Configuration Guide

ARCAD Secure Sockets Layer (SSL)

Version 23.0

Publication Date: January, 2023

Prepared by the ARCAD Documentation Team

North America & LATAM
1 N. State St, 15th Floor
Chicago, IL
USA
1-603-371-9074
1-603-371-3256 (support calls only)
sales-us@arcadsoftware.com

EMEA (HQ)
55 Rue Adrastée – Parc Altaïs
74650 Chavanod/Annecy
France
+33 450 578 396
sales-eu@arcadsoftware.com

Asia Pacific
5 Shenton Way #22-04
UIC Building
Singapore 068808
sales-asia@arcadsoftware.com

Contact ARCAD

Headquartered in France at the foot of the Alps, ARCAD offers global services and has offices and partners all over the world. ARCAD partners with leading-edge companies throughout the world to offer full services, close to home.

Visit our website to Contact Us and find out more about our company and partners, or to request a demo.

The ARCAD Customer Portal is intended for current and potential customers that have full or trial versions of ARCAD software. If you already use or are interested in using an ARCAD product, the portal lets you view all of your current licenses and generate your own temporary license keys for most ARCAD products. It grants you access to the ARCAD product knowledge base (new releases, release notes and current documentation).

Do you have a request for change or have you encountered a bug? Log into the ARCAD Helpdesk and create a ticket.

ARCAD guarantees consultant support 24 hours a day, 5 days a week (24/5) to registered members. Calls received are redirected, according to the hour, to put you in contact with a support team in or near your timezone.

Country	Address	Account Contact	Support Contact
France	ARCAD Software (HQ) 55 Rue Adrastée 74650 Chavanod ARCAD Software 17 chemin de la plaine 07200, Saint-Didier-sous-Aubenas	+33 4 50 57 83 96 sales-eu@arcadsoftware.com	Worldwide 24/7: +1 603 371 3256 France only: +33 450 57 28 00 support@arcadsoftware.com ARCAD Helpdesk
Germany	ARCAD Software Deutschland GmbH c/o Pramex International GmbH Savignystr. 43, 60325 Frankfurt am Main		
China	ARCAD Software #2035, Yuehai Plaza, 180 Wanbo 2nd Road, Nancun, Panyu District, Canton	+86 (020)22324643 +86 (020)22324649 sales-asia@arcadsoftware.com	
India	ARCAD Software D-280/281/282, Vibhuti Khand Gomti Nagar, Lucknow		
Singapore	ARCAD Software 5 Shenton Way #22-04 UIC Building Singapore 068808		
USA	ARCAD Software 1 N. State St, 15th Floor Chicago, IL	+1 (603) 371-9074 +1 (603)-371-3256 (support calls only) sales-us@arcadsoftware.com	

Table 1: Contact ARCAD

Contents

Contact ARCAD 3

Contents 4

Preface 5

1 Prerequisites 6

2 Exporting the certificate from IBM i 7

3 Importing the certificate 9

3.1 Import the certificate into a Java Runtime Environment (JRE) 9

3.2 Import the certificate into RDi 9

4 Connecting to an ARCAD Server via SSL 12

5 Verifying the SSL Connection on IBM i 14

Preface

Document purpose

This document is intended for system administrators with access to the Digital Certificate Manager (DCM). You must also have access to the Java keystores if the default password was changed. This configuration is not ARCAD-specific but required for all applications you wish to make secure communications with, such as the Rational Team Concert build engine.

This document assumes your IBM i system(s) are properly configured to use SSL.

The screen-shots that appear in this document are representative. They are intended to help understand the product's functionality and do not necessarily demonstrate best practice.

In order to completely understand the notions in this document, you should have sufficient knowledge of the various functions available in the ARCAD product suite.

Publication record

Product version	Document version	Publication date	Update record
≥ 23.0	1.6	January, 2023	No functional changes.
22.0	1.5	January, 2022	No functional changes.

Table 2: ARCAD Secure Sockets Layer (SSL) Configuration Guide publication record

1 Prerequisites

ARCAD ≥10.08.10

Java ≥1.7

IBM i ≥7.1

A Certificate Authority and Local Root Certificate must be configured on your IBM i system. For more information, refer to IBM's documentation:

http://Configuring an IBM i host for SSL

⚠ **Important!**

The following Application Servers on the host IBM i must be assigned a certificate:

- Central Server
- Database Server
- Data Queue Server
- Remote Command Server
- Signon Server
- IBM i TCP/IP Telnet Server
- IBM i DDM/DRDA Server - TCP/IP
- Host Servers
- File Server
- Management Central Server

2 Exporting the certificate from IBM i

If you do not have a copy of your system's certificate, you can export it from DCM.

