Entire Net-Work Client Installation and Administration Guide

Using Encryption with Entire Net-Work

Version 1.3.1

October 2021

ADABAS & NATURAL

This document applies to Entire Net-Work Client Version 1.3.1 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: WCL-OWSLDOC-131-20210428

Table of Contents

1 About this Documentation

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
`Monospace font`	Identifies service names and locations in the format *`folder.subfolder.service`*, APIs, Java classes, methods, properties.
`Italic`	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at **https://documentation.softwareag.com**.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at **https://empower.softwareag.com/**.

You can find product information on the Software AG Empower Product Support website at **https://empower.softwareag.com**.

To submit feature/enhancement requests, get information about product availability, and download products, go to **Products**.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the **Knowledge Center**.

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at **https://empower.softwareag.com/public_directory.aspx** and give us a call.

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at **http://techcommunity.softwareag.com**. You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

2 Using Encryption with Entire Net-Work

Encryption of TCP/IP connections is typically accomplished with the Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS). The term SSL is often used to refer to both SSL and TLS. SSL provides both privacy and data integrity over TCP/IP networks. Privacy is achieved through encryption and data integrity is achieved through authentication (both parties are who they claim to be) and integrity checks (nothing has been altered, added or deleted).

Entire Net-Work does not provide built-in support for SSL on z/OS. Software AG recommends the use of the IBM product AT-TLS (Application Transparent-Transport Layer Security). AT-TLS is a component of the z/OS Communication Server.

AT-TLS will convert any configured TCP/IP connection made through the z/OS TCP/IP stack to an SSL connection and works independently of the z/OS application that either initiates the connection (client) or accepts the connection (server).

This documentation is organized as follows:

Certificates

SSL/TLS (and AT-TLS) require a certificate and a private key. A certificate from a certificate authority is recommended in situations where the SSL/TLS client must verify the identity of the SSL/TLS server. In cases where the identity of the SSL/TLS server is not in question, then a self-signed certificate may be used. A self-signed certificate may be generated using many available tools. One tool that may be used is the z/OS UNIX System Services utility GSKKYMAN. Another tool is the OpenSSL Toolkit by openssl.org.

Maintaining Certificates in z/OS

Certificates, which are to be used with AT-TLS, may be maintained in RACF key rings or in key databases, which are located in the z/OS UNIX file system.

IBM delivers a set of commonly used Certificate Authority root certificates with each z/OS system delivery. If key rings are going to be used to hold server certificates, those root certificates must be manually imported into the key rings by the system administrator. If IBM delivers newer replacements for expired root certificates, all affected key rings need to be updated accordingly.

Unlike key rings, key databases contain the current set of root certificates automatically after they have been newly created. However, the need for maintaining always the latest set of root certificates applies to the key database alternative as well.

Using RACF Key Rings

In RACF, digital certificates are stored in so-called key rings. The RACF command RACDCERT is used to create and maintain key rings and certificates, which are contained in those key rings.

See z/OS Security Server RACF Security Administrator's Guide, IBM manual SA22-7683-11, and z/OS Security Server RACF Command Language Reference, IBM manual SA22-7687-11.

Using Key Databases

Alternatively to RACF, certificates can be kept in key databases, which reside in the z/OS UNIX services file system. For the creation and maintenance of key databases, the GSKKYMAN utility is used.

See z/OS Cryptographic Services PKI Services Guide and Reference, IBM manual SA22-7693-10.

AT-TLS

AT-TLS is enabled in the z/OS TCP/IP stack by the `TTLS` parameter of the `TCPCONFIG` statement in the TCP/IP profile. See the *z/OS Communications Server: IP Configuration Reference* for a full description.

Individual TCP/IP connections where SSL is required are defined in the *z/OS Policy Agent* Configuration dataset. The Policy Agent Configuration statements are documented in the *z/OS Communications Server: IP Configuration Reference*. More information on the Policy Agent may be found in the section on policy based networking in the *z/OS Communications Server: IP Configuration Guide*.

