FORTRA™

Access Client Solutions Secure Deployment

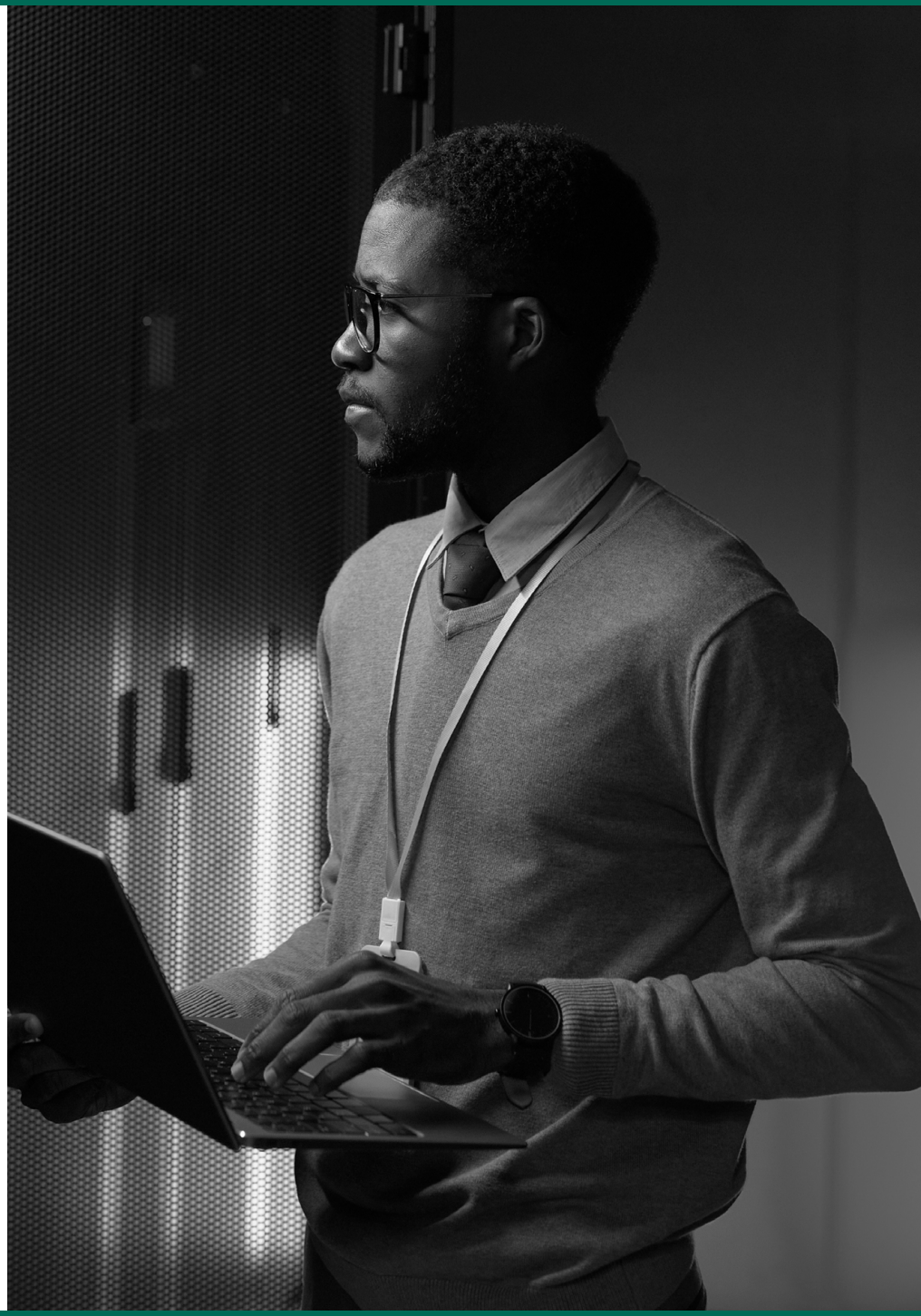
Secure Deployment Considerations

IBM i Access Client Solutions (ACS) is the newest member of the IBM i Access family, replacing the IBM i Access for Windows client.

