IBM

@server

iSeries. mySeries.

V5R3 Security

Common Belgium
June 2, 2004

Agenda

- Network security enhancements
- IBM eServer i5/OS (OS/400) security enhancements
- Application security enhancements
- Additional information

Network security enhancements

- Kerberos, EIM support.
- Universal Connection Wizard
- Virtual Private Networking (VPN)
- Secure Sockets Layer (SSL)
- New cryptographic APIs
- Digital Certificate Manager (DCM)

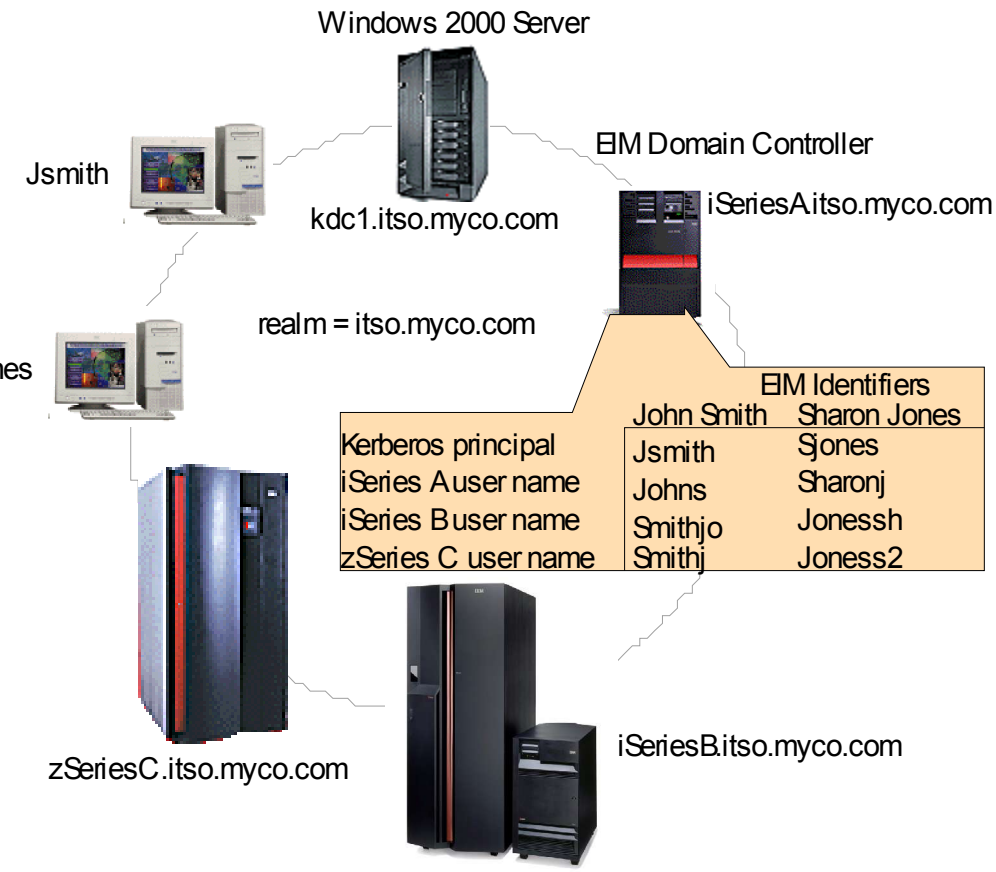
Enterprise Identity Mapping (EIM) and Kerberos

Enterprise Identity Mapping (EIM)

- EIM overview
- EIM – Wizard enhancements
- Synchronize functions wizard
- Mapping policy support
- User profile command enhancement
- Enabled OS/400 applications

Enterprise Identity Mapping - Overview

- Enterprise Identity Mapping (EIM) is a mechanism for mapping (associating) a person or entity to the appropriate user identities in various registries throughout the enterprise
- EIM provides an infrastructure that lowers the expense for application developers to provide single sign-on solutions



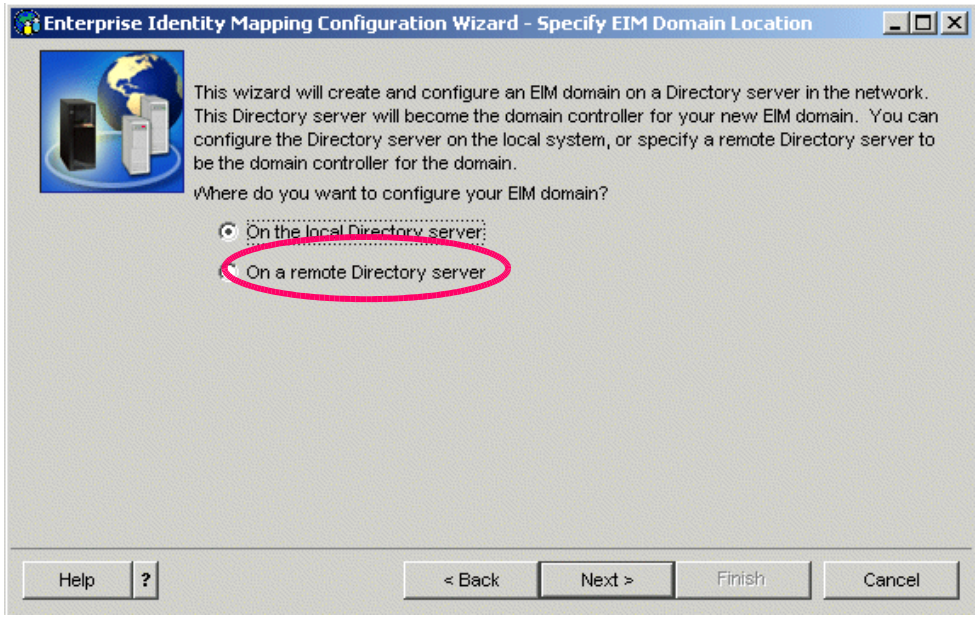
EIM defined: Identity associations across user registries associated with OS platforms, applications, and middleware.

Notes: Enterprise Identity Mapping - Overview

- Enterprise Identity Mapping (EIM) provides an infrastructure that lowers the expense for application developers to provide single sign-on solutions. OS/400's exploitation of EIM and Kerberos, along with exploitation by other IBM ~ platforms and IBM software, provides single sign-on capabilities. This, in turn, provides users, administrators, and application developers the benefits of easier password and user identity management across multiple platforms — without changing the underlying security schema.
- EIM allows for OS programmers and ISVs to independently implement support for a single sign-on environment without having to wait for support from a specific product vendor.
- EIM is part of IBM's Autonomic Computing initiative, which goal is to give businesses the ability to manage systems and technology infrastructures that are hundreds of times more complex than those in existence today.
- The initiative represents the next stage of development under new tools. Self-managing servers are the ultimate in new tools for our customers. They're self-optimizing, self-configuring, self-healing, and self-protecting.

EIM – Wizard enhancements

- An EIM domain can be created locally as well as remotely
- Requirements for remote server EIM domain controller are
  - iSeries server with V5R2 and the latest LDAP PTFs installed
  - iSeries server running V5R3
  - Server running IBM Directory Server V5.1 or later
  - LDAP server supporting LDAP V3 and the EIM schema



Notes: EIM – Wizard enhancements

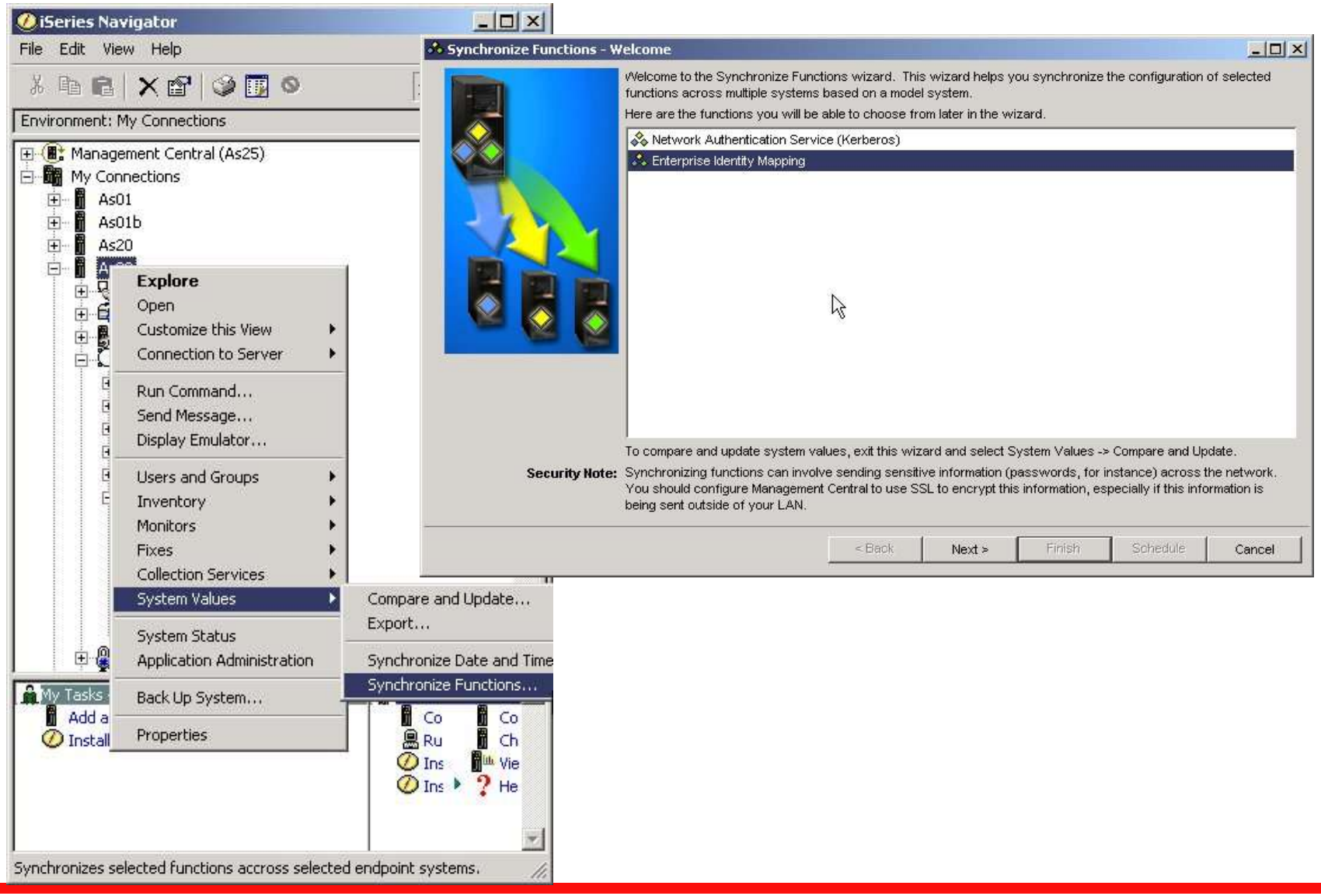
The EIM configuration wizard in V5R3 allows you to create the EIM domain controller on a remote system. Prior to V5R3, the EIM domain controller was automatically created on the system the wizard was running on.

