

# Configuring Access Client Solutions to Use SSL/TLS

Protecting your system from prying eyes



# Today's Speaker



**ROBIN TATAM, CBCA CISM PCI-P**  
*Global Director of Security Technologies*



[robin.tatam@helpsystems.com](mailto:robin.tatam@helpsystems.com)



[@robintatam](https://twitter.com/robintatam)



# Agenda

- ▶ Why are encrypted sessions important?
- ▶ What is SSL/TLS?
- ▶ Using Digital Certificate Manager (DCM)
  - ▶ Create a certificate or CSR
  - ▶ Assign the certificate to the servers
- ▶ Configuring Access Client Solutions (ACS)

# Why Encrypted Sessions?

- ▶ Required by many laws and regulations:
  - ▶ Payment Card Industry's Data Security Standard (PCI DSS)
    - ▶ Non-console administrator access must be encrypted (Section 2.3)
    - ▶ Password cannot flow in the clear (Section 8.2.1)
  - ▶ GDPR
  - ▶ NY Cyber Security Law
- ▶ Foils credential theft
- ▶ Protects data from being read 'in transit'

Sign On

System . . . . . : EARL  
Subsystem . . . . . : QINTER  
Display . . . . . : QPADEV0004

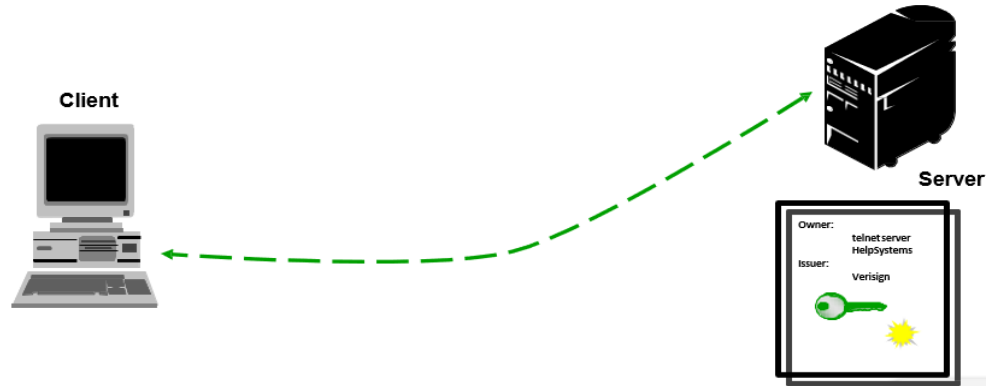
User . . . . . :  
Password . . . . . :



Program/procedure . . . . . : \_\_\_\_\_  
Menu . . . . . : \_\_\_\_\_  
Current library . . . . . : \_\_\_\_\_

# End-to-End Encrypted Communication Sessions

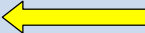
1. Client is configured to request an encrypted session from the server
2. Client contacts the server and provides it with the list of ciphers available to use to encrypt the session
3. Server responds with info on its digital certificate and which cipher it will use
4. Client verifies the server's digital certificate
5. Client generates a session key and rest of session is encrypted using symmetric key



# Digital Certificate

- ▶ Allows:
  - ▶ the client to trust the server
  - ▶ enables encrypted sessions
- ▶ Issued by a CA (Certificate Authority)
  - ▶ Well-known
  - ▶ Internal
  - ▶ IBM i
- ▶ Have a validity period
  - ▶ CA (issuer of the certificate)
  - ▶ Certificate itself
- ▶ Helps determine the strength of the encryption used on the connection

# History of the Protocols

Protocol	Invented	Deprecated
SSLv2	1995	2011
SSLv3	1996	2015
TLS 1.0	1999	2020
TLS 1.1	2006	2020
TLS 1.2 	2008	
TLS 1.3	Approved 2018	



# Configuring the Protocols Allowed on IBM i

- ▶ QSSLPCL – defines which protocols are enabled
  - ▶ \*OPSYS – (Default) actual values vary by release.
  - ▶ Or to control, specify one or more of the following:
    - ▶ **\*TLSV1.3** (available in IBM i 7.4)
    - ▶ **\*TLSV1.2**
    - ▶ \*TLSV1.1
    - ▶ \*TLSV1
    - ▶ \*SSLV3
    - ▶ \*SSLV2

*Note: This is not an ordered list*

# Protocols Available (by Release)

OS Release	SSLv2	SSLv3	TLS1.0	TLS1.1	TLS1.2	TLS1.3
V7R1	YES	YES	YES			
V7R1 w/TR6	YES	YES	YES	YES	YES	
V7R2	YES	YES	YES	YES	YES	
V7R3	YES	YES	YES	YES	YES	
V7R4	--	--	YES	YES	YES	YES

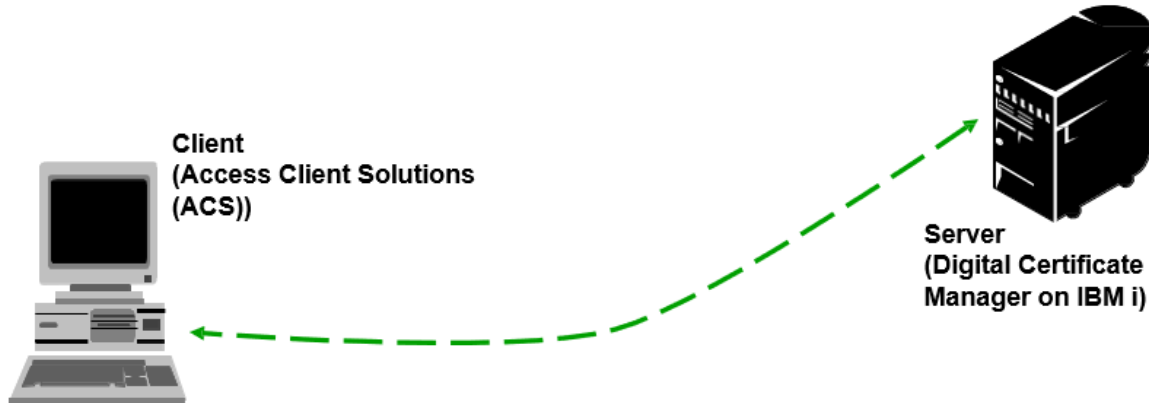
*Note: Protocol may not be available by default*

# Controlling the Cipher Suites

- ▶ QSSLCSLCTL – determines who controls the list specified in QSSLCSL – the system (\*OPSYS - default) or user (\*USRDFN)
  - ▶ To edit QSSLCSL, you must specify \*USRDFN
- ▶ QSSLCSL – contains list of cipher suites to be used on an SSL/TLS connection. This *is* an ordered list and is read-only unless the QSSLCSLCTL value is set to \*USRDFN

# Configuration

- ▶ Configuration must occur on both the client and the server to allow an encrypted session to be established



## Configuring the Server (IBM i)

# DCM – Digital Certificate Manager

- ▶ DCM allows you to assign digital certificates to servers so that encrypted communications can occur
- ▶ Regardless of the protocol used (SSL vs TLS), a digital certificate must be assigned to servers listed in DCM
  - ▶ Note: Servers (FTP, Telnet, etc) are called “Applications” in DCM
- ▶ Once the certificate has been assigned, you can further configure which protocols and which ciphers are used for each application (server)
- ▶ To access DCM, open a browser and go to:

**`http://<IBM i name or IP address>:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0`**

# DCM

**Select a Certificate Store**

Select the certificate store that you want to open.

