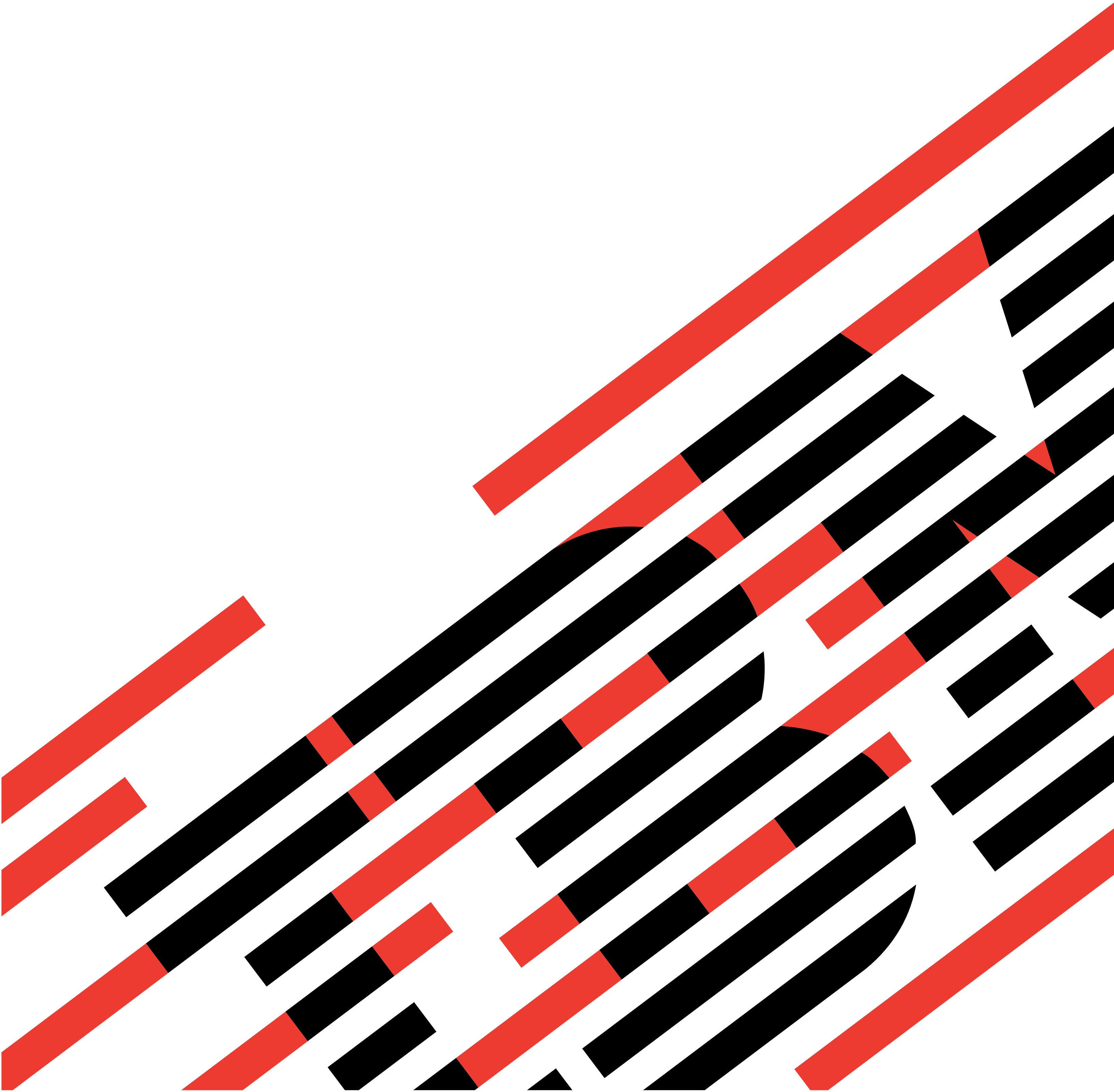
IBM

eserver

iSeries

Network authentication service



iSeries

Network authentication service

Contents

Network authentication service 1
What's new for V5R2 2
Print this topic 4
How does network authentication service work?. 4
Network authentication service terminology 7
Network authentication service protocols 9
Network authentication service scenarios. 10
Scenario: Configure network authentication service with existing KDC 12
Configuration details 15
Scenario: Enable single sign-on 18
Configuration details 25
Plan network authentication service. 26
Configure network authentication service 26
Define iSeries to the key distribution center 27
Create a home directory 28
Verify TCP/IP domain information 28
Test network authentication service configuration 28
Manage network authentication service 29
Synchronize system times 30
Add realms. 31
Delete realms 31
Add a key distribution center to a realm 31
Add password server 32
Create a trust relationship between realms 32
Change host resolution 32
Add encryption settings 33
Obtain or renew ticket granting tickets 33
kinit 35
Display credentials cache or keytab file 36
klist 38
Manage keytab files 38
keytab 39
Change Kerberos passwords 40
kpasswd. 41
Delete expired credentials cache files 42
kdestroy 43
Manage Kerberos service entries in LDAP directories 44
ksetup 46
Troubleshoot network authentication service 46
Network authentication service errors and recovery 47
Application connection problems and recovery. 48
Related information. 50
Special terms and conditions 51

Network authentication service

Network authentication service allows the iSeries and several iSeries services, such as iSeries Access for Windows, to use a Kerberos ticket as an optional replacement for a user name and password for authenticating a user. Kerberos protocol, developed by Massachusetts Institute of Technology, allows a principal (a user or service) to prove its identity to another service within an insecure network. Authentication of principals is completed through a centralized server called a key distribution center (KDC). The KDC authenticates a user with a Kerberos ticket. These tickets prove the principal's identity to other services in a network. After a principal is authenticated by these tickets, they can exchange encrypted data with a target service. Network authentication service verifies the identity of a user or service in a network. Applications can securely authenticate a user and securely pass on his or her identity to other services on the network. Once a user is known, separate functions are needed to verify the user's authorization to use the network resources. Network authentication service implements the following specifications:

- Kerberos Version 5 protocol Request for Comment (RFC) 1510
- Many of the de facto standard Kerberos protocol APIs prevalent in the industry today
- Generic Security Service (GSS) APIs as defined by RFCs 1509, 1964, and 2743

Network authentication service on the iSeries interoperates with authentication, delegation,and data confidentiality services compliant with these RFCs, such as Microsoft's Windows 2000 Security Service Provider Interface (SSPI) APIs.

In addition, network authentication service can be used with Enterprise Identity Mapping (EIM) to enable a single sign-on environment. Single sign-on benefits users, administrators, and application developers by enabling an easier password management system across multiple platforms without the need to change underlying security policies. The following articles provide details on single sign-on enablement by using network authentication service and Enterprise Identity Mapping (EIM):

Single sign-on enablement
This article provides conceptual information on the benefits of single sign-on and an overview of how network authentication service and Enterprise Identity Mapping (EIM) work together to create a single sign-on environment.

Scenario: Single sign-on enablement
This article provides an example of how the administrator of MyCo's Order Receiving Department enabled a single sign-on environment. The administrator wants user to be authenticated to iSeries applications by using their Windows (R) domain ID and password. Step-by-step instructions are included to show how MyCo's administrator configured network authentication service and EIM to enable single sign-on.

This discussion of network authentication service includes the following topics:

What's new for V5R2
This topic describes and links to more information on new function for network authentication service for this release.

Print this topic
This topic provides instructions to download and print a PDF version of this information.

How does network authentication service work?
This topic provides an overview on how network authentication service works within a network that uses the Kerberos protocol to authenticate users.

Network authentication service terminology
This topic defines terminology that is related to network authentication services.

Network authentication service protocols
This topic provides basic discussions of the Kerberos protocol and Generic Security Services (GSS) APIs. Links are provided to RFCs and other related information.

Network authentication service scenarios
This topic describes some different business scenarios in which network authentication service is implemented.

Plan network authentication service
This topic describes what you need to do prior to working with network authentication service.

Configure network authentication service
This topic describes how to configure network authentication service in iSeries Navigator.

Manage network authentication service
This topic describes tasks that administrators and users can use to manage network authentication service.

Troubleshoot network authentication service
This topic describes messages and problem resolution for network authentication service and related applications.

Related information
This topic describes and provides links to other topics related to Kerberos protocol and Generic Security Services (GSS) APIs.

Legal information
This topic provides important legal information that deals with the use of the Kerberos protocol and its associated APIs.

«

What’s new for V5R2

» Network authentication service allows the iSeries to participate in a network that uses Kerberos protocol to authenticate users on the network.

Network authentication service in iSeries Navigator
The network authentication service wizard provides easy configuration of an iSeries to participate in a Kerberos network. The wizard allows you to configure the iSeries to participate in a Kerberos realm. Thus using the Kerberos protocol, tickets can then be passed to services on a user's behalf, authenticating him or her to resources on the network. See these topics to complete the configuration:

- Network authentication service scenarios
  Provides brief descriptions of two customer situations that use network authentication service.
-
- Configure network authentication service
  Provides an overview of all the steps that are needed to configure network authentication service.
-
- Manage network authentication service
  Provides an overview of all the tasks that you can complete using iSeries Navigator.

Support for new Qshell command
Users can request and work with tickets with Qshell commands. This release, the **kpasswd** command has been added to allow users to change their passwords on the key distribution center.

- Change Kerberos passwords
  Provides information on how to use the kpasswd Qshell command.

Enterprise Identity Mapping (EIM)
Enterprise Identity Mapping (EIM) is a mechanism for mapping a person or entity (such as a service) to the appropriate user identities in various user registries throughout the enterprise. When used with network authentication service, EIM enables a single sign-on environment. The iSeries uses EIM to enable OS/400 interfaces to authenticate users through network authentication service. iSeries and applications can also accept Kerberos tickets and use EIM to map a user ID on one system to its associated Kerberos principal.

- Single sign-on enablement
  Provides conceptual information on the benefits of single sign-on and an overview of how network authentication service and Enterprise Identity Mapping (EIM) work together to create a single sign-on environment.
- Scenario: Enable single sign-on
  Provides detailed example of a situation where network authentication service and EIM are used together to enable a single sign-on environment.

Authentication support for several iSeries applications:

- **Structured Query Language (SQL)/ Distributed Relational Database Architecture (DRDA)**
  SQL/DRDA now supports the use of a Kerberos ticket to authenticate users accessing database functions. DRDA checks for a ticket granting ticket for a specified user. If a ticket exists then it will be used to obtain service tickets for that user.
-
- **Distributed Data Management (DDM)**
  DDM now supports the use of a Kerberos ticket to authenticate users accessing remote files. DDM checks for a ticket granting ticket for a specified user. If a ticket exists then it will be used to obtain service tickets for that user. **Note:** If you have a default realm specified in the Kerberos configuration file but are not using Kerberos as your authentication method, you need to remove the default realm before setting up authentication for DDM. For information on recovering from this problem, see Application connection problems and recovery .
-

- **iSeries Access for Windows and OS/400 Host Servers**
  iSeries Access for Windows and OS/400 Host Servers will support authentication through Kerberos tickets. From the client, a user can specify that a Kerberos ticket will be used when accessing iSeries Access Host Servers.
-
- **iSeries NetServer**
  iSeries NetServer clients can use Kerberos tickets to authenticate with the server if you have configured Kerberos in your network. Only clients that support Kerberos v5 can connect to iSeries NetServer when this support is enabled. For more details on requirements for iSeries NetServer support of Kerberos, see iSeries NetServer support for Kerberos v5 authentication.
-
- **QFileSvr.400**
  QFileSvr.400 will determine if a ticket granting ticket exists for the current user. If a ticket granting ticket exists then a server ticket will be created to authenticate the user on the target system. If no ticket exists then the current method of password substitution will be used. **Note:** If you have a default realm specified in the Kerberos configuration file but are not using Kerberos as your authentication method, you need to remove the default realm before setting up authentication for QFileSvr.400. For information on recovering from this problem, see Application connection problems and recovery .

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to Users . «

Print this topic

To view or download the PDF version, select Network authentication service (about 199 KB or 50 pages).