Items are included that indicate attributes of a TCP/IP connection and the desired SSL/TLS connection, such as:

1. Job or Started Task name of the z/OS application involved in the connection (either the client or the server).
2. Source IP address (or a range of IP addresses) and source port number (or a range of port numbers).
3. Destination IP address (or a range of IP addresses) and destination port number (or a range of port numbers).
4. Direction – Are connections coming into a z/OS application (Inbound to a server) or do the connections originate from a z/OS application (Outbound from a client).
5. Location of the z/OS Unix Key Database or RACF Key Ring.

Example

In the following example, Entire Net-Work is running on z/OS as started task MYWCP. MYWCP has links that connect to WCPs running on Windows and are listening on port 1620. MYWCP is the client in this case. The links may use any source port in the range 1024 – 65535 and connect to destination port 1620. It is required that any connections from MYWCP to any host on port 1620 be an SSL/TLS connection using TLS version 1.1. The z/OS Unix Key Database to be used is in file /u/ada/wcp/wcpcerts.kdb with password mysecret.

The following Policy Agent configuration will implement this example:

```
TTLSRule                          ConnRule01~41
{
  LocalAddr                       ALL
  RemoteAddr                      ALL
  LocalPortRangeRef               portR2
  RemotePortRangeRef              portR23
  Jobname                         MYWCP
  Direction                       Outbound
  Priority                        215
  TTLSGroupActionRef              gAct1
  TTLSEnvironmentActionRef        eAct12~MYWCP
  TTLSConnectionActionRef         cAct6
}

PortRange                         portR2
{
  Port                            1024-65535
}

PortRange                         portR23
{
  Port                            1620
}

TTLSGroupAction                   gAct1
{
  TTLSEnabled                     On
  Trace                           6
}

TTLSEnvironmentAction             eAct12~MYWCP
{
  HandshakeRole                   Client
  EnvironmentUserInstance         0
  TTLSKeyringParmsRef             keyR10
}

TTLSKeyringParms                  keyR10
{
  Keyring                         /u/ada/wcp/wcpcerts.kdb
  KeyringPw                       mysecret
}

TTLSConnectionAction              cAct6
{
  HandshakeRole                   Client
  TTLSCipherParmsRef              cipher1~AT-TLS__Silver
  TTLSConnectionAdvancedParmsRef  cAdv5
  CtraceClearText                 Off
  Trace                           6
}
```

```
TTLSCipherParms                    cipher1~AT-TLS__Silver
{
  V3CipherSuites                   TLS_RSA_WITH_DES_CBC_SHA
  V3CipherSuites                   TLS_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                   TLS_RSA_WITH_AES_128_CBC_SHA
}

TTLSConnectionAdvancedParms        cAdv5
{
  SSLv3                            On
  TLSv1                            On
  TLSv1.1                          On
  SecondaryMap                     Off
  TLSv1.2                          Off
}
```

AT-TLS Troubleshooting

Guidelines for diagnosing AT-TLS issues may be found in the *z/OS Communications Server: IP Diagnosis Guide* in the chapter entitled *Diagnosing Application Transparent Transport Layer Security (AT-TLS)*.

Verify AT-TLS Configuration

To verify that the policy agent has processed the configuration successfully, look in the policy agent job log for this message:

```
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR <your TCP/IP address space>: ↩
TTLS
```

If the message:

```
EZZ8438I PAGENT POLICY DEFINITIONS CONTAIN ERRORS FOR <your TCP/IP address space>: ↩
TTLS
```

appears, then there are errors in the configuration. In this case, check the syslog.log file for more information.

Verify the TCP/IP Connection is Handled by AT-TLS

After starting the application making the configured TCP/IP connection, check syslog.log for a message that your job/started task name matched a policy. From our example above, this message would be seen when MYWCP makes a connection:

```
Jan 28 20:57:39 PROD TTLS[50397264]: 21:57:39 TCPIP     EZD1281I TTLS Map
CONNID: 00014956 LOCAL: 10.20.74.61..14292 REMOTE: 10.130.96.163..1620 JOBNAME:
MYWCP USERID: ACF2STC TYPE: OutBound STATUS: Enabled RULE: ConnRule01~41
ACTIONS: gAct1 eAct12~DAACSSL cAct6
```