ACS runs on most operating systems supporting Java. Because ACS uses different technology and deployment approach than IBM i Access for Windows, the considerations for securely deploying ACS are different than IBM i Access for Windows. Some of the considerations for ACS are:

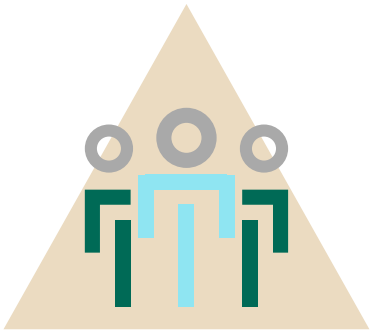
- The product is readily available for download by anyone with an IBM ID.
- The components selected during the install do not control the functions that can be available to the user (desktop installation).
- Users can change the configuration file to access more ACS functions than initially configured.
- The product can be executed and updated without a traditional Windows install.
- ACS can be deployed to a network server allowing a single install image to be leveraged by multiple users.

Read this guide for expert guidance on addressing the security concerns related to ACS deployment in the Windows environment. The discussion that follows does not include all installation and configuration steps—only those steps related to security.

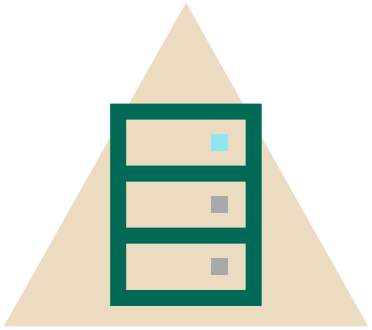


Deployment Types

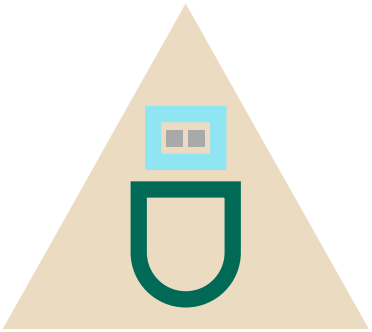
Three deployment types are available for ACS:



Client



Server



USB

The client deployment installs the product and user specific files on the desktop.

The default install locations are:

Location	Purpose
C:\Users\Windows User Name\IBM\ClientSolutions or C:\Users\Public\IBM\ClientSolutions	ACS image directory
C:\Users\Windows User Name\Documents\IBM\iAccessClient	User configuration files including the certificate store used by the product

The server deployment places the product and user specific files on a file server. The user specific files are in a designated directory on the file server.

The USB deployment locates the product files on removable media. This method will not be discussed in this document.

Desktop Deployment

The desktop install uses java script rather than the standard Windows installer. The install is performed by executing a java script at the Windows command prompt:

Install Script	Purpose
ACS Image Directory/Windows_Application/install_acs_xx.js	*Installs product in C:\Users\Windows_User_Name\IBM\ClientSolutions*
ACS Image Directory/Windows_Application/install_acs_xx_allusers.js	*Installs product in C:\Users\Public\IBM\ClientSolutions*

where "xx" is the same as the bitness (32 or 64) of the Java installed on the desktops where ACS is being installed. For ease of management, installation in Public is recommended.

When the Windows security warning is displayed for the acslaunch_win-xx.exe, click Run. The installer will prompt to enable each ACS function. However, declining to enable a function does not prevent the user from accessing a function. The user may edit the property (shown below) in the AcsConfig.properties file to remove any restrictions put in place by simply deleting any text after the "=".

com.ibm.iaccess.ExcludeComps=console, hmcprobe, vcp

Rather than relying on the AcsConfig.properties file to control available functions, truly restricting functions on the desktop requires a different method.

Controlling Available Functions for the Desktop Deployment

The recommended method for restricting the functions available to the desktop user is through the "Restrictions" tab in the Preferences. This method uses settings in the Windows registry to control the functions available to the user. The functions limited via the restrictions tab are maintained even when:

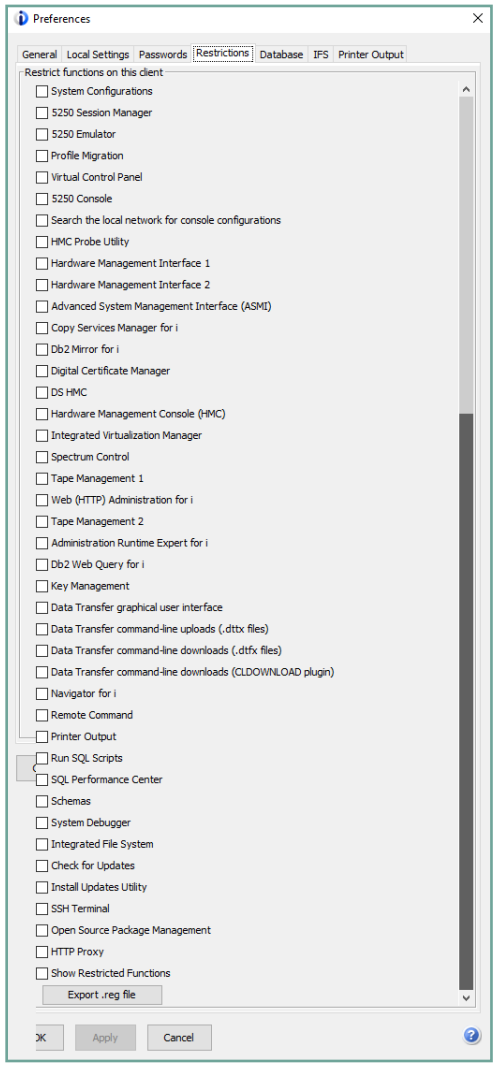
- The acsbundle.jar is replaced.
- The acsbundle.jar is in a different location (download, USB drive, file server, etc.)
- The AcsConfig.properties file is modified.

The "Restrictions" tab is only available when ACS is started on the desktop with administrator privileges.

To access the "Restrictions" tab:

1. Start ACS with administrator privileges
2. Start Access Client Solutions.
3. Click Edit>Preferences.

4. Click the “Restrictions” tab near the top of the Preferences panel. The panel below is the captured list of all functions.



5. Select the functions that should not be permitted on the client.
6. Click OK.

Restrictions may be exported and applied to other desktops via two methods. The “Export .reg file” button on the “Restrictions” tab will export the restrictions to a .reg file that can be deployed with the ACS install. Before exporting the .reg file, click Apply or OK. Below is the content of the registry file.

```
Windows Registry Editor Version 5.00
[-HKEY_LOCAL_MACHINE\Software\JavaSoft\prefs\com\ibm\iaccess\base\restrictions]
[HKEY_LOCAL_MACHINE\Software\JavaSoft\prefs\com\ibm\iaccess\base\restrictions]
“cfg”=”r”
“sm”=”r”
“5250”=”u”
“pm5250”=”r”
“vcp”=”r”
“console”=”r”
“consoleprobe”=”r”
“hmcprobe”=”r”
“hmi1”=”r”
“hmi2”=”r”
“asmi”=”r”
“csmi”=”r”
“db2mirror”=”r”
“dcm”=”r”
“dshmc”=”r”
“hmc”=”r”
“ivm”=”r”
“specctrl”=”r”
“tapemgmtl”=”r”
```

The .reg file can be manually edited to allow (“u”) or restricted (“r”) each function. A .reg file should be built for each combination of allowed functions, distributed to the desktop and executed after ACS is installed on the desktop.

The Windows .reg file can alternatively be generated using the following command:

ACS Image Directory\Start_Programs\Windows_Architecture>acslaunch_win-XX.exe /PLUGIN=restrict /exportreg =<file>

Where Architecture and XX are based on Java bitness and <file> is the target .reg file. The command line function requires Windows administrator access the same as the graphical interface.

One of the advantages of using the registry keys for ACS function management is the ability to add and remove ACS functions by deploying a new registry file to the desktop, which eliminates the need for customized ACS installations.

Server Deployment

The strategy for server deployment is to build individual ACS images for each unique group of functions. Functions included are often based on user role. For example, image A enables only telnet and will be used by end users. Image B enables telnet, data transfer, and printer output and will be used by power users; and image C enables telnet, data transfer, printer output, integrated file system and run SQL scripts to be used by developers and database administrators. Each of the customized images are created in a unique path on a file server.

Functions available to the user are controlled by the com.ibm.iaccess.ExcludeComps property in the AcsConfig.properties file. All functions not included in the com.ibm.iaccess.ExcludeComps property will be available to users.