The requirements for the remote server to be able to act as an EIM domain controller are as follows:

- An iSeries server with V5R2 and the newest LDAP PTF's installed
  - The PTF's will update the schema to include the V5R3 EIM schema extensions.
  - A list of PTFs can be found at: http://www-1.ibm.com/servers/eserver/iseries/ldap/whatsnew41.htm
- An iSeries server running OS/400 V5R3.
- A system running IBM Directory Server V5.1
- A system running a LDAP server that supports LDAP version 3 and has its schema extended to support the EIM schema.

The EIM schema definition can be found in InfoCenter under Security and Directory Server->Enterprise Identity Mapping (EIM)->EIM concepts->LDAP concepts for EIM->EIM schema for LDAP.

EIM – Synchronize functions wizard

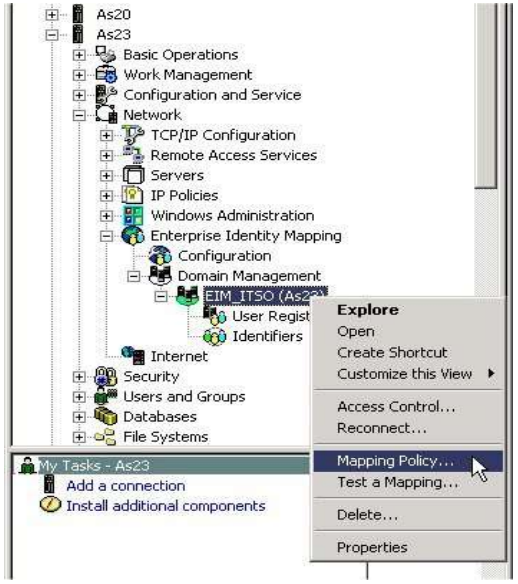


Notes: EIM – Synchronize functions wizard

Starting with V5R3, you can use the new Synchronize Functions wizard in iSeries Navigator to propagate network authentication service (Kerberos) and EIM configurations to a group of V5R3 systems. You can select a model endpoint system and a set of target endpoint systems, and then use the wizard to duplicate the model system's Kerberos and/or EIM configurations on the specified target systems. Synchronizing these functions from the model system saves you time by eliminating the task of individually configuring each function on each target system. Management central is being used for the synchronization process.

EIM – Mapping policy support

- Allows you to enable and disable use of policy associations
  - For the entire domain
  - For each specific target user registry
- Provides many-to-one mappings
- Mapping lookups using policy associations are disabled for the domain



Notes: EIM – Mapping policy support

The V5R3 EIM mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain.

You can create and use policy associations to define direct relationships between user identities in different user registries. A policy association provides a means of creating many-to-one mappings between a source set of multiple user identities in one user registry and a single target user identity in a target user registry.

The new mapping policies provide the following many-to-one mappings for:

- Unknown users of the entire domain to a single user for a specific target registry
- Unknown users from a given source registry to a single user in a specific target registry
- Certificate distinguished names via a filter to a single user in a specific target registry

The default setting for the EIM domain is that mapping lookups that use policy associations are disabled for the domain. So, all mapping lookup operations for the domain will return results only by using specific identifier associations between user identities and EIM identifiers. You have to explicitly enable this support within iSeries Navigator.

EIM – User profile command enhancement

- Additional parameter EIMASSOC
  - CRTUSRPRF
  - CHGUSRPRF
- Defines EIM identifier association for user profile in local registry

Notes: User profile command enhancement

An additional parameter, called EIMASSOC, has been added to the Create user profile (CRTUSRPRF) command and the Change user profile (CHGUSRPRF) command.

The EIMASSOC parameter allows you to define EIM identifier associations for the specified user profile for the local registry.

In order to use this parameter, you specify the following:

- EIM identifier
- an action option for the association (*ADD, *REPLACE or *REMOVE)
- the type of identifier association (target, source, both target and source, administrative)
- whether to create the specified EIM identifier if it does not already exist

This command function complements the original V5R2 iSeries Navigator interface to add an association to an EIM identifier.

Kerberos and EIM enabled OS/400 applications

- Host servers (used by iSeries Access for Windows)
- Telnet server (used by PC5250 and Host On-Demand V8)
- QFileSrv.400, DRDA, ODBC, JDBC
- HTTP Server for iSeries (powered by Apache) V5R3 PTFed at V5R2
- Management Central V5R3
- LDAP Server (Kerberos authentication only)
- Windows Integration V5R3
- FTP Server (EIM only when using client authentication with certificates or with an FTP logon exit point program)

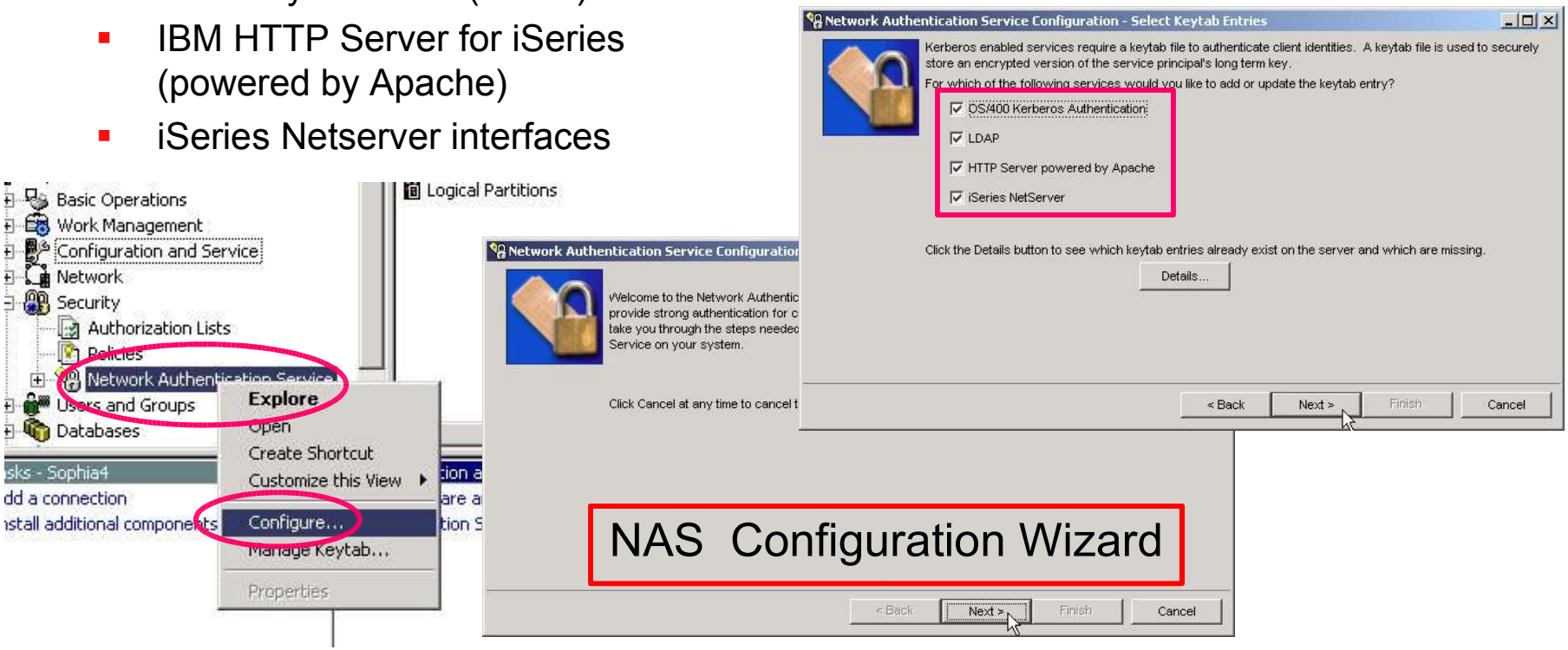
Notes: Kerberos and EIM enabled OS/400 applications

- OS/400 client and server applications that are currently enabled for single signon are:
  - OS/400 Host Servers (5722-SS1 Option 12): currently used by iSeries Access for Windows and iSeries Navigator.
  - Telnet server: currently used by PC5250 and Host On-Demand Version 8: Web Express Logon feature.
  - Open DataBase Connectivity (ODBC): allows single signon access to OS/400 databases through ODBC.
  - Java Database Connectivity (JDBC): allows single signon access to OS/400 databases through ODBC.
  - Distributed Relational Database Architecture (DRDA): allows single signon access to OS/400 databases through ODBC.
  - QFileSrv.400
  - LDAP Server (the LDAP server supports Kerberos authentication only. EIM is not used during the authentication process)
- The following applications were enabled for EIM and/or Kerberos in V5R3:
  - Management Central for authentication between endpoint systems and the central system.
  - Windows Integration for user enrollment and for submitting network server commands.
  - HTTP Server for iSeries (powered by Apache) when using Microsoft's Internet Explorer 5.0 or higer. This support was also added to V5R2 via the HTTP group PTF.
  - The V5R3 enhancement of storing user certificates in LDAP servers, provides also the ability for OS/400 applications, such as the FTP server, to use EIM for lookup operation of a target association. This function only pertains to OS/400 applications using digital certificates for client authentication. It is not related to Kerberos at all.