Local Certificate Authority (CA)

\*OBJECTSIGNING

Other System Certificate Store

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](#)

- ▶ Select a Certificate Store
- ▶ If \*SYSTEM does not appear in the list, click on Create New Certificate Store

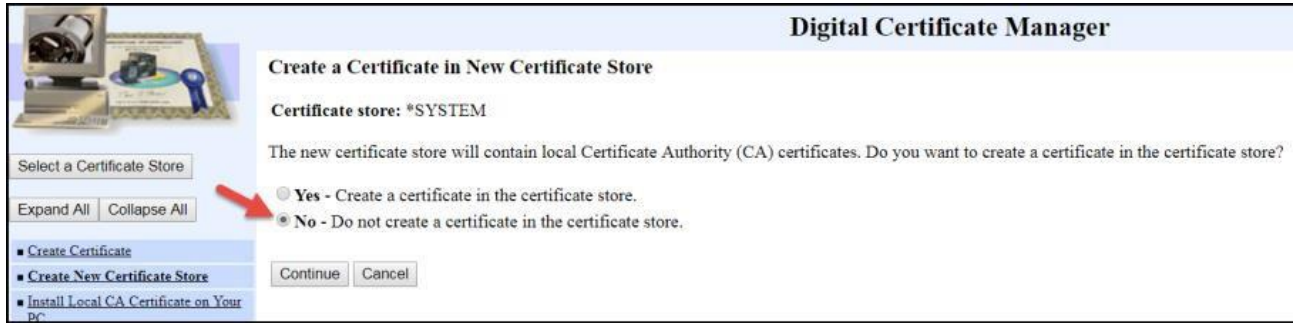
# DCM – Create a \*SYSTEM Store



- ▶ Click on Create New Certificate Store
- ▶ Continue



# Create a Certificate Store - continued



- ▶ No – Do not create a certificate
- ▶ Continue

# Create a Certificate Store - continued

**Digital Certificate**

**Certificate Store Name and Password**

Certificate store: \*SYSTEM

You must enter a password for the new certificate store and enter the password again to confirm it.

Certificate store password: ..... (required)

Confirm password: ..... (required)

Continue Cancel

Select a Certificate Store

Expand All Collapse All

- Create Certificate
- **Create New Certificate Store**

- ▶ Enter a password
- ▶ Continue

# \*SYSTEM Store Created

## Certificate Store Created

Message The certificate store has been created.

File name:

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB



- ▶ Click on Select a Certificate Store
- ▶ Select \*SYSTEM
- ▶ Continue

# Enter Password for the Certificate Store



The screenshot shows the 'Digital Certificate Manager' window with the 'Certificate Store and Password' dialog box open. The dialog box contains the following fields and controls:

- Certificate Store and Password** (Section Header)
- Enter the certificate store password.
- Certificate type:** Server or client
- Certificate store:** \*SYSTEM
- Certificate store path and filename:** /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
- Certificate store password:** [Empty text box]
- Buttons: Continue, Reset Password, Cancel

On the left side of the dialog box, there is a 'Fast Path' section with the following options:

- Fast Path
- Create Certificate
- Create New Certificate Store

At the top left of the dialog box, there is an image of a computer monitor and a certificate. Below the image are buttons for 'Select a Certificate Store', 'Expand All', and 'Collapse All'.

- ▶ Enter the password
- ▶ Continue

(If you're signed on with a profile that has \*ALLOBJ and \*SECADM you can reset the password)

# Create a Certificate Request (CSR)



- ▶ Click on Create Certificate
- ▶ Choose 'Server or client certificate'
- ▶ Continue

# Creating a Certificate from a Well-known or Internal CA



# Generate the CSR

## Create Certificate

Certificate type: Server or client

Certificate store: \*SYSTEM

Use this form to create a certificate in the certificate store listed above.

Key algorithm:

RSA ▾

Key size:

2048 ▾ (bits)

Certificate label:

Sample Cert (required)

## Certificate Information

Common name:

jericho.helpsysdev.com (required)

Organization unit:

Organization name:

HelpSystems (required)

Locality or city:

Eden Prairie

State or province:

Minnesota (required:minimum of 3 characters)

Country or region:

US (required)

