IDS
Creating Requirement Maps
Traffic Descriptors
Security Levels
Name and Type
IPSec
AT-TLS
Cipher Selections
SSLv2 Cipher Suites
Client Authentication
Tuning
Signature and Key Share
Signature and Key Share Defaul
Renegotiation
Other Advanced AT-TLS settings
Finish
Priority Levels
Traffic Shaping Levels
IDS Requirement Maps
Address Groups
Route Tables
Search Results
Configuration > Network Configuration Assistant task > Security Levels > AT-TLS > Signature and Key Share > Signature and Key Share Defaults

Signature and Key Share Defaults

When you choose to use default AT-TLS values for signatures and key shares, you get the following results:

The defaults for Named Groups supported by the client for TLS 1.3 key share are shown in Table 1. The defaults for Named Groups supported by the client for TLS 1.0 - TLS 1.2 key exchange, in order of preference, are shown in Table 2.

Table 1. Defaults for Named Groups for TLS 1.3 key share

Named Group
secp256r1
secp384r1
secp521r1
X25519
X448

Table 2. Defaults for Named Groups for TLS 1.0 – TLS 1.2 key exchange

Named Group
secp256r1
secp384r1
secp521r1
secp224r1
secp192r1

When you choose to use default AT-TLS values for signatures and key shares, you get the following results:

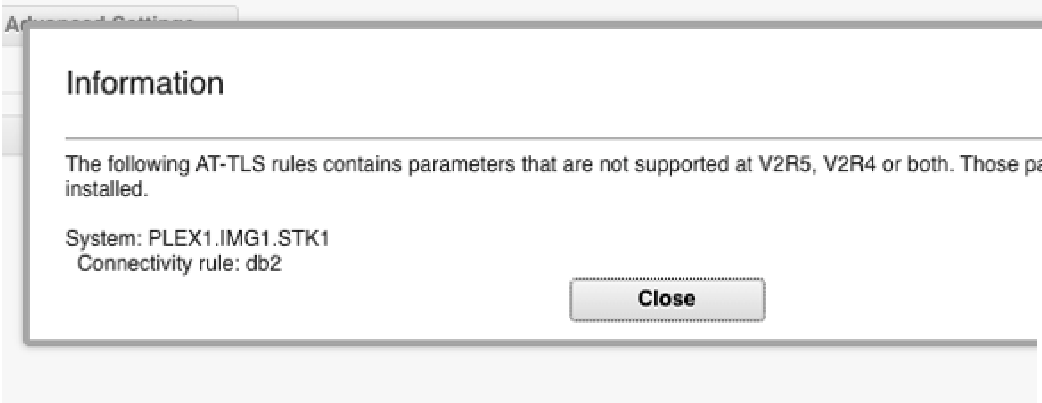
The defaults for Named Groups supported by the client, in order of preference, are shown in Table 3:

This help file lists the default values for all the settings on the Signature and Key Share tab. Note that NCA defaults align with AT-TLS defaults.

Usage & Invocation – NCA release-level considerations

Release-level considerations

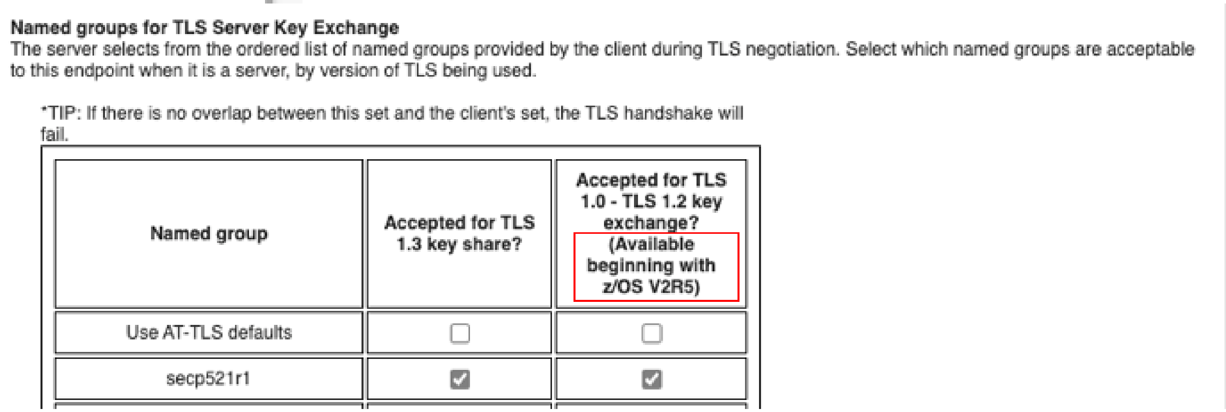
- The GUI will allow you to configure it for any stack at any release level
- When generating configuration files, NCA will simply skip generating configuration not supported at the stack’s release level
  - This allows users to smoothly change release levels of stacks without having to alter configuration



Information

The following AT-TLS rules contains parameters that are not supported at V2R5, V2R4 or both. Those parameters will not be installed.

System: PLEX1.IMG1.STK1
  Connectivity rule: db2



Named groups for TLS Server Key Exchange

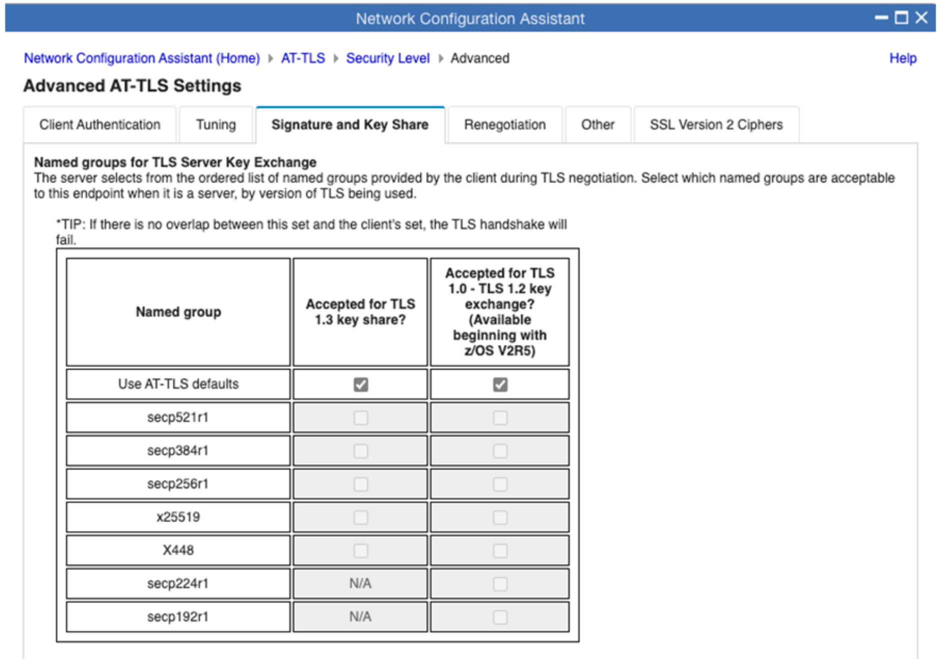
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☐	☐
secp521r1	☑	☑

Usage & Invocation – NCA configuration examples (1 of 2)

NCA configuration examples (1/2)


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced
Help
Client Authentication
Tuning
Signature and Key Share
Renegotiation
Other
SSL Version 2 Ciphers