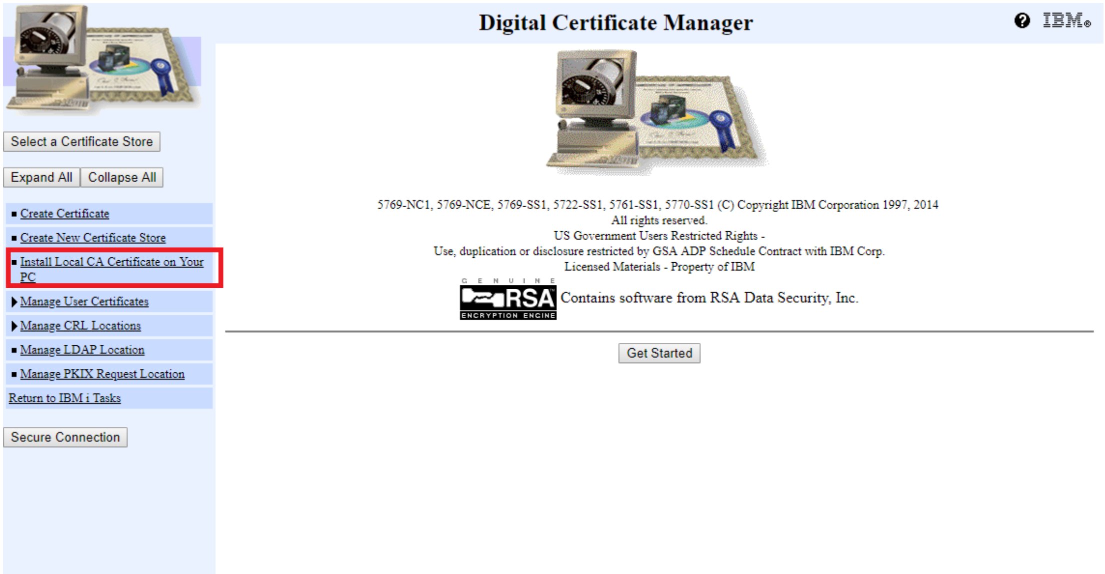
Step 1 Navigate to *http://<systemname>:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0* in your browser and login.

Step 2 From the menu on the left, click the **Select Certificate Store** button.

Step 3 Select the Certificate Store that holds the certificate you need to export.

Step 4 Enter the **password** to access the Certificate Store.

Step 5 From the menu on the left, click **Install Local CA Certificate on Your PC**.