Continue

Cancel

# Copy the CSR

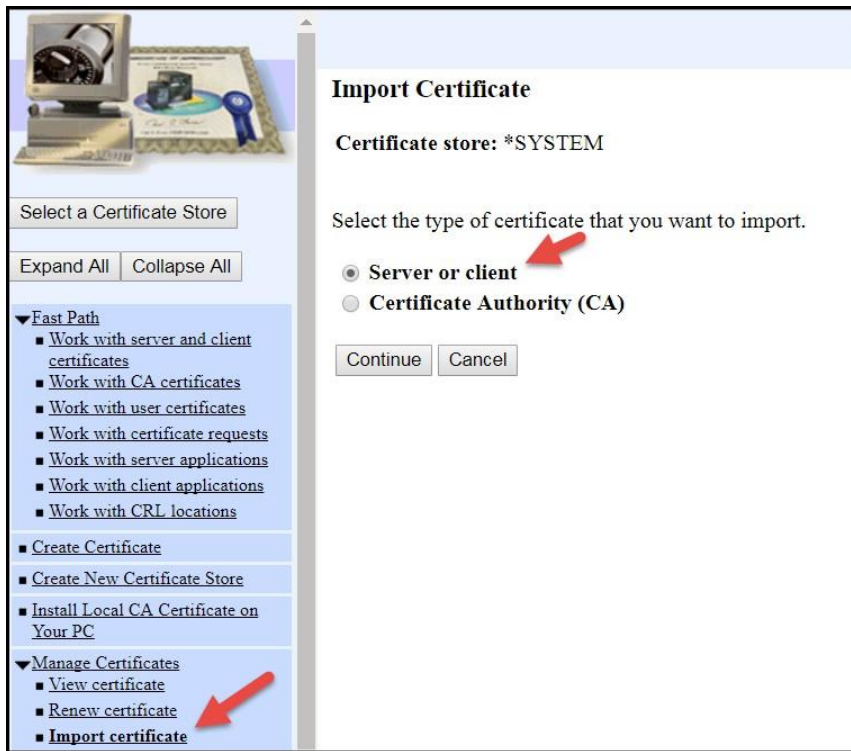
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwDELMAkGA1UEBhMCVWxjeJAQ8gNVBhAgTCU1pbm5lc290YTEV
MBMGA1UEBxMMRWR1biBQcmFpcm11MRQwEgyDVQQKEwtIZWxwU31zdGVtczEYMBYG
A1UEAaxMPaGVscHN5c3R1bXMuY29tMITBtjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAX8jTYo3xLrv2Aft5cnY1BwJyexQSheZ1S7cqmvmRIqaDhaK4ndAzjW61
R6RnF2Jq9dIrzfddDLGsZC7TtZNHkdQL1wMgQ0/DZ2MAKbw1kC8p6C7Bwmq3SHZa
obS7G7XiQMn+Dgr30kwftsegW/n9wNB7A0HXMe3Xdh8ogJ7V/X3K7RIDfCoMBPjs
y0r2L91PfyknqFdC051dirS1oxy6sEF3AQi3HtbU2nE2ky/aGVeg2nMK0NjEsaFr
oMYvs92Wk9t/1ThkU2K9qzhx5Qsn7NkrbdcQ+o5Rkbt8CUBb2xSEr1oZ3A8hXV
uPba5GTG10INWS0m3nEWxahI4MM1rwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEB
ABjuFN2WfpyXZ6mKPS++dJWhi01XevY5V/oNnIFKsJyBQwHqt14HqB3Suk4F5C3T
/GsB6gZjUYEaFCBuX8bJsmXwr3dnz9o25VBuMjPkn9zkyE76x5MoHzTWbifiy6
u1A12FmosVnk+GJX9yh+qwZGZe9yMIbvcWpcfiEQSy3T8FXm1YWwb7vFLBcs3reJ
11SA1xkozCZ2xX2FjzvWvJ1pTkjvWLV41B9I30Gr112J2zZCIHuYUgnzAE70usK5
IM0XSfh/bQsXyQa1Inf3cdzED/ukqfBZRGH2K85Ugrkjco/7ndC5dNogScWb9C0
A4E6K/4U0zvTuk8rmJ+XJ14=
-----END NEW CERTIFICATE REQUEST-----
```

- ▶ Copy the ENTIRE certificate request, including the preceding and trailing dashes '-----'
- ▶ Send the CSR to the CA



# Receiving the Certificate

- ▶ Certificate will be returned to you – likely via email
  - ▶ If you receive an email with multiple links (for various formats) choose **PKCS#7** bin encoded
- ▶ Save the certificate on your PC
- ▶ Move the certificate into the IFS and remember the path!



- ▶ Select a Certificate Store – select and provide the password for the \*SYSTEM store
- ▶ Click Import certificate
- ▶ Click Server or client

# Enter the Path

### Digital Certificate Manager

#### Import Server or Client Certificate

**Certificate type:** Server or client  
**Certificate store:** \*SYSTEM

Specify the fully qualified path and file name of the certificate that you want to import.

Example path and file name: /MYDIRECTORY/MYFILE.EXT

**Import file:**

#### Import Server or Client Certificate

**Message** The certificate has been imported.

Use the Assign certificate task under Manage Certificates to specify which applications should use this certificate.

## Digital Certificate Manager



### Manage Certificates

Select the type of action that you want to perform.

- View certificate** - View information pertaining to a certificate.
- Renew certificate** - Replace an existing certificate with a new certificate.
- Import certificate** - Add a certificate to this certificate store.
- Export certificate** - Copy a certificate to a file or another certificate store.
- Delete certificate** - Remove a certificate from this certificate store or remove a certificate from a specific user identity.
- Validate certificate** - Validate a certificate in this certificate store.
- Assign certificate** - Assign a certificate to applications.
- Check expiration** - Check the expiration dates of certificates.
- Set CA status** - Enable or disable a Certificate Authority (CA) certificate in this certificate store.
- Update CRL location assignment** - Assign the Certificate Revocation List (CRL) location for a Certificate Authority (CA).
- Assign a user certificate** - Assign a user certificate to a user identity.