To save a PDF on your workstation for viewing or printing:

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

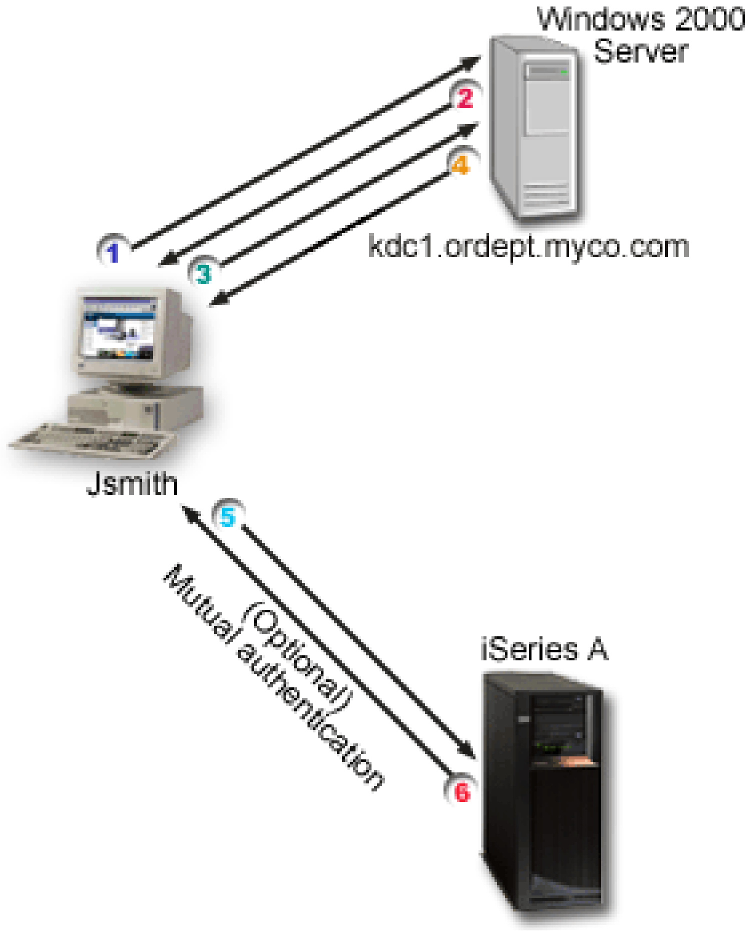
If you need Adobe Acrobat Reader to view or print the PDF, you can download a copy from the Adobe Web site (www.adobe.com/product/acrobat/readstep.html).

How does network authentication service work?

» As a network administrator, you can configure network authentication service so your iSeries system will accept Kerberos tickets created by a centralized key distribution center (KDC), which maintains a database of all users and services within a realm. The iSeries and several iSeries-specific applications act as a client/server within a Kerberos network, requesting tickets for users and for services. When a user requests a ticket from the KDC, he or she is issued an initial ticket, called a ticket granting ticket (TGT). The user can then use the TGT to request a service ticket to access other services and applications on the network. For authentication to work successfully, an administrator must register the users, iSeries service principal, and applications that will use Kerberos protocol with the KDC. The iSeries can act either as a server, where principals request authentication to services, or it can act as a client requesting tickets for applications and services on the network. The following graphics show how tickets flow in both these situations.

iSeries as a server

This graphic shows how authentication works when an iSeries acts a server in a Kerberos network. In this graphic, the Windows (R) 2000 KDC issues tickets to the principal, Jsmith. Jsmith wants to access an application on iSeries-A. In this case, Enterprise Identity Mapping (EIM) would be used on the server to map the Kerberos principal to an iSeries user profile. This would be done for any kerberized iSeries server function, such as iSeries-Access for Windows.



*

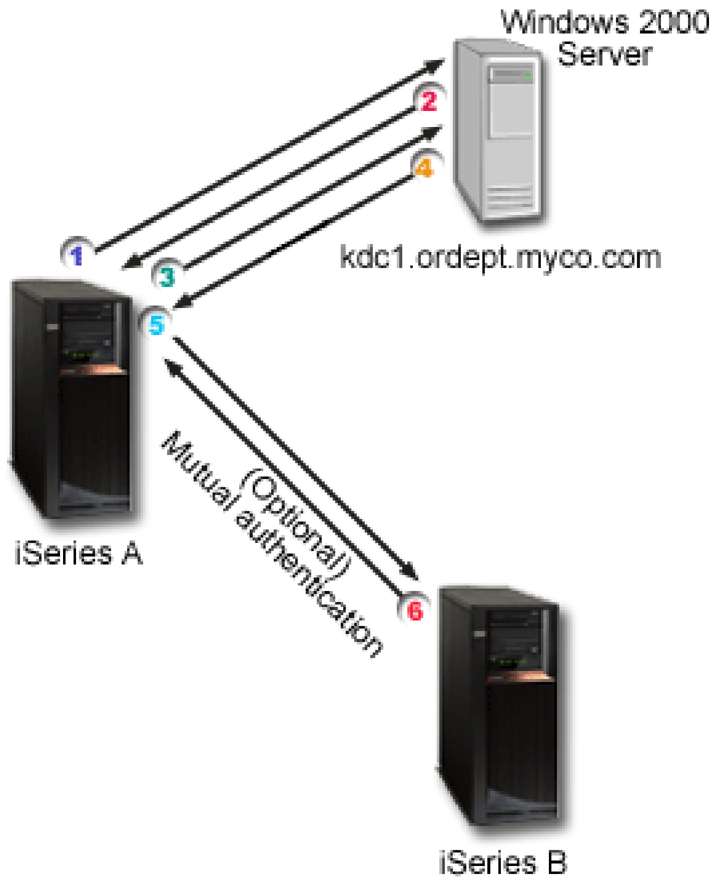
This description provides an overview of how this authentication process works within a network:

1. The user, Jsmith, requests a ticket from the KDC when he signs into the Kerberos network. This sends a request to the KDC for a ticket granting ticket.
2. The KDC validates his principal name and password and sends a ticket granting ticket to Jsmith.
3. Jsmith needs access to an application on an iSeries server. By calling the network authentication service APIs, the application sends Jsmith's TGT to the KDC to request a service ticket for the specific application or service. The principal's local machine manages a credentials cache which holds tickets and other identifying information for the user. These credentials are read from the cache as they are needed and new credentials are stored in the cache as they are obtained. This relieves the application of the responsibility for managing the credentials itself.
4. The KDC responds with the service ticket.
5. The application sends the server ticket to the iSeries service to authenticate the user.

6. The server application validates the ticket by calling the network authentication service APIs and optionally can send a response back to the client for mutual authentication.

iSeries as a client

This graphic shows how authentication works when an iSeries acts a client in a Kerberos network. In this graphic, the Windows [(R)] 2000 KDC issues tickets to the iSeries-A principal. The iSeries-A can be authenticated to other services. In this example, EIM would be used on the iSeries B to map the kerberos principal to an iSeries user profile. This would be done for any kerberized iSeries server function, such as QFileSvr.400.



*

This description provides an overview of how this authentication process works within a network:

1. A principal, Jsmith signs in to iSeries-A and then requests a ticket granting ticket by performing a kinit command in the Qshell Interpreter. The iSeries sends this request to the KDC.
2. The KDC validates his principal name and password and sends a ticket granting ticket to Jsmith.
3. Jsmith needs access to an application on an iSeries server. By calling the network authentication service APIs, the application sends Jsmith's TGT to the KDC to request a service ticket for the specific application or service. The principal's local machine manages a credentials cache which holds tickets, session keys, and other identifying information for the user. These credentials are read from the cache as they are needed and new credentials are stored in the cache as they are obtained. This relieves the application of the responsibility for managing the credentials itself.
4. The KDC responds with the service ticket. **Note:** A service principal for iSeries-B would need to be added to the KDC and network authentication service would also have to be configured on iSeries-B.

5. The application sends the server ticket to the iSeries service to authenticate the user.
6. The server application validates the ticket by calling the network authentication service APIs and optionally can send a response back to the client for mutual authentication.

«

Network authentication service terminology

» Network authentication service uses the following Kerberos protocol terminology:

forwardable tickets
Forwardable tickets allow a server to pass on the credentials of the requester to another service. For this to happen, the initial TGT must have been requested with the forwardable option and the server is allowed to delegate credentials.

key distribution center (KDC)
A network service that provides tickets and temporary session keys. The KDC maintains a database of principals (users and services) and their associated secret keys. It is composed of the authentication server and the ticket granting ticket server. It is important that you use a secure machine to act as your KDC. If someone gained access to the KDC, your entire realm could be compromised. **Note:** KDC support does not exist on the iSeries system.

key table
A file on the service's host system. Each entry in the file contains the service principal's name and secret key. On the iSeries, a key table file is created during configuration of network authentication service. When a service requests authentication to an iSeries with Network Authentication Service configured, that iSeries checks the key table file for that service's credentials. To ensure that users and services are authenticated properly, you must have users and services enrolled on the KDC and on the iSeries.

password server
Allows clients to change their password on the KDC remotely. The password server typically runs on the same machine as the KDC.

principal
The name of a user or service in a Kerberos network. A user is considered a person where a service is used to identify a specific application or set of operating system services. On iSeries, the **krbsvr400** service principal is used to identify the service used by iSeries Access for Windows, QFileSrv.400 and Telnet servers when authenticating from the client to the iSeries.

proxiable tickets
A proxiable ticket is a ticket granting ticket (TGT) that allows you to get a ticket for a service with IP addresses other than those in the TGT. Unlike forwardable tickets, you cannot proxy a new TGT from your current TGT; you can only proxy service tickets. Forwardable tickets let you transfer your complete identity (TGT) to another machine, where proxiable tickets only let you transfer particular tickets. Proxiable tickets allow a service to perform a task on the behalf of a principal. The service must be able to take on the identity of the principal for a particular purpose. A proxiable ticket tells the KDC that it can issue a new ticket to a different network address, based on the original ticket granting ticket. With proxiable tickets, a password is not required.

realm
A set of users and servers for which a given key distribution center (KDC) is the authenticating authority.

realm trust
The Kerberos protocol either searches the configuration file to determine realm trust or by default looks for trust relationships within the realm hierarchy. Using **Trusted realms** in network authentication service allows you to bypass this process and creates a shortcut for authentication. Realm trust can be used in networks where realms are in different domains. For example, if a company has one realm at NY.myco.com and another at LA.myco.com, then you can establish trust between these two realms. If two realms trust each other their associated KDCs must share a key. Before creating a shortcut, you must set up the KDCs to trust each other.

renewable tickets
In some cases, an application or service may want to have tickets which are valid for an extended period of time. However, the extended time could allow someone to steal these credentials which would be valid until the ticket expired. Renewable tickets allow for applications to obtain tickets that are valid for extended periods while lessening the chances for theft. Renewable tickets contain two expiration times. The first expiration applies to the current instance of the ticket and the second time applies to the latest permissible expiration for the ticket.

service ticket
A ticket that authenticates a principal to a service.

ticket granting service (TGS)
A service provided by the KDC that issues service tickets.

ticket granting tickets (TGT)
A ticket that allows access to the ticket granting service on the KDC. Ticket granting tickets are passed to the principal by the KDC after the principal has completed a successful request. In a Windows (R) 2000 environment, a user logs on to the network and the KDC will verify the principal's name and encrypted password and then send a ticket granting ticket to the user. From an iSeries server, users can request a ticket using the kinit command within the Qshell Interpreter in the character-based interface.

«

Network authentication service protocols

» Network authentication service uses the Kerberos protocol in conjunction with Generic Security Services (GSS) APIs for authentication to provide authentication and security services. The following sections provide general description of these protocols and how they are used on the iSeries. For more complete information on these standards, links have been provided to associated Request for Comments and other external sources.

Kerberos protocol

The Kerberos protocol provides third party authentication where a user proves his or her identity to a centralized server, called the key distribution center (KDC), which issues tickets to the user. The user can then use these tickets to prove his or her identity on the network. The ticket eliminates the need for multiple sign-ons to different systems. The Kerberos APIs that the iSeries supports originated from Massachusetts Institute of Technology and have become the defacto standard for using the Kerberos protocol.

Security environment assumptions

The Kerberos protocol assumes that all data exchanges occur in an environment where packets can be inserted, changed, or intercepted at will. Use Kerberos as one layer of an overall security plan. Although the Kerberos protocol allows you to authenticate users and applications across your network, you should be aware of some limitations when you define your network security objectives:

- The Kerberos protocol does not protect against denial-of-service attacks. There are places in these protocols where an intruder can prevent an application from participating in the proper authentication steps. Detection and solution of such attacks are usually best left to human administrators and users.
- Key sharing or key theft can allow impersonation attacks. If intruders somehow steal a principal's key, they will be able to masquerade as that user or service. To limit this threat, prohibit users from sharing their keys and document this policy in your security regulations.
- The Kerberos protocol does not protect against typical password vulnerabilities, such as password guessing. If a user chooses a poor password, an attacker might successfully mount an offline dictionary attack by repeatedly attempting to decrypt messages that are encrypted under a key derived from the user's password.

For more information on the Kerberos protocol, see the following sources:

The Kerberos Network Authentication Service (V5) .
The Internet Engineering Task Force (IETF) formally defines the Kerberos protocol in Request for Comments 1510.

Kerberos: The Network Authentication Protocol (V5) .
Massachusetts Institute of Technology's official documentation of the Kerberos protocol provides programming information and describes features of the protocol.

Network Authentication Service Application Programmable Interfaces (APIs)

This Information Center topic provides a listing of Network Authentication Service APIs and brief descriptions of their functions.

Generic Security Services (GSS) APIs

GSS APIs provides security services generically and are supported by a range of security technologies, like the Kerberos protocol. This allows GSS applications to be ported to different environments. Because of this reason, it is recommended that you use these APIs instead of Kerberos APIs. You can write applications that use GSS APIs to communicate with other applications and clients in the same network. Each of the communicating applications plays a role in this exchange. Using GSS APIs, applications can perform the following operations:

- Determine another application's user identification.
- Delegate access rights to another application.
- Apply security services, such as confidentiality and integrity, on a per-message basis.