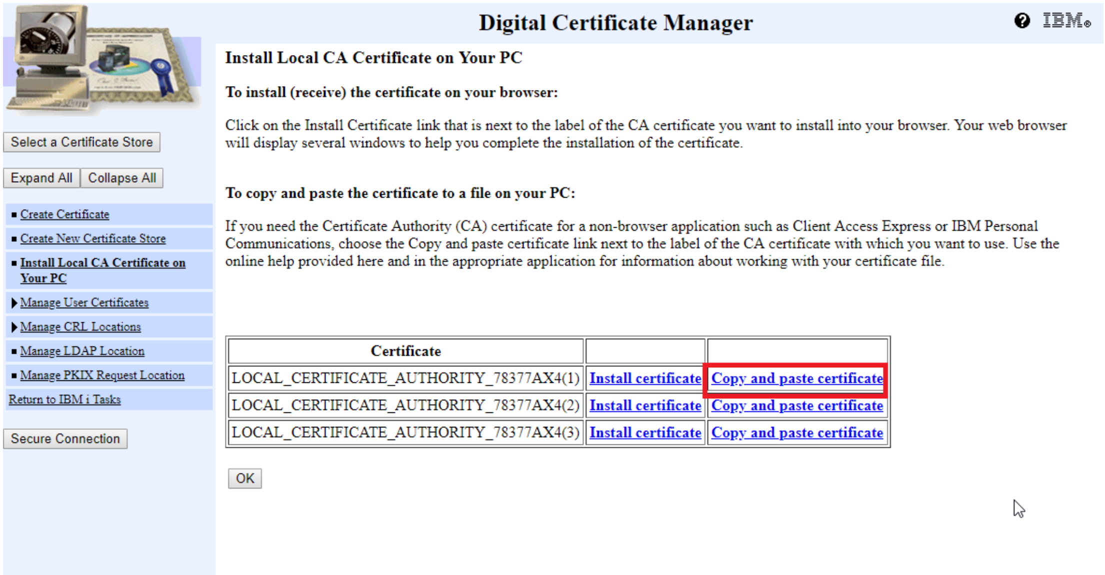

Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to IBM i Tasks
Secure Connection
GENUINE RSA ENCRYPTION ENGINE
Get Started

5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2014
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Figure 1: Install Local CA Certificate on Your PC

Step 6 For the certificate you've assigned to the application servers, choose the option Copy and paste certificate from the table.


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to IBM i Tasks
Secure Connection
OK

Install Local CA Certificate on Your PC

To install (receive) the certificate on your browser:

Click on the Install Certificate link that is next to the label of the CA certificate you want to install into your browser. Your web browser will display several windows to help you complete the installation of the certificate.

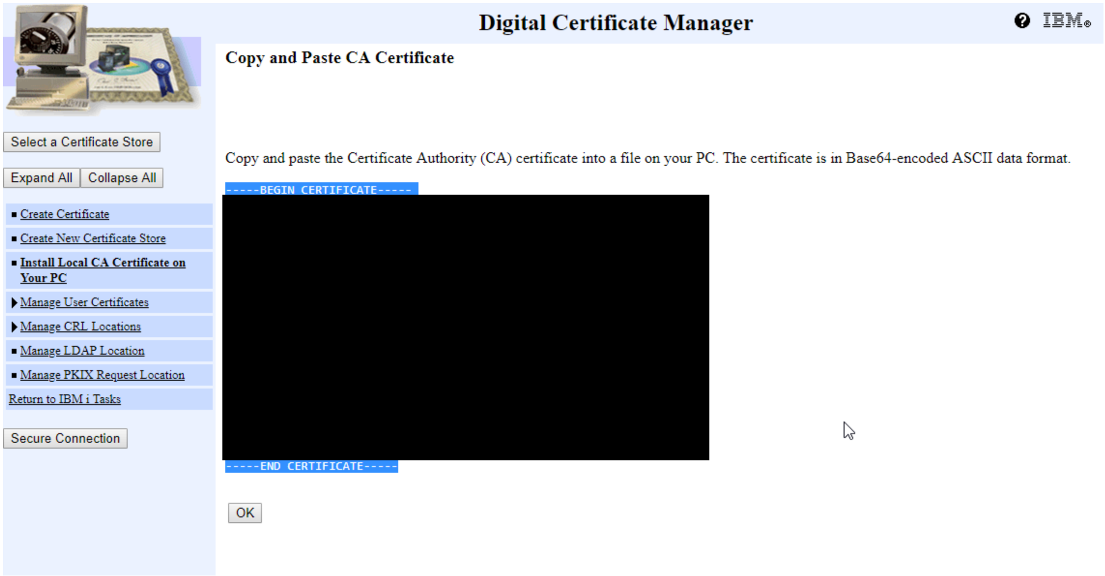
To copy and paste the certificate to a file on your PC:

If you need the Certificate Authority (CA) certificate for a non-browser application such as Client Access Express or IBM Personal Communications, choose the Copy and paste certificate link next to the label of the CA certificate with which you want to use. Use the online help provided here and in the appropriate application for information about working with your certificate file.