Continue

Cancel

# Assign to Applications (aka TCP Servers)

## Assign Certificate

**Certificate type:** Server or client

**Certificate store:** \*SYSTEM

**Default certificate label:** No default certificate found in certificate store.

Select a certificate, then select a button to perform an action on the certificate.

	Certificate	Common name
<input checked="" type="radio"/>	Sample Cert	jericho.helpsysdev.com
<input type="radio"/>	Sample Cert	system_name.helpsystems.com
<input type="radio"/>	JerichoDefaultPage1	Jericho.helpsystems.com
<input type="radio"/>	Security Testing ECDSA	Security Testing ECDSA



# Select the Applications and Assign the Certificates

## Select Applications


**Certificate type:** Server or client

**Certificate store:** \*SYSTEM

**Certificate label:** Sample Cert

Select which applications will use this certificate:

**Warning:** When you assign a certificate to a client application and a server requests client authentication, then the server authenticates all users of the application based on that certificate. Consequently, the server does not authenticate users on an individual basis. To ensure that the server authenticates each user of a client application individually outside the SSL protocol, do not assign a certificate to the client application.



<input checked="" type="checkbox"/>	Application	Type	Assigned certificate
<input checked="" type="checkbox"/>	Central Server	Server	Security Testing ECDSA
<input checked="" type="checkbox"/>	Database Server	Server	Security Testing ECDSA

- ▶ Click to assign all servers
- ▶ Click on Append (at the bottom of the Window)

## Configuring IBM i to be a Certificate Authority

# Create a CA on your IBM i



**Select a Certificate Store**

Select the certificate store that you want to open.

Local Certificate Authority (CA)  
 \*SYSTEM  
 \*OBJECTSIGNING  
 Other System Certificate Store

Select a Certificate Store

- [Create Certificate](#)
- [Create New Certificate Store](#)
- [Install Local CA Certificate on Your PC](#)
- [Create a Certificate Authority \(CA\)](#)



## Create a Certificate Authority (CA)

**Certificate type:** Certificate Authority (CA)

**Certificate store:** Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

**Key algorithm:**  ▼

**Key size:**  ▼ (bits)

**Hash algorithm:**  ▼

### Certificate Information

**Certificate Authority (CA) name:**  (required)

**Organization unit:**

**Organization name:**  (required)

**Locality or city:**

**State or province:**  (required minimum of 3 characters)

**Country or region:**  (required)

**Validity period of Certificate Authority (CA) (2-7300):**  (days)

# Install the CA Cert into your Browser

## Install Local CA Certificate

**Certificate type:** Certificate Authority (CA)

**Certificate store:** Local Certificate Authority (CA)

A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.

You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click on the certificate you want to install into your browser. Your web browser will display several windows to help you complete the installation of the certificate.

### [Install certificate](#)

After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this CA.