Network Authentication Service (NAS)

Network Authentication Service (NAS)

- Kerberos service principal configuration wizard
  - New wizard in iSeries Navigator
  - Add service principals for
    - OS/400 Kerberos authentication
    - Directory Services (LDAP)
    - IBM HTTP Server for iSeries (powered by Apache)
    - iSeries Netserver interfaces



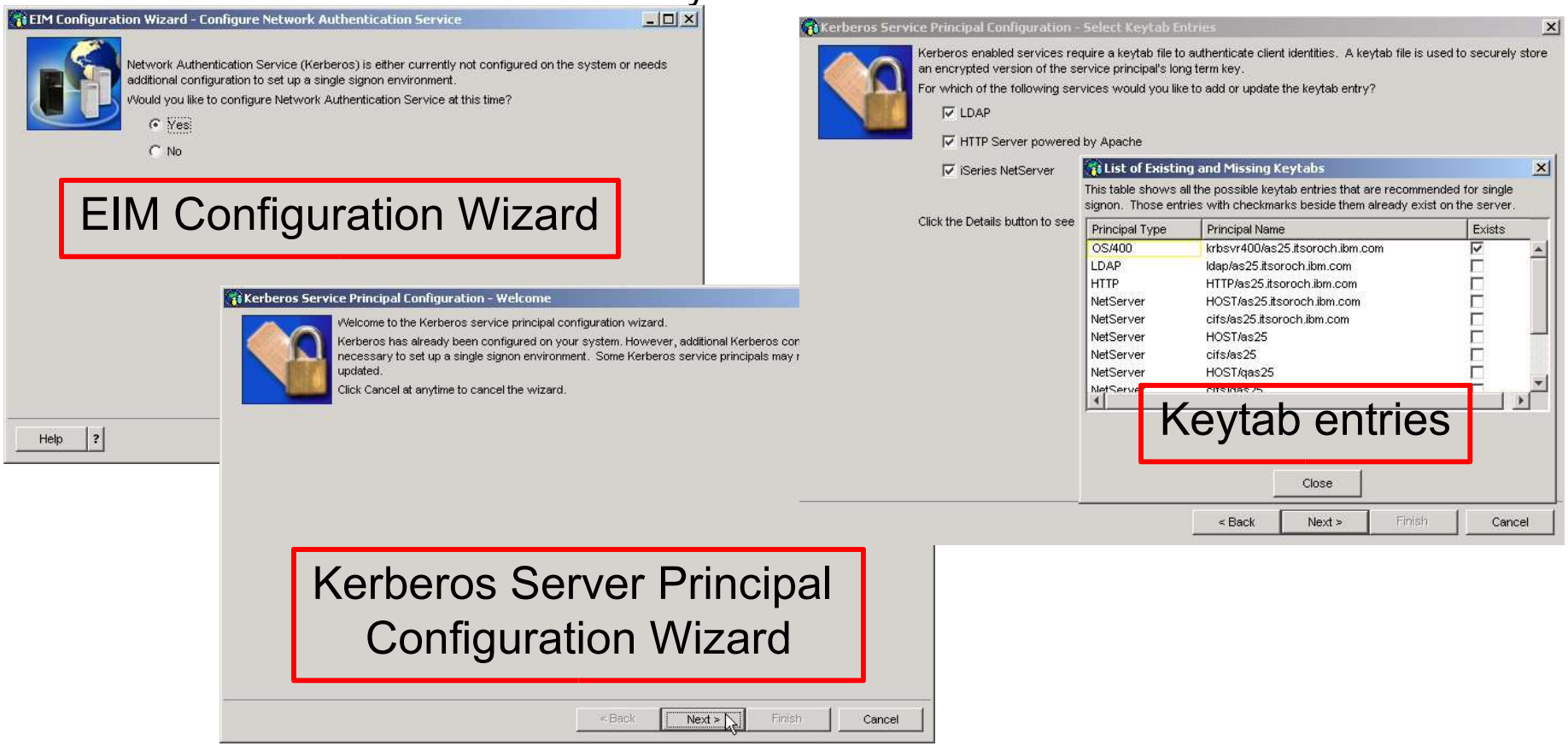
Notes: Network Authentication Service (NAS)

This new V5R3 wizard in iSeries Navigator allows administrators to add service principals for OS/400 Kerberos Authentication, Directory services (LDAP), IBM HTTP Server for iSeries or iSeries NetServer interfaces.

During Enterprise Identity Mapping (EIM) configuration, the EIM wizard will check if network authentication service is configured. If it is, the wizard will then check if keytab entries for any of these system interfaces are missing. The EIM wizard will then start the Kerberos service principal wizard, so that the administrator can add these services to the keytab file.

Network Authentication Service (NAS) - continued

- EIM configuration wizard checks if NAS is configured
  - Checks for missing keytab entries
  - New wizard is started to add keytab entries

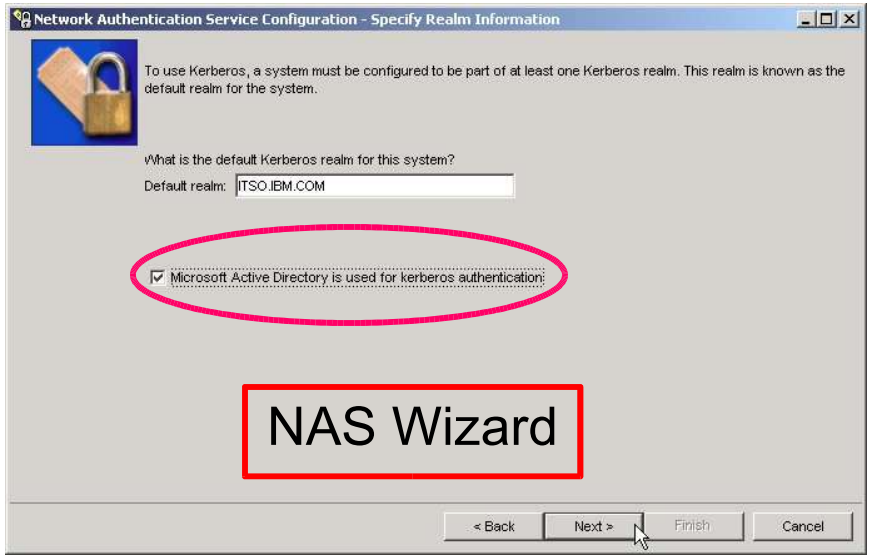


Notes: Network Authentication Service (NAS)

During Enterprise Identity Mapping (EIM) configuration, the EIM wizard will check if network authentication service is configured. If it is, the wizard will then check if keytab entries for any of these system interfaces are missing. The EIM wizard will then start the Kerberos service principal wizard, so that the administrator can add these services to the keytab file.

Network authentication service (NAS) - continued

- Improved host name resolution
  - Alert messages when host names from PC and iSeries do not match
- New interoperability tool with Microsoft Windows Active Directory
  - Batch file support to operate with iSeries server



Notes: Network Authentication Service (NAS)

Improved host name resolution

In a Kerberos environment, both the client and the server use some method of host name resolution to determine the host name for the system on which a particular application or service resides. If the iSeries and the PCs use a Domain Name System (DNS) server, it is important that they use the same DNS server to perform host name resolution or, if they use more than one DNS server, that the host names are the same on both DNS servers.

If your iSeries system or PC resolve host names locally (from a local host table or file) they might resolve a host name that is different than the corresponding host name recorded on the DNS server. This might cause network authentication service to fail.

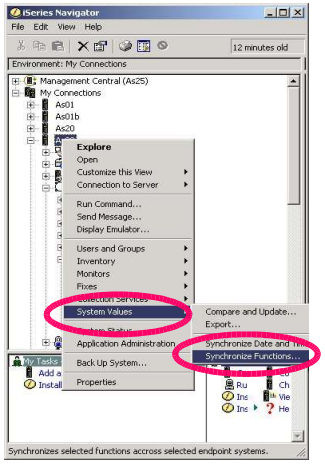
Within the network authentication service and Kerberos service principal configuration wizard, administrators will be provided with messages that alert them when host names resolved from a PC and the iSeries do not match. If host names do not resolve, administrators can optionally create multiple keytab entries for each of these host names.