User Object Location

To eliminate conflicts, the server deployment requires a unique path for each user’s configuration objects. The path for the users’ files is designated using the com.ibm.iaccess.AcsBaseDirectory property in the AcsConfig.properties file. One of two path configurations are recommended and are in the table below.

com.ibm.iaccess.AcsBaseDirectory Value	Purpose
{PRODUCTDIR}/config_directory/{USER}/	The user configuration directory is in the product directory of the image executed by the user. The image will contain a configuration directory for each user of the image.
{ROOT}/config_directory/{USER}/	The user configuration directory is distinct from the product directory. This approach enables all user configurations across all images to be located within a single directory structure.

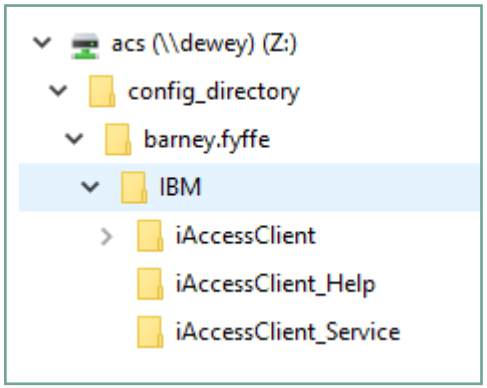
An advantage of the location outside the product directory is a common directory for all users when multiple ACS images are in the environment.

ACS Image Directory and File Security

To ensure the configuration cannot be modified, the access control settings for the ACS directories on the file server should be configured as shown in the following table. This configuration protects the ACS image but allows operation of the application:

Directory	User(s)	Security
ACS product directory	Public	Read and Execute
Directories and files in the ACS product directory	Public	Read and Execute
User configuration directory	Public	Read and Execute
Directory for user in the configuration directory	Public	None
	User	Read, Write and Execute

The directories in the ACS product directory should be similar to the image below. (This deployment has the user configuration directory is in the ACS product directory.) Creating the user's configuration directory in the parent configuration directory, ensuring user's directory has the correct security controls prior to the user starting ACS for the first time. The configuration directory will be like the image below.



Server Install

Use the following steps to perform a customized installation of Access Client Solutions on the file server.

1. Copy the contents of the downloaded ACS .zip file to the server directory designated for the ACS image.
2. On the Windows command line navigate to the server directory below containing the ACS image.

   ACS Image Directory/Windows_Application
3. Run the command below from the Windows command line.

   install_acs_xx.js /AdminConfig

   where "xx" is the same as the bitness (32 or 64) of the Java installed on the desktops accessing ACS.
4. When prompted for a response to the "Do you want to change the current configuration?" question, click Yes.
5. Click Yes when prompted with "Is it OK to begin with the default configuration?"
6. At the "Do you want multiple users to share a common location of product files?" prompt, click Yes.
7. When the message "The next set of questions will determine what functions you make available to your users." is displayed, click OK.
8. Click Yes when the "Do you want to use 5250 emulation?" prompt is displayed if telnet should be included in the image.
9. When the "Do you want to make ACS the default program for your existing 5250 session profiles?" message is displayed, click Yes if ACS should be used to open existing .ws files (IBM i Access for Windows) session profiles. A file association will be created to open .ws files with ACS.
10. Click Yes or No to include or exclude each additional function.
11. If the product shortcuts should be included on the desktop, click Yes when the "Do you want product shortcuts on the Desktop?" message is displayed.
12. When the "You have finished setting up the configuration." message is displayed, click OK. The customization is complete.

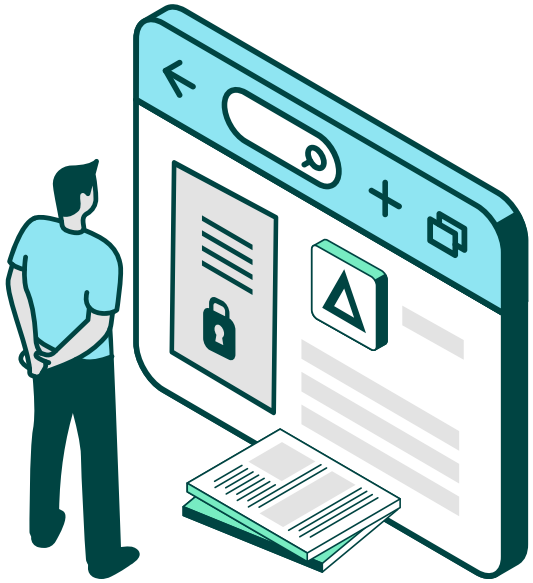
The desktop install for the server deployment is performed by executing the same Java script that created the ACS image but without the AdminConfig parameter. The ACS product files are not installed on the desktop by the Java script.