For more information on the GSS APIs, see the following sources:

Generic Security Service Application Program Interface Version 2, Update 1 .
The Internet Engineering Task Force (IETF) formally defines GSS APIs in RFC 2743.

Generic Security Service API : C-bindings .
The Internet Engineering Task Force (IETF) specifies GSS APIs C-bindings in RFC 1509.

The Kerberos Version 5 GSS-API Mechanism .
The Internet Engineering Task Force (IETF) defines Kerberos Version 5 and GSS API specifications in this RFC 1964.

Generic Security Service Application Programmable Interfaces (GSS APIs)
This Information Center topic provides a listing of GSS APIs and brief descriptions of their functions.

«

Network authentication service scenarios

» The following scenarios provide descriptions of common environments where network authentication service can be used to allow the iSeries to participate in a Kerberos network. Review the following scenarios to become familiar with the technical and configuration details involved with configuring network authentication service:

Scenario: Configure network authentication service with existing KDC
This topic describes a customer situation where an administrator is configuring network authentication in a Windows (R) 2000 environment, where a key distribution center has been installed and configured.

Scenario: Enable single sign-on
This scenario shows how to use network authentication service with Enterprise Identity Mapping (EIM) to enable single sign-on. The adminstrator wants to allow users to use their Windows (R) 2000 sign-on to authenticate to the iSeries systems and iSeries Access for Windows applications.

«

Scenario: Configure network authentication service with existing KDC

Situation

» You are a network administrator that manages the network for the order receiving department in your company. You recently added an iSeries to your network to house several necessary applications for your department. Currently you have a Windows (R) 2000 server that acts as a key distribution center (KDC) for the realm. The users within this network all have principal names and passwords stored on the KDC. You want to add the iSeries to the KDC. You plan to add the iSeries to this realm and continue to use the Windows (R) 2000 server as the authentication server. You have your own Kerberos-enabled applications that use GSS APIs.

This scenario has the following advantages:

- Simplifies authentication process for users
- Eases the overhead of managing access to servers in the network
- Minimizes threat of password theft

Objectives

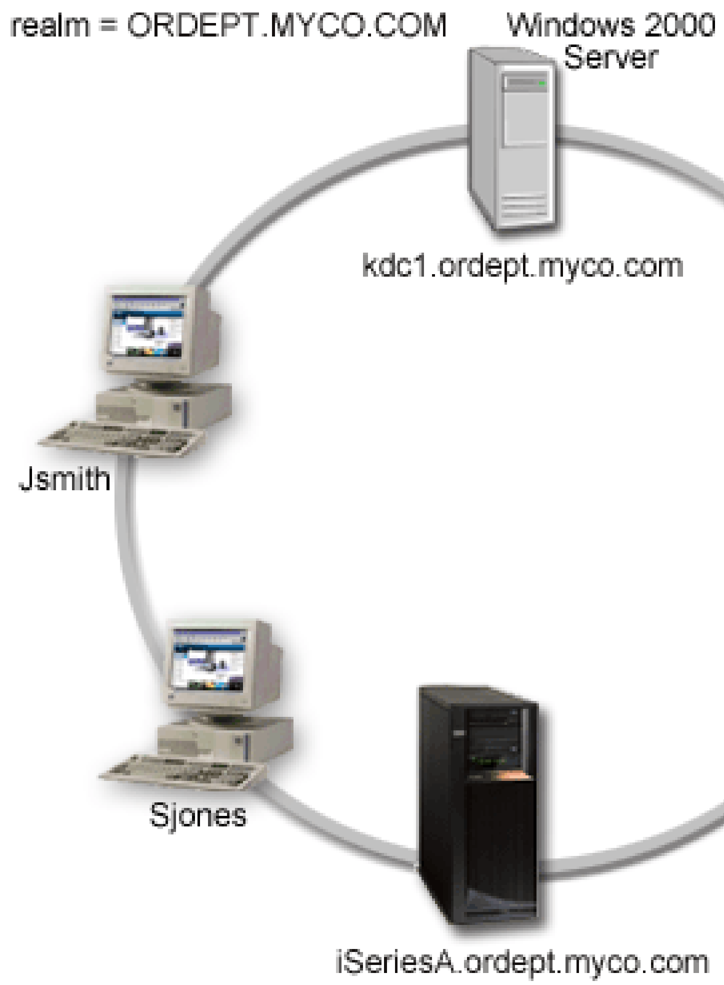
In this scenario, MyCo, Inc. wants to add an iSeries system to an existing realm where a Windows (R) 2000 server acts as the key distribution center. The iSeries contains several business critical applications that need to be accessed by the proper users. Users need to be authenticated by the KDC to gain access to these applications. The iSeries needs to be added to the KDC of the Windows (R) 2000 server.

The objectives of this scenario are as follows:

- Allow the iSeries to participate with an existing key distribution center
- Allow for both principal names and user names in the network
- Allow Kerberos users to change their own passwords on the KDC

Scenario details

The following figure illustrates the network characteristics of MyCo.



*

Order Receiving department

- iSeries-A runs on OS/400 Version 5 Release 2 (V5R2) and contains several business applications.
- The KDC's DNS name is kdc1.ordept.myco.com
- iSeries-A's principal name is krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
- The default realm for the KDC is ORDEPT.MYCO.COM
- Client PCs run Windows (R) 2000.

Configuration steps for this scenario

1. Complete (See 13) the planning worksheets and checklists for network authentication service.
2. Configure (See 14) network authentication service on iSeries-A.
3. Add (See 14) iSeries-A to the KDC.
4. Create (See 15) a home directory for each user on iSeries-A
5. Verify (See 15) TCP/IP domain information for iSeries-A
6. Test (See 15) network authentication service configuration on iSeries-A.

Configuration details

Step 1: Complete the planning worksheets

The following planning checklists illustrate the type of information you need before you begin configuring network authentication service. All answers on the prerequisite checklist should be YES before you proceed with network authentication service setup.

Prerequisite checklist	**Answers**
Is your OS/400 V5R2 (5722-SS1) or later?	Yes
Is Cryptographic Access Provider (5722-AC3) installed on your iSeries systems?	Yes
Is iSeries Access for Windows (5722-XE1) installed on all the PCs in your network and your iSeries systems?	Yes
Is the Security subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	Yes
Is the Network subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following installed on the secure system that will act as a key distribution center? If so which one? 1. Windows $^{(R)}$ 2000 Server 2. Windows $^{(R)}$ XP Server 3. AIX Server 4. zSeries	Yes Windows $^{(R)}$ 2000 Server
For Windows $^{(R)}$ 2000 Server and Windows $^{(R)}$ XP Server, do you have Windows $^{(R)}$ Support Tools, which provides the ktpass tool, installed on the system being used as the key distribution center?	Yes
Are all your PCs in your network configured in a Windows $^{(R)}$ 2000 domain?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the iSeries system time within five minutes of the KDC's system time? If not see Synchronize system times.	Yes

You need this information to configure network authentication service	**Answers**
What is the name of the Kerberos default realm to which iSeries-A will belong?	ORDEPT.MYCO.COM
What is the KDC for this Kerberos default realm? What is the port on which the KDC listens?	kdc1.ordept.myco.com 88 (**Note:** This is the default port for the KDC.)
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this KDC? What is the port on which the password server listens?	Yes kdc1.ordept.myco.com 464 (**Note:** This is the default port for the password server.)

You need this information to configure network authentication service	Answers
What is the password for your iSeries service principal(s)?	iseriesa123 **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.
What additional realms will your iSeries systems interact with?	N/A
For each realm, what is the host name of the key distribution center?	N/A

Step 2: Configure network authentication service on iSeries-A

Use the the information from your worksheets to configure network authentication service on iSeries-A as follows:

1. In iSeries Navigator, expand **iSeries-A —>Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard. **Note:** After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the **Welcome** page for information about what objects the wizard creates. Click **Next**.
4. On the **Specify realm information** page, enter `ORDEPT.MYCO.COM` in the **Default realm** field. Click **Next**.
5. On the **Specify KDC information** page, enter `kdc1.ordept.myco.com` in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the **Specify password information** page, select **Yes**. Enter `kdc1.ordept.myco.com` in the **Password server** field and 464 in the **Port** field. Click **Next**.
7. On the **Create keytab entry** page, select the **iSeries Kerberos Authentication**. Click **Next**.
8. On the **Create iSeries keytab entry** page, write down the keytab and principal for iSeries-A. You will need the principal name when you add this to the KDC. Enter and confirm a password. For example, the administrator for MyCo, entered `iseriesa123`. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.
9. Click **Next**.
10. On the **Summary** page, review the network authentication service configuration details. Click **Finish**.

You are now finished configuring network authentication service on iSeries-A. The next step is to add the principal name to the KDC.

Step 3: Add iSeries-A principal name to the KDC

To add the iSeries system to the Windows [(R)] 2000 KDC, use the documentation that corresponds with adding principals to the KDC. By convention, the iSeries system name can be used as the username. Add the following principal name to the KDC:

```
krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
```

On a Windows [(R)] 2000 server, follow these steps:

1. Use the Active Directory [(R)] Management tool to create a user account for the iSeries system (select the **Users** folder, right-click, select **New**, then select **User**.) Specify iSeriesA as the Active Directory user.

2. Access the properties on the Active Directory user iSeriesA. From the **Account** tab, select the **Account is trusted for delegation**. This will allows the iSeries-A service principal to access other services on behalf of a signed-in user.
3. Map the user account to the principal by using the **ktpass** command. The ktpass tool is provided in the **Service Tools** folder on the Windows (R) 2000 Server installation CD. To map the user account, enter the following:

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   where `iseriesa123` is the password that you specified just a when you configured (See 14) network authentication service. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.

Step 4: Create a home directory for users on iSeries-A

Each user that will connect to the iSeries and iSeries applications needs a directory in the /home directory. This directory will contain the name of the user's Kerberos credentials cache. To create a home directory for a user, complete the following:

1. On an iSeries command line, enter:

   ```
   CRTDIR '/home/username'
   ```

   where `username` is the iSeries username for the user.
   For example, the administrator for MyCo entered the following:
   `CRTDIR '/home/Johns'` for the user John Smith.
2. Repeat these steps for all your users.

Step 5: Verify TCP/IP domain information for iSeries-A

1. On an iSeries command line, enter:

   ```
   CFGTCP
   ```

2. Select Option 10 (Work with TCP/IP host table entries).
3. In host name field, verify that the fully qualified host name for iSeries-A is lowercase. Also verify that the fully qualified host name appears first if there are multiple host name entries. For example, iSeries A should have the host name entry: iseriesa.ordept.myco.com.
4. After you have verified the host name entry, press F3 to return to Configure TCP main menu.
5. Select Option 12 (Change TCP/IP domain information).
6. Verify that your system name appears in the host name field. Also verify that your domain name is correct. In this example, the host name would be `iseriesa` and the domain name would be `ordept.myco.com` .

Step 6: Test network authentication service on iSeries-A

At this point, you can verify that you have configured network authentication service correctly by requesting a ticket granting ticket for iSeries-A principal name:

1. On a command line, enter `QSH` to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. In this scenario, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM should display as the principal name for iSeries-A. **Note:** If you chose to configure principals for LDAP and iSeries NetServer, there will be other entries in the keytab file. In this scenario, the administrator chose not to configure principals for these services.

3. Enter `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`. If this is successful then the QSH command will display without errors.
4. Enter `klist` to verify that the default principal is krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.

«

Scenario: Enable single sign-on

»

Situation

You are a network administrator that manages a network for the Order Receiving Department in your company. Currently your users have Windows $^{(R)}$ 2000 desktops. They need to manage their Windows IDs and passwords and their OS/400 usernames. You want to allow the Windows $^{(R)}$ 2000 sign-on to be used for iSeries authentication. You do not want to make the Windows $^{(R)}$ 2000 IDs and OS/400 usernames the same nor do you want to use password caching or synching due to security problems that these solutions present. You have heard that the iSeries server can enable single sign-on by configuring network authentication service and Enterprise Identity Mapping (EIM) on your server. While network authentication service allows an iSeries system to participate in a Window $^{(R)}$ 2000 domain, EIM provides a mechanism for associating the Windows $^{(R)}$ 2000 IDs to a single EIM identifier that represents that user in the enterprise. Because of these associations, Kerberos principals on the network can access some iSeries applications without the need to sign in with their iSeries username and password. For more details on the benefits of using single sign-on and how EIM and network authentication service work together, see the topic, Single sign-on enablement.

Scenario advantages

This scenario has the following advantages:

- Simplifies authentication process for users
- Eases the overhead of managing access to servers in the network
- Minimizes the threat of password theft
- Avoids the need for multiple signons
- Simplifies user identity management across the network

Objectives

In this scenario, MyCo, Inc. wants to add an iSeries system to an existing Windows $^{(R)}$ 2000 domain for authentication purposes. The iSeries systems contain several applications that need to be accessed by users. Users need to be authenticated by the KDC to gain access to these applications. The iSeries service principal needs to be added to the KDC of the Windows $^{(R)}$ 2000 server to allow principals to request service tickets. In addition, you will configure EIM and then create associations to map OS/400 user profiles and Kerberos principals to an EIM identifier representing a single user in the enterprise. Because users in the Order Receiving Department use iSeries Access for Windows applications, you have decided to use a Kerberos principal as the preferred authentication method for iSeries Access for Windows and its related applications.