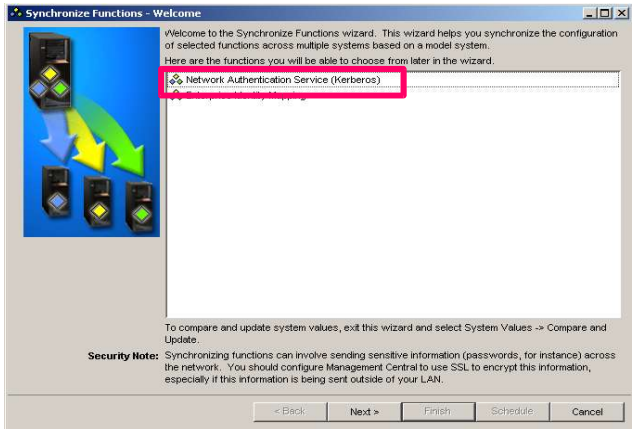
Interoperability with Microsoft Windows Active Directory

When running the NAS wizard and selecting the option that Microsoft Active Directory is used for authentication, a batch file will be created when finishing the wizard. This batch file will contain the necessary commands to set up a domain user account for a service and then map the Kerberos service principal to the corresponding account. The wizard prompts for a batch file name and location. It also allows an administrator to decide whether the service passwords are stored within the batch file. If you select not to store the passwords in the file, Windows will prompt you for the passwords when running the batch file on the Windows server.

Network authentication service (NAS) - continued

- Kerberos server support in V5R3 OS/400 PASE
  - Also known as KDC (Key Distribution Center)
- Support for IBM HTTP Server for iSeries (powered by Apache)
  - Keytab entries can be created for HTTP server
  - HTTP instances accept Kerberos tickets to authenticate users
- New Synchronize Functions Wizard in iSeries Navigator
  - Propagate configuration info from model system to endpoint systems





Notes: Network Authentication Service (NAS)

Kerberos server support in V5R3 of OS/400 (Key Distribution Center or KDC)

An administrator can now configure a Kerberos server in OS/400 Portable Application Solutions Environment (PASE). OS/400 PASE provides an integrated run-time environment for AIX applications. Please refer to the V5R3 Infocenter in order to configure the Kerberos server in PASE.

The following licensed programs are needed to run the Kerberos server on iSeries within a PASE environment:

- OS/400 Host Servers (5722-SS1 Option 12)
- OS/400 PASE (5722-SS1 Option 33)
- Qshell Interpreter (5722-SS1 Option 30)
- Cryptographic Access Provider (5722-AC3)
- iSeries Access for Windows (5722-XE1)

Kerberos support for IBM HTTP Server for iSeries (powered by Apache)

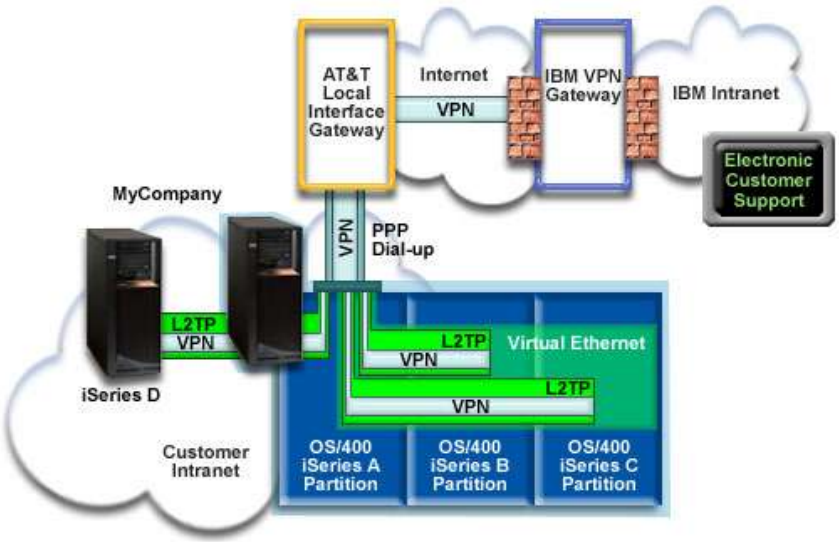
HTTP server for iSeries now supports Kerberos authentication. During configuration of network authentication service, administrators can optionally create keytab entries for HTTP server and configure their HTTP server instances to accept Kerberos tickets to authenticate users.

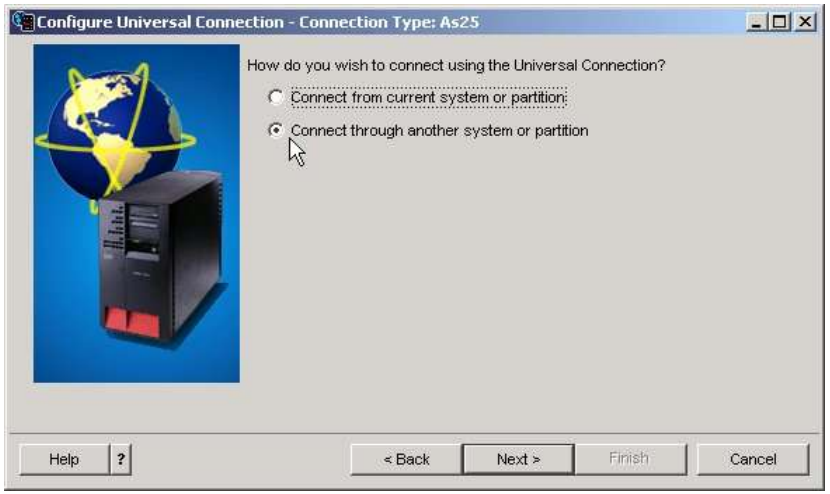
New Synchronize Functions Wizard

This new wizard in iSeries Navigator allows you to propagate a network authentication service configuration from a model system to multiple endpoint systems. Management Central is used to pass the NAS configuration info from the model system towards the endpoint system(s).

Universal Connection Wizard

- iSeries servers or partitions can access eCare services through another server's modem or Internet connectivity
- V5R3 connectivity options require:
  - Digital Certificate Manager
    - 5722-SS1 option 34
  - Cryptographic Access Provider
    - 5722-AC3
- V5R3 connectivity options are protected by a Virtual Private Network (VPN)





Notes: Universal Connection Wizard

In case you used the AT&T or Multi-hop connectivity options of the IBM Universal Connection in previous releases and you want to continue using them in V5R3, you will now will need Digital Certificate Manager (OS/400 option 34) and the Cryptographic Access Provider product (5722-AC3) installed.

Previously, you only needed those when the Universal Connection was used with a Virtual Private Network (VPN) through a customer–provided Internet Service Provider (ISP).

Starting with V5R3, all connectivity options are now protected by a VPN.

In V5R3, it is now possible for an iSeries server or partition to access IBM electronic customer support services, through another server's modem or Internet connectivity.

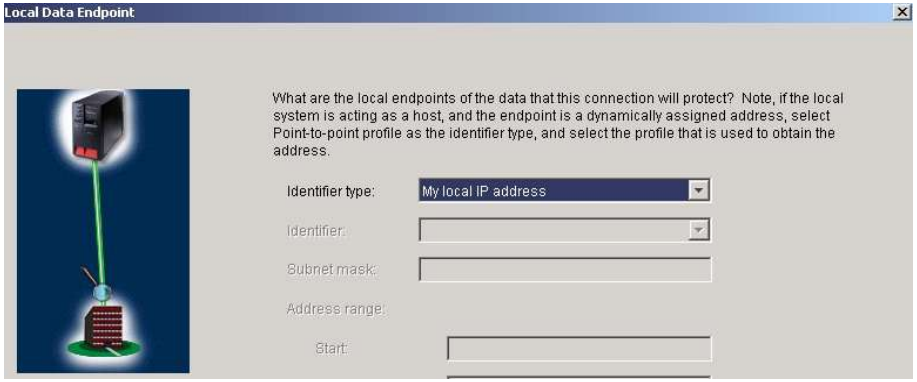
In our foil we have the following example to connect to IBM electronic customer support services,: the iSeries A partition uses a PPP connection through its local modem to an AT&T Local Interface Gateway (LIG). If iSeries B partition, iSeries C partition or iSeries D connects, a PPP connection is made through an L2TP tunnel using the remote modem on iSeries A partition to the AT&T LIG.

iSeries A partition acts as a connecting point for iSeries B partition, iSeries C partition as well as for iSeries D by using a L2TP terminator profile on iSeries A partition. All partitions in this example are running V5R3 of OS/400.

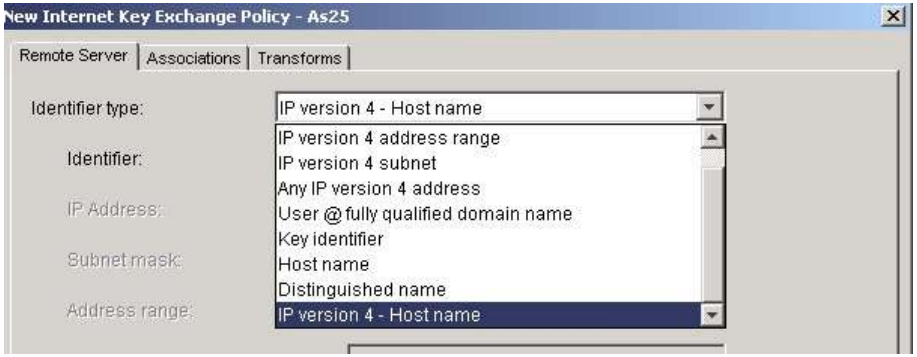
If running V5R3, a VPN is established through the AT&T LIG and the Internet to a VPN Gateway at IBM.