# Set the Policy for the CA

## Certificate Authority (CA) Policy Data

Your Certificate Authority (CA) was created with the default policy data shown below. Change the data if you want and then select Continue.

Allow creation of user certificates:  Yes  No

Validity period of certificates that are issued  
by this Certificate Authority (CA) (1-2000):  (days)

Days until Certificate Authority (CA) certificate expires:

:

Continue

Cancel

### Select Applications to Trust this Certificate Authority (CA)

Message: The policy data for the Certificate Authority (CA) was successfully changed.

**Certificate type:** Certificate Authority (CA)

**Certificate store:** Local Certificate Authority (CA)

Select the applications that should include this Certificate Authority (CA) in the application Certificate Authority (CA) trust list:

Select All

Clear All

	Application	Type	Assigned certificate
<input checked="" type="checkbox"/>	IBM i TCP/IP Telet Server	Server	Security Testing RSA
<input checked="" type="checkbox"/>	IBM i TCP/IP Telet Client	Client	Security Testing RSA
<input checked="" type="checkbox"/>	Cluster Security	Server	None assigned
<input checked="" type="checkbox"/>	IBM Tivoli Directory Server	Server	None assigned
<input checked="" type="checkbox"/>	IBM Directory Server publishing	Client	None assigned
<input checked="" type="checkbox"/>	IBM Directory Server client	Client	None assigned
<input checked="" type="checkbox"/>	IBM i VPN Key Manager	Server	None assigned
<input checked="" type="checkbox"/>	HTTP Server Monitor	Server	None assigned
<input checked="" type="checkbox"/>	IBM i TCP/IP SMTP Server	Server	Security Testing RSA
<input checked="" type="checkbox"/>	IBM i TCP/IP SMTP Client	Client	Security Testing RSA
<input checked="" type="checkbox"/>	IBM i TCP/IP FTP Server	Server	Security Testing RSA
<input checked="" type="checkbox"/>	IBM i TCP/IP FTP Client	Client	Security Testing RSA

- ▶ Click on 'Select All' to allow all servers to trust certificates issued by this CA or skip this step – this is only used if SSL/TLS has been configured to perform client authentication. We are not doing this. Click Continue.

## Application Status

Message The applications you selected will trust this Certificate Authority (CA).

Select Continue to create the default object signing certificate store (\*OBJECTSIGNING)

Continue

Cancel

- ▶ We are not going to create any object signing certificates, so click Cancel

# Create a Certificate using your Local (IBM i) CA



**Select a Certificate Store**

Select the certificate store that you want to open.

Local Certificate Authority (CA)

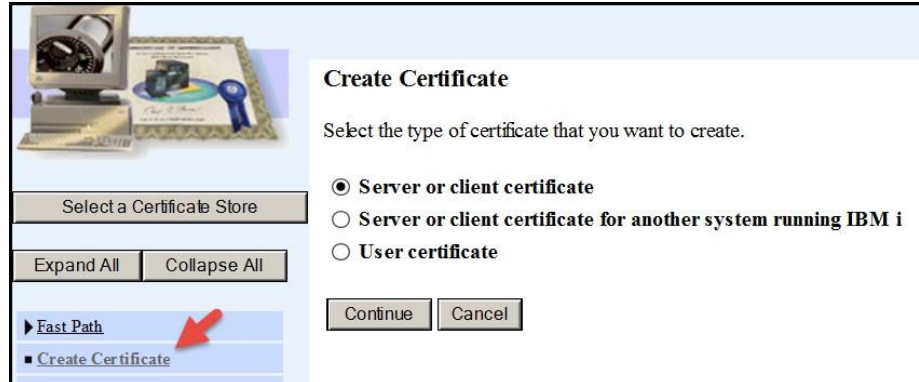
\*SYSTEM

Other System Certificate Store

Continue Cancel

Select a Certificate Store

Expand All Collapse All



**Create Certificate**

Select the type of certificate that you want to create.

Server or client certificate

Server or client certificate for another system running IBM i

User certificate

Continue Cancel

Select a Certificate Store

Expand All Collapse All

Fast Path

Create Certificate

# Create a Server Cert from your Local CA

## Select a Certificate Authority (CA)

**Certificate type:** Server or client

**Certificate store:** \*SYSTEM

Select the type of Certificate Authority (CA) that will sign this certificate.