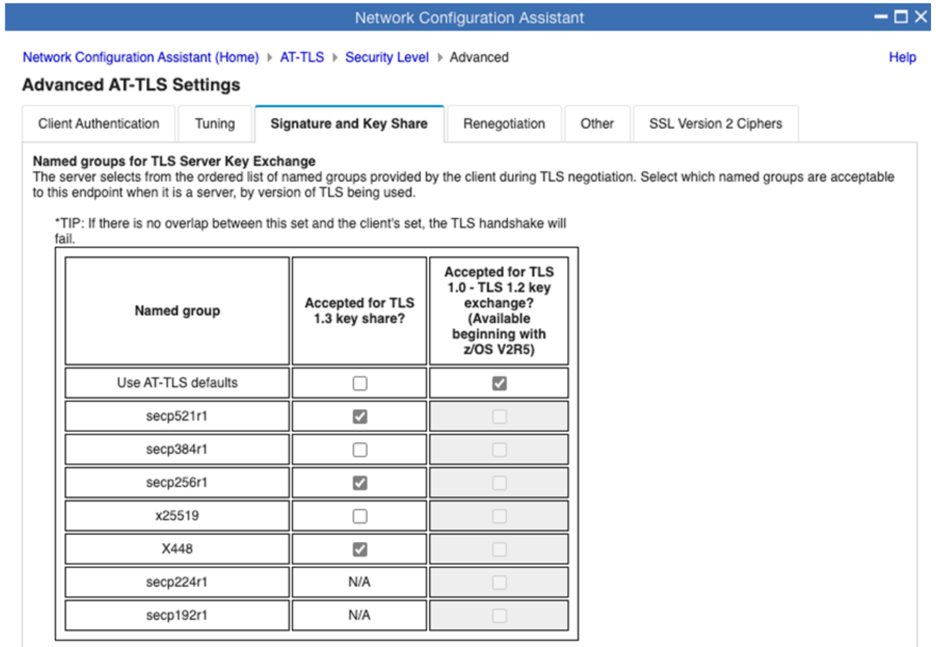
Advanced AT-TLS Settings

Named groups for TLS Server Key Exchange
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☑	☑
secp521r1	□	□
secp384r1	□	□
secp256r1	□	□
x25519	□	□
X448	□	□
secp224r1	N/A	□
secp192r1	N/A	□

Result: No parameters for server key share created in the TTLSSignatureParms group. No TTLSSignatureParms group created if no other parameters are needed.


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced
Help
Client Authentication
Tuning
Signature and Key Share
Renegotiation
Other
SSL Version 2 Ciphers

Advanced AT-TLS Settings

Named groups for TLS Server Key Exchange
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	□	☑
secp521r1	☑	□
secp384r1	□	□
secp256r1	☑	□
x25519	□	□
X448	☑	□
secp224r1	N/A	□
secp192r1	N/A	□

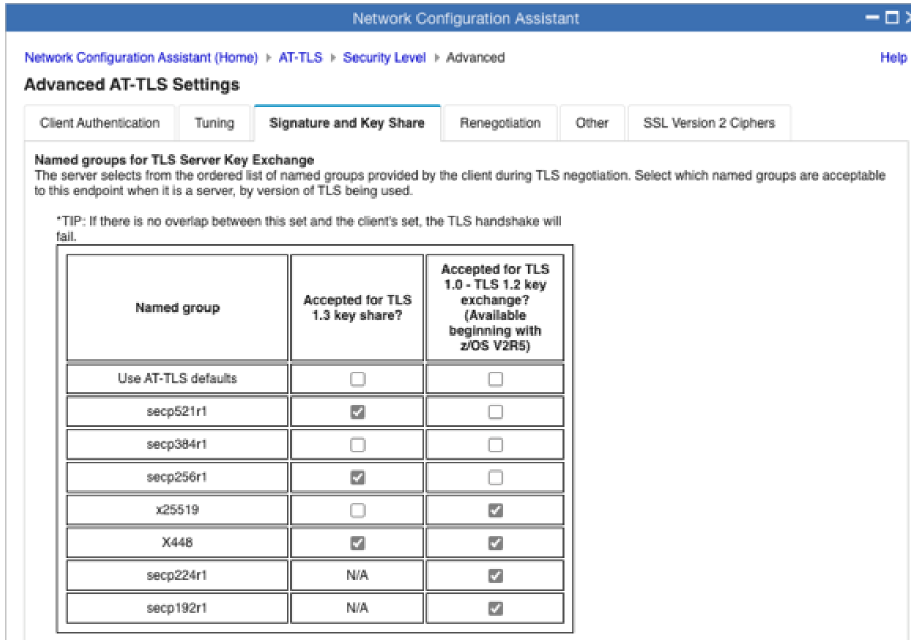
Result:

```
TTLSSignatureParms  sig1~mysl
{
    ServerKeyShareGroups   secp521r1
    ServerKeyShareGroups   secp256r1
    ServerKeyShareGroups   X448
    [any other parameters in this statement]
}
```

Usage & Invocation – NCA configuration examples (2 of 2)

Function externals: NCA Configuration…8

NCA configuration examples (2/2)


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced
Help
Client Authentication
Tuning
Signature and Key Share
Renegotiation
Other
SSL Version 2 Ciphers

Advanced AT-TLS Settings

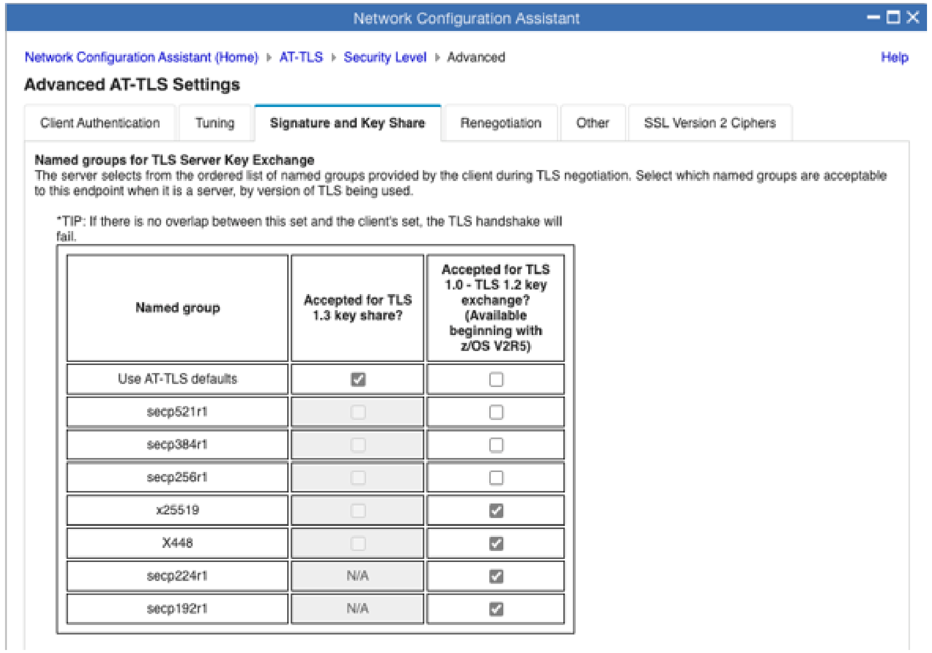
Named groups for TLS Server Key Exchange
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☐	☐
secp521r1	☑	☐
secp384r1	☐	☐
secp256r1	☑	☐
x25519	☐	☑
X448	☑	☑
secp224r1	N/A	☑
secp192r1	N/A	☑

Result:

```
TTLSSignatureParms  sig1~mysl
{
    ServerKeyShareGroups   secp521r1
    ServerKeyShareGroups   secp256r1
    ServerKeyShareGroups   X448
    ServerKexECurves       secp224r1
    ServerKexECurves       secp192r1
    ServerKexECurves       X25519
    ServerKexECurves       X448
        [any other parameters in this statement]
}
```


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced
Help
Client Authentication
Tuning
Signature and Key Share
Renegotiation
Other
SSL Version 2 Ciphers

Advanced AT-TLS Settings

Named groups for TLS Server Key Exchange
The server selects from the ordered list of named groups provided by the client during TLS negotiation. Select which named groups are acceptable to this endpoint when it is a server, by version of TLS being used.