Virtual Private Networking

- There are 2 new identifier types
  - My Local IP address
    - This represents all local IP addresses on an initiator system
    - Does not require policy filters to be created
    - Solves local key server and data endpoint problem on multi-homed systems



  - IPv4 host name
    - Can be defined in the following places:
      - The remote key server identifier type in an Internet Key Exchange Policy
      - The remote address identifier in the connection's properties
      - The policy filter definition for a connection group's properties



Notes: Virtual Private Networking

Within V5R3, there are two new identifier types that can be selected when defining VPN key exchange policies and connection data endpoints. The identifier types include local IP address and IPv4 host name.

My local IP address

The identifier type, My Local IP Address, can be selected to define the local key server type for an Internet Key Exchange Policy or the local data endpoint in a connection definition.

When selected, VPN uses an available IPv4 address. VPN connections which use this identifier type must not use a policy filter.

The local system must be the initiator of the connection.

IPv4 host name

The identifier IPv4 host name can be selected to define a few different parameters:

- The remote key server identifier type in an Internet Key Exchange Policy
- The remote address identifier in the connection's properties
- The policy filter definition for a connection group's properties

The IPv4 host name resolves to the IP address of the host name specified as the identifier type.

Secure Sockets Layer

- GSKit 6B version of GSKit APIs
- System SSL default cipher list changes
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
- Existing applications using default cipher suite list are NOT impacted
- Applications using iSeries native SSL_C APIs for secure sockets
  - New include qsossl.h contains info previously in ssl.h
  - ssl.h remains available and points to qsossl.h

Notes: Secure Sockets Layer

The Global Secure ToolKit (GSKit) is a set of programmable interfaces that allow an application to be SSL enabled. It is part of OS/400 V5r3. Just like the SSL_ APIs, GSKit APIs allow you to access SSL and TLS functions from your socket application program (they are easier to program in than the previous SSL_APIs).

In the previous release, they were based on the GSKit 4D version, while starting with V5R3, they are based on the GSKit 6B version.

A description of these APIs can be found within the V5R3 Infocenter in the Socket Programming topic under Programming->Communications.

The System SSL default cipher suite list in V5R3 contains two Transport Layer Security (TLS) Version 1 Advanced Encryption Standard (AES) ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The AES ciphers are valid only with the TLS Version 1 protocol and when 5722-AC3 is installed.

In V5R1, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite was already supported but the SSL enabled application needed to be altered in order to allow using it.

Existing applications that use a default cipher list support will now support both cipher suites without any code change. Applications that use a configured cipher suite list instead, need to be changed though in order to use these new cypher suites.

If you still have an application written to the SSL_ C API, your source code should be updated to include qsossl.h rather than ssl.h. The new include qsossl.h contains the same prototypes and other information previously contained in ssl.h. The ssl.h will contain a pointer to qsossl.h.

New cryptographic APIs

- V5R3 OS/400 Cryptographic Services APIs
  - Data privacy
  - Data integrity
  - Authentication of communicating parties
  - Non-repudiation of messages
- Cryptographic Access Provider 128-bit for iSeries required
- PTFed back for V5R2
- #4806 PCI-X Cryptographic Co-processor
  - See V5R3 Hardware presentation for details

Notes: New cryptographic APIs

With V5R3, there is a set of new OS/400 Cryptographic Services APIs allowing you to ensure the following:

- Privacy of data
- Integrity of data
- Authentication of communicating parties
- Non-repudiation of messages

The Cryptograhic Services APIs include the following:

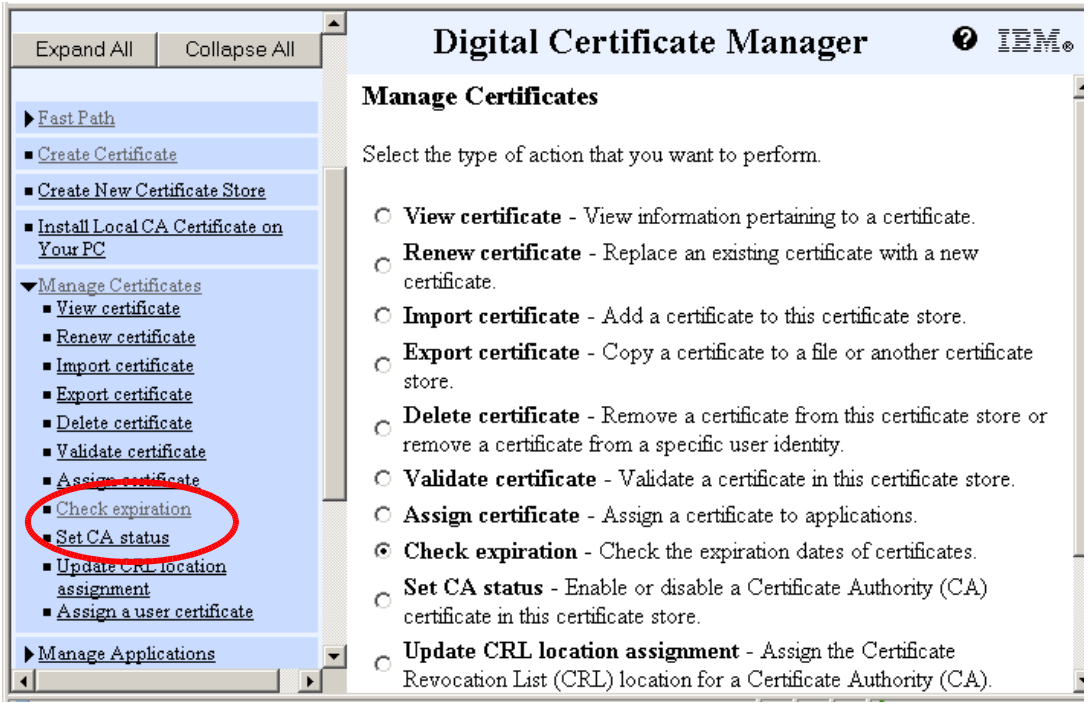
- Encryption and Decryption APIs
- Authentication APIs
- Key Generation APIs
- Pseudorandom Number Generation APIs
- Cryptographic Context APIs

In order to enable full cryptographic capabilities, you need to install 5722-AC3, Cryptographic Access Provider 128-bit for iSeries. The APIs perform cryptographic functions within OS/400 itself or on the 2058 Cryptographic Accelerator for iSeries. Several of these APIs above are made available for V5R2 with PTFs SI10060, SI10105 and MF31101. For more info related to Cryptographic APIs, please use the V5R3 Infocenter.

For info related to the #4806 PCI-X Cryptographic Co-processor, please see the V5R3 Hardware presentation.

Digital Certificate Manager – Expiration check

- New V5R3 DCM function allows you to view and manage certificates based on certificate expiration date
  - Client and server certificates
  - Object signing certificates
  - User certificates



Notes: Digital Certificate Manager – Expiration check

In V5R3, the Digital Certificate Manager (DCM) allows you to view and manage certificates based on certificate expiration date.

You can check certificate expiration for server or client certificates and object signing certificates on the local system.

You can also check user certificate expiration: either for a specific user profile, for all user certificates on the system, or even for all user certificates within an enterprise when EIM is configured on the system.

For a complete details

Digital Certificate Manager – LDAP location

- In V5R3 the administrator can store user certificates in the LDAP directory
- Prior to V5R3 user certificates stored with OS/400 user profile
- New LDAP location option available in Digital Certificate Manager
- Requires EIM to be configured as well as target association for user
- User certificate is added to the LDAP directory and EIM source association is created for EIM identifier

Notes: Digital Certificate Manager – LDAP location

Prior to V5R3, Digital Certificate Manager (DCM) was storing the user certificates issued by the Local Certificate Authority (CA) with the OS/400 user profile signed on to DCM.

In V5R3, it is possible to configure DCM to store user certificates in an LDAP directory. In order to be able to do this, the system must be configured to participate in Enterprise Identity Mapping (EIM).

The following tasks need to be performed in order to be able to store user certificates in an LDAP directory:

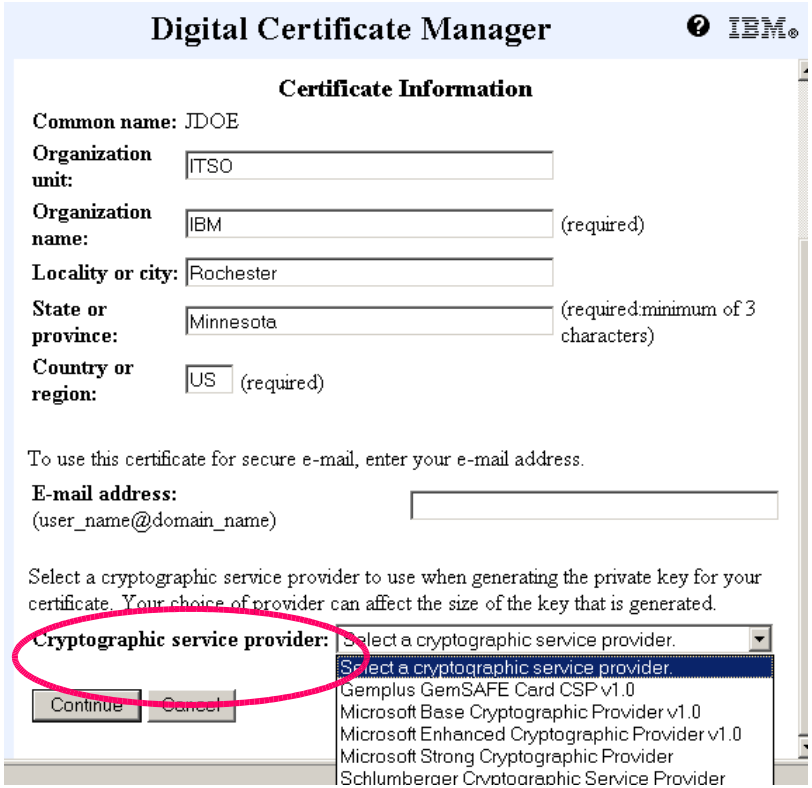
- Use the Enterprise Identity Mapping wizard to set up EIM
- Create a new X.509 system registry within the iSeries Navigator EIM domain management
- Register the X.509 registry with the EIM domain
- Add an EIM identifier and a target association for the OS/400 user profile
- Set up and enable the LDAP location in DCM
- Have the users sign on to DCM to create the user certificates.