- Local Certificate Authority (CA)
- VeriSign or other Internet Certificate Authority (CA)

Continue


Cancel

**Create Certificate**

Certificate type: Server or client  
 Certificate store: \*SYSTEM

Use this form to create a certificate in the certificate store listed above.

Certificate Authority (CA): LOCAL\_CERTIFICATE\_AUTHORITY\_7824BBX28(11) : RSA-4096 : SHA512 with RSA

Key algorithm: ECDSA 

Key size: 521 (bits)

Certificate label: HelpSystems Security Services (required)

**Certificate Information**

Common name: system\_name helpsystems.com (required)

Organization unit:

Organization name: HelpSystems Professional Security Services (required)

Locality or city: Eden Prairie

State or province: Minnesota (required minimum)

Country or region: US (required)

**Subject Alternative Name**

Note: Certificate extensions are not necessary for Secure Sockets Layer (SSL), but are recommended for Virtual Private Network (VPN).

IP version 4 address: [ ] . [ ] . [ ] . [ ]

Fully qualified domain name: (host\_name.domain\_name)

E-mail address: (user\_name@domain\_name)

- ▶ Be sure to select a Key algorithm that the client will support. (For example, Client Access doesn't support ECDSA – Elliptical curve). The other option is RSA which has proven to have vulnerabilities.



**Select Applications**

Message: Your certificate was created and placed in the certificate store listed below.

**Certificate type:** Server or client  
**Certificate store:** \*SYSTEM  
**Certificate label:** HelpSystems Security Services

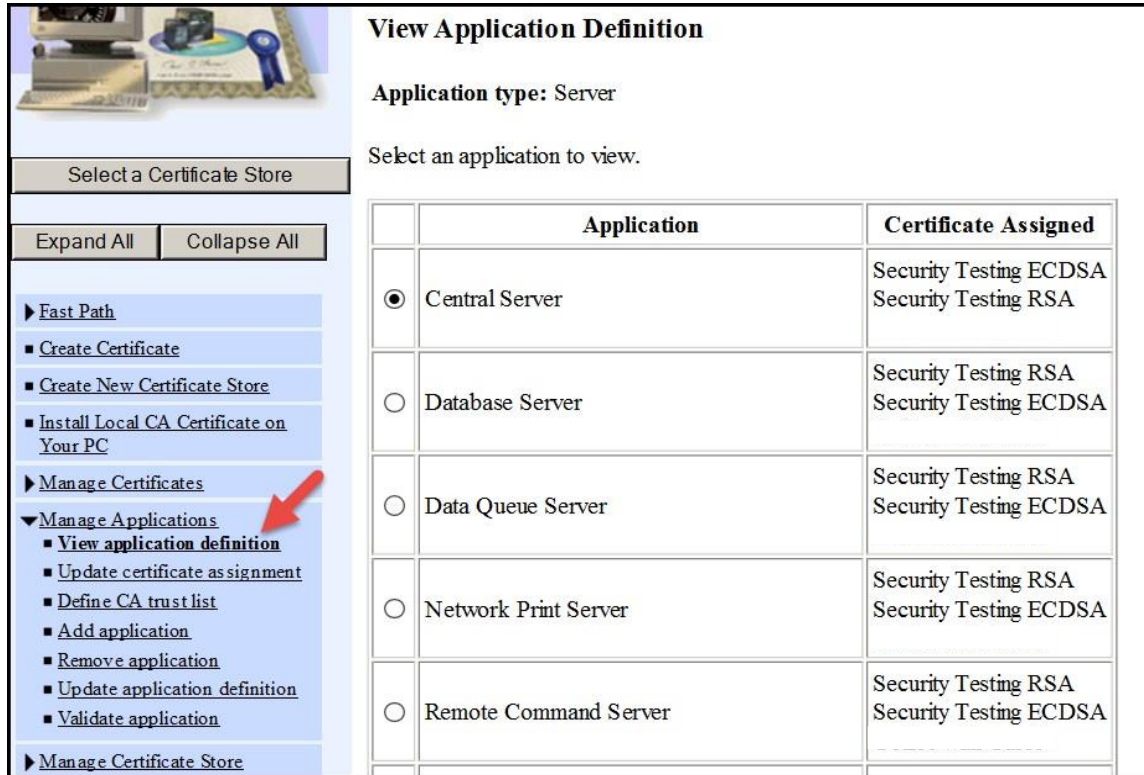
Select which applications will use this certificate:

**Warning:** When you assign a certificate to a client application and a server requests client authentication, server does not authenticate users on an individual basis. To ensure that the server authenticates client application.

<input checked="" type="checkbox"/>	Application	Type	Assigned certificate
<input checked="" type="checkbox"/>	Central Server	Server	Security Testing ECDSA Security Testing RSA
<input checked="" type="checkbox"/>	Database Server	Server	Security Testing RSA Security Testing ECDSA
<input checked="" type="checkbox"/>	Data Queue Server	Server	Security Testing RSA Security Testing ECDSA
<input checked="" type="checkbox"/>	Network Print Server	Server	Security Testing RSA Security Testing ECDSA
<input checked="" type="checkbox"/>	Remote Command Server	Server	Security Testing RSA Security Testing ECDSA
<input checked="" type="checkbox"/>	Signon Server	Server	Security Testing RSA Security Testing ECDSA
<input checked="" type="checkbox"/>	IBM i TCP/IP Tehet Server	Server	Security Testing RSA Security Testing ECDSA

- ▶ Check the box to assign the certificate to all servers. It doesn't affect anything to assign a certificate to a server! It will only be used if a client has been configured to request an encrypted session. Note: V7R2 allows multiple certs to be assigned to a server.
- ▶ Click Append.

# Verify Assignment



**View Application Definition**

Application type: Server

Select an application to view.

Select a Certificate Store

Expand All Collapse All

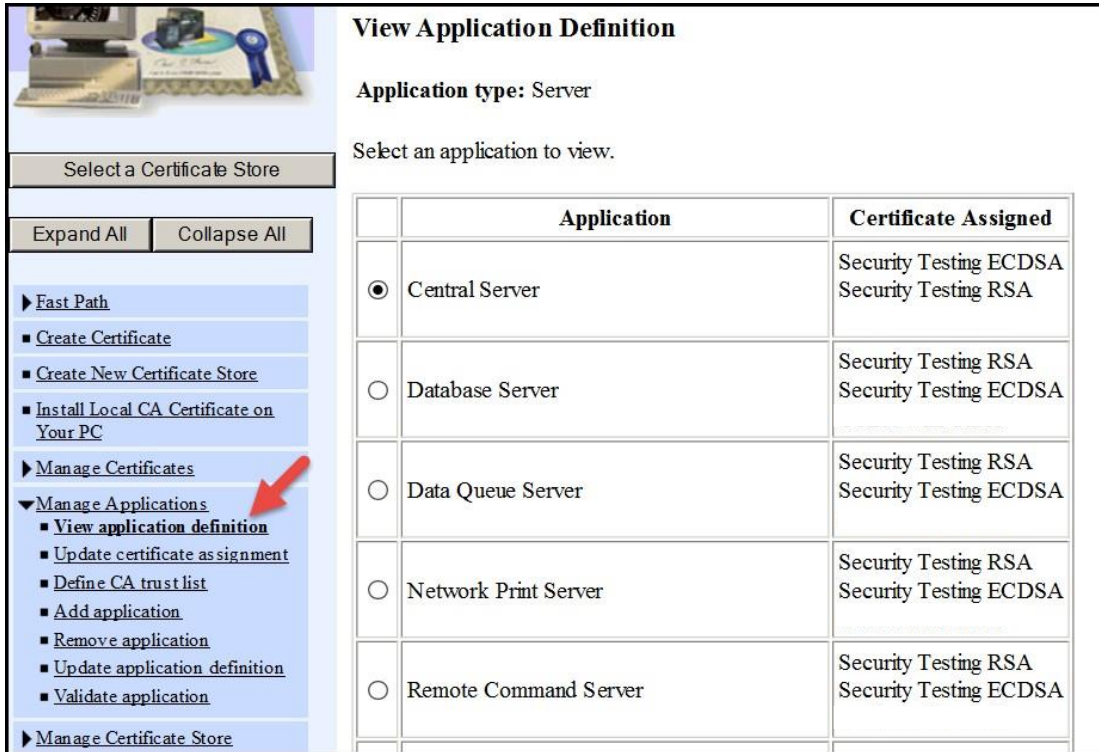
- Fast Path
  - Create Certificate
  - Create New Certificate Store