*TIP: If there is no overlap between this set and the client's set, the TLS handshake will fail.

Named group	Accepted for TLS 1.3 key share?	Accepted for TLS 1.0 - TLS 1.2 key exchange? (Available beginning with z/OS V2R5)
Use AT-TLS defaults	☑	☐
secp521r1	☐	☐
secp384r1	☐	☐
secp256r1	☐	☐
x25519	☐	☑
X448	☐	☑
secp224r1	N/A	☑
secp192r1	N/A	☑

Result:

```
TTLSSignatureParms  sig1~mysl
{
    ServerKexECurves       secp224r1
    ServerKexECurves       secp192r1
    ServerKexECurves       X25519
    ServerKexECurves       X448
        [any other parameters in this statement]
}
```

Usage & Invocation - z/OS UNIX pasearch output

- Pasearch is a command to display a configured policy
- Pasearch output display for a server environment TTLS action with configured ServerKexECurves values

```
TTLSSignatureParms:
 ClientECurves:
  0019 secp192r1
  0021 secp224r1
  0023 secp256r1
  0024 secp384r1
  0025 secp521r1
 ClientKeyShareGroups:
  0025 secp521r1
 ServerKeyShareGroups:
  0025 secp521r1
 ServerKexECurves:
  0023 secp256r1
  0024 secp384r1
  0025 secp521r1
  0029 x25519
  0030 x448
```

Usage & Invocation - Netstat TTLS/-x DETAIL

- Netstat TTLS/-x display output for a server TTLS environment action with configured ServerKexECurves values

```
TTLSEnvAction:            env_act_serv
EnvironmentUserInstance: 8
HandshakeRole:          Server
...
ClientECurves:          0024 secp384r1
                        0025 secp521r1
ClientKeyShareGroups:   0025 secp521r1
ServerKeyShareGroups:   0025 secp521r1
ServerKexECurves:       0023 secp256r1
                        0024 secp384r1
                        0025 secp521r1
                        0029 x25519
                        0030 x448
SignaturePairs:         0401 TLS_SIGALG_SHA256_WITH_RSA
                        0403 TLS_SIGALG_SHA256_WITH_ECDSA
                        0804 TLS_SIGALG_SHA256_WITH_RSASSA_
...
```

Diagnosis – AT-TLS syslog messages

- ➢Log contains messages showing the values set for GSK_CLIENT_ECURVE_LIST and GSK_SERVER_ALLOWED_KEX_ECURVES
- ➢Contains the negotiated ecurve value (GSK_CONNECT_KEX_ECURVE)

```
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000D CONNID: 000000F7  RC:    0 Set GSK_CLIENT_ECURVE_LIST(215) -  00210023002400250019002900 30
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000F CONNID: 000000F8  RC:    0 Set GSK_SERVER_ALLOWED_KEX_ECURVES(230) -  00300029
...
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Call GSK_SECURE_SOCKET_INIT - 00000050114283B0
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_CONNECT_SEC_TYPE(208) -  TLSV1.2
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_CONNECT_CIPHER_SPEC(207) -  C027
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_CONNECT_KEX_ECURVE(231) -  0030
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_TLSEXT_MFL(413) - 0000000000000215
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_SID_VALUE(212) - 000000000000002C
EZD1284I TTLS Flow  GRPID: 00000005 ENVID: 0000000E CONNID: 000000F8  RC:    0 Get GSK_SID_VALUE(212) - 000000000000002C
```

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Upgrade consideration:
  - System SSL provided the ability for a TLS server to limit the ecurve values accepted in z/OS V2R4 and V2R5 with APAR OA61783
  - AT-TLS provided the ServerKexECurves configuration value in z/OS V2R5 with APAR PH45902
  - In V2R4 an environment variable can be configured to take advantage of the function even without the AT-TLS configuration
  - In V2R5 with PH45902 or in z/OS 3.1, the AT-TLS configuration must be used to configure the desired value. The environment variable is overridden
    - If the AT-TLS ServerKexECurves parameter is not configured, the environment variable is overridden by the Policy Agent default value.
- Coexistence considerations: None

Installation & Configuration

- Policy should be updated either through NCA or manually, a MODIFY PAGENT,UPDATE or REFRESH can be issued to install the new policy.
  The z/OS UNIX pasearch command can be used to confirm that the policy is configured as expected.

- To use x25519 and x448 ecurves for TLSv1.2 and earlier, update existing client and server AT-TLS policy with the new ecurves on the ClientECurves parameter on the client and ServerKexECurves parameter on the server, in order to be used for key exchange negotiation

- To limit the server’s ecurve list, update the server’s AT-TLS policy with the limited ecurves on the ServerKexECurves parameter

Summary

- This initiative allows elliptic curves x25519 and x448 to be used in key exchange negotiation during handshake process for TLSv1.0, TLSv1.1, and TLSv1.2 protocol
- AT-TLS server also has the ability limit its curve list used for key exchange negotiation
- This function is available in z/OS V2R5 with APAR PH45902
  - System SSL APAR (OA61783) is required
  - NCA APAR PH47400 provides the ability to configure the new parameters for V2R5

AT-TLS Currency with System SSL (ZRM-9856) – TLSv1.3 Sysplex Session Ticket Caching

Overview

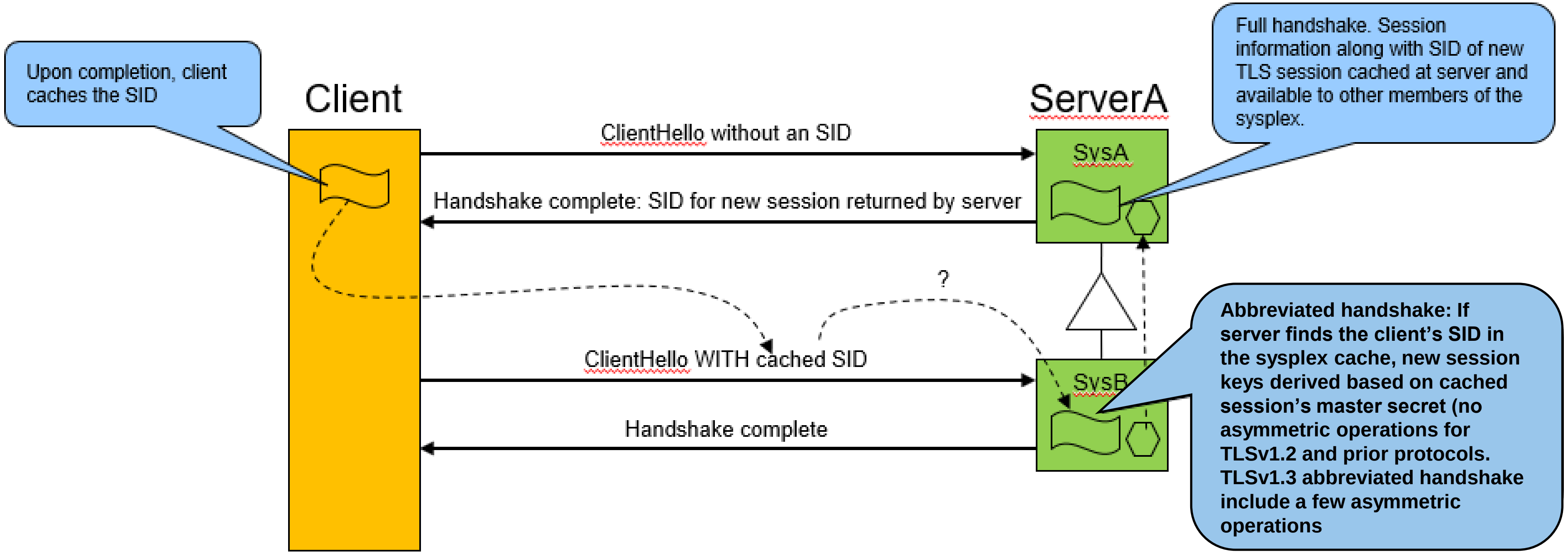
- Who
    - z/OS network security administrator with responsibility for protecting applications with AT-TLS
- What (Solution)
    - AT-TLS Currency with System SSL – Optimized TLSv1.3 Sysplex Session Ticket Caching
- Wow (Benefit / Value, Need Addressed)
    - You can enable sysplex-wide session ticket caching for TLSv1.3 protocol to benefit from session resumption
    - AT-TLS client has the ability to configure maximum number of TLSv1.3 session tickets that can be stored per session in its cache