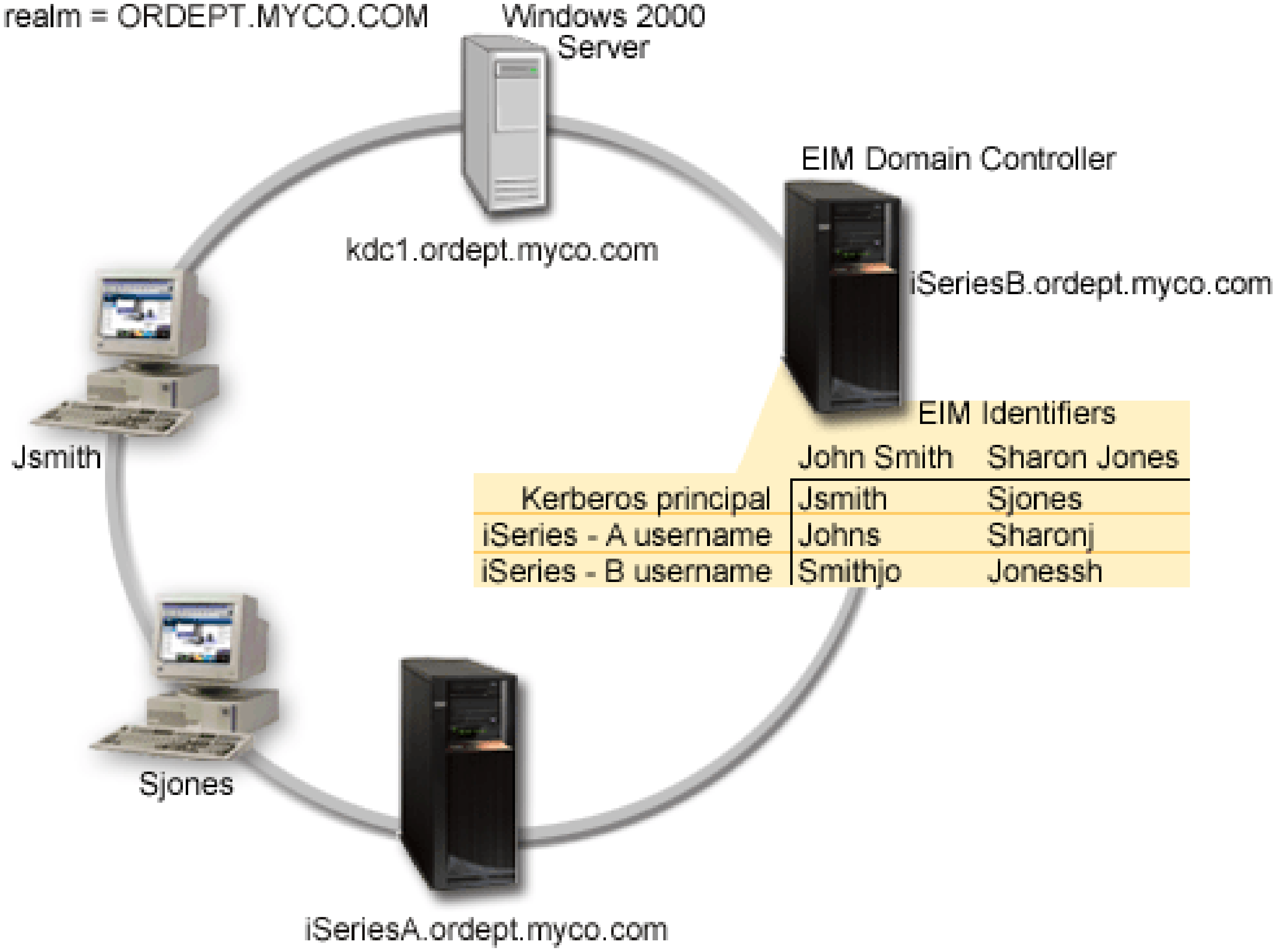
The objectives of this scenario are as follows:

- Allow iSeries-A and iSeries-B to participate with an existing key distribution center

- Configure the Directory Server on iSeries-B to operate as the EIM domain controller for the domain
- Allow user profiles on iSeries-A and iSeries-B and Kerberos principals to be mapped to a single EIM identifier
- Use Kerberos principal to authenticate to the iSeries Access for Windows applications

Scenario details

The following figure illustrates the network characteristics of MyCo.



	EIM Identifiers	
	John Smith	Sharon Jones
Kerberos principal	Jsmith	Sjones
iSeries - A username	Johns	Sharonj
iSeries - B username	Smithjo	Jonessh

*

Order Receiving department

- iSeries-A and iSeries-B run on OS/400 Version 5 Release 2 (V5R2) and contains several business applications.
- The KDC's name is `kdc1.ordept.myco.com`.
- iSeries-A's principal name is `krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`.
- iSeries-A's DNS name is `iSeriesA.ordept.myco.com`.
- The default realm for the KDC is `ORDEPT.MYCO.COM`.
- The Directory Server (LDAP) on iSeries-B will be configured to act as the EIM domain controller for the network. **Note:** LDAP configuration must be done prior to configuring EIM; however, the EIM

configuration wizard provides LDAP configuration if it is not configured on the system. In this scenario, iSeries-B does not have LDAP configured. The administrator plans to configure LDAP during EIM configuration.

- iSeries-B’s DNS name is `iSeriesB.ordept.myco.com`.
- iSeries-B’s principal name is `krbsvr400/iSeriesB.ordept.myco.com@ORDEPT.MYCO.COM`.
- Client PCs run Windows (R)2000.
- Kerberos principals, Jsmith and Sjones, have been registered on the KDC.

Configuration steps for this scenario

1. Complete (See 18) the planning worksheets for iSeries-A and iSeries-B
2. Configure (See 20) network authentication service on iSeries-A
3. Add (See 20) iSeries-A service principals to the KDC
4. Create (See 21) a home directory for each user on iSeries-A
5. Verify (See 21) TCP/IP domain information for iSeries-A
6. Test (See 21) network authentication service configuration on iSeries-A
7. Repeat steps 2-6 on iSeries-B
8. Configure (See 22) the EIM domain and configure the directory server on iSeries-B to be the EIM domain controller
9. Configure (See 23) iSeries-A to participate in the EIM domain
10. Create (See 23) EIM identifiers for users in the enterprise
11. Add (See 24) EIM associations for the OS/400 user profiles and principal names to the EIM identifier
12. Configure (See 25) iSeries Access for Windows connections to use Kerberos principals as authentication method
13. Verify (See 25) network authentication service and EIM set up

«

Configuration details

»

Step 1: Complete the planning worksheets

The following planning checklists illustrate the type of information you need before you begin configuring network authentication service and Enterprise Identity Mapping (EIM). All answers on the prerequisite checklist should be YES and the information for configuring network authentication should be complete before you proceed with network authentication service setup.

Prerequisite checklist	**Answers**
Is your OS/400 V5R2 (5722-SS1) or later?	Yes
Is Cryptographic Access Provider (5722-AC3) installed on your iSeries systems?	Yes
Is iSeries Access for Windows (5722-XE1) installed on all the PCs in your network and your iSeries systems?	Yes
Is the Security subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	Yes

Is the Network subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following systems acting as the key distribution center? Which one? 1. Windows $^{(R)}$ 2000 Server 2. Windows $^{(R)}$ XP Server 3. AIX Server 4. zSeries	Yes Windows $^{(R)}$ 2000 Server
For Windows $^{(R)}$ 2000 Server and Windows $^{(R)}$ XP Server, do you have Windows Support Tools, which provides the ktpass tool, installed?	Yes
Are all your PCs in your network configured in a Windows $^{(R)}$ 2000 domain?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the iSeries system time within five minutes of the KDC's system time? If not see Synchronize system times.	Yes

You need this information to configure network authentication service	**Answers**
What is the name of the Kerberos default realm to which your iSeries will belong?	ORDEPT.MYCO.COM
What is the KDC for this Kerberos default realm? What is the port on which the KDC listens?	kdc1.ordept.myco.com 88 (**Note:** This is the default port for the KDC.)
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this KDC? What is the port on which the password server listens?	Yes kdc1.ordept.myco.com 464 (**Note:** This is the default port for the password server.)
What is the password for your iSeries service principal(s)?	iseriesa123 iseriesb345 **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.
What additional realms will your iSeries interact with?	N/A
For each realm, what is the host name of the key distribution center?	N/A

You need this information to configure Enterprise Identity Mapping (EIM)	Answers
What is the LDAP administrator's distinguished name and password ?	distinguished name: cn=administrator password: mycopwd **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.
What is the name of the Directory Services (LDAP) server?	iSeriesB.ordept.myco.com
What is the port number of the Directory Services (LDAP) server?	389

Step 2: Configure network authentication service on iSeries-A

Use the the information from your worksheets to configure network authentication service on iSeries-A by completing the following tasks:

1. In iSeries Navigator, expand **iSeries-A —>Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard. **Note:** After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the **Welcome** page for information about what objects the wizard creates. Click **Next**.
4. On the **Specify realm information** page, enter `ORDEPT.MYCO.COM` in the **Default realm** field. Click **Next**.
5. On the **Specify KDC information** page, enter `kdc1.ordept.myco.com` in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the **Specify password information** page, select **Yes**. Enter `kdc1.ordept.myco.com` in the **Password server** field and 464 in the **Port** field. Click **Next**. **Note:** The password needs to be the same as the password entered when the principal is added to the KDC.
7. On the **Create keytab entry** page, select the **iSeries Kerberos Authentication**. Click **Next**.
8. On the **Create iSeries keytab entry** page, write down the keytab and principal for iSeries-A. You will need the principal name when you add this to the KDC. Enter and confirm a password. For example, the administrator for MyCo used the password, `iseriesa123`. this password will be used when iSeries-A is added to the KDC. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration. Click **Next**.
9. On the **Summary** page, review the network authentication service configuration details. Click **Finish**.

You are now finished configuring network authentication service on iSeries-A. The next step is to add the principal name to the KDC.

Step 3: Add iSeries-A principal name to the KDC

To add the iSeries to the Windows (R) 2000 KDC, use the documentation that corresponds with adding principals to the KDC. By convention, the iSeries name can be used as the username. Add the following principal name to the KDC:

```
krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
```

On a Windows (R) 2000 server, follow these steps:

1. Use the Active Directory (R) Management tool to create a user account for iSeries-A (select the **Users** folder, right-click, select **New**, then select **User**.) Specify iSeriesA as the Active Directory user.
2. Access the properties on the Active Directory user iSeriesA. From the **Account** tab, select the **Account is trusted for delegation**. This will allows the iSeries-A service principal to access other services on behalf of a signed-in user.
3. Map the user account to the principal by using the **ktpass** command. The ktpass tool is provided in the **Service Tools** folder on the Windows (R) 2000 Server installation CD. To map the user account, enter the following:

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   where `iseriesa123` is the password that you specified in step 6 when you configured (See 20) network authentication service. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.

Step 4: Create a home directory for users on iSeries-A

Each user that will connect to the iSeries and iSeries applications needs a directory in the /home directory. This directory will contain the name of the user's Kerberos credentials cache. To create a home directory for a user, complete the following:

1. On an iSeries command line, enter:

   ```
   CRTDIR '/home/username'
   ```

   where `username` is the iSeries username for the user.
   For example, the administrator for MyCo entered the following:
   `CRTDIR '/home/Johns'` for the user John Smith.
2. Repeat these steps for all your users.

Step 5: Verify TCP/IP domain information for iSeries A

1. On an iSeries command line, enter:

   ```
   CFGTCP
   ```

2. Select Option 10 (Work with TCP/IP host table entries).
3. In host name field, verify that the fully qualified host name for iSeries A is lowercase. Also verify that the fully qualified host name appears first if there are multiple host name entries. For example, iSeries A should have the host name entry: iseriesa.ordept.myco.com.
4. After you have verified the host name entry, press F3 to return to Configure TCP main menu.
5. Select Option 12 (Change TCP/IP domain information).
6. Verify that your system name appears in the host name field. Also verify that your domain name is correct. In this example, the host name would be `iseriesa` and the domain name would be `ordept.myco.com` .

Step 6: Test network authentication service on iSeries-A

At this point, you can verify that you have configured network authentication service correctly by requesting a ticket granting ticket for iSeries-A principal name:

1. On a command line, enter `QSH` to start the Qshell Interpreter.

2. Enter `keytab list` to display a list of principals registered in the keytab file. In this scenario, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM should display as the principal name for iSeries-A.
3. Enter `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`. If this is successful then the QSH command will display without errors.
4. Enter `klist` to verify that the default principal is krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.

Step 7: Repeat steps 2 and 6 for iSeries-B.