  - Install Local CA Certificate on Your PC
- Manage Certificates
- Manage Applications
  - View application definition**
  - Update certificate assignment
  - Define CA trust list
  - Add application
  - Remove application
  - Update application definition
  - Validate application
- Manage Certificate Store

	Application	Certificate Assigned
<input checked="" type="radio"/>	Central Server	Security Testing ECDSA Security Testing RSA
<input type="radio"/>	Database Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Data Queue Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Network Print Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Remote Command Server	Security Testing RSA Security Testing ECDSA

These are the server applications

## Configuring an HTTP Web Instance

# Verify Assignment



The screenshot shows a software interface for managing certificates and applications. On the left, there is a navigation pane with a tree view. The 'Manage Applications' folder is expanded, and 'View application definition' is selected, indicated by a red arrow. The main area displays the 'View Application Definition' dialog for a 'Server' application type. It prompts the user to 'Select an application to view.' and shows a table of applications with their assigned certificates.

**View Application Definition**

Application type: Server

Select an application to view.

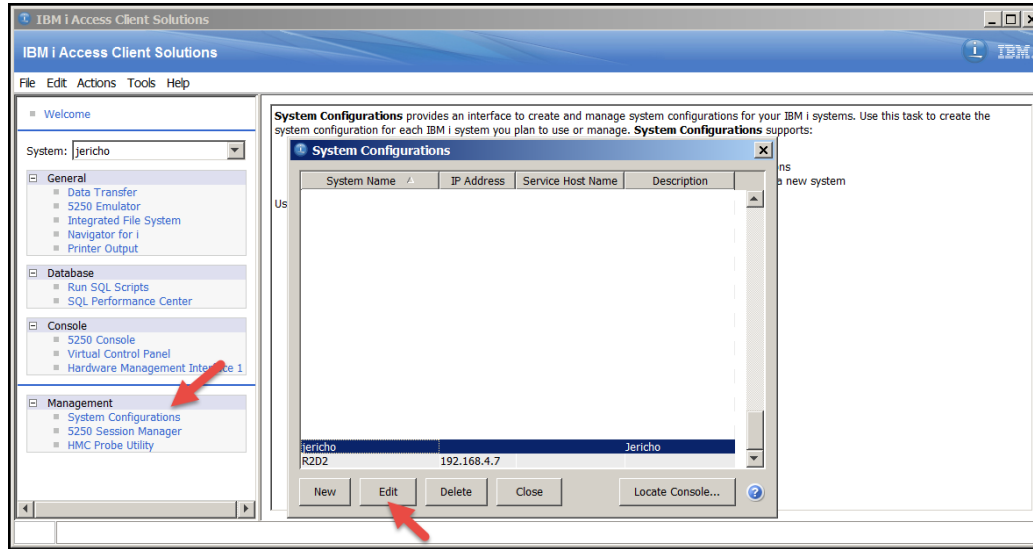
	Application	Certificate Assigned
<input checked="" type="radio"/>	Central Server	Security Testing ECDSA Security Testing RSA
<input type="radio"/>	Database Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Data Queue Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Network Print Server	Security Testing RSA Security Testing ECDSA
<input type="radio"/>	Remote Command Server	Security Testing RSA Security Testing ECDSA

# Enable SSL/TLS in web application configurations

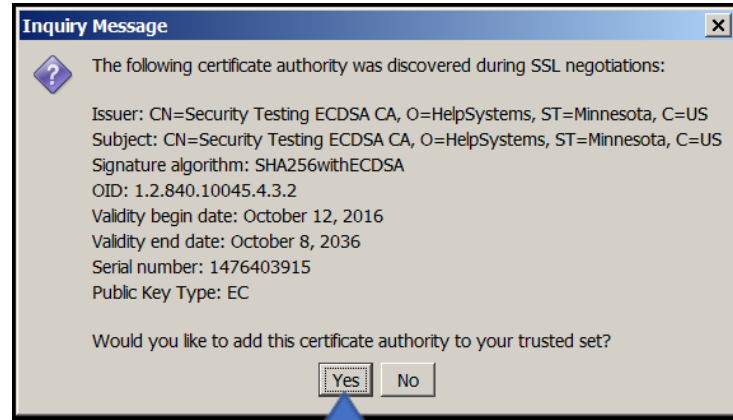
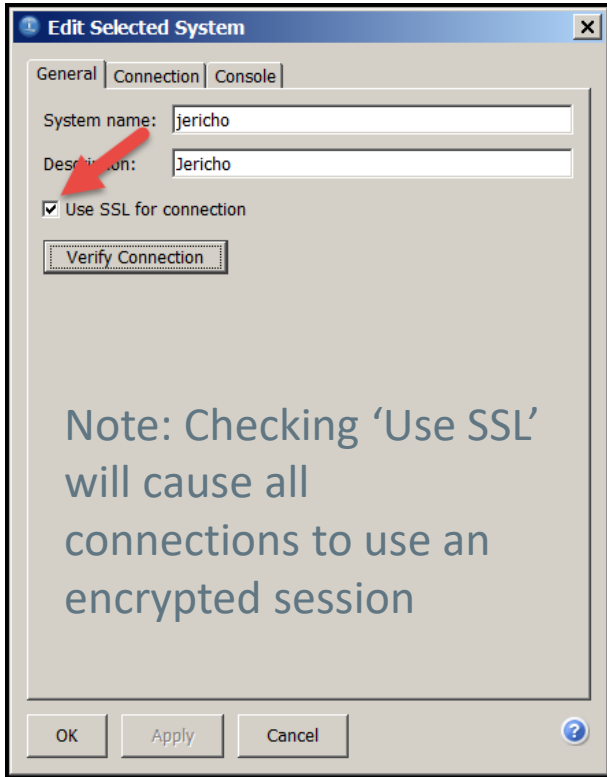
The screenshot shows the IBM Web Administration for i console. The main navigation bar includes 'Setup', 'Manage', 'Advanced', and 'Related Links'. Below this, there are tabs for 'All Servers', 'HTTP Servers', 'Application Servers', and 'Installations'. The current server is 'SKYVIEWWEB - Apache' and the server area is 'Global configuration'. The left sidebar contains a tree view with categories like 'Common Tasks and Wizards', 'HTTP Tasks and Wizards', 'Server Properties', 'Request Processing', 'Security', 'Proxy', and 'WebSphere Application Server'. The main content area is titled 'SKYVIEWWEB > Security' and has a 'Security' sub-header. Under 'Security', there are tabs for 'Authentication', 'Control Access (Deprecated)', and 'Control Access'. The 'SSL Proxy' and 'SSL Proxy Advanced' tabs are active. Below these, there are tabs for 'SSL with Certificate Authentication', 'Control Certificate Access', and 'SSL Advanced'. The 'SSL' dropdown menu is set to 'Optional', indicated by a red arrow. The 'Server application ID' dropdown is set to 'QIBM\_HTTP\_SERVER\_SKYVIEWW...', also indicated by a red arrow. Under 'Client certificates when establishing the connection', the 'Do not request client certificate for connection' radio button is selected. The 'HTTPS\_PORT environment variable' is set to '443'. At the bottom, there are 'OK', 'Apply', and 'Cancel' buttons.