Overview - Background – Sysplex-wide TLS Session Resumption (1 of 2)

- Up through TLSv1.2 System SSL supported sysplex-wide Session ID (SID) caches
- Enabled through special configuration parameter

  GSK_SYSPLEX_SIDCACHE ON

- Requires GSKSRVER started task (⬢) to be running


Upon completion, client caches the SID
Client
ServerA
ClientHello without an SID
SysA
Handshake complete: SID for new session returned by server
?
ClientHello WITH cached SID
SysB
Handshake complete

Full handshake. Session information along with SID of new TLS session cached at server and available to other members of the sysplex.

Abbreviated handshake: If server finds the client's SID in the sysplex cache, new session keys derived based on cached session's master secret (no asymmetric operations for TLSv1.2 and prior protocols. TLSv1.3 abbreviated handshake include a few asymmetric operations

Overview - Background – TLS Session Resumption (2 of 2)

- TLSv1.3 protocol supports session resumption through a different approach
  - Uses “session tickets” that contain all the information the server needs to resume a TLSv1.3 session
  - No server-side cache
  - Client caches one-time-use “session tickets” returned by server
  - Session ticket is encrypted and decrypted by server using AES
  - To perform an abbreviated handshake, the client sends a Client Hello message to the server that contains a cached session ticket from the client cache
  - If the server recognizes the ticket and can successfully decrypt it, it continues with the abbreviated handshake with many of the same advantages seen in previous TLS versions

- AT-TLS supported TLSv1.3 beginning in V2R4 including support for session resumption using session tickets but only within the scope of a single application address space. No sysplex-wide support.

Overview – Solution

- System SSL is adding sysplex-wide support for TLSv1.3 session tickets
  - Requires GSKSRVR started task

- AT-TLS is providing new parameters for exploiters to be able to use the new function
  - To enable sysplex-wide TLSv1.3 session ticket caching for an AT-TLS server
    - Configure the new AT-TLS parameter **GSK_SYSPLEX_SESSION_TICKET_CACHE** on the TTLSGskAdvancedParms statement
    - GSKSRVR task must be started for all systems in the sysplex that require TLS session resumption
  - Optionally configure **GSK_SESSION_TICKET_CLIENT_MAXCACHED** parameter on the client to specify the maximum number of session tickets that are allowed to be cached by the client for each unique TLSv1.3 session

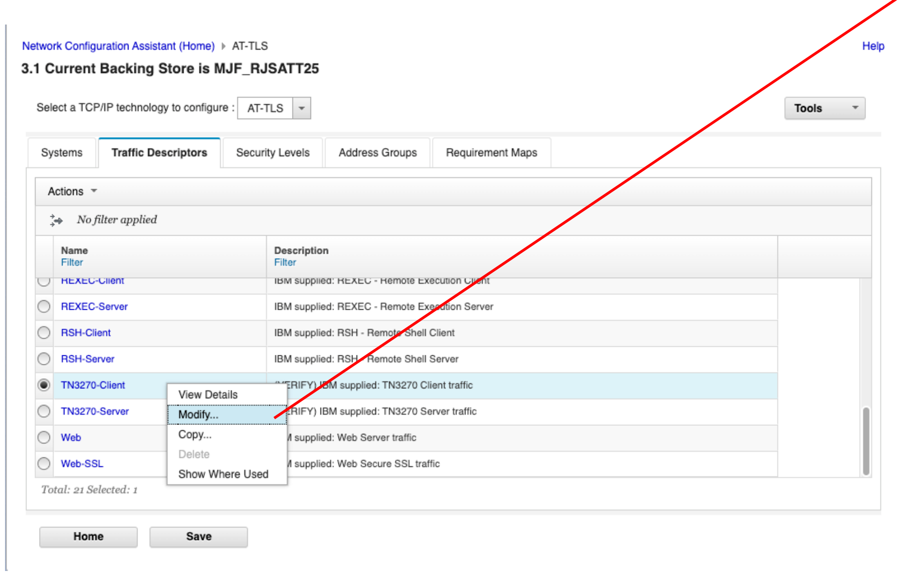
Usage & Invocation - Function externals: AT-TLS Policy

TTLSGskAdvancedParms configuration for AT-TLS

```
TTLSGskAdvancedParms Parameters
. . .
>--+------------------------------+---------------------------------->
   +-GSK_SYSPLEX_SIDCACHE-+-On--+-'
                          '-Off-'

>--+------------------------------------------+---------------------->
   +-GSK_SYSPLEX_SESSION_TICKET_CACHE-+-On--+-'
                                      '-Off-'
. . .

   .-GSK_SESSION_TICKET_CLIENT_MAXSIZE 8192--.
   |                                         |
>--+-----------------------------------------+------------------------>
   +-GSK_SESSION_TICKET_CLIENT_MAXSIZE value-’


>--+-------------------------------------------+---------------------->
   +-GSK_SESSION_TICKET_CLIENT_MAXCACHED value-'

. . .

   .-GSK_SESSION_TICKET_SERVER_TIMEOUT default_value---.
   |                                                   |
>--+---------------------------------------------------+-------------->
   +-GSK_SESSION_TICKET_SERVER_TIMEOUT value-----------'
```

Usage & Invocation – Navigating to the traffic descriptor (TD)

Traffic descriptor – getting to advanced parameters



Network Configuration Assistant (Home) ▸ AT-TLS

Help

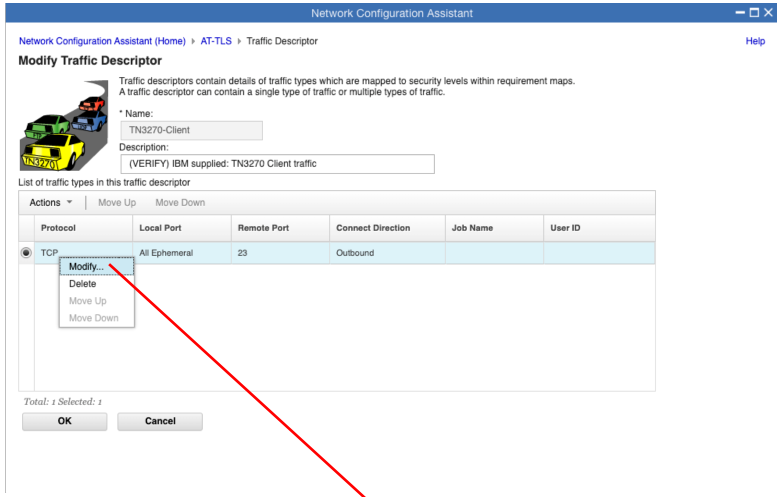
3.1 Current Backing Store is MJF_RJSATT25

