Contents

The following Help Topics are available:

Access Control Concepts

Internet Addresses

Computers connected to the Internet communicate using the TCP/IP protocol suite. A connection to a TCP/IP network is identified by an IP address, which is expressed in the form of four numbers separated by dots (for example, 130.65.2.6).

An IP address uniquely identifies a connection to a network: no two computers , or hosts, may share an address.

A message sent from one host to another is marked with a source and destination IP address, analogous to the way that letters are marked with source and destination street addresses.

To restrict access to a particular host, specify that hosts IP address under IPX(tm)/IP Gateway Host Restrictions. For details, see Configuring Host Restrictions.

Port Number Identifies Service

In addition to an IP address, a message must be directed to a specific port number on the destination machine. A port number does not refer to anything physical. Instead, it identifies the type of message.

For example, Web browsers send messages to port number 80 (HTTP) and news readers use port number 119 (NNTP). The same port numbers are used universally for common types of traffic.

To restrict access to a certain type of service, specify the port number under IPX/IP Gateway Service Restrictions. For details, see Configuring Service Restrictions.

Configuring Service Restrictions

The IPX(tm)/IP Gateway Service Restrictions page describes the access control restrictions placed on an object. You may view or edit the configuration displayed here.

Access control may be configured for User, Group, Organization and Organizational Unit objects. For details on the inheritance of access control settings, see Inheritance and Exceptions.

Important: The OK and Cancel buttons affect the entire object dialog, not just this page. Do not choose OK until you have entered all changes to this page and other pages. If you choose Cancel, you lose all changes in every page of this dialog.

Screen regions and buttons

Inherited default access
Indicates that access control configuration is inherited from a parent container.

Unlimited access to all services
Indicates that the selected object may access any Internet service, except those specified under Access Control Exceptions.

No access to any service
Indicates that that the selected object has no access to Internet services, except those specified under Access Control Exceptions.

Access Time
Indicates the daily time period during which Internet services may be accessed, except as noted under Access Control Exceptions.

Access Control Exceptions
Indicates any configured exceptions to the access control policy for the selected object.

Configuring Host Restrictions

The IPX/IP Gateway Host Restrictions page describes the access control restrictions placed on an object. You may view or edit the configuration displayed here.

Access control may be configured for User, Group, Organization and Organizational Unit objects. For details on the inheritance of access control settings, see Inheritance and Exceptions.

Important: The OK and Cancel buttons affect the entire object dialog, not just this page. Do not choose OK until you have entered all changes to this page and other pages. If you choose Cancel, you lose all changes in every page of this dialog.

Screen regions and buttons

Add allows you to add a host restriction by specifying a host IP address and an optional accessible time period.

Edit allows you to edit a host restriction.

Delete allows you to delete a host restriction.

Inheritance and Exceptions

IPX(tm)/IP Gateway service and host restrictions may be configured for the following types of objects:

User
Group
Organizational Unit
Organization

If a user object does not have access control configured, it will inherit the configuration from its parent container. For example, if a service restriction is entered for an organization object, that restriction applies to all users contained within that organization.

Restrictions entered at a lower level in the tree take priority over those entered at a higher level. For example, if access control restrictions are entered for a user object, any restrictions entered for the organization or organizational unit to which that user belongs are ignored.

Restrictions entered for a group object are combined with any other restrictions that are effective for a user that belongs to that group.

View an IPX/IP Gateway Server 

The Identification page describes the IPX(tm)/IP Gateway Server object. The fields in this page are for your information and reference only. You may not change them.

Screen regions and buttons

Name is the name of the IPX/IP Gateway Server object.

Host Server is the name of the NetWare(R) server on which the gateway server resides.

Cancel closes this dialog.

IPX/IP Gateway Server

An IPX(tm)/IP gateway server allows a NetWare(R) network to connect transparently to the Internet or any TCP/IP-based intranet without running IP within the network.

TCP/IP

TCP (or Transmission Control Protocol) and IP (or Internet Protocol) form the basis of the collection of communication protocols that computers use on the Internet.

Host

Host refers to any computer or device connected to the Internet.

HTTP

HyperText Transfer Protocol is used by web browsers to access remote hosts on the Internet.

NNTP

Network News Transfer Protocol is used to access news groups on the Internet.