Controlling Available Functions for the Network Deployment

Registry Entries

The preferred method of restricting ACS functions is using registry entries for security to eliminate the need for image customizations. A .reg file may be deployed to the desktop of users that will use the ACS image just as in the desktop deployment. For example, if all functions were restricted in the ACS image except telnet (5250), the com.ibm.iaccess.ExcludeComps property in the AcsConfig. properties file would be:

com.ibm.iaccess.ExcludeComps=Cfg, Checkupdates, Cldownload, Console, Consoleprobe, db2, db2tools, download, dtgui, hmcprobe, ifs, installupdates, keyman, l1c, osssetup, restrictview, rmtcmd, rss, sm, splf, ssh, sysdbg, upload, vcp.



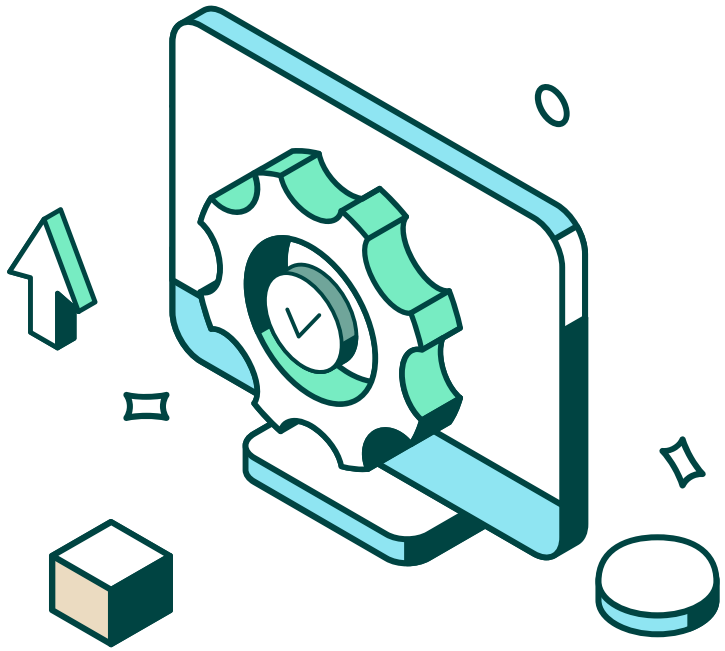
The more secure approach is deploying the .reg file below to the desktop.

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\Software\JavaSoft\prefs\com\ibm\iaccess\base\restrictions]

[HKEY_LOCAL_MACHINE\Software\JavaSoft\prefs\com\ibm\iaccess\base\restrictions]

“cfg”=”r”

“sm”=”r”

“5250”=”u”

“pm5250”=”r”

“vcp”=”r”

“console”=”r”

“consoleprobe”=”r”

“hmcprobe”=”r”

“hmi1”=”r”

“hmi2”=”r”

“asmi”=”r”

“csmi”=”r”

“db2mirror”=”r”

“dcm”=”r”

“dshmc”=”r”

“hmc”=”r”

“ivm”=”r”

“specctrl”=”r”

“tapemgmt1”=”r”

“httpadmin”=”r”

“tapemgmt2”=”r”

“are”=”r”

“db2webquery”=”r”

“keyman”=”r”

“dtgui”=”r”

“upload”=”r”

“download”=”r”

“cldownload”=”r”

“l1c”=”r”

“rmtcmd”=”r”

“splf”=”r”

“rss”=”r”

“db2tools”=”r”

“db2”=”r”

“sysdbg”=”r”

“ifs”=”r”

“checkupdates”=”r”

“installupdates”=”r”

“ssh”=”r”

“osssetup”=”r”

“httpproxyui”=”r”