Select a TCP/IP technology to configure : AT-TLS

No filter applied

	Name Filter	Description Filter
○	REXEC-Client	IBM supplied: REXEC - Remote Execution Client
○	REXEC-Server	IBM supplied: REXEC - Remote Execution Server
○	RSH-Client	IBM supplied: RSH - Remote Shell Client
○	RSH-Server	IBM supplied: RSH - Remote Shell Server
●	TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
○	TN3270-Server	ERIFY) IBM supplied: TN3270 Server traffic
○	Web	supplied: Web Server traffic
○	Web-SSL	supplied: Web Secure SSL traffic

Total: 21 Selected: 1



Network Configuration Assistant

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Traffic Descriptor

Help

Modify Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps.
A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name: TN3270-Client

Description: (VERIFY) IBM supplied: TN3270 Client traffic

List of traffic types in this traffic descriptor

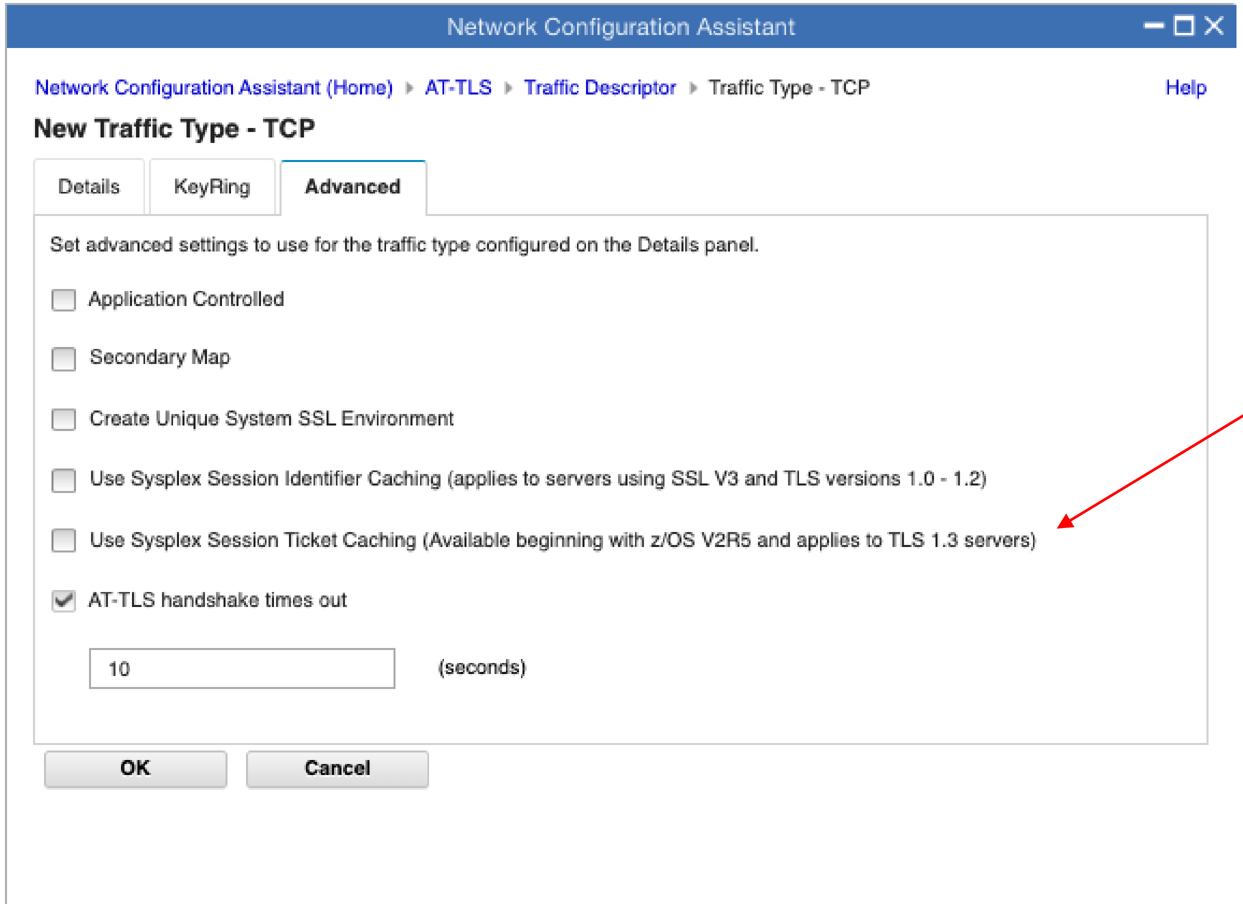
	Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID
●	TCP	All Ephemeral	23	Outbound		

Total: 1 Selected: 1

Next slide

Usage & Invocation – Enabling sysplex session ticket caching on the Traffic Descriptor

Controlling sysplex-wide session ticket caching


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Traffic Descriptor ▸ Traffic Type - TCP
Help
Details
KeyRing
Advanced
OK
Cancel

New Traffic Type - TCP

Set advanced settings to use for the traffic type configured on the Details panel.

□ Application Controlled

□ Secondary Map

□ Create Unique System SSL Environment

□ Use Sysplex Session Identifier Caching (applies to servers using SSL V3 and TLS versions 1.0 - 1.2)

□ Use Sysplex Session Ticket Caching (Available beginning with z/OS V2R5 and applies to TLS 1.3 servers)

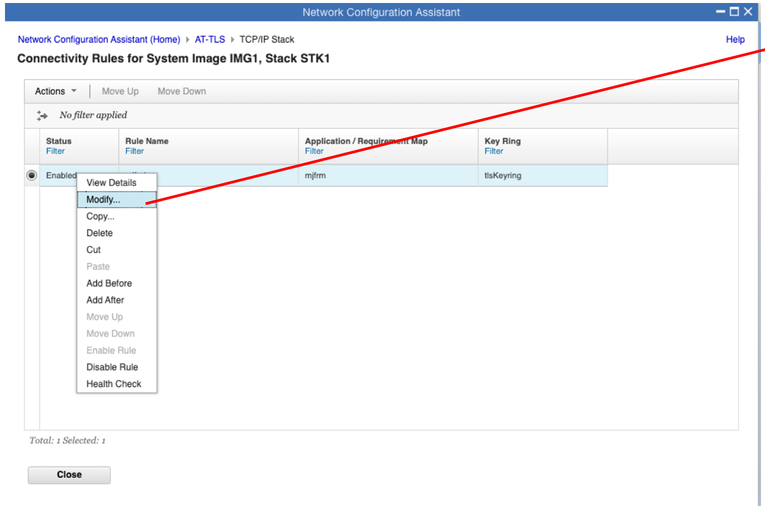
☑ AT-TLS handshake times out

10 (seconds)

New parameter to control sysplex session ticket caching for this traffic type

Usage & Invocation - Navigating to a Traffic Descriptor within a connectivity rule

Sysplex-wide session ticket caching can be overridden in the connectivity rule’s advanced parameters, by traffic descriptor