Step 8: Configure EIM and EIM domain controller on iSeries-B

You now need to configure an EIM domain in your network. You also need to configure iSeries-B to be the EIM domain controller for the new EIM domain. When you have finished this step, you will have completed the following tasks:

- Created a new EIM domain.
- Configured the Directory Server on iSeries-B to be the EIM domain controller.
- Created EIM registries for iSeries-B and Kerberos user registry in the domain.
- Configured iSeries-B to participate in the EIM domain.

1. In iSeries Navigator, expand **iSeries-B —>Network—>Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure** to start the configuration wizard.
3. On the **Welcome** page, select **Create and join a new domain**. Click **Next**.
4. On the **Configure Directory Server** page, in the **Port** field accept the default 389. In the **Distinguished name** field, enter `cn=administrator`. Enter and confirm a password. This password will be used when accessing EIM domain management tasks. For example, the administrator for MyCo, entered `mycopwd` in the password and confirm password fields. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.Click **Next**.
5. On the **Specify Domain** page, enter the name of the domain. For example, the administrator for MyCo, entered `mycoeimDomain` in the **Domain** field. **Note**: The domain name cannot contain any of the following characters: = + < > , # ; \ and *. The **Description** field is optional. If you want, enter a brief description of the domain controller. Click **Next**.
6. On the **Specify Parent DN for Domain** page, select **No**. Click **Next**.
7. On the **Registry Information** page, select **Local OS/400** and **Kerberos**. Select **Kerberos user identities are case sensitive**. Click **Next**. Write down the registry names. You will need these registry names when creating associations to EIM identifiers. **Note:** Registry names must be unique to the domain.
8. On the **Specify EIM System User** page, select the system EIM user. Accept the defaults that appear on this page. For example, MyCo had the following information on this page:
    - User type: Distinguished name and password
    - Distinguished name: cn=administrator
    - Password: mycopwd
      Note: Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.

Click **Next**.

9. On the **Summary** page, confirm the EIM configuration information. Click **Finish**.

You have now configured the directory server on iSeries-B as the EIM domain controller for the newly configured EIM domain in the network. Now you must specify iSeries-A as a participant in this EIM domain.

You now need to configure iSeries-A to participate in the EIM domain.

1. In iSeries Navigator, expand **iSeries-A —>Network—>Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure** to start the configuration wizard.
3. On the **Welcome** page, select **Join an existing domain**. Click **Next**.
4. On the **Specify Domain Controller** page, enter the name of the domain controller. For example, the administrator for MyCo entered, `iSeriesB.ordept.myco.com` in the **Domain controller name** field. Click **Next**.
5. On the **Specify User for Connection** page, select **Distinguished name and password** for the user type. For example, the administrator for MyCo, entered `cn=administrator` in the **Distinguished name** field and `mycopwd` in the password and confirm password fields. **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration. Click **Next**.
6. On the **Specify Domain** page, select the name of the domain that you want to participate in. Click **Next**. For example, the administrator for MyCo selected **mycoeimDomain**.
7. On the **Registry Information** page, select **Local OS/400**. Click **Next**. Write down the registry names. You will need these registry names when creating associations to EIM identifiers. **Note:** Registry names must be unique to the domain.
8. On the **Specify EIM System User** page, select the system EIM user. Accept the defaults that appear on this page. For example, MyCo had the following information on this page:
   - User type: Distinguished name and password
   - Distinguished name: cn=administrator
   - Password: mycopwd
     Note: Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.

   Click **Next**.
9. On the **Summary** page, confirm the EIM configuration. Click **Finish**.

You have now configured iSeries-A to participate in the domain.

You now need to create EIM identifiers for each user in the enterprise. An EIM identifier represents user or entity on the network. In the case of MyCo, the administrator created two EIM identifiers, John Smith and Sharon Jones.

1. On iSeries-B, expand **Network**—> **Enterprise Identity Mapping**.
2. Right-click on the **Domain Management** and select **Add Domain...**
3. On the **Add Domain** dialog, these defaults should display for MyCo’s EIM domain:
   - Port: 389
   - Domain: mycoeimDomain
   - Parent DN: none
   - Domain controller: iSeriesB.ordept.myco.com

   Note: These defaults were created during EIM domain controller configuration.
4. Click **OK**.

5. The iSeries Navigator hierarchy refreshes with **mycoeimDomain** under **Domain Management**. Click **mycoeimDomain**. You will be prompted with the **Connect to EIM Domain Controller** dialog. You must connect to the EIM domain controller before you can manage the domain.
6. On the **Connect to EIM Domain Controller** page, enter the Domain Controller's administrator distinguished name and password. These are the same distinguished name and password that are created during the configuration of the EIM domain controller. For MyCo, the administrator entered the following:
   - Distinguished name: cn=administrator
   - Password: mycopwd **Note:** Any and all passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.
7. Click **OK**.
8. Two new folders will display. Right-click **Identifiers** and select **New Identifier**.
9. On the **New EIM Identifier** page, enter an identifier in the **Identifier** field. Repeat this step until all users have an identifier. MyCo added the following identifiers:
   - John Smith
   - Sharon Jones
10. Click **OK**.

Now that unique EIM identifiers have been created for John Smith and Sharon Jones, we can now associate their OS/400 user names on iSeries-A and iSeries-B and their Kerberos principals to these EIM identifiers.

Step 11: Add EIM associations for the OS/400 user profiles and principal name to the EIM identifier

To complete this task, MyCo's administrator completed the following steps:

1. On iSeries-B, expand **Identifiers** and right-click **John Smith** and select **Properties**. There will be three associations for this identifier: Kerberos principal, the user profile on iSeries-A and the user profile for iSeries-B.
2. To associate the Kerberos principal with the identifier, John Smith:
   a. On the **Associations** tab, click **Add**.
   b. On the **Add Association** page, click **Browse** in the **Registry** field, and select `ORDEPT.MYCO.COM`. This is the Kerberos user registry that was added during EIM configuration.
   c. In the **User** field, enter `Jsmith`.
   d. In the **Association type** field, select **Source**.
   e. Click **OK**.
3. To associate the user name on iSeries-A with the identifier, John Smith:
   a. On the **Associations** tab, click **Add**.
   b. On the **Add Association** page, click **Browse** in the **Registry** field and select `iSeriesA.ordept.myco.com`. This is the OS/400 user registry for iSeries-A.
   c. In the **User** field, enter `Johns`.
   d. In the **Association type** field, select **Target**.
   e. Click **OK**.
4. To associate the user name on iSeries-B with the identifier, John Smith:
   a. On the **Associations** tab, click **Add**.
   b. On the **Add Association** page, click **Browse** in the **Registry** field and select `iSeriesB.ordept.myco.com`. This is the OS/400 user registry on iSeries-B.
   c. In the **User** field, enter `Smithjo`.

    d. In the **Association type** field, select **Target**.
    e. Click **OK**.
5. Repeat steps 1-4 for the EIM identifier, Sharon Jones.

You now need to configure iSeries Access for Windows applications on both the Jsmith and Sjones PCs to use Kerberos when authenticating to the iSeries-A and iSeries-B.

From Jsmith's PC, configure iSeries-A and its applications to use Kerberos authentication by completing the following steps:

1. In iSeries Navigator, right-click **iSeries-A** and select **Properties**.
2. On the **Connection** tab, select **Use Kerberos principal name, no prompting**. This will allow iSeries Access for Windows connections to use the Kerberos principal name and password for authentication.
3. Repeat these steps for iSeries-B.
4. Repeat these steps on Sjones's PC.

Step 13: Verify network authentication service and EIM set up

At this point, all configuration steps are completed. To verify the network authentication service and EIM have been set up correctly, the administrator had Sharon Jones and John Smith log on to the Windows (R) 2000 domain by signing in to their PCs. He then had them open iSeries Navigator on the iSeries-A. If no iSeries sign-on prompt displays, EIM successfully mapped the Kerberos principal to an identifier on the domain. In addition to iSeries Access for Windows applications, these other applications support Kerberos authentication:

- Telnet Server
- iSeries NetServer
- QFileSrv.400
- Distributed Relational Database Architecture (DRDA)

«

Plan network authentication service

» To successfully configure network authentication service, you must understand the requirements and complete the necessary planning steps. This topic provides a prerequisite checklist and planning worksheet to ensure all necessary steps are completed. Use the following checklist and worksheet to aid in your configuration of network authentication service.

Prerequisite checklist	Answers
Is your OS/400 V5R2 (5722-SS1) or later?	
Is Cryptographic Access Provider (5722-AC3) installed on your iSeries systems??	
Is iSeries Access for Windows (5722-XE1) installed on all the PCs in your network and your iSeries systems?	
Is the Security subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	

Is the Network subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	
Do you have one of the following installed on a secure system that will act as a key distribution center? Which one? 1. Windows $^{(R)}$ 2000 Server 2. Windows $^{(R)}$ XP Server 3. AIX Server 4. zSeries	
For Windows $^{(R)}$ 2000 Server and Windows $^{(R)}$ XP Server, do you have Windows Support Tools, which provides the ktpass tool, installed on the system being used as the key distribution center?	
Are all your PCs in your network configured in a Windows $^{(R)}$ 2000 domain?	
Have you applied the latest program temporary fixes (PTFs)?	
Is the iSeries system time within five minutes of the KDC's system time? If not see Synchronize system times.	

You need this information to configure network authentication service	**Answers**
What is the name of the Kerberos default realm to which iSeries-A will belong?	
What is the KDC for this Kerberos default realm? What is the port on which the KDC listens?	
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this KDC? What is the port on which the password server listens?	
What is the password for your iSeries service principal(s)?	
What additional realms will your iSeries interact with?	
For each realm, what is the host name of the key distribution center?	
What service principal names will applications on your iSeries use?	

«

Configure network authentication service

» Before you configure network authenication service, you should have completed all the necessary planning steps. In addition, network authentication service assumes you have a key distribution center (KDC) configured on a secure system in your network. Currently, KDC support does not exist on the iSeries. Microsoft Windows $^{(R)}$ 2000 and Windows $^{(R)}$ XP and z/OS support KDC functionality. See the appropriate documentation that corresponds with the Kerberos configuration for the system that will be used as a KDC.

It is recommended that you configure the KDC prior to configuring network authentication service on the iSeries. To configure network authentication service complete the following steps:

1. In iSeries Navigator, expand **iSeries-A —>Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard. **Note:** After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the **Welcome** page for information about what objects the wizard creates. Click **Next**.
4. On the **Specify realm information** page, enter the name of the default realm in the **Default realm** field. Click **Next**.
5. On the **Specify KDC information** page, enter the name of the Key distribution center for this realm in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the **Specify password information** page, select either **Yes** or **No** for setting up a password server. The password server allows principals to change passwords on the KDC. If you selected **Yes**, enter the password server name in the **Password server** field. The password server has the default port of 464. Click **Next**.
7. On the **Create keytab entry** page, select the **iSeries Kerberos Authentication**. In addition you can also create keytab entries for the LDAP server and the iSeries NetServer if you want these services to use Kerberos authentication. Click **Next**.
8. On the **Create iSeries keytab entry** page, enter and confirm a password. Click **Next**. **Note:**This is the same password you will use when you define the iSeries to the KDC.
9. On the **Summary** page, review the network authentication service configuration details. Click **Finish**.

Network authentication service is now configured.

What do I do next?

Define the iSeries to the key distribution center

Define iSeries to the key distribution center

After you configure network authentication service on your iSeries, you must define your iSeries to the key distribution center (KDC). Network authentication service provides an iSeries principal name, **krbsvr400** for the server and all the native iSeries applications.

For example, in our configuration scenarios, we referred to an iSeries with a host name of iSeriesA.ordept.myco.com. In order for a client to obtain a service ticket to present to this iSeries, the principal krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM needs to be defined with the KDC.

z/OS
Consult the documentation for the **Kadmin** command.