An entry will be created in the LDAP directory with a common name of the EIM identifier and the certificate will be stored in the user certificate attribute. A source association for the user certificate will be created for the corresponding EIM identifier.

OS/400 applications can now use the EIM certificate to user profile mapping for authentication purposes. So, if you are using the FTP server with certificate-based client authentication, the FTP server looks up the target user profile based on the user certificate that is being presented.

Digital Certificate Manager – Creating user certificates

- New cryptographic service provider selection list when creating user certificates
- Supported by Microsoft Internet Explorer browsers only
- Allows private/public key pair strength selection



Notes: DCM – creating user certificates

In V5R3, a new option list is added, allowing the user to select a cryptographic service provider when creating a user certificate.

A cryptographic service provider specifies the encryption and hashing algorithms as well as supported key lengths that are available for cryptographic operations. When a user certificate is created in DCM, the service provider defines the key length of the public/private key pair that is being created for a certificate signing request (CSR). As user certificate's key pair is generated on the user's workstation.

The list of cryptographic service providers is only available for Internet Explorer browsers. The items that are available to select from in the list depend on the installed cryptographic service providers in Windows.

We recommend selecting the strongest providers available: the longer the RSA (Rivest, Shamir and Adleman – public key cryptography algorithm) keys are, the better is the protection strength.

IBM eServer i5/OS (OS/400) Security enhancements

- IFS Antivirus scanning
- Object integrity enhancement
- Audit data enhancement
- Changed security tools CL command authorities
- Miscellaneous OS/400
- Application administration

IFS Antivirus Scanning Enablement

- Hosting the virus scanner on the system (iSeries) where the data is stored simplifies management
- V5R3 Exit points
  - QIBM_QP0L_SCAN_OPEN
  - QIBM_QP0L_SCAN_CLOSE

***STMF files in *TYPE2 directories**

- Two new general security system values for IFS virus scanning using the V5R3 exit points
  - QSCANFS (*ROOT**OPNUD** or *NONE).
    - Specifies the integrated file systems in which objects will be scanned
    - IFS *TYPE2 only file systems /root, **QOpenSys** and **UDFS**
  - QSCANFSCTL
    - If *ROOTOPNUD, scan file systems control values: ***NONE**, ***FSVRONLY** ***ERRFAIL**, ***NOWRTUPG**, ***USEOCOATR**, ***NOFAILCLO**, ***NOPOSTRST**, ...

- New IFS scan object attribute for stream (*STMF) file and directory (*DIR) objects
  - *STMF: *SCAN (yes/no/chgonly)
  - *DIR: *CRTOBJSCAN (yes/no/chgonly)

- Enablement for third-party tools to scan files in file systems
  - Example: **StandGuard™ Anti-Virus** from Bytware, Inc

Notes: IFS Antivirus Scanning

The iSeries operating system cannot become infected in the same way that Windows operating systems can. To date there have been no viruses discovered that can hide within an OS/400 program object or file object and affect the iSeries when used. Since OS/400 will not run a dot execute (.exc) file, any virus contained in such a file would not affect the iSeries.

However, the iSeries is well known as a file server, especially with its powerful Integrated File System (IFS) capabilities. Therefore the iSeries could serve as a storage place for a virus that in turn could be transferred to an operating system that could be victimized by that virus.

To address this situation Bytware offers anti-virus scan programs for files within the IFS. New in V5R3 is the enablement structure for a more automatic scanning and detection of viruses within the IFS.

The enablement itself does not scan, detect or clean viruses, but instead provides the necessary enhancements to allow a third-party native anti-virus solution to scan upon open and close (On-access). The enablement feature, which is shipped with a default of "ON," is designed to tie into a native anti-virus solution to scan for, detect , and clean viruses. The addition of a native anti-virus solution is required in order to use this new functionality of V5R3.

This can be set up using either new OS/400 V5R3 command interfaces or new options using the iSeries Navigator interface, discussed on this and the following slides.

Two new exit programs options are available in V5R3:

- QIBM_QP0L_SCAN_OPEN: Integrated File System Scan on Open Exit Program For this exit point, the integrated file system scan on open exit program is called to do scan processing when an integrated file system object is opened under certain conditions.
- QIBM_QP0L_SCAN_CLOSE: Integrated File System Scan on Close Exit Program For this exit point, the integrated file system scan on close exit program is called to do scan processing when an integrated file system object is closed under certain conditions.

Note, there is currently a vendor product available from Bytware, called StandGuard Antivirus. It runs on OS/400 V5R1 and higher and scans IFS files for viruses and e-mail processed via the mail server framework. There are 5250 commands and menus for the configuration and there is an iSeries Navigator plug-in to set up the product.

This slide introduces the new with V5R3 exit program registrations, system values, and object attributes that affect what can be scanned and when.

Notes: IFS Antivirus Scanning -2

Hosting the virus scanner on the system (iSeries) where the data is stored makes scanning easier and less complex to manage.

Following slides give examples and discuss the Bytware StandGuard Antivirus product.

In V5R3 QSCANFS and QSCANFSCTL are two new system values that enable programs to be called from two new registered exit program entries. Registered programs are intended to scan the files in the integrated file system and "return the results" to the system. Once a virus is detected, the appropriate action can be taken in order to eliminate the virus.

Note, do not scan the IFS using iSeries NetServer. Mapping a drive with all object authority exposes the system to virus attack by a PC virus. Consider this could:

- Use up network resources
- Move data across the network in the "clear"
- Scanner can go into infinite loops

QSCANFS system value: The QSCANFS system value allows you to specify the integrated file system in which objects will be scanned.

The value *ROOTOPNUD (default) means that objects of type *STMF in *TYPE2 directories in /root, QOpenSys and User Defined File System (UDFS) are to be scanned. The file system the object is in must be fully converted to type 2 to do so ,You can use the CVTDIR OPTION(*CHECK) command to determine if the file system has fully converted. If Not the file system will show as *PENDINGCONVERSION while it is waiting for this conversion.

The Integrated file system scanning is configured by registering exit programs to the integrated file system scan-related exit points. These exit programs entries are QIBM_QP0L_SCAN_OPEN (Integrated File System Scan on Open Exit Program) and QIBM_QP0L_SCAN_CLOSE (Integrated File System Scan on Close Exit Program).

Note that only objects with IFS *TYPE2 directories are scanned.

QSCANFSCTL system value: The system value QSCANFSCTL controls the integrated file system scanning behavior and properties for file open and updates changes) if QSCANFS is set to *ROOTOPNUD. *NOPOSTRST (explained later) applies anytime the IFS object is restored.

To limit the performance impact of virus scanning, OS/400 will only call the exit program (scanning software) to scan files for viruses, when a file has changed or when the virus definition file has been updated.

Notes: IFS Antivirus Scanning - 3

Valid **QSCANFSCTL** parameter values include:

- **Default (*NONE specified)**: This indicates that the system uses the following scanning options when calling the registered exit programs:
  - Perform write access upgrades
  - Fail close request if scan fails during close
  - Scan on next access after object has been restored
- **Scan accesses through file servers only (*FSVRONLY specified):** By selecting this option, only accesses from a file server to the iSeries server are scanned. Accesses through the Network File System (NFS) are scanned as well as other file server methods. However, native or direct connections to the iSeries server are not scanned. If this option is not selected, all accesses will be scanned no matter if you connect directly to the iSeries or through a file server.

Note, do not scan the IFS using iSeries NetServer. Mapping a drive with all object authority exposes the system to virus attack by a PC virus!

  - Uses up network resources
  - Moves data across network in the "clear"
  - Scanners can go into infinite loops

- **Fail request if exit program fails (*ERRFAIL specified):** By selecting this option, you are specifying to fail the request or operation which triggered the call to the exit program, if there are errors when the exit program is called. Possible errors may be that the program is not found or the program is not coded properly to handle the exit program request. If this happens, the requested operation receives an indication that the object failed a scan. If this option is not selected, the system will skip the failing exit program and treat the object as if it was not scanned by this exit program.
- **Perform write access upgrades (*NOWRTUPG not specified):** By selecting this option (*NOWRTUPG not specified), you are specifying to allow the iSeries system to upgrade the access for the scan descriptor passed to the exit program to include write access, if possible. Use this option if you want the exit program to be able to fix or modify objects even though they were originally opened with read-only access. If this option is not selected, the system will not upgrade the access to include write access.

Notes: IFS Antivirus Scanning - 4

Valid **QSCANFSCTL** parameter values continued

- **Use "only when objects have changed" attribute to control scan (*USEOCOATR specified):** By selecting this option, the system will use the specification of the 'object change only' attribute to only scan the object if it has been modified (not also because scan software has indicated an update). If this is not specified, this 'object change only' attribute will not be used, and the object will be scanned after it is modified and when scan software indicates an update.
- **Fail close request if scan fails during close (*NOFAILCLO not specified):** When this option is selected (*NOFAILCLO not specified), the system will fail the close request if an object failed a scan during close processing. This option only applies to close requests.