Network Configuration Assistant

Network Configuration Assistant (Home) ▸ AT-TLS ▸ TCP/IP Stack

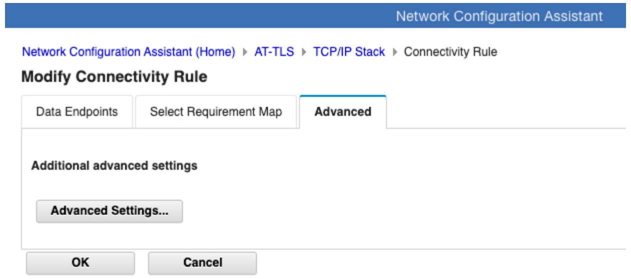
Connectivity Rules for System Image IMG1, Stack STK1

Actions | Move Up Move Down

No filter applied

	Status Filter	Rule Name Filter	Application / Requirement Map Filter	Key Ring Filter
●	Enabled		mjfrm	tlsKeyring

Total: 1 Selected: 1

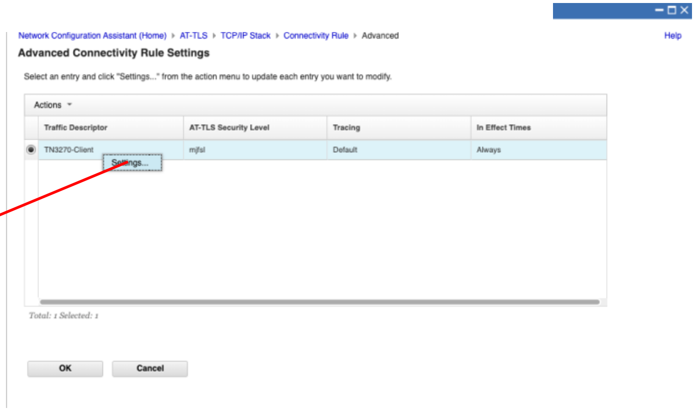


Network Configuration Assistant

Network Configuration Assistant (Home) ▸ AT-TLS ▸ TCP/IP Stack ▸ Connectivity Rule

Modify Connectivity Rule

Additional advanced settings



Network Configuration Assistant (Home) ▸ AT-TLS ▸ TCP/IP Stack ▸ Connectivity Rule ▸ Advanced

Advanced Connectivity Rule Settings

Select an entry and click "Settings..." from the action menu to update each entry you want to modify.

Actions

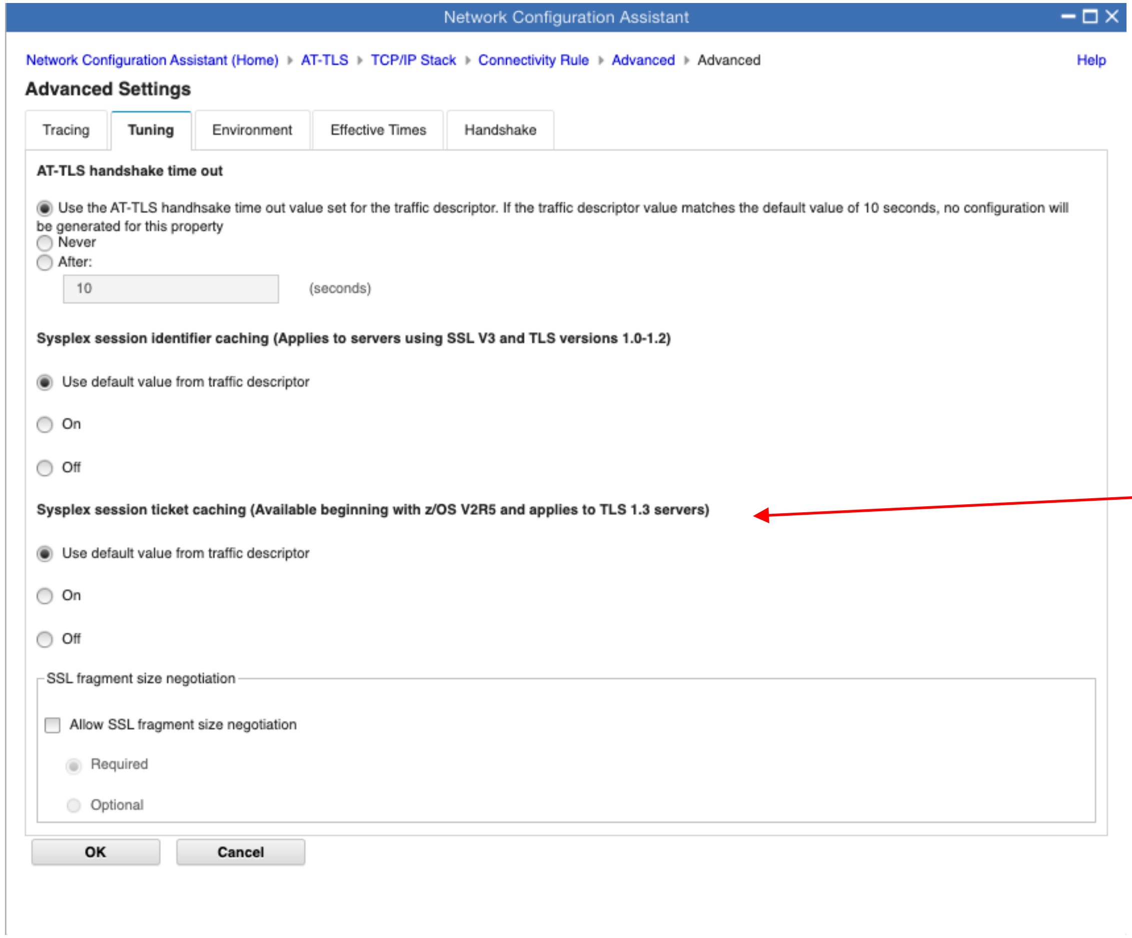
	Traffic Descriptor	AT-TLS Security Level	Tracing	In Effect Times
●	TN3270-Client	mjfsl	Default	Always

Total: 1 Selected: 1

Next slide

Usage & Invocation - Enabling sysplex session ticket caching on the Connectivity Rule

Overriding sysplex session ticket caching in the connectivity rule



Network Configuration Assistant (Home) ▸ AT-TLS ▸ TCP/IP Stack ▸ Connectivity Rule ▸ Advanced ▸ Advanced

Advanced Settings

AT-TLS handshake time out

● Use the AT-TLS handhsake time out value set for the traffic descriptor. If the traffic descriptor value matches the default value of 10 seconds, no configuration will be generated for this property
○ Never
○ After:
10 (seconds)

Sysplex session identifier caching (Applies to servers using SSL V3 and TLS versions 1.0-1.2)

● Use default value from traffic descriptor
○ On
○ Off

Sysplex session ticket caching (Available beginning with z/OS V2R5 and applies to TLS 1.3 servers)