Windows (R) 2000 server

1. Use the Active Directory (R) Management tool to create a user account for the iSeries. Specify a name for the iSeries as the Active Directory user. For example, a valid name could be iSeriesA.
2. Access the properties on the Active Directory user that you created in Step 1. From the **Account** tab, select the **Account is trusted for delegation**. This will allows the iSeries service principal to access other services on behalf of a signed-in user.
3. Map the user account to the principal by using the **ktpass** command. For example, you could enter the following:
   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM -mapuser iSeriesA
   -pass xxxxxx
   ```
   where `xxxxxx` is the password you specified during network authentication service configuration.

What do I do next? Create a home directory

Create a home directory

»

After you have defined the iSeries to the key distribution center, you need to create a /home directory for each user that will connect to the iSeries and iSeries applications. This directory will contain the name of the user’s Kerberos credentials cache. To create a home directory for a user, complete the following:

On an iSeries command line, enter:

```
CRTDIR ’/home/username’
```

where `username` is the iSeries username for the user.

What do I do next:

Verify TCP/IP domain information

«

Verify TCP/IP domain information

» After you have created a home directory, you should verify that you have the correct host table entries for your server.

1. On an iSeries command line, enter:

   ```
   CFGTCP
   ```
2. Select Option 10 (Work with TCP/IP host table entries).
3. In host name field, verify that the fully qualified host name for iSeries A is lowercase. Also verify that the fully qualified host name appears first if there are multiple host name entries. For example, iSeries A should have the host name entry: iseriesa.ordept.myco.com.
4. After you have verified the host name entry, press F3 to return to Configure TCP main menu.
5. Select Option 12 (Change TCP/IP domain information).
6. Verify that your system name appears in the host name field. Also verify that your domain name is correct. For example, the host name could be `iseriesa` and the domain name could be `ordept.myco.com` .

What do I do next:

Test network authentication service configuration «

Test network authentication service configuration

»

After you have verified the correct domain information, you should test the network authentication service configuration by requesting a ticket granting ticket for your iSeries principal name:

1. On a command line, enter `QSH` to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. For example, a valid principal name could be krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.
3. Enter `kinit -k krbsvr400/system.domain@realm`. For example, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM would be a valid principal name for the iSeries. If this is successful then the QSH command will display without errors.
4. Enter `klist` to verify that the default principal is krbsvr400/system.domain@realm.

What do I do next:

Configure Enterprise Identity Mapping (EIM)
This step is optional if you are using network authentication service with your own applications. However, it is recommended for use with native-iSeries applications to manage multiple user identities across a network. «

Manage network authentication service

» After you have configured network authentication service, you can request tickets, work with key table files, and administer realm trust relationships. You can also work with credentials files and back up configuration files. The following topics describe how to complete these tasks:

Administrator tasks

The following is a brief list of tasks can be performed by an administrator in iSeries Navigator. For more task-based information, see the iSeries Navigator help for network authentication service. In addition to these tasks, administrators need to ensure that users are deleting old credentials by using the kdestroy command.

- Synchronize system times
  For tickets to be exchanged between an iSeries and a KDC, the system times must be within five minutes of each other. You can configure the maximum clock difference from the network authentication service Properties. The default maximum clock difference is 5 minutes or 300 seconds. This topic describes how you can synchronize times between systems.
-
- Add realms
  This topic describes how you can add a new realm to the network authentication service configuration.
-
- Delete realms
  This topic describes how you can remove realms from the network authentication service configuration.
-
- Add a key distribution center to a realm
  This topic describes how you can add a key distribution center to your current configuration of network authentication service.
-
- Add password server
  This topic describes how to add a password server to your network authentication service configuration so users can change their Kerberos passwords.
-
- Create a trust relationship between realms
  This topic describes how to set up a trust relationship between realms. This function is optional because by default the Kerberos protocol will search the realm hierarchy looking for trust. However, this function is useful if you have realms in different domains and would like to make this process faster.
-
- Change host resolution
  This topic describes how you can change host resolution for realm names.
-
- Add encryption settings
  This topic describes how to add encryption types for ticket granting tickets (TGT) and ticket granting service (TGS).

iSeries user tasks

The iSeries can also operate as a client in a Kerberos-enabled network. Users can log onto the iSeries and perform Kerberos-related tasks through the Qshell Interpreter. The following tasks use several Qshell commands to perform common tasks for iSeries users.

- Create a home directory
  This topic describes how to create a home directory.
-
- Obtain new ticket granting tickets
  This topic describes how to obtain or renew a ticket granting ticket with the **kinit** Qshell command.
-
- Change Kerberos passwords
  This topic describes how to change passwords with the Qshell command, **kpasswd**.
-
- Manage keytab files
  This topic describes how to manage keytab files with the Qshell command, **keytab**.
-
- Delete expired credentials cache
  This topic describes how to delete expired credentials cache that are stored on the client with the **kdestroy** Qshell command. It is important to periodically for users delete their credential cache.
-
- Display credentials cache or keytab file
  This topic describes how to list credentials and keytab files associated with a user with the **klist** Qshell command.
-
- Manage Kerberos service entries in LDAP directories
  This topic describes how to manages Kerberos service entries in the Directory Service (LDAP) directories with the **ksetup** QSHELL command.

«

Synchronize system times

»

Network authentication service uses 5 minutes (300 seconds) as the default for the maximum amount of time that system times can be different. You can change the clock difference by working with the network authentication service properties.

Before synchronizing system times, use the QUTCOFFSET system value to set your system time according to your time zone. You can synchronize these system times by changing the KDC time or use the QTIME system value to change the iSeries system time. However, to keep system times in a network synchronized, you should configure Simple Network Time Protocol (SNTP). SNTP allows multiple systems to base their time on a single time server. To configure SNTP, complete the following:

To configure SNTP on an iSeries, enter `CHGNTPA` on a command line.

To configure SNTP on Windows $^{(R)}$ systems, use **NET HELP TIME** to display configuration information for a SNTP server.

«

Add realms

» As the network administator, you may want to add a new realm to the network authentication service configuration. Before you can add a realm to the iSeries configuration, the KDC must be configured for the new realm. Before you can add a realm to the iSeries network authentication service task, you need the realm name, the KDC name and the port on which the KDC listens.

To add a realm to the network authentication service, complete the following steps:

1. In iSeries Navigator, select **your iSeries server** —> **Security** —> **Network Authentication Service**.
2. Right-click **Realms** and select **Add Realm**.
3. In the **Realm to add** field, enter the host name of the realm that you wish to add. For example, a valid realm name could be: ORDEPT.MYCO.COM.
4. Enter the name of the KDC for the realm that you are adding. For example, a valid KDC name could be: kdc1.ordept.myco.com.
5. Enter the port number on which the KDC listens for requests. A valid port number can be 1-65535. The default port for the KDC is 88.
6. Click **OK**.

«

Delete realms

» As the network administrator, you may want to delete a realm from the network authentication service configuration. Realms may no longer be needed or used on a network. You may also need to remove a default realm to recover from some iSeries-native application problems.

For example, if you have configured network authentication service without setting up the key distribution center (KDC) in your network, QFileSvr.400 and Distributed Data Management (DDM) will assume that you are using Kerberos authentication. Prior to setting up authentication for these products, you should delete the default realm that you have specified during network authentication service configuration.

To delete a realm to the network authentication service, complete the following steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security** —> **Network Authentication Service** —> **Realms**.
2. Right-click the name of the realm that you would like to delete and select **Delete**.
3. Click **OK** to confirm the deletion.

«

Add a key distribution center to a realm

» As the network administrator, you can add a key distribution center (KDC) to a realm using network authentication service. Before you can add the KDC to the realm, you need to know the KDC name and the port on which it listens.

To add a key distribution center to a realm, complete these steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security** —> **Network Authentication Service** —> **Realms**.
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **General** tab, enter the name of the KDC that you wish to add to this realm. The KDC is required for all realms. For example, kdc2.ordept.myco.com could be a valid entry.
4. Enter the port number on which the KDC listens for requests. A valid port number can be 1-65535. The default port for the KDC is 88.
5. Click **Add**. The new KDC will appear in the **Key Distribution Center (KDC) for this realm** list.

6. Click **OK**.

«

Add password server

»

The password server allows Kerberos principals to change their passwords. To add a password server to a realm, complete the following steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security** —> **Network Authentication Service** —> **Realms**.
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **Password Server** tab, enter the name of the password server. For example, a valid name for the password server could be: psvr.ordept.myco.com.
4. Enter the port number that corresponds with the password server. A valid port number can be 1-65535. The default port for the password server is 464.
5. Click **Add**. The new password server will be added to the list.
6. Click **OK**.

«

Create a trust relationship between realms

» Establishing a trust relationship between realms creates a shortcut for authentication. This function is optional because by default the Kerberos protocol will search the realm hierarchy looking for trust. This function is useful if you have realms in different domains and would like to make this process faster. To set up realm trust, each KDC for each realm must share a key. Before you can create a trust relationship, you must set up the KDCs to trust one another. To create a trust relationship among realms, complete the following steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security** —> **Network Authentication Service** —> **Realm**.
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **Trusted Realms** tab, enter the names of the realms that you want to establish trust. For example, valid names for the trust relationship could be: NY.myco.com and LA.myco.com.
4. Click **Add**. This will add the trust association in the table.
5. Click **OK**.

«

Change host resolution

» With network authentication service, you can specify a Directory service (LDAP) server, a Domain Name System (DNS), and static mappings that are added to the configuration file to resolve host names and realm names. You can also select all three of these methods to resolve host names. If you do select all of these methods, network authentication service will check the directory server first, the DNS entries second, and finally the static mappings to resolve host names.

To change host resolution, complete the following steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security**.
2. Right-click **Network Authentication Service** and select **Properties**.
3. On the **Host Resolution** page, select **Use LDAP lookup**, **Use DNS lookup**, and/or **Use static mappings**.

4. If you select **Use LDAP lookup** as the host resolution type, enter the name of the directory server and its corresponding port. For example, ldapsrv.ordept.myco.com could be a valid name for the directory server. A valid port number can be 1-65535. The default port for the directory server is 389.
5. If you select **Use DNS lookup** as the host resolution type, you must have configured the DNS to map to realm names.
6. If you select **Use static mappings** as the host resolution type, enter the name of the realm name and its corresponding DNS name. For example, the host name might be mypc.mycompanylan.com and the realm name is ORDEPT.MYCO.COM. You can also map generic host names to a specific realm. For instance if all machines that end with myco.lan.com are part of the ORDEPT.MYCO.COM, you could enter `myco.lan.com` as the DNS name and ORDEPT.MYCO.COM as the realm. This creates an association between the realm name and the DNS name in the configuration file. Click **Add** to create a static mapping between the DNS and realm name in the configuration file.
7. After you have entered the pertinent information for the selected host resolution type, click **OK**.

«

Add encryption settings

» You can select the encryption types for ticket granting tickets (TGT) and ticket granting service (TGS). Encryption hides data that flows across a network by making it unidentifiable. A client would encrypt data and the server would decrypt it. To ensure that encryption works correctly, you must use the same encryption type that is specified on the KDC or the other communicating application. If these encryption types do not match, then encryption will fail. You can add encryption values for both TGT and TGS. **Note:** The default encryption values for the TGT and TGS are des-cbc-crc and des-cbc-md5. During configuration default encryption values are set. You can add other encryption values for tickets to the configuration by completing these steps:

1. In iSeries Navigator, expand **your iSeries server** —> **Security**.
2. Right-click **Network Authentication Service** and select **Properties**.
3. On the **Tickets** page, select the encryption value from either the Ticket Granting Ticket or the Ticket Granting Service list of available encryption types.
4. Click either **Add Before** or **Add After** to add the encryption type to the list of selected encryption types. Each of these selected encryption types will be attempted in the order they are listed. If one encryption type fails, the next one in the list will be attempted.
5. Click **OK**.

«

Obtain or renew ticket granting tickets

» The **kinit** command obtains or renews a Kerberos ticket granting ticket. If no ticket options are specified on the **kinit** command, the key distribution center (KDC) options specified in the Kerberos configuration file are used.

If an existing ticket is not being renewed, the credentials cache is re-initialized and contains the new ticket granting ticket received from the KDC. If the principal name is not specified on the command line, the principal name is obtained from the credentials cache. The new credentials cache becomes the default credentials cache unless the cache name is specified by the `-c` option.

Ticket time values are expressed as *nwndnhnmns*, where *n* represents a number, *w* indicates weeks, *d* indicates days, *h* indicates hours, *m* indicates minutes, and *s* indicates seconds. The components must be specified in this order, but any component may be omitted (for example, *4h5m* represents 4 hours and 5 minutes, and *1w2h* represents 1 week and 2 hours). If only a number is specified, the default is hours.

To obtain a ticket granting ticket that has a lifetime of 5 hours for principal Jsmith:

on the Qshell command line, enter:

```
kinit -l 5h Jsmith
```

Or

On an iSeries command line, enter:

```
call qsys/qkrbkinit parm('-l' '5h' 'Jsmith')
```

See the usage notes on this Qshell command, for specifics on its usage and restrictions. «

kinit

»

Syntax