If this option is not selected (*NOFAILCLO specified), the system will not fail the close request if an object failed a scan even if the "Fail request if exit program fails option" is selected. For example, if the Fail request if exit program fails option is selected and this option is not selected, the system will not send a failure indication even though an object failed a scan during close processing. However, the object will be marked as failing a scan.

- **Scan on next access after object has been restored (*NOPOSTRST not specified):** By selecting this option (*NOPOSTRST not specified), objects will be scanned at least once after being restored no matter what its object scan attribute is. If the object scan attribute is that 'the object will not be scanned,' the object will be scanned once after being restored. If the object scan attribute is that 'the object will only be scanned if it has been modified since the last time it was scanned,' the object will be scanned after being restored because the restore will be treated as a modification to the object.

If this option is not selected (*NOPOSTRST specified), objects will not be scanned just because they are restored. Scanning depends on the object's scanning attribute. In general, it is good practice to scan restored objects at least once. However, you may not select this option if you know that the objects being restored were scanned before they were saved or they came from a trusted source.

Notes: IFS Antivirus Scanning - 5

There are two new object attributes. *CRTOBJSCAN applies to a directory object and *SCAN applies to a byte stream file object . They can be set either through the CHGATR command, the QpOISetAttr API, or the iSeries Navigator interface. These new attributes are defined as follows:

- Byte Stream File: *SCAN (yes/no/change only) states when the stream file will be scanned.
- Directory: *CRTOBJSCAN (yes/no/change only) states which *SCAN attribute will be given a stream file when a stream file is created into that directory.

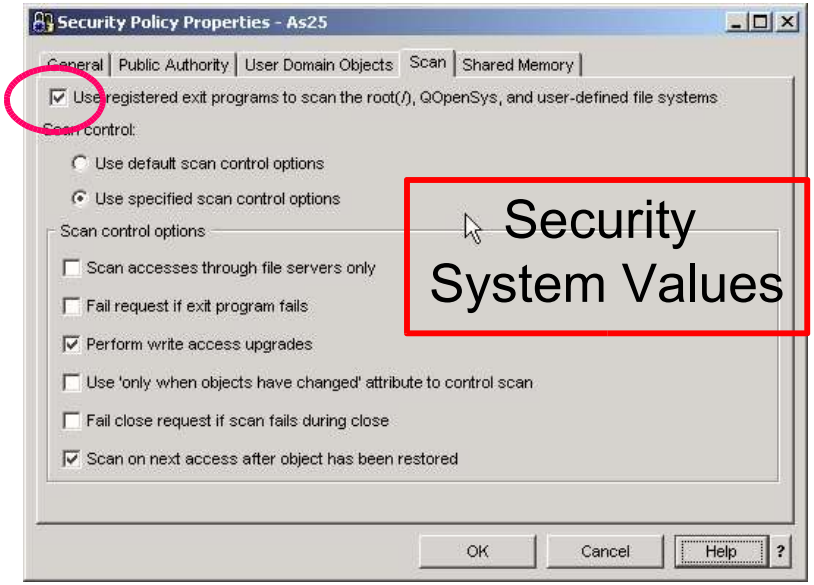
Important

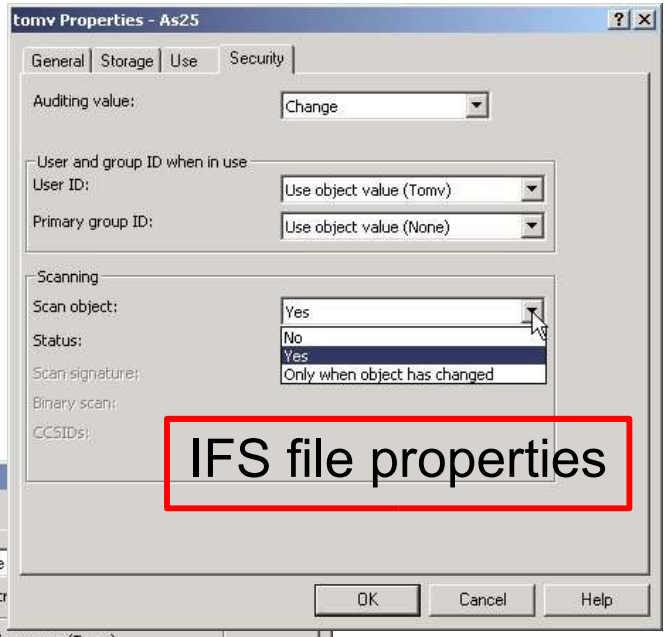
The file system the object is in must be completely converted (all objects within the directory) to a *TYPE 2. You can use the Convert Directory (CVTDIR) command's OPTION(*CHECK) to determine if the file system has been completely converted. In V5R3, shortly after the initial IPL, the system starts a background task that will find any *TYPE1 to *TYPE2. Therefore it may appear that as if a file is in an *TYPE2 directory, but the file system may not have yet completed this conversion. The SCAN status for an object will show as *PENDING/CONVERSION if it is awaiting conversion.

The object attributes can be specified for either *TYPE1 (before conversion) or *TYPE2 directory file systems. The actual scanning, if enabled, only occurs if the object exists in a file system that has been completely converted to *TYPE2.

The next slides includes an IFS object with the new scan Properties information shown.

IFS Antivirus scanning – iSeries Navigator





iSeries. mySeries.

Notes: IFS Antivirus Scanning – iSeries Navigator

The left window on this foil shows the iSeries Navigator interface for the QSCANFS and the QSCANFSCTL system values. They can be found on the Scan tab of the Security Policy within the Security container.

The **Perform write access upgrades** in the Scan control options allow the iSeries system to upgrade the access for the scan descriptor passed to the exit program to include write access, if possible. You should use this option if you want the exit program to be able to fix or modify objects even though they were originally opened with read-only access. If this option is not selected, the system will not upgrade the access to include write access.

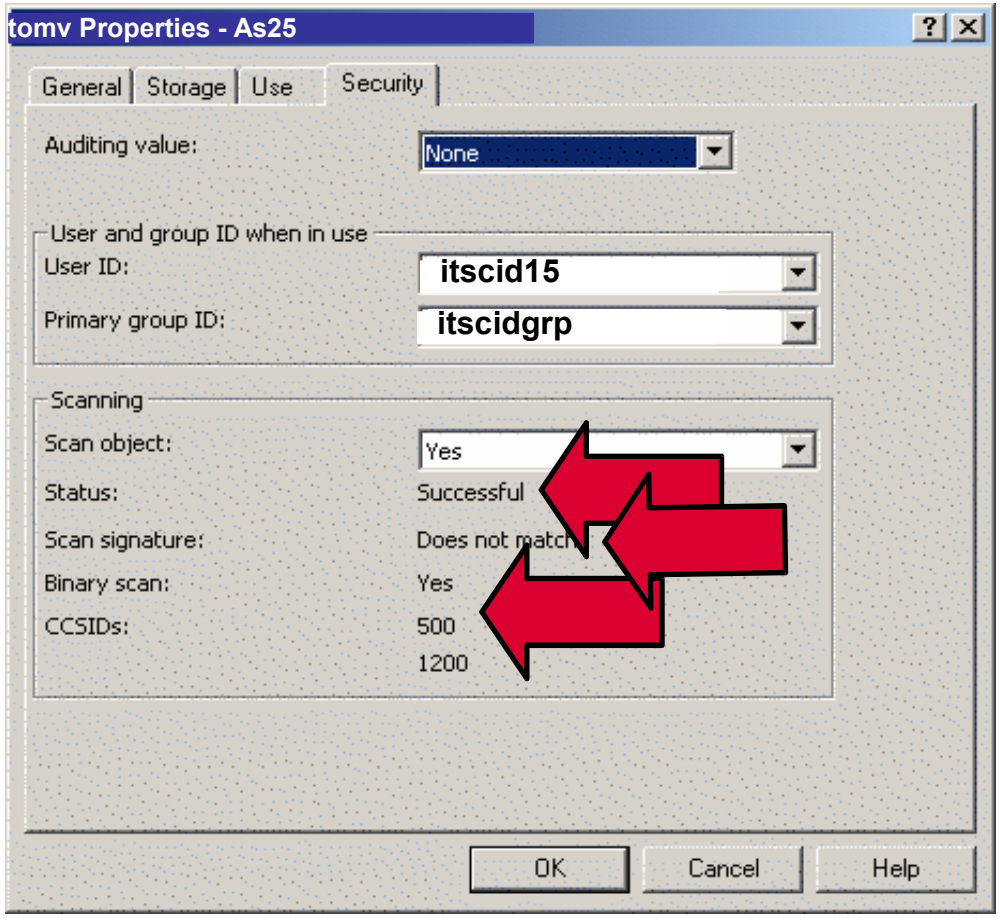
Within iSeries Navigator, you can right-click on the *TYPE2 directory tomv (IFS folder properties window shown, lowest window) object where you have the Scanning option on the Security tab on the Properties page. This corresponds with the *CRTOBJSCAN attribute. When you right-click on a stream file object within that *TYPE2 directory, you have the Scan object parameter on the Security tab on the Properties page as shown in the upper right window. This corresponds with the *SCAN attribute.

The next window shows the properties of a file after an object has been scanned.

File properties: scan results example

Scanning Properties and Status

- Security tab
- Object scanned
  - In binary
  - Successfully
  - In CCSIDs 500 and 1200
- Scan signature “does not match”
  - Object needs to be rescanned
  - Indicates a scanning update such as new virus definitions loaded
- See InfoCenter at Files and file systems -> Integrated file system -> Concepts -> Scanning support



iSeries. mySeries.