● Use default value from traffic descriptor
○ On
○ Off

SSL fragment size negotiation

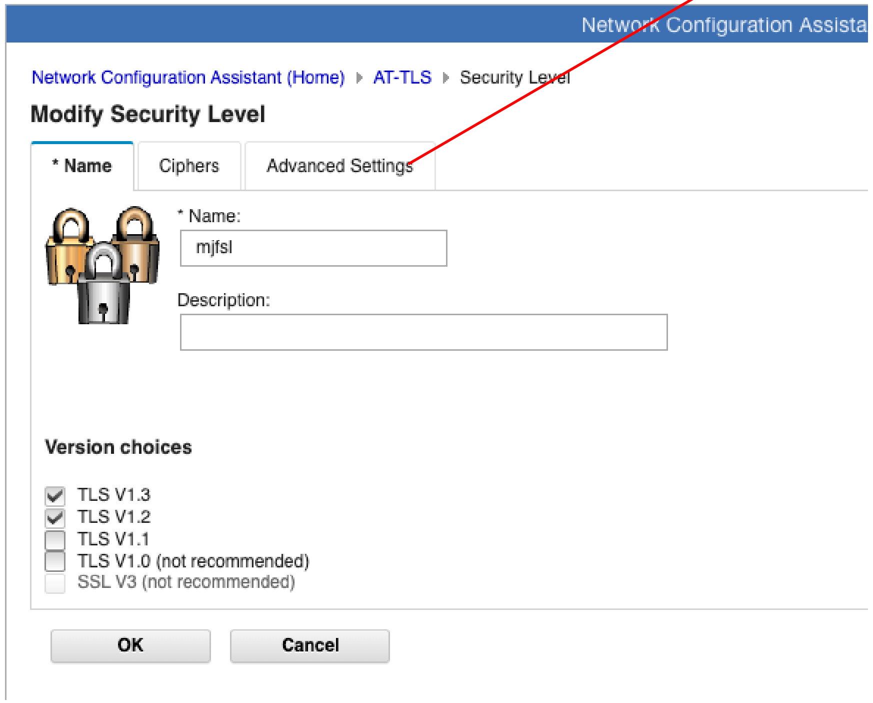
□ Allow SSL fragment size negotiation
● Required
○ Optional

New parameter added

The value in the traffic descriptor will be used in this example. If On or Off is selected, it overrides the traffic descriptor for this rule.

Usage & Invocation - Navigating to the maximum cached session tickets

Controlling maximum cached session tickets in the AT-TLS security level: locating


Network Configuration Assista
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level
* Name
Ciphers
Advanced Settings
OK
Cancel

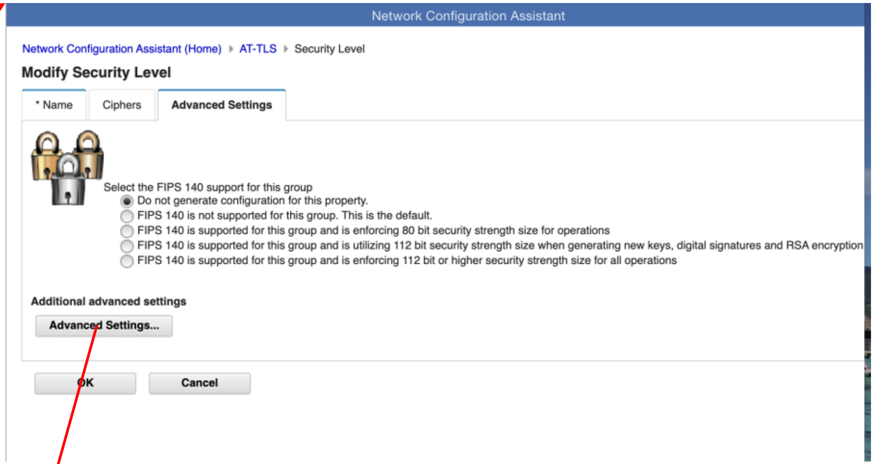
Modify Security Level

* Name: mjfsl

Description:

Version choices

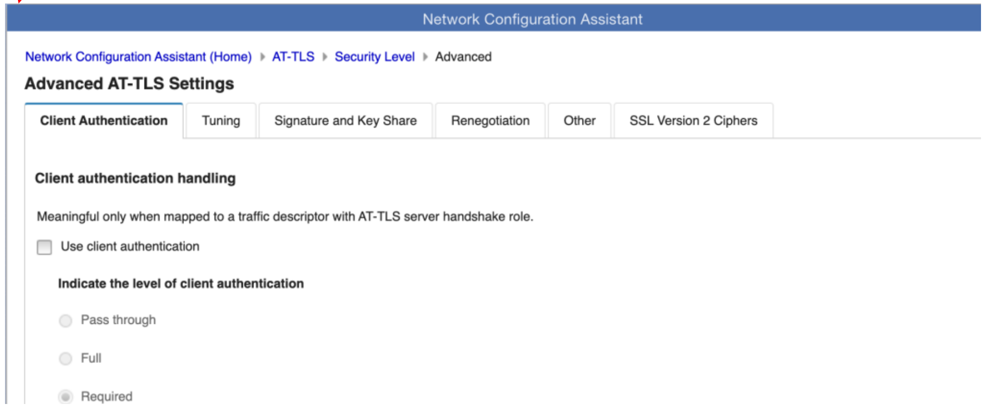
☑ TLS V1.3
☑ TLS V1.2
□ TLS V1.1
□ TLS V1.0 (not recommended)
□ SSL V3 (not recommended)


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level
* Name
Ciphers
Advanced Settings
Advanced Settings...
OK
Cancel

Modify Security Level

Select the FIPS 140 support for this group
● Do not generate configuration for this property.
○ FIPS 140 is not supported for this group. This is the default.
○ FIPS 140 is supported for this group and is enforcing 80 bit security strength size for operations
○ FIPS 140 is supported for this group and is utilizing 112 bit security strength size when generating new keys, digital signatures and RSA encryption
○ FIPS 140 is supported for this group and is enforcing 112 bit or higher security strength size for all operations

Additional advanced settings


Network Configuration Assistant
Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced
Client Authentication
Tuning
Signature and Key Share
Renegotiation
Other
SSL Version 2 Ciphers

Advanced AT-TLS Settings

Client authentication handling

Meaningful only when mapped to a traffic descriptor with AT-TLS server handshake role.