```
kinit [-r time] [-R] [-p] [-f] [-A] [-l time] [-c cache] [-k] [-t keytab] [principal]
```

Default public authority: *USE

The Qshell command **kinit** obtains or renews the Kerberos ticket granting ticket .

Options

-r time
The time interval for renewing a ticket. The ticket can no longer be renewed after the expiration of this interval. The renew time must be greater than the end time. If this option is not specified, the ticket is not renewable (a renewable ticket may still be generated if the requested ticket lifetime exceeds the maximum ticket lifetime).

-R
An existing ticket is to be renewed. When you renew an existing ticket, you cannot specify any other ticket options .

-p
The ticket can be a proxy. If you do not specify this option, the ticket cannot be a proxy.

-f
The ticket can be forwarded. If you do not specify this option, the ticket cannot be forwarded.

-A
The ticket will not contain a list of client addresses. If you do not specify this option, the ticket will contain the local host address list. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

-l time
The ticket end-time interval. After this interval expires, the ticket cannot be used unless it has been renewed. If you do not specify this option, the interval is set to 10 hours.

-c cache
The name of the credentials cache that the kinit command will use. If you do not specify this option, the command uses the default credentials cache.

-k
The key for the ticket principal is to be obtained from a key table. If you do not specify this option, the system prompts you to enter the password for the ticket principal.

-t keytab
The key table name. If you do not specify this option but do specify the `-k` option, the system uses the default key table. The `-t` option implies the `-k` option.

principal
The ticket principal. If you do not specify the principal on the command line, the system obtains the principal from the credentials cache.

Authorities

Object Referred to	Authority Required
Each directory in the path name preceding the key table file if `-t` option is specified	*X
Key table file when `-t` is specified	*R
Each directory in the path name preceding the credentials cache file to be used	*X
Parent directory of the cache file to be used, if specified by the **KRB5CCNAME** environment variable, and the file is being created	*WX
Credentials cache file	*RW
Each directory in the paths to the configuration files	*X
Configuration files	*R

To enable the Kerberos run time to find your credentials cache file from any executing process, the name of the cache file is normally stored in the home directory in a file named **krb5ccname**. The storage location of the cache file name can be overridden by setting the environment variable **_EUV_SEC_KRB5CCNAME_FILE**. To access this file, the user profile must have ***X** authority to each directory in the path, and ***R** authority to the file where the cache file name is stored. The first time that a user creates a credentials cache, the user profile must have ***WX** authority to the parent directory.

Messages

- The `option_name` option requires a value.
- `command_option` is not a valid command option.
- No options allowed when renewing or validating ticket.
- Unable to obtain name of default credentials cache.
- Unable to resolve credentials cache `file_name`.

- No initial ticket available.
- Principal name must be specified.
- Unable to retrieve ticket from credentials cache `file_name`.
- Initial ticket is not renewable.
- `option_value` option is not valid for `request_name` request.
- Unable to obtain initial credentials.
- Unable to parse principal name.
- Unable to resolve key table `file_name`.
- Password is not correct for `principal_name`.
- Unable to read password.
- Unable to store initial credentials in credentials cache `file_name`.
- Time delta value is not valid.

For an example of how this command is used, see Obtain or renew a ticket granting ticket . «

Display credentials cache or keytab file

» The **klist** command displays the contents of a Kerberos credentials cache or key table.

To list all the entries in your default credentials cache and to show the ticket flags:

On a Qshell command line, enter

```
klist -f -a
```

Or

On an iSeries command line, enter

```
call qsys/krbklist parm(’-f’ ’-a’)
```

See the usage notes on this Qshell command, for specifics on its usage and restrictions. «

klist

»

Syntax

```
klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [filename]
```

Default public authority: *USE

The Qshell command **klist** displays the contents of a Kerberos credentials cache or key table.

Options

-a
Show all tickets in the credentials cache, including expired tickets. If you do not specify this option, expired tickets are not listed. This option is valid only when you list a credentials cache.

-e
Display the encryption type for the session key and the ticket. This option is valid only when you list a credentials cache.

-c
List the tickets in a credentials cache. If neither the `-c` nor the `-k` option is specified, this is the default. This option is mutually exclusive with the `-k` option.

-f
Show the ticket flags, using the following abbreviations:

Abbreviation	Meaning
F	Ticket can be forwarded
f	Forwarded ticket
P	Ticket can be a proxy
p	Proxy ticket
D	Ticket can be postdated
d	Postdated ticket
R	Renewable ticket
I	Initial ticket
i	Ticket not valid
A	Preauthentication used
O	Server can be a delegate
C	Transit list checked by the KDC

This option is valid only when you list a credentials cache.

-s
Suppress command output, but set the exit status to 0 if a valid ticket granting ticket is found in the credentials cache. This option is valid only when you list a credentials cache.

-k
List the entries in a key table. This option is mutually exclusive with the **-c** option.

-t
Display timestamps for key table entries. This option is valid only when you list a key table.

-K
Display the encryption key value for each key table entry. This option is valid only when you list a key table.

filename
Specifies the name of the credentials cache or key table. If no filename is specified, the default credentials cache or key table is used

Authorities

Object Referred to	Authority Required
Each directory in the path name preceding the file if `-k` option is specified as keytab	*X
Keytab file when `-k` is specified	*R
Each directory in the path name preceding the credentials cache file if the `-k` option is not specified	*X
Credentials cache file if the `-k` option is not specified	*R

To enable the Kerberos run time to find your credentials cache file from any running process, the name of the cache file is normally stored in the home directory in a file named **krb5ccname**. The storage location of the cache file name can be overridden by setting the environment variable **_EUV_SEC_KRB5CCNAME_FILE**. To access this file, the user profile must have ***X** authority to each directory in the path and ***R** authority to the file where the cache file name is stored. The first time that a user creates a credentials cache, the user profile must have ***WX** authority to the parent directory.

Messages

- The `option_name` option requires a value.
- `command_option` is not a valid command option.
- `command_option_one` and `command_option_two` cannot be specified together.
- No default credentials cache found.
- Unable to resolve credentials cache `file_name`.
- Unable to retrieve principal name from credentials cache `file_name`.
- Unable to retrieve ticket from credentials cache `file_name`.
- Unable to decode ticket.
- No default key table found.
- Unable to resolve key table `file_name`.

For an example of how this command is used, see Display credentials cache or keytab file . «

Manage keytab files

» The keytab command is used to add or delete a key from a key table or to display the entries in a key table.

For example, to add a key for the service principal, krbsvr400, on the host, kdc1.ordept.myco.com, in realm ORDEPT.MYCO.COM:

On a Qshell command line, enter

```
keytab add krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM
```

Or

On a iSeries command line, enter

```
call qsys/qkrbkeytab parm(’add’ ’krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM’)
```

You will be prompted for the password that was used when the service was defined to the KDC.

See the usage notes on this Qshell command, for specifics on its usage and restrictions. «

keytab

»

Syntax

```
keytab add principal [-p password] [-v version] [-k keytab] keytab delete principal [-v
version] [-k keytab] keytab list [principal] [-k keytab]
```

Default public authority: *USE

The Qshell command **keytab** manages a key table.

Options

-k
The key table name. If this option is not specified, the default key table is used.

-p
Specify the password. If this option is not specified, users are prompted to enter the password when they add an entry to the key table.

-v
The key version number. When you add a key, if this option is not specified, the next version number is assigned. When you delete a key, if this option is not specified, all keys for the principal are deleted.

principal
The principal name. When you list the key table, if this option is not specified, all principals are displayed.

Authorities

Object Referred to	Authority Required
Each directory in the path name preceding the target keytab file to be opened	*X
Parent directory of the target keytab file when add is specified, if the keytab file does not already exist	*WX
Keytab file when list is specified	*R
Target keytab file when add or delete is specified	*RW
Each directory in the paths to the configuration files	*X
Configuration files	*R

Messages

- You must specify *add*, *delete*, *list*, or *merge*.
- *command_option* is not a valid command option.
- *command_option_one* and *command_option_two* cannot be specified together.
- *option_value* option is not valid for *request_name* request.
- The *option_name* option requires a value.
- Unable to parse principal name.
- You must specify the principal name.
- Unable to read password.
- No default key table found.
- Unable to resolve key table *key_table*.
- Unable to read entry from key table *key_table*.
- Unable to remove entry from key table *key_table*.
- Unable to add entry to key table *key_table*.
- No entries found for principal *principal_name*.
- Value is not a valid number.
- The key version must be between 1 and 255.
- Key version *key_version* not found for principal *principal_name*.

For an example of how this command is used, see Manage keytab files.

Change Kerberos passwords

The **kpasswd** command will change the password for the specified Kerberos principal using the password change service. You must supply the current password for the principal as well as the new password. The password server will apply any applicable password policy rules to the new password before changing the password. The password server is configured during the installation and configuration of the KDC. See the documentation that corresponds with that system. During network authentication service configuration you can specify that name of the password server. If one has not been specified during configuration, you can add a password server.

You may not change the password for a ticket-granting service principal (krbtgt/realm) using the **kpasswd** command.

To change the password for the default principal:

On a Qshell command line, enter

```
kpasswd
```

Or

On a command line, enter

```
call qsys/qkrbkpsswd
```

To change the password for another principal:

On a Qshell command line, enter

```
kpasswd jsmith@ordept.myco.com
```

Or

On an command line, enter

```
call qsys/qkrbkpsswd parm ('jsmith@ordept.myco.com')
```

For more details on the use of this command, see kpasswd usage notes. «

kpasswd

»

Syntax

```
kpasswd [-A ] [principal]
```

Default public authority: *USE

The Qshell command kpasswd changes a password for a kerberos principal.

Options

-A The initial ticket used by the kpasswd command will not contain a list of client addresses. The ticket will contain the local host address list if this option is not specified. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

principal
The principal whose password is to be changed. The principal will be obtained from the default credentials cache if the principal is not specified on the command line.

Messages

- Principal %3$s is not valid.
- Unable to read default credentials cache file_name.
- No default credentials cache.
- Unable to retrieve ticket from credentials cache file_name.
- Unable to read password.
- Password change canceled.
- Password is not correct for principal_name.
- Unable to obtain initial ticket.
- Password change request failed.

For an example of how this command is used, see Change Kerberos passwords . «

Delete expired credentials cache files

»

The **kdestroy** command deletes a Kerberos credentials cache file. Users need to periodically delete old credentials by using the kdestroy command.

The *-e* option causes the **kdestroy** command to check all of the credentials cache files in the default cache directory (**/QIBM/UserData/OS400/NetworkAuthentication/creds**). Any file that contains only expired tickets that have been expired for the *time_delta* is deleted. The *time_delta* is expressed as *nwndnhnmns*, where *n* represents a number, *w* indicates weeks, *d* indicates days, *h* indicates hours, *m* indicates minutes, and *s* indicates seconds. The components must be specified in this order, but any component may be omitted (for example, *4h5m* represents 4 hours and 5 minutes, and *1w2h* represents 1 week and 2 hours). If only a number is specified, the default is hours.

To delete your default credentials cache:
On a Qshell command line, enter

```
kdestroy
```

Or

On an iSeries command line, enter

```
call qsys/qkrbkdstry
```

To delete all credentials cache files that have expired tickets older than 1 day:

On a Qshell command line, enter

```
kdestroy -e 1d
```

Or

On an iSeries command line, enter

```
call qsys/qkrbkdstry parm ('e' '-1d')
```

See the usage notes on this Qshell command, for specifics on its usage and restrictions. «

kdestroy

»

Syntax

```
kdestroy [-c cache_name] [-e time_delta]
```

Default public authority: *USE

The Qshell command **kdestroy** destroys a Kerberos credentials cache.

Options

-c cache_name
The name of the credentials cache to be destroyed. If no command options are specified, the default credentials cache is destroyed. This option is mutually exclusive with the `-e` option.

-e time_delta
All credentials cache files that contain expired tickets are deleted if the tickets have been expired at least as long as the `time_delta` value.

Authorities

When the credentials cache is of type **FILE** (see **krb5_cc_resolve()** for more information on cache types), the default behavior is that the credentials cache file is created in the /QIBM/UserData/OS400/NetworkAuthentication/creds directory. The placement of the credentials cache file can be changed by setting the KRB5CCNAME environment variable.

If the credentials cache file does not reside in the default directory, the following authorities are required:

Object Referred to	Data Authority Required	Object Authority Required
Each directory in the path name preceding the credentials cache file	*X	None
Parent directory of the credentials cache file	*WX	None
Credentials cache file	*RW	*OBJEXIST
Each directory in the paths to the configuration files	*X	None
Configuration files	*R	None

If the credentials cache file resides in the default directory, the following authorities are required:

Object Referred to	Data Authority Required	Object Authority Required
All directories in the path name	*X	None
Credentials cache file	*RW	None
Each directory in the paths to the configuration files	*X	None
Configuration files	*R	None

To enable the Kerberos protocol to find your credentials cache file from any running process, the name of the cache file is normally stored in the home directory in a file named krb5ccname. A user wishing to use Kerberos authentication on the iSeries must have a home directory defined. By default the home directory is /home/. This file is used to find the default credentials cache if no command options are specified. The storage location of the cache file name can be overridden by setting the environment variable _EUV_SEC_KRB5CCNAME_FILE. To access this file, the user profile must have ***X** authority to each directory in the path and ***R** authority to the file where the cache file name is stored.

Messages

- Unable to resolve credentials cache *cache_file_name*.
- Unable to destroy credentials cache *cache_file_name*.
- The *function_name* function detects an error.
- Unable to retrieve ticket from credentials cache *file_name*.
- The *option_name* option requires a value.
- *command_option* is not a valid command option.
- *command_option_one* and *command_option_two* may not be specified together.
- No default credentials cache found.
- Time delta value *value* is not valid.

For an example of how this command is used, see Delete expired credentials cache files .

Manage Kerberos service entries in LDAP directories

The **ksetup** command manages Kerberos service entries in the Directory Service (LDAP) directories. The following subcommands are supported:

addhost host-name realm-name
This subcommand adds a host entry for the specified realm. The fully qualified host name should be used so that it resolves correctly no matter what default DNS domain is in effect on the Kerberos clients. If no realm name is specified, the default realm name is used.

addkdc host-name:port-number realm-name
This subcommand adds a KDC entry for the specified realm. If a host entry does not already exist, one is created. If a port number is not specified, it is set to 88 . Use the fully qualified host name so that it resolves correctly no matter what default DNS domain is in effect on the Kerberos clients. If no realm name is specified, the default realm name is used.

delhost host-name realm-name
This subcommand deletes a host entry and any associated KDC specification from the specified realm. If no realm name is specified, the default realm name is used.

delkdc host-name realm-name
This subcommand deletes a KDC entry for the specified host. The host entry itself is not deleted. If no realm name is specified, the default realm name is used.

listhost realm-name
This subcommand lists the host entries for a realm. If no realm name is specified, the default realm name is used.

listkdc realm-name
This subcommand lists the KDC entries for a realm. If no realm name is specified, the default realm name is used.

exit
This subcommand ends the ksetup command.

Examples

To add the host, kdc1.ordept.myco.com, to the server, ldapserv.ordept.myco.com, as the KDC for realm ORDEPT.MYCO.COM, using an Directory Services (LDAP) administrator ID of Administrator and a password of verysecret, complete the following steps:

> On a Qshell command line, enter: `ksetup -h ldapserv.ordept.myco.com -n CN=Administrator -p verysecret`

Or

1. On an iSeries command line, enter:

   ```
   call qsys/qkrbksetup parm('-h' 'ldapserv.ordept.myco.com' '-n' 'CN=Administrator' '-p'
   'verysecret')
   ```
2. When the Directory Services (LDAP) server is successfully contacted, a subcommand prompt is displayed. Enter

   ```
   addkdc kdc1.ordept.myco.com ORDEPT.MYCO.COM
   ```

See the usage notes on this Qshell command, for specifics on its usage and restrictions. «

ksetup

» Syntax