Certificate		
LOCAL_CERTIFICATE_AUTHORITY_78377AX4(1)	Install certificate	Copy and paste certificate
LOCAL_CERTIFICATE_AUTHORITY_78377AX4(2)	Install certificate	Copy and paste certificate
LOCAL_CERTIFICATE_AUTHORITY_78377AX4(3)	Install certificate	Copy and paste certificate

Figure 2: Copy and paste the certificate assigned to your application servers

Step 7 The following screen displays the certificate encoded in Base64 ASCII to copy. Select the text and copy it into an external text editor.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to IBM i Tasks
Secure Connection
OK

Copy and Paste CA Certificate

Copy and paste the Certificate Authority (CA) certificate into a file on your PC. The certificate is in Base64-encoded ASCII data format.

```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

Figure 3: Copy the certificate

Step 8 Save the file with the extension *.cer*

Important!
You must include the text “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----"

3 Importing the certificate

The IBM i certificate in *.cer* format is valid for both JREs and RDi.

3.1 Import the certificate into a Java Runtime Environment (JRE)

The IBM i certificate must be imported into the JRE TrustStore for every Java product that needs to connect to IBM i via a remote secure connection. This includes ARCAD Client, ARCAD Plug-ins installed on generic Eclipse IDEs, RTC, Jazz Build Engine (JBE), and any stand-alone ARCAD product such as ARCAD Builder, DOT Anonymizer, DOT Verifier, DROPS and the DROPS Agent.

Step 1 Locate the Java Runtime Environment (JRE) installation(s) used by the target product(s).

> **Note**