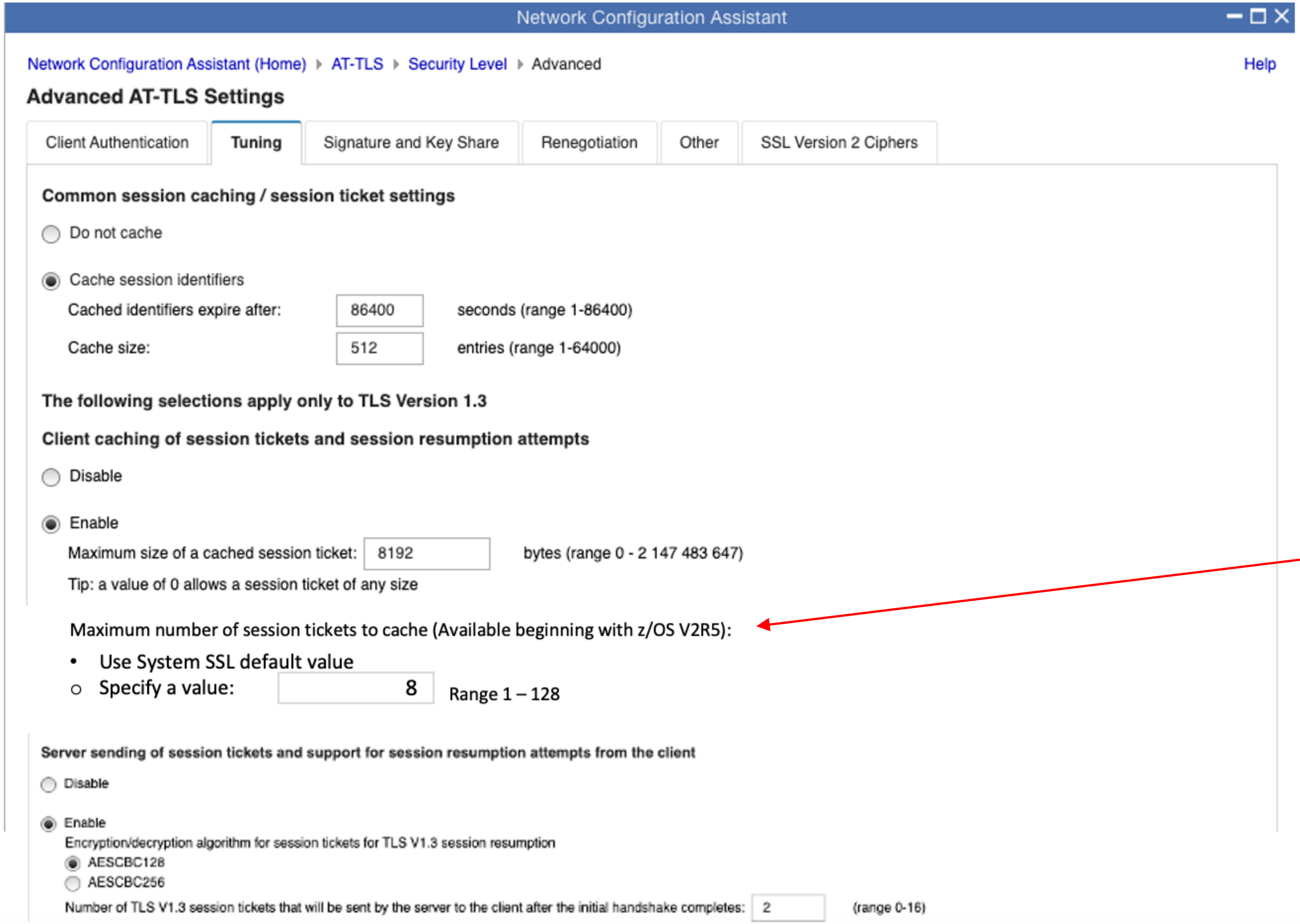
□ Use client authentication

Indicate the level of client authentication

○ Pass through
○ Full
● Required

Usage & Invocation – Setting max cached session tickets on the Security Level

NCA AT-TLS security level, advanced, tuning



Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced   Help

Advanced AT-TLS Settings

Common session caching / session ticket settings

○ Do not cache

● Cache session identifiers

Cached identifiers expire after: 86400 seconds (range 1-86400)

Cache size: 512 entries (range 1-64000)

The following selections apply only to TLS Version 1.3

Client caching of session tickets and session resumption attempts

○ Disable

● Enable

Maximum size of a cached session ticket: 8192 bytes (range 0 - 2 147 483 647)

Tip: a value of 0 allows a session ticket of any size

Maximum number of session tickets to cache (Available beginning with z/OS V2R5):

● Use System SSL default value

○ Specify a value: 8 Range 1 – 128

Server sending of session tickets and support for session resumption attempts from the client

○ Disable

● Enable

Encryption/decryption algorithm for session tickets for TLS V1.3 session resumption

● AESCBC128

○ AESCBC256

Number of TLS V1.3 session tickets that will be sent by the server to the client after the initial handshake completes: 2 (range 0-16)

New parameter added for GSK_SESSION_TICKET_CLIENT_MAXCACHED

Usage & Invocation - z/OS UNIX pasearch output

- ➢ Pasearch output for new parameters with configured values

Server rule with TLSv1.3 sysplex session ticket caching enabled

```
TTLS Action:              Secure_Telnet_Server_Conn

...

TTLSGskAdvancedParms:
   GSK_SYSPLEX_SIDCACHE:                  On
   GSK_SYSPLEX_SESSION_TICKET_CACHE:      On
   GSK_V3_SESSION_TIMEOUT:                86400
   GSK_V3_SIDCACHE_SIZE:                  512

   ...
```

Client rule with a configured maximum TLSv1.3 session ticket value

```
TTLS Action:              Client_Conn

...

TTLSGskAdvancedParms:
   GSK_V3_SESSION_TIMEOUT:                86400
   GSK_V3_SIDCACHE_SIZE:                  512
   GSK_SESSION_TICKET_CLIENT_ENABLE:      On
   GSK_SESSION_TICKET_CLIENT_MAXSIZE:     8192
   GSK_SESSION_TICKET_CLIENT_MAXCACHED:   8

   ...
```

Usage & Invocation - Netstat TTLS/-x DETAIL

Netstat TTLS/-x output for a TTLS environment action

Server rule with TLSv1.3 sysplex session ticket caching enabled

```
MVS TCP/IP NETSTAT CS 3.1   TCPIP Name: TCPCS    19:51:22
ConnID: 000000B8
...
TTLSRule: ftp_serv_21
...

  TTLSEnvAction: env_act_serv
  ...
    GSK_V3_SESSION_TIMEOUT:     86400
    GSK_V3_SIDCACHE_SIZE:       512
    GSK_SYSPLEX_SIDCACHE:       On
    GSK_SYSPLEX_SESSION_TICKET_CACHE:      On
  ...
```

Client rule with a configured maximum TLSv1.3 session ticket value

```
MVS TCP/IP NETSTAT CS 3.1   TCPIP Name: TCPCS    19:51:22
ConnID: 000000B8
...
TTLSRule: client_conn
...

  TTLSEnvAction: env_act_client
  ...
    GSK_SESSION_TICKET_CLIENT_ENABLE:      On
    GSK_SESSION_TICKET_CLIENT_MAXSIZE:     8192
    GSK_SESSION_TICKET_CLIENT_MAXCACHED:   8
```

Diagnosis – AT-TLS syslog messages…GSK parms

- Log contains messages showing the values set for the new parameters:

```
EZD1284I TTLS Flow  GRPID: 00000002 ENVID: 00000002 CONNID: 00000067  RC:    0 Set
GSK_SYSPLEX_SESSION_TICKET_CACHE(450) -  ON(630)

EZD1284I TTLS Flow  GRPID: 00000002 ENVID: 00000002 CONNID: 00000067  RC:    0 Set
GSK_SESSION_TICKET_CLIENT_MAXCACHED(332) - 8
```

Interactions & Dependencies…(1 of 2)

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations…(1 of 2)

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Upgrade consideration: None
- Coexistence considerations: None

Installation & Configuration…(1 of 2)

- If your server is configured to use session ticket caching, you can enable sysplex-wide session ticket caching by
  - Configuring GSK_SYSPLEX_SESSION_TICKET_CACHE on the server rule for each system requiring TLS session resumption
  - Starting GSKSRVR task for each system requiring TLS session resumption

Summary…ZRM-9856

- The TLSv1.3 Sysplex Session Ticket Caching allows the benefits of TLS session resumption in a sysplex-wide environment for TLSv1.3 protocol
    - To allow client session ticket caching, GSK_SESSION_TICKET_CLIENT_ENABLE must be set ON and GSK_V3_SESSION_TIMEOUT and GSK_V3_SIDCACHE_SIZE settings must be set to values greater than 0
    - AT-TLS client applications can specify the maximum number of TLSv1.3 session tickets that can be stored per session in its cache

Appendix

Reference:

- z/OS Communication Server: IP Configuration Guide
  - Chapter 20: Application Transparent Transport Layer Security data protection
- z/OS Communication Server: IP Configuration Reference
  - Chapter 16: Policy Agent and policy applications
- z/OS Communication Server: New Function Summary
- z/OS Cryptographic Services System Secure Sockets Layer Programming