Ascend

# Ascend Access Control

FAQ

1. *What is Ascend Access Control?*

   Ascend Access Control is a network-wide security management and authentication solution that runs on UNIX platforms. It provides a comprehensive user authentication capability for both analog and digital users. The major functions of Access Control include:

   - User identification
   - User authentication
   - User authorization and user profile information
   - Call accounting

2. *Is Access Control RADIUS compliant?*

   Yes, Access Control is RADIUS (Remote Authentication Dial In User Service) compliant.

3. *What is RADIUS?*

   RADIUS is a de facto standard that provides management services to authenticate dial-in users. It was developed for service providers, carriers and corporations that need flexible, centralized user authentication and call accounting. It stores authentication information about all of the network's users as well as complete user profiles consisting of access restrictions. Used in conjunction with PAP/CHAP or other third-party authentication servers, a single RADIUS server can administer multiple security systems across complex networks.

4. *How can I configure and manage Access Control?*

   Access Control Manager is a Java-based application with a point-and-click interface for configuration and management. It maintains lists of all the attributes/features, which can be added to the profile on a per-user basis. User profile templates may be created and copied whenever you add new users.

5. *Does Access Control work with network access servers from other vendors?*

   Yes, as long as those network access servers comply with the RADIUS standard. Also, check with the vendor for support of the Ascend extensions, commonly known as the Ascend Dictionary, for enhanced feature support.

6. *What is the Proxy-RADIUS feature in Access Control?*

   Proxy-RADIUS is a function that allows Access Control to act as a proxy to several other authentication servers and is ideal for Intranet/Virtual Private Network (VPN) applications. Typically, Access Control acting as the Proxy-RADIUS resides at the central site of a carrier or an ISP while another Ascend Access Control server (or some other authentication server) resides at the corporate network. When a user dials into the ISP or carrier site, the Proxy-RADIUS checks for the domain name within the user ID (i.e. "joe@corp-A.com"). The authentication request is then forwarded for authentication to the respective authentication server that resides on the "corp-A.com" network.

ASCEND

7. *What is Ascend Intranet Authentication?*

   Ascend Intranet Authentication is a centralized means of delivering user authentication for an Intranet or a VPN. Carriers and service providers that offer VPN/Intranet services to corporations can use Access Control to maintain a central database with tables for each corporation. The network administrators from these corporations are allowed to manage the respective tables, which may include their clients' user names, passwords and user profiles. Corporate network administrators can view only the tables that belong to their respective corporation. This eliminates the need for separate authentication servers at the corporate sites. Authentication of users occurs through the Access Control server at the carrier/ISP site.

8. *Can I use an ODBC-compliant database for security management?*

   Yes, Access Control is ODBC-compliant and, therefore, communicates with ODBC-compliant database servers such as Sybase, Oracle and Informix. An ODBC-compliant database offers an efficient way to manage several hundreds or thousands of users and is scalable.

9. *What kind of authorization rules are available on a per-user basis in Access Control?*

   Access Control provides a comprehensive yet adaptable authorization mechanism to tighten your remote networking security. The authorization permits you to set up Access Control on a per-user basis, which is enforced when the user actually dials into your network and remains active until the session is terminated.

   You may utilize the data filters within the Access Control server to give individual users access only to specific hosts, specific subnetworks or specific networks based on source and destination IP addresses. Additionally, authorization may be controlled based on the type of protocols such as UDP, TCP and ICMP. It can also be based on the type of application such as FTP, TFTP, PING and WWW using source/ destination ports.

   Call filters enhance authorization by allowing you to define what types of data traffic are considered legitimate. In other words, even though a user may be permitted to send and receive ICMP data, they may not be permitted to maintain the connection with a simple, continuous Ping to an interface for more than a pre-configured duration. As a result, you can open ports for other legitimate users to dialing into your network.

   For protocols other than IP such as IPX and NetBios, Access Control offers generic filters to perform similar types of authorization and manage users' access to your network resources.

   The "immediate telnet" feature can be used to force end users to connect to a specific host using telnet.

10. *Does it support token card security?*

    Yes, Access Control supports a wide range of token card security such as Security Dynamic's ACE/Server, AssureNet Pathways' Defender server, Enigma Logic's SafeWord server, Bellcore's S/Key and Cryptocard.

    Access Control simplifies using token card security by providing the necessary client library for each of the supported token card security servers.

11. *Can I have back-up for Access Control Servers?*

    Yes, you may have up to two back-up servers per Ascend MAX WAN Access Switch. If the primary server fails, then the MAX device communicates with the secondary server for authentication. If the secondary server fails, then the MAX product contacts the tertiary server.

    This is true for accounting servers as well.

12. *Does Access Control support accounting?*

    Yes, Access Control offers comprehensive accounting information for billing and reporting. The accounting information includes but is not limited to: UserName, connection date/time, duration of the call, analog or digital, IP address assignment, number of input/output packets and data rate. Accounting information may be stored as a simple ASCII text file or automatically formatted and sent to an ODBC-compliant database.

    The same Access Control server can support both authentication and accounting. By installing two Access Control daemons, either on separate hardware platforms or on the same machine, you can separate the authentication and accounting functionality.

13. *Can the MAX and Pipeline products act as the client for the Access Control?*

    Pipeline products cannot act as clients to the Access Control, whereas all MAX products can act as clients to Access Control. For instance, when analog or digital users dial in, the MAX prompts users for username and password, and it then contacts Access Control for authentication. If approved, the connection is established and user profile information forwarded to the MAX, otherwise the connection is terminated.

14. *Can Access Control be configured to facilitate dial-out calls?*

    Yes. When users on the LAN side of the MAX want to send data to one of the several remote locations, the MAX fetches the necessary information from the Access Control server to securely call the correct remote location and then forwards the data.

15. *What UNIX platforms does Access Control support?*

    Access Control is supported on the following platforms:

    - SunOS 4.1.4 (Sun Sparc)
    - Solaris 2.5.1 (Sun Sparc)
    - Solaris 2.5.1 (Intel x86)
    - HP-UX 10.0 (PA RISC)
    - IBM AIX 4.1 (RS 6000)

16. *Does Ascend Access Control run under Microsoft Windows?*

    Ascend Access Control for Windows NT is planned for the end of 1996.

Remote Networking
Solutions That Work.™

Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, USA
TEL: 510.769.6001
FAX: 510.814.2300

E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 415.688.4343
Internet Home Page:
http://www.ascend.com