> If you do not know which version(s) the product(s) use, you can configure all of the versions of Java installed on your system.

Step 2 Copy the *.cer* certificate to a temporary location on the system that will run the product(s).

Step 3 From a command line, run the following command: *<absolute java path>*`/bin/keytool -import -alias` *<remote IBM i name>* `-file` *<absolute path to the .cer file>* `-keystore` *<absolute path to the JRE keystore>* `-storepass` *<keystore password>*

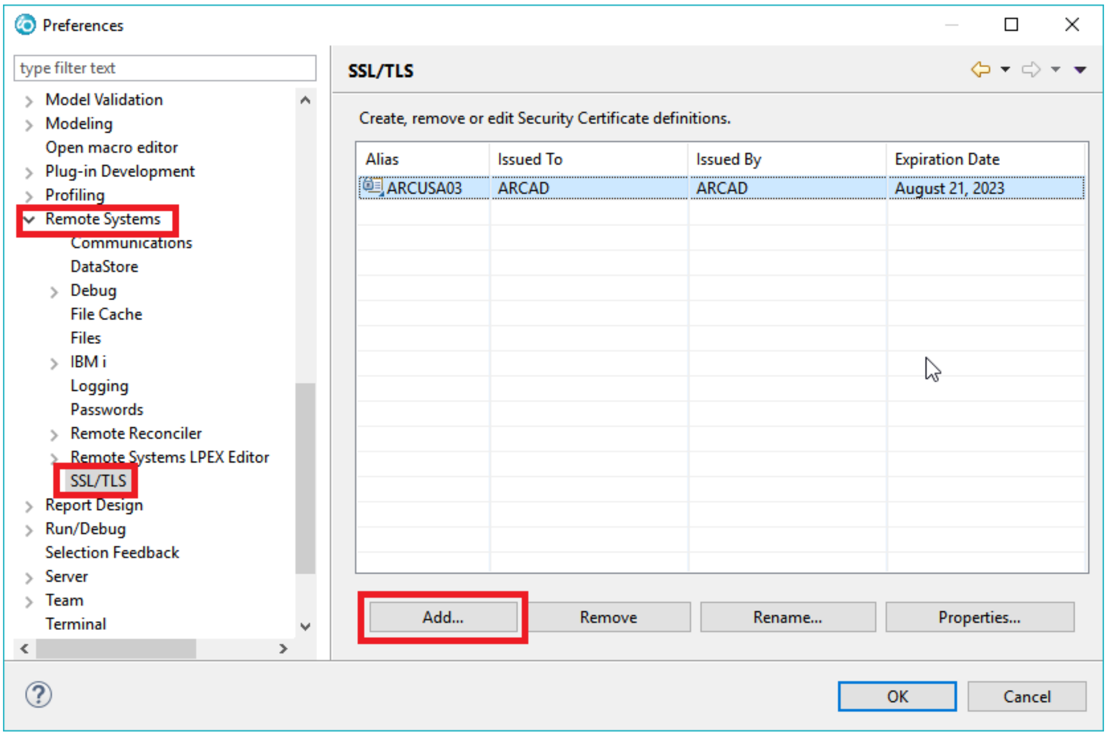
Step 4 Enter **Yes** if you are prompted to trust the certificate.

3.2 Import the certificate into RDi

All of the plugins installed on RDi, including ARCAD plugins, will use the same certificate imported into RDi. Arcad has the ability to use an existing Remote Systems Explorer (RSE) connection.

Step 1 Connect to RDi as administrator.

Step 2 Navigate to **Window** > **Preferences**. From the left panel in the Preferences dialog, select **Remote Systems** > **SSL/TLS**.



Create, remove or edit Security Certificate definitions.

Alias	Issued To	Issued By	Expiration Date
ARCUSA03	ARCAD	ARCAD	August 21, 2023

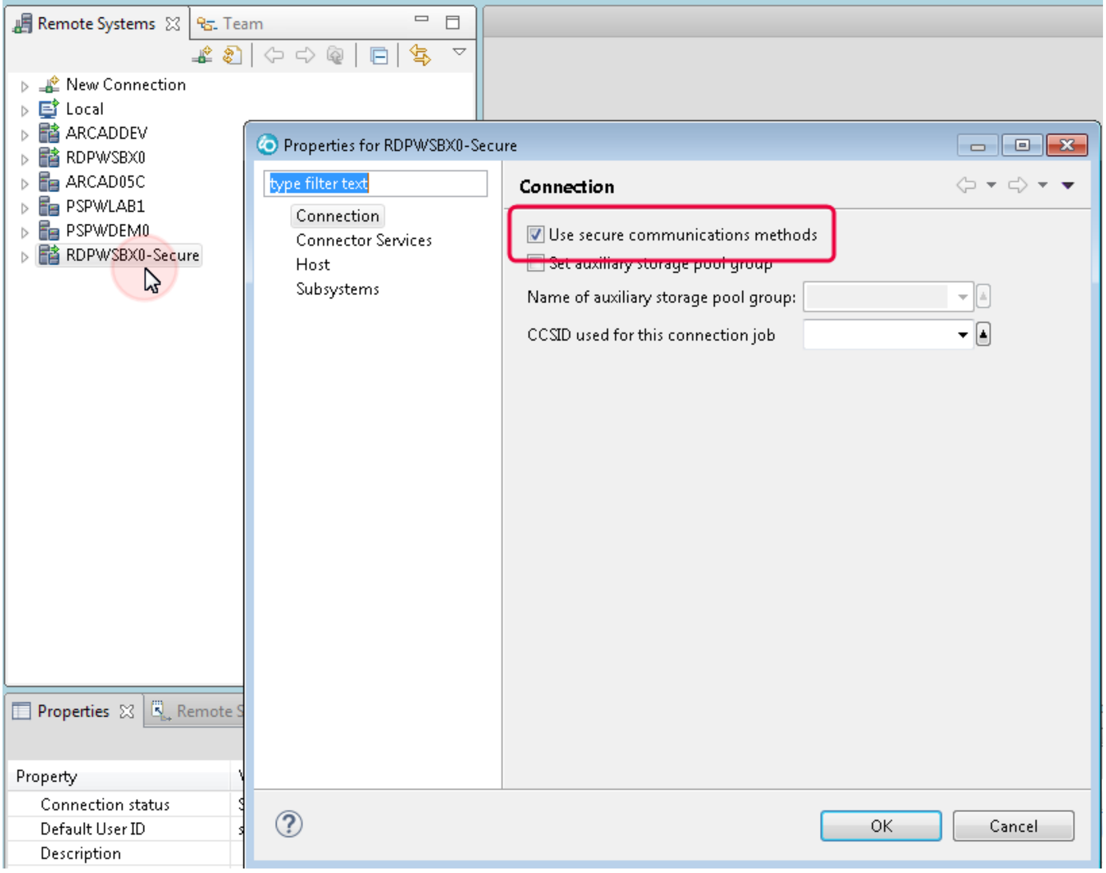
Figure 4: Add an SSL Certificate in RDi

Step 3 Click the Add button.

Step 4 From the **Add Certificate** dialog, browse to the *.cer* file. By default, the **Alias** will be the file name.
Click **OK** to save.

Step 5 To activate the secure connection for RSE connections, right-click on the RSE connection and select **Properties**.

Step 6 From the **Properties** dialog, select **Connection**, then tick the **Use secure communication methods** checkbox.



Properties for RDPWSBX0-Secure

Connection

☑ Use secure communications methods