“restrictview”=”r”
```

AcsConfig.properties File

In the network deployment, ACS functions may be controlled only if the user cannot update the AcsConfig.properties file.

The table to the right list the functions and function groups that can be included on the com.ibm.iaccess.ExcludeComps property.



Function	Description
5250	5250 Emulator
Cfg	System Configuration
Checkupdates	Check for available updates
Cldownload	Data transfer command-line downloads
Console	5250 Console
Consoleprobe	Search the local network for console configurations
hmcprobe	Search an HMC for partitions
hmi1	Hardware Management Interface 1
hmi2	Hardware Management Interface 2
keyman	SSL/TLS certificate management
dtgui	Data Transfer graphical user interface
upload	Data Transfer batch uploads
download	Data Transfer command-line download
cldownload	Data Transfer batch downloads
l1c	IBM Navigator for i (Level 1 Console)
rmtcmd	Remote command (available from the command-line)
splf	Printer Output (spool files)
ifs	Integrated File System
db2	Schemas
rss	Run SQL Scripts
db2tools	SQL Performance Center
sysdbg	IBM i System Debugger
checkupdates	Check for available updates
Ssh	Secure Shell
installupdates	Install updates from an IBM i configured location
osssetup	Open Source Package Management
restrictview	Restrict view of currently restricted functions
sm	5250 Session Manager
vcp	Virtual Control Panel

Below are the hardware management interfaces.

Hardware Management Interface	Description
hmi1	Hardware Management Interface 1
hmi2	Hardware Management Interface 2
asmi	Advanced System Management Interface (ASMI)
csmi	Copy Services Manager for i
dcm	Digital Certificate Manager
dshmc	DS HMC
hmc	Hardware Management Console (HMC)
httpadmin	Web (HTTP) Administration for i
ivm Integrated	Virtualization Manager
specctrl	Spectrum Control
tapemgmt1	Tape Management 1
tapemgmt2	Tape Management 2
are	Administration Runtime Expert
db2webquery	Db2 Web Query

Below are the function groups that may be used instead of individual functions.

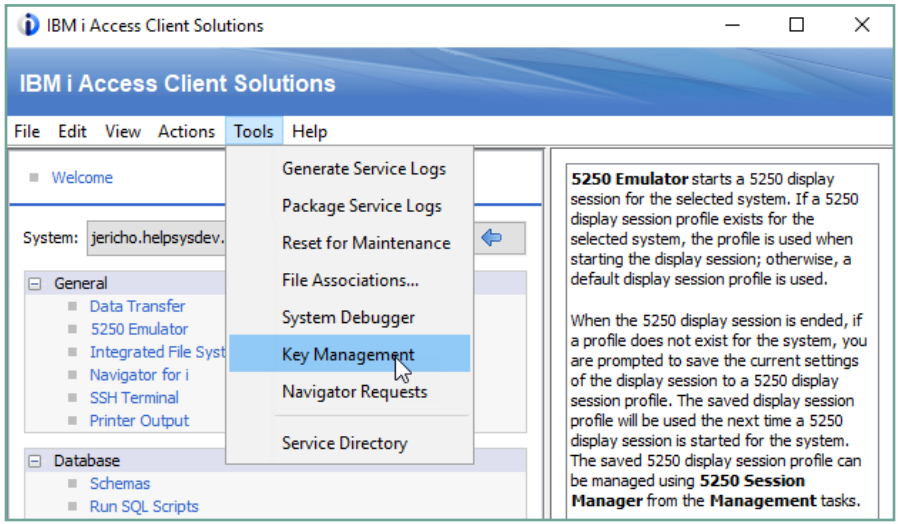
Function Group	Description
dataxfer	dtgui,upload,download,cldownload
emulator	sm,5250
keyman	keyman
opconsole	console,vcp,consoleprobe,hmcprobe
rmtcmd	rmtcmd
splf	splf
ifs	ifs
hwconsole	hmi1, hmi2, asmi, csmi, dcm, dshmc, hmc, httpadmin, ivm, specctrl, tapemgmt1, tapemgmt2, are, db2webquery
l1cplugin	l1c
database	db2, rss,db2tools
debugger	sysdbg
checkupdates	checkupdates

Standardized TLS/SSL Certificate Keystore

The sections below describe deployment of common TLS/SSL certificate stores for Access Client Solutions and the Access Client Solutions Windows Application Package.

Access Client Solutions

If you plan to configure ACS to use encrypted (TLS/SSL) sessions, consider using a standardized TLS/SSL certificate store. The certificate authority certificate(s) for the IBM i system(s) may be imported into the TLS/SSL certificate store using Tools>Key Management in the main ACS window.