```
ksetup -h host-name -n bind-name -p bind-password -e
```

Default public authority: *USE

The Qshell command **ksetup** manages Kerberos service entries in the Directory Service (LDAP) directory for a Kerberos realm.

Options

-h
The host name for the Directory Service (LDAP) server. If you do not specify this option, the Directory Service (LDAP) server specified in the Kerberos configuration file is used.

-n
The distinguished name to use when you bind to the Directory Service (LDAP) server. If you do not specify this option, the Directory Service (LDAP)_BINDDN environment variable is used to obtain the name.

-p
The password to use when you bind to the Directory Service (LDAP) server. If this option is not specified, the Directory Service (LDAP)_BINDPW environment variable is used to obtain the password.

-e
Echo each command line to stdout. This is useful when stdin is redirected to a file.

Authorities

Object Referred to	Authority Required
Each directory in the paths to the configuration files	*X
Configuration files	*R

Messages

- `subcommand` is not a valid subcommand.
- Valid subcommands are `addhost`, `addkdc`, `delhost`, `delkdc`, `listhost`, `listkdc`, `exit`.
- `command_option_one` and `command_option_two` cannot be specified together.
- Unable to initialize LDAPclient.
- Unable to bind to Directory Service (LDAP) server.
- Realm name must be specified.
- Host name must be specified.
- Too many positional parameters.
- Host `host` already exists.
- Root domain `domain` is not defined.
- Realm name `realm` is not valid.
- The `LDAP function name` function detects an error.
- Insufficient storage available.
- Host name `host` is not valid.
- Port number `port` is not valid.
- Host `host` is not defined.
- No KDC defined for host `host`.
- Unable to obtain default realm name.

For an example of how this command is used, see Manage Kerberos service entries in LDAP directories .
«

Troubleshoot network authentication service

» This section provides links to troubleshooting information about common problems for network authentication service, Enterprise Identity Mapping (EIM), and iSeries-native applications that support Kerberos authentication.

1. All prerequisites have been completed.
2. Ensure that the user has a user profile on the iSeries and a principal name on the KDC. On the iSeries, verify the user exists by opening the Users and Groups in iSeries Navigator or using the `WRKUSRPRF` for a command line. On Windows $^{(R)}$ systems, verify the user exists by accessing the Active Directory $^{(R)}$ Users and Computers folder.
3. Check to see if the iSeries is contacting the KDC by using the kinit command from Qshell Interpreter. If the kinit fails, check to see if the iSeries service principal has been registered on the KDC. If it has not, you can add the iSeries principal name to the KDC.

For information on specific messages, see the following topics:

- Network authentication service errors and recovery
  You may encounter these messages during the network authentication service wizard or when you are managing network authentication service properties in iSeries Navigator.
- Application connection errors and recovery
  This topic discusses the common error messages when applications use network authentication service, EIM, and some iSeries-native applications that can occur when the iSeries, service, or user tries to connect to the KDC.

«

Network authentication service errors and recovery

»

You may encounter these messages during the network authentication service wizard or when you are managing network authentication service properties in iSeries Navigator.

Message	Recovery
KRBWIZ_CONFIG_FILE_FORMAT_ERROR The Format of the Network Authentication Service configuration file is in error.	Reconfigure network authentication service. See Configure network authentication service for details.
KRBWIZ_CRYPTO_NOT_INSTALLED The required cryptographic product is not installed on the system.	Install the Cryptographic Access Provider (572-AC3) on the system.
KRBWIZ_ERROR_READ_CONFIG_FILE Error reading Network Authentication Service configuration file.	Reconfigure network authentication service. See Configure network authentication service for details.
KRBWIZ_ERROR_WRITE_CONFIG_FILE Error writing Network Authentication Service configuration file.	The service used to write the configuration file is unavailable. Try again later.
KRBWIZ_PASSWORD_MISMATCH New password and confirm new password not the same	Re-enter new password and confirm new password.
KRBWIZ_PORT_ERROR The port number must be between 1 and 65535.	Re-enter a port number between 1 and 65535.
KRBWIZ_ERROR_WRITE_KEYTAB Error writing key table file	The service used to write the keytab may be temporarily unavailable. Try again later.
KRBWIZ_NOT_AUTHORIZED_CONFIGURE Not authorized to configure Network Authentication Service.	Ensure that you have the following authorities: *ALLOBJ and *SECADM.
KrbPropItemExists Item already exists.	Enter a new item.
KrbPropKDCInListRequired Must have a KDC in the list.	Specified KDC does not exist in the list. Select a KDC from the list.
KrbPropKDCValueRequired A KDC name must be entered.	Enter a valid name for the KDC. The KDC must be configured on a secure system in the network.

KrbPropPwdServerRequired A password server name must be entered.	Enter a valid name for the password server.
KrbPropRealmRequired A realm name must be entered.	Enter the name of the realm in which this system belongs.
KrbPropRealmToTrustRequired A name must be entered for the realm to trust.	Enter the name of the realm for which a trust relationship is being established.
KrbPropRealmValueRequired A realm name must be entered.	Enter a valid name for the realm.
CPD3E3F Network Authentication Service error &2 occurred.	See the specific recovery information that corresponds with this message.

«

Application connection problems and recovery

»

You may encounter these messages when applications use network authentication service.

Problem	Recovery
You receive this error: Unable to obtain name of default credentials cache.	Determine if the user signed on to the iSeries has a directory in the /home directory. If the directory for the user does not exist, create a home directory for the credentials cache.
CPD3E3F Network Authentication Service error &2 occurred.	See the specific recovery information that corresponds with this message.

DRDA/DDM connection fails on an iSeries system that previously connected.	Check to see if the default realm specified during network authentication service configuration exists. If a default realm and key distribution center (KDC) have not been configured, the network authentication service configuration is incorrect and DRDA/DDM connections will fail. To recover from this error, you can do one of the following tasks: 1. If you are not using Kerberos authentication, then complete the following: a. Delete the default realm specified in the network authentication service configuration. 2. If you are using Kerberos authentication, complete these steps: a. Configure a default realm and KDC on a secure system on the network. See the documentation that corresponds with that system. **Note:** Currently the iSeries does not support a KDC. b. Reconfigure network authentication service specifying the default realm and KDC that you created in Step 1. c. Configure (See 25) iSeries Access for Windows applications to use Kerberos authentication. This will set Kerberos authentication on all iSeries Access for Windows applications, including DRDA/DDM.
QFileSvr.400 connection fails on an iSeries system that previously connected.	Check to see if the default realm specified during network authentication service configuration exists. If a default realm and key distribution center (KDC) have not been configured, the network authentication service configuration is incorrect and QFileSvr.400 connections will fail. To recover from this error, you can do one of the following tasks: 1. If you are not using Kerberos authentication, then complete the following: a. Delete the default realm specified in the network authentication service configuration. 2. If you are using Kerberos authentication, complete these steps: a. Configure a default realm and KDC on a secure system on the network. See the documentation that corresponds with that system. **Note:** Currently the iSeries does not support a KDC. b. Reconfigure network authentication service specifying the default realm and KDC that you create in Step 1. c. Configure (See 25) iSeries Access for Windows applications to use Kerberos authentication. This will set Kerberos authentication on all iSeries Access for Windows applications, including DRDA/DDM.
CWBSY1011 Kerberos client credentials not found.	The user does not have a ticket granting ticket (TGT). This connection error occurs on the client PC when a user does not log into a Windows $^{(R)}$ 2000 domain. To recover from this error log into the Windows $^{(R)}$ 2000 domain.

Error occurred while verifying connection settings. URL does not have host. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, complete the following: 1. In iSeries Navigator, expand **your iSeries**—> **Network**—>**Servers**—> **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the **General** page, validate that the administrator's distinguished name and password match those you entered during EIM configuration.
Error occurred while changing local directory server configuration. GLD0232: Configuration cannot contain overlapping suffixes. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, complete the following: 1. In iSeries Navigator, expand **your iSeries**—> **Network**—>**Servers**—> **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the **Database/Suffixes** page, remove any **ibm-eimDomainName** entries and reconfigure EIM.
Error occurred while verifying connection settings. Exception occurred calling an iSeries program. The called program is eimConnect. Details are: com.ibm.as400.data.PcmlException. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, complete the following: 1. In iSeries Navigator, expand **your iSeries**—> **Network**—>**Servers**—> **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the **Database/Suffixes** page, remove any **ibm-eimDomainName** entries and reconfigure EIM.

«

Related information

Kerberos protocol specifications

The Kerberos Network Authentication Service (V5) .
The Internet Engineering Task Force (IETF) formally defines the Kerberos protocol in Request for Comments 1510.

Kerberos: The Network Authentication Protocol (V5) .
Massachusetts Institute of Technology's official documentation of the Kerberos protocol provides programming information and describes features of the protocol.

Generic Security Services (GSS) API specifications

For more information on the Kerberos and GSS APIs, see the following sources:

Generic Security Service Application Program Interface Version 2, Update 1 .
The Internet Engineering Task Force (IETF) formally defines GSS APIs in Request for Comments 2743.

Generic Security Service API : C-bindings .
The Internet Engineering Task Force (IETF) specifies GSS APIs C-bindings in Request for Comments 1509.

The Kerberos Version 5 GSS-API Mechanism .
The Internet Engineering Task Force (IETF) defines Kerberos Version 5 and GSS API specifications in this Request for Comments 1964.

Information Center related topics

Network Authentication Service Application Programmable Interfaces (APIs)
This Information Center topic provides a listing of Network Authentication Service APIs and brief descriptions of their functions.

Generic Security Service Application Programmable Interfaces (GSS APIs)
This Information Center topic provides a listing of GSS APIs and brief descriptions of their functions.

Enterprise Identity Mapping (EIM)
Enterprise Identity Mapping (EIM) is a mechanism for mapping a person or entity (such as a service) to the appropriate user identities in various user registries throughout the enterprise. The iSeries uses EIM to enable OS/400 interfaces to authenticate users through network authentication service. iSeries and applications can also accept Kerberos tickets and use EIM to find a user ID on this system associated with the Kerberos principal.

Special terms and conditions

The following terms and conditions apply only to network authentication service code, contained in the service program QKRBGSS in the library QSYS, in the member KRB5 in the file H in the library QSYSINC, and in message catalogs skrbdll.cat and skrbkut.cat contained in the directory /QIBM/ProdData/OS400/NetworkAuthentication/.

IBM LICENSES NETWORK AUTHENTICATION SERVICE OBJECT CODE ″AS IS″ WITHOUT ANY WARRANTIES OF ANY KIND, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE.

IBM DOES NOT WARRANT THAT THE USE OF SUCH CODE WILL NOT INFRINGE ANY COPYRIGHT, TRADE SECRET, PATENT, OR OTHER INTELLECTUAL PROPERTY, PROPRIETARY, OR CONTRACTUAL RIGHT OF ANY THIRD PARTY.

The contributors require the following notices:

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Copyright 1994 by the Massachusetts Institute of Technology.
Copyright (c) 1994 CyberSAFE Corporation.
Copyright (c) 1993 Open Computing Security Group
Copyright (c) 1990, 1991 by the Massachusetts Institute of Technology.

All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Neither M.I.T., the Open Computing Security Group, nor CyberSAFE Corporation make any representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Copyright 1995, 1996 by Richard P. Basch. All Rights Reserved.
Copyright 1995, 1996 by Lehman Brothers, Inc. All Rights Reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Richard P. Basch, Lehman Brothers and M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Richard P. Basch, Lehman Brothers and M.I.T. make no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

These special terms and conditions apply only to network suthentication service code as described above, and to no other part of OS/400 or Licensed Internal Code. «

Printed in U.S.A.