□ Set auxiliary storage pool group

Name of auxiliary storage pool group:

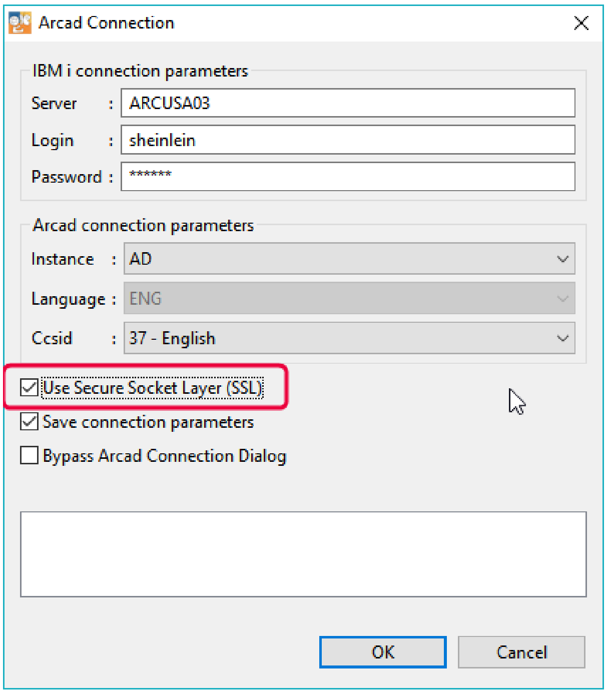
CCSID used for this connection job

Figure 5: Activate the secure connection for RSE connections

4 Connecting to an ARCAD Server via SSL

When connecting to an ARCAD Server, ensure that the **Use Secure Socket Layer (SSL)** checkbox is ticked so that the product calls the *.cer* certificate on your system.

The following are examples from multiple ARCAD products that use SSL connections.



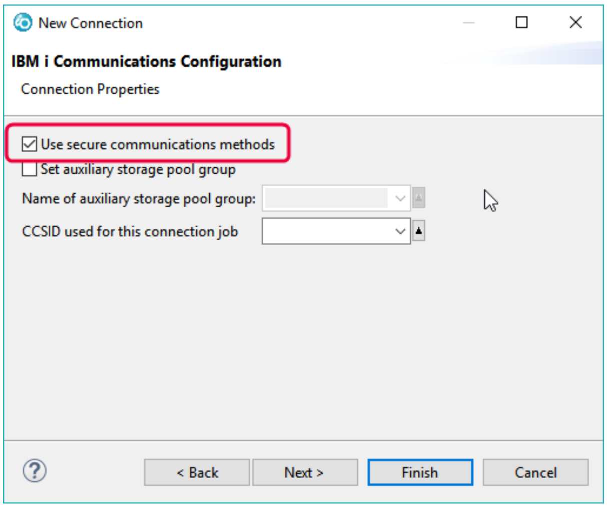
Arcad Connection

IBM i connection parameters
Server : ARCUSA03
Login : sheinlein
Password : ******

Arcad connection parameters
Instance : AD
Language : ENG
Ccsid : 37 - English

☑ Use Secure Socket Layer (SSL)
☑ Save connection parameters
□ Bypass Arcad Connection Dialog

Figure 6: Confirming SSL for an existing ARCAD Server connection in RDi

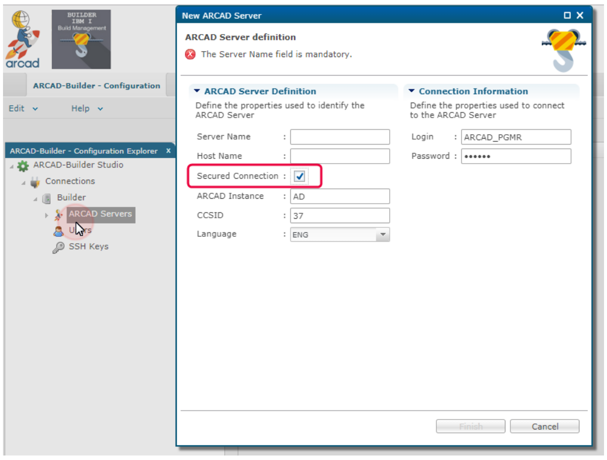


New Connection

IBM i Communications Configuration
Connection Properties

☑ Use secure communications methods
□ Set auxiliary storage pool group
Name of auxiliary storage pool group:
CCSID used for this connection job

Figure 7: ARCAD Skipper: Creating an RSE connection (2nd page of New Connection dialog)



New ARCAD Server

ARCAD Server definition

The Server Name field is mandatory.

ARCAD Server Definition

Define the properties used to identify the ARCAD Server

Server Name :

Host Name :

Secured Connection : ☑

ARCAD Instance : AD

CCSID : 37

Language : ENG

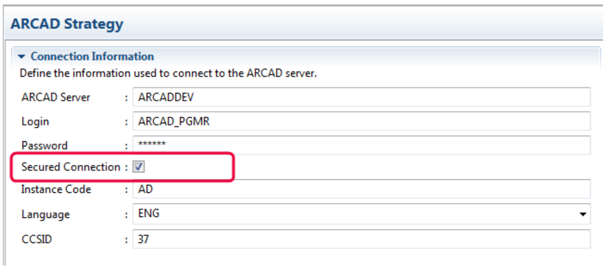
Connection Information

Define the properties used to connect to the ARCAD Server

Login : ARCAD_PGMR

Password : ••••••