After the certificate store is populated with the required certificates, the cacerts file may be copied to other desktops and servers so that end users don't have to interact with the certificate installation process. The SSL keystore file by default is in:

document path for windows user\Documents\IBM\iAccessClient\Private\windows user

However, for ease of management, the path of /Users/Public/Documents/IBM/Security is recommended with the inclusion of the com.ibm.iaccess.CertFile in the AcsConfig.properties file.

com.ibm.iaccess.CertFile=/Users/Public/Documents/IBM/Security/cacerts

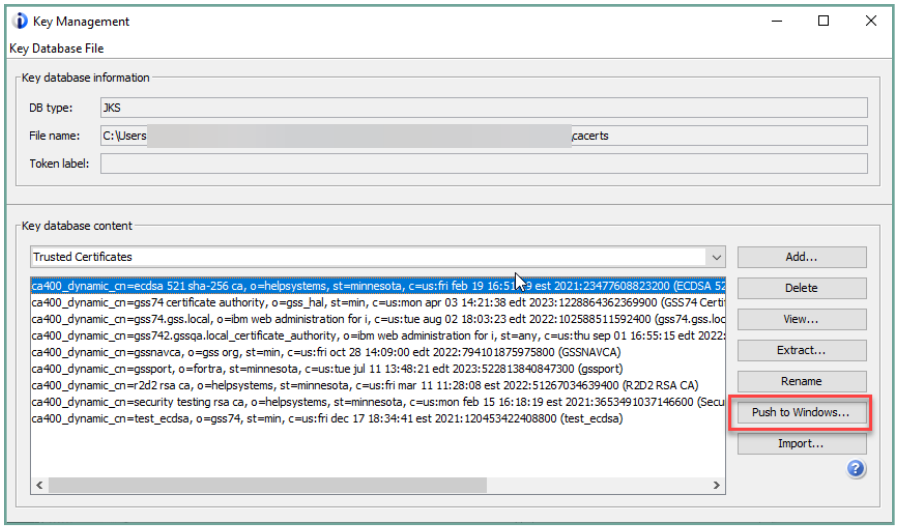
The */Users/Public/Documents/IBM/Security/cacerts* should be secured with read-only access. This approach is applicable to both desktop and network deployments.

Access Client Solutions Windows Application Package

The Access Client Solutions Windows Application Package (WAP) contains ACS APIs for Windows as well as ODBC and OLE. WAP has a separate TLS/SSL certificate store from the ACS application. The WAP certificate store consists of two files, cwbssldf.kdb and cwbssldf.sth, and is in:

C:\Users\Public\Documents\IBM\Client Access.

Certificates are added to the WAP certificate store through the ACS key management interface discussed previously. Click on the certificate to add to the WAP certificate store. Then click the "Push to Windows..." button. The prompt for the WAP certificate store will appear. The default password is "CA400".



The two files that comprise the WAP certificate store can be distributed just as the ACS certificate store. However, the WAP certificate store will always be distributed to the desktop.

Function Usage

Some ACS functions are controllable through Function Usage (Application Administration in the legacy Navigator for i) or the Work with Function Usage (WRKFCNUSG) command (function IDs beginning with QIBM_XE1, not QIBM_XE1_OPNAV).

Reference

The following links provide reference information for ACS deployment.

- ACS home page
- ACS Getting Started
- ACS Quick Start Guide
- ACS Customization and Deployment Made Easy
- Restricting Function Access

About the Author

Steve Sisk is a Senior Security Services Consultant at Fortra, LLC. Steve has engineered and administered IBM i, Power Systems, and predecessors for more than 26 years in single-entity and multi-entity environments. Prior to joining Fortra in 2016, Steve has held a variety of positions including lead architect for an IBM Global Services Strategy team, solution architect and lead engineer designing and implementing solutions for compliance requirements of general controls, PCI DSS, and HIPAA in large IBM i installations of numerous organizations. Steve's experience spans supply chain, finance, health care, insurance, ecommerce, retail, utilities and manufacturing. Steve holds the PCI Professional certification.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-pt-gd-1223-rb