Object integrity enhancements

- New QydoCheckSystem API
  - OS/400 system integrity verification
  - Verify integrity of the code checking function
- CHKOBJITG command
  - New SCANFS (*STATUS | *YES | *NO) parameter

Notes: Object integrity enhancements

Starting with V5R2 of OS/400, a code checking function can be used to verify the integrity of signed objects on your system, including all operating system code that IBM ships and signs for your iSeries system.

With V5R3, you can use the new QydoCheckSystem API to verify the integrity of the code checking function itself, as well as key operating system objects. You need *AUDIT special authority. When you run the API it checks key system objects, including the *pgm and *svrpgm and selected *CMD objects in the QSYS library.

The CHKOBJITG command checks the objects owned by the specified user profile, the objects that match the specified path name, or all objects on the system to determine if any objects have integrity violations.

With V5R3 a new parameter Scan file systems (SCANFS) is added: it specifies whether objects in the integrated file systems identified by the QSCANFS system value should be scanned or if their existing scan status should be returned. This was explained earlier on a previous slide.

The OS/400 V5R3 support is an enablement function – no system function to do the scanning is provided. Any programmer could perform the scanning functions. One example of such a scanning program is the one provided by BytWare, StandGuard ™ Anti-Virus. We discuss this product on the following slides.

StandGuard Anti-Virus for iSeries, from Bytware, Inc.

- Native "green-screen" and iSeries Navigator graphical interfaces
- Can be scheduled to run using iSeries job schedulers
- Powered by McAfee iSeries native scanning engine
- Automatic download of virus definitions direct from McAfee
- New V5R3 version takes advantage of new OS/400 V5R3 scan exit points
  - Now provides "On-Access" scanning (open, change, save)
  - Uses the QIBM_QP0L_SCAN_OPEN, QIBM_QP0L_SCAN_CLOSE exit points
  - Called by OS/400 only "as needed" (On-Demand)
  - Updates the file 'Scan status' flag to indicate if the file is good or infected
  - OS/400 prevents infected files from being opened
  - New V5R3 scan status flag eliminates need to rescan files that do not need to be scanned again
  - Full system scan substantially faster on V5R3 if virus definition files have not changed

Notes: StandGuard Anti-Virus for iSeries, from Bytware

The StandGuard Anti-Virus for iSeries product has been available since V5R1. It can be and continues in V5R3 to be able to be scheduled to run automatically using the OS/400 job scheduler, the Advanced Job Scheduler (5722-JS1), or any other third party job scheduling product.

The new V5R3 version contains enhancements, that include:

- Uses the same virus definitions as McAfee PC versions, so there is no 'lag' time for OS400 support
- Can also configure product to get files from a network path, in case customer already has McAfee .DAT files somewhere on the network
- Can be called by OS/400 exit points (listed on the slide) when file is opened and closed as specified via V5R3 system values and iSeries Navigator file interfaces.

Uses the same virus definitions as McAfee PC versions, which means there is no 'lag' time for OS400 support when this product is enhanced. You can also configure the product to get files from a network path, in case the customer already has McAfee .DAT files somewhere on the network.

In addition to being able to be scheduled via the OS400 job schedule, the scan can be performed when the IFS file is opened or changed ("on access").

Under a heavy network load it is strongly recommended to restrict access to netserver while the scan is running

StandGuard Anti-Virus for V5R3 will be available for OS/400 V5R3 upon IBM's announcement of general availability. Customers with V5R3 systems can request full-featured trials by contacting Bytware directly at http://www.bytware.com or call 775-851-2900.

Note: If you are using a PC to scan the IFS, most companies do their scans once a week or only 'as needed' because it takes so long and interferes with normal operations. Note, under a heavy network load, we strongly recommend restricting access to NetServer while scans are running.

Audit data enhancement

- New QAUDLVL2 system value
  - Extends possible number of auditing values being specified
  - Can be used in conjunction with QAUDLVL system value
    - Specifying *AUDLVL2 in QAUDLVL system value
- *NETCMN and *SECURITY auditing values split up in smaller units
  - More granularity instead of all or nothing
  - Audit journals filled up with entries users did not need

Notes: Audit data enhancement

The system value QAUDLVL could only store 16 auditing values prior to V5R3.

By introducing new auditing values, a new system value QAUDLVL2 is added: it can contain up to 99 auditing values.

It may be used in conjunction with the QAUDLVL value to store all available auditing values if necessary.

In case you specify *AUDLVL2 in system value QAUDLVL, you end up adding the values in QAUDLVL and QAUDLVL2 for auditing reasons. You can also use *AUDLVL2 in the QAUDLVL system value and then specify the necessary auditing values in system value QAUDLVL2.

The security auditing in V5R3 is updated with more granular auditing controls to let the user be more specific in what they audit and to help reduce the flooding of audit journals.

The networking and security auditing values have been split up in smaller categories:

*NETBAS, *NETCLU, *NETFAIL, *NETSCK

*SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY, *SECVLDL

If you still want to log all information of networking or security event, you can still specify the existing *NETCMN and *SECURITY values.

It will now be possible to better control the amount of data that is being logged and journaled by using the more granular level of auditing.

Changed security tools CL command authorities

- Prior to V5R3, these commands are
  - Shipped with public authority *EXCLUDE
  - Requiring *ALLOBJ special authority
- Starting with V5R3, the commands are
  - Shipped with public authority *USE
  - Require *AUDIT special authority
  - Require *ALLOBJ and any other required special authority

DSPSECAUD	Display Security Auditing
PRTADPOBJ	Print Adopting Objects
DSPAUDJRNE	Display Audit Journal Entries
PRTPVTAUT	Print Private Authorities
PRTPUBAUT	Print Publicly Auth Objects
PRTCMNSEC	Print Communications Security
PRTJOBDAUT	Print JOBD Authority
PRTQAUT	Print Queue Authority
PRTSBSDAUT	Print Subsystem Description
PRTSYSSECA	Print System Security Attribute
PRTTRGPGM	Print Trigger Programs
PRTUSROBJ	Print User Objects
PRTUSRPRF	Print User Profile

Notes: Changed security tools CL command authorities

Prior to V5R3, the following commands required *ALLOBJ special authority.

They were shipped with *EXCLUDE public authority.

Starting in V5R3, the commands are shipped with *USE public authority.

In V5R3, a user that only has *AUDIT special authority (as well as users who have *ALLOBJ and any other required special authorities) now can run the commands shown on the slide.

Miscellaneous OS/400

- OS/400 message handling changes
  - The active user profile is stored with each message
  - Can be different from the user in the qualified job name
- New user profile parameter fields
  - LCLPWDMGT parameter
    - specifies whether user profile password should be managed locally
  - EIMASSOC parameter
    - specifies whether EIM association should be added to EIM identifier for the user
    - you can also specify whether or not the EIM identifier should be created
- Authorization changes
  - Default value for AUT parameter on several CRT commands (LIN,CTL,DEV)
    - Changed from *LIBCRTAUT to *CHANGE
    - Solves problem with public authority of automatically created configuration objects

Notes: Miscellaneous OS/400

Starting with V5R3, the active user profile is being stored with each message. The active user (or current user) profile is the user profile that the job is doing work for. It can be different from the user name in the qualified job name if the job had swapped to run under another user profile. This is being shown as the 'From' user on the DSPMSG or WRKMSG additional message information screen.

New user profile parameter fields

- The LCLPWDMGT (Local password management) parameter specifies whether the user profile password should be managed locally. If you do not want to manage the password locally, the password value is still sent to other IBM products that do password synchronization (for example: iSeries Integration for Windows Server). By specifying *NO, the local password is set to *NONE and the user is not able to sign on to the system directly, nor is he able to use the CHGPWD command to change its own password. This value should be used if the user only needs to access the iSeries through some other platform, such as Windows.
- The EIMASSOC (EIM association) parameter allows you to define EIM identifier associations for the specified user profile for the local registry. To use this parameter, you specify the EIM identifier, an action option for the association, the type of identifier association, and whether to create the specified EIM identifier if it does not already exist.

The QCRTAUT system value provides the default public authority granted when new objects are created that refer to this system value in their command's authority AUT parameter or via the library default create authority. The default value for the QCRTAUT system value is *CHANGE. This may introduce a higher authority level to new objects than actually needed. However, prior to V5R3, when changing this system value to *USE or *EXCLUDE caused problems for some objects, such as automatically created device descriptions. In V5R3, the default value for the AUT parameter has changed from *LIBCRTAUT to *CHANGE on several CRT commands for line, controller and device description. This solves the problem with public authority of automatically created configuration objects we had prior to V5R3.

Application administration

- iSeries Navigator Application Administration functions available also on new CL command support
  - WRKFCNUSG (Work with Function Usage)
  - CHGFCNUSG (Change Function Usage)
  - DSPFCNUSG (Display Function Usage)
  - Consider writing a CL program
    - Distribution to other systems across the network is supported

Notes: Application administration

The Application Administration interface in iSeries Navigator provides the administrator with an interface to manage access to iSeries Access for Windows, iSeries Navigator and OS/400 and TCP/IP applications.

Prior to V5R3, the only way to define access to these applications was through the graphical Application Administration interface.

With V5R3, new CL commands Display Function Usage (DSPFCNUSG), Work with Function Usage (WRKFCNUSG) and Change Function Usage (CHGFCNUSG) are available to manage access through the 5250 command line interface. On one system, the administrator can now write a CL program that contains all access policies and restrictions. Afterwards, he can distribute the program to other systems within the network.

Application security enhancements

- API changes

Additional information

- iSeries Information Center at http://publib.boulder.ibm.com/pubs/html/as400/infocenter.htm
- V5R3 iSeries Security Reference, SC41-5302-07