Figure 8: ARCAD Builder: Creating a connection to an ARCAD Server



ARCAD Strategy

Connection Information

Define the information used to connect to the ARCAD server.

ARCAD Server : ARCADDEV

Login : ARCAD_PGMR

Password : ******

Secured Connection : ☑

Instance Code : AD

Language : ENG

CCSID : 37

Figure 9: DROPS: Creating a connection to an ARCAD Server

5 Verifying the SSL Connection on IBM i

Follow the subsequent steps to verify the SSL connection from an emulator (5250).

Step 1 Enter `GO TCPADM` in the command line.

Step 2 Select option 7 **Work with TCP/IP network status**.

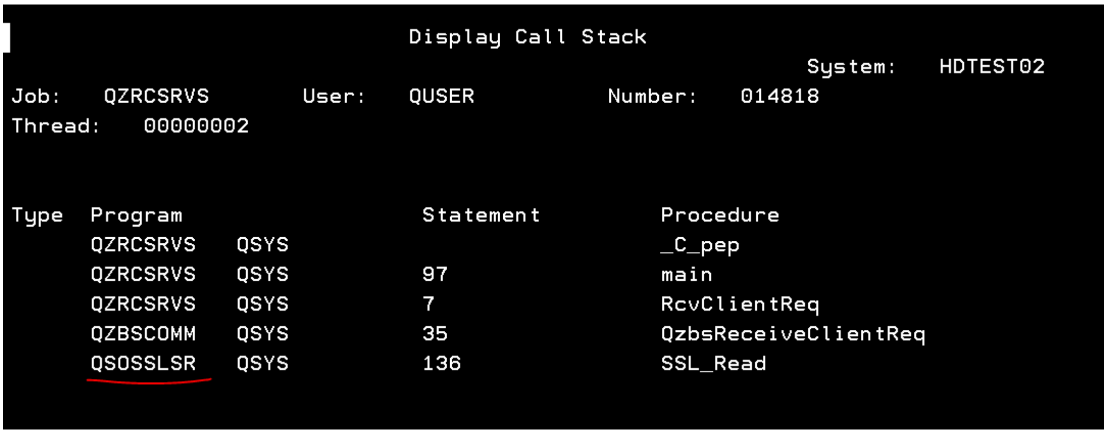
Step 3 Select option 3.**Work with IPv4 connection status**.

Step 4 Enter option 8 for the remote IP address and corresponding port for the connection to test.

Step 5 Verify the user in the **Display Jobs Using Connection** screen, then select option 5.

Step 6 In the **Work with Job** screen, select option 11 **Display call stack, if active**.

Step 7 Verify that the Program QSOSSLSR is present in the Call Stack screen.



```
                              Display Call Stack
                                                            System:   HDTEST02
Job:   QZRCSRVS       User:   QUSER          Number:   014818
Thread:   00000002


Type  Program                   Statement          Procedure
      QZRCSRVS   QSYS                              _C_pep
      QZRCSRVS   QSYS           97                 main
      QZRCSRVS   QSYS           7                  RcvClientReq
      QZBSCOMM   QSYS           35                 QzbsReceiveClientReq
      QSOSSLSR   QSYS           136                SSL_Read
```

Figure 10: Verify the SSL connection on IBM i