# Configuring ACS (Access Client Solutions) to request an Encrypted Session

# Modify your System Configuration



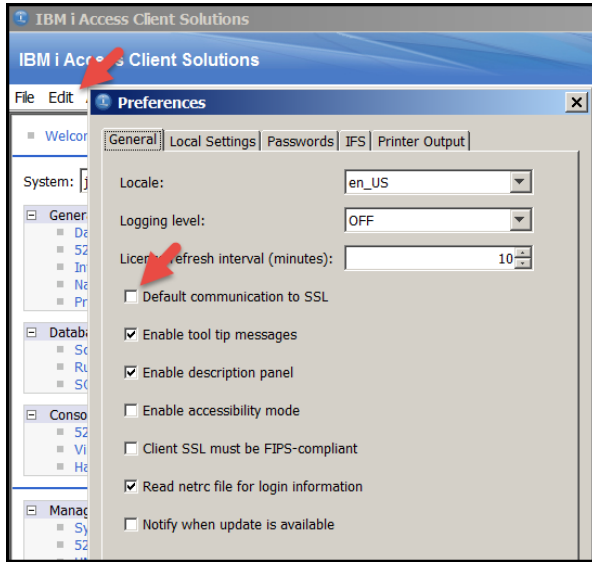
- ▶ Click System Configurations
- ▶ Choose the system
- ▶ Click Edit



- ▶ Clicking Yes, adds the CA Cert into the client keystore. This allows your client to trust the certificate the server will pass to the client during the initial negotiation (start) of the connection.



# Defaulting New Configurations



- ▶ To ensure new connections default to use SSL, choose Edit->Preferences
  - ▶ Click 'Default communication to SSL'
- (Note: this change has no affect on existing configurations)*

# Verifying Telnet

Sign On

Subsystem . . . . . : QINTER  
Display . . . . . : QPADEV0001

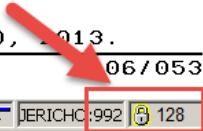
User . . . . . : \_\_\_\_\_  
Password . . . . . : \_\_\_\_\_

Program/procedure . . . . . : \_\_\_\_\_  
Menu . . . . . : \_\_\_\_\_  
Current library . . . . . : \_\_\_\_\_

(C) COPYRIGHT IBM CORP. 1980, 2013.

MA+ A 06/053

| JERICHO:992 | 128



# Configuring only Telnet

The image shows a configuration dialog box with a tree view on the left and a main configuration area on the right. The tree view includes 'Connection', 'Screen', and 'Preferences'. The 'Connection' section is expanded, showing fields for Session Name, Destination Address, Destination Port (23), Protocol (Use IBM | Access Client Solutions setting), Workstation ID (Use IBM | Access Client Solutions setting), Screen Size (Telnet - Not secured), and Host Code Page (037 United States). There are also radio button options for Unicode, DBCS, and Auto-Connect/Reconnect.

Field	Value
Session Name	
Destination Address	
Destination Port	23
Protocol	Use IBM   Access Client Solutions setting
Workstation ID	Use IBM   Access Client Solutions setting
Screen Size	Telnet - Not secured
Host Code Page	037 United States

Unicode Options:

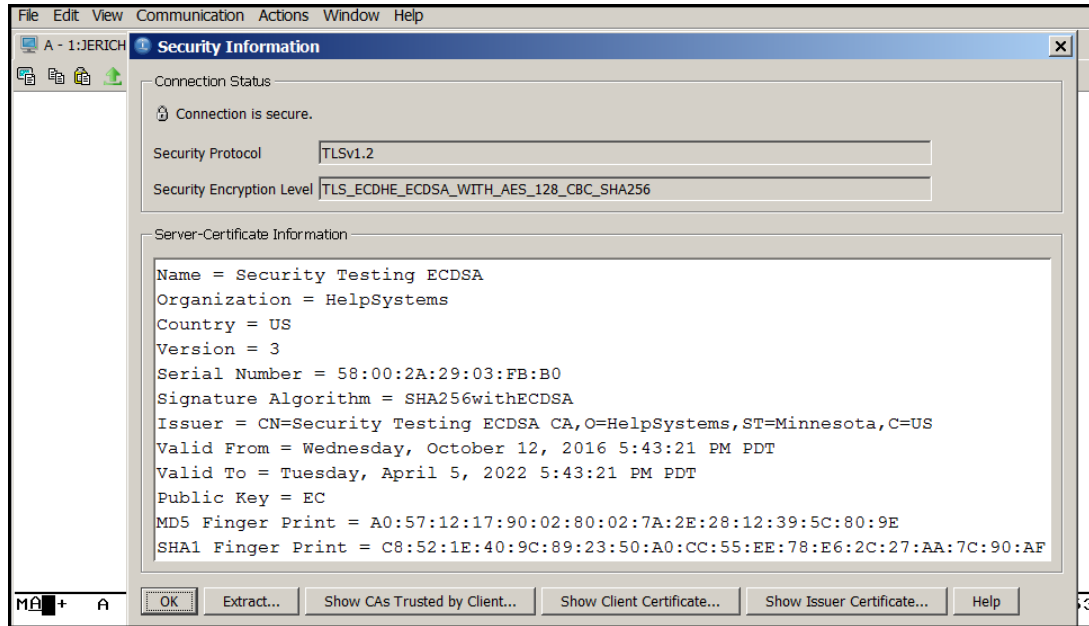
- Enable Unicode Data Stream:  Yes  No
- Enable DBCS in Unicode Fields:  Yes  No
- Protect Unicode Field Length:  Yes  No

Auto-Connect:  Yes  No

Auto-Reconnect:  Yes  No

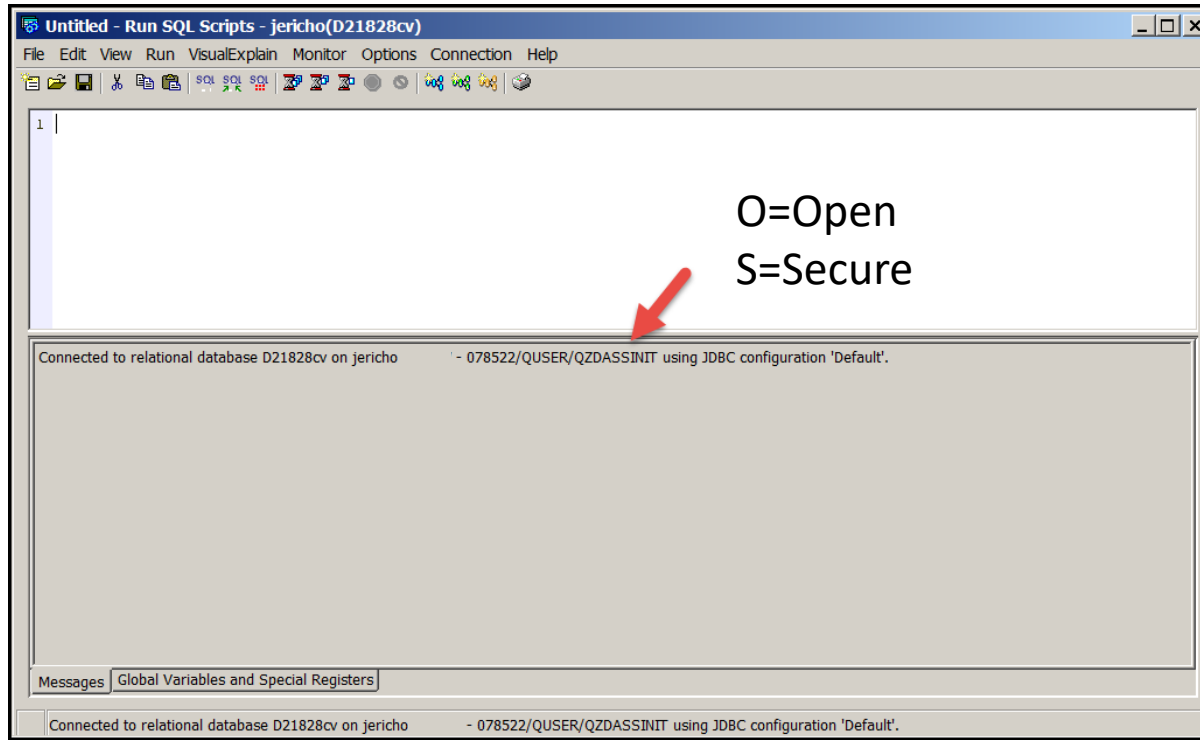
Buttons: OK, Cancel, Keyboard..., Help

# Discovering What Protocol and Cipher are in Use



► Click Communication ->Security ...

# Verifying ODBC – QZDAS(O/S)INIT



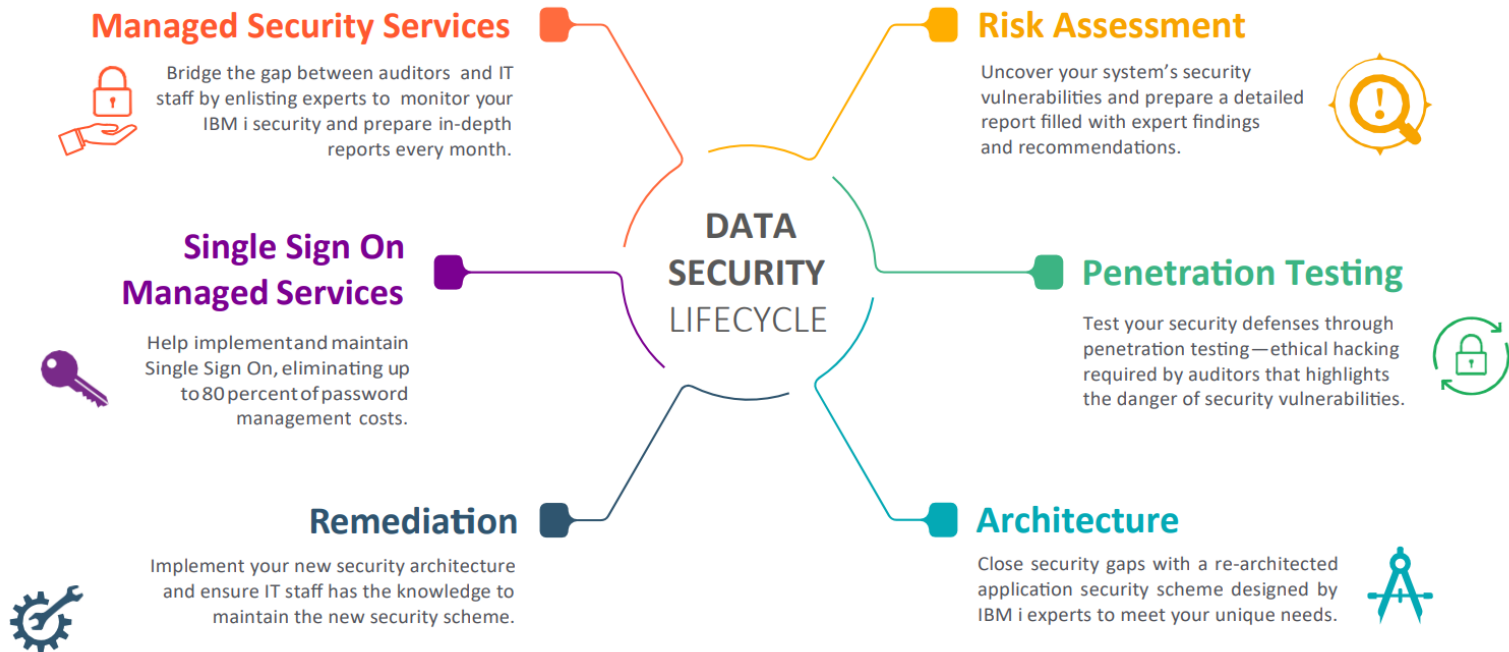
# Additional Reading

- ▶ Getting Started with DCM –
  - ▶ <http://www-01.ibm.com/support/docview.wss?uid=nas8N1014938>
- ▶ DCM FAQs –
  - ▶ <http://www-01.ibm.com/support/docview.wss?uid=nas8N1010356>
- ▶ Access Client Solutions Deployment – COMMON presentation by Wayne Bowers
  - ▶ [http://schd.ws/hosted\\_files/commons17/97/ACSAdmin\\_COMMON.pdf](http://schd.ws/hosted_files/commons17/97/ACSAdmin_COMMON.pdf)

# HelpSystems' Solution-Based Offerings



# Professional Security Services





A horizontal bar composed of three segments: a blue segment on the left, a light blue segment in the middle, and a black segment on the right.

## Thank you for joining us

 [www.helpsystems.com](http://www.helpsystems.com)

 [info@helpsystems.com](mailto:info@helpsystems.com)