product information

Ascend Access Control



Managing thousands of users can be a burden on you and your network resources. Take command of your remote network with Ascend Access Control.

Remote Access ▾ Internet/Intranet Access ▾ Corporate LAN

Ascend Access Control™ is a comprehensive network-wide security management system that lets corporations and service providers manage, control and secure analog as well as digital remote access connections. Using Access Control, administrators can identify legitimate callers, perform authentication and authorization, monitor access to network resources and compile extensive billing and accounting details. It works with any RADIUS-compliant network access server such as Ascend's MAX™ product family, and it supports all of the popular platforms, protocols, authentication methods, token cards and database servers.

Access Control is the ideal solution for handling the dial-up traffic on corporate Intranets and Virtual Private Networks (VPNs). Administrators can supervise the network activities of thousands of remote callers using Access Control Manager—a Java-based application with a point-and-click interface. When used in conjunction with Ascend's Secure Access™ products, Access Control delivers a surefire, single-vendor solution for protecting the entire network.

ASCEND

Networking Solutions with Built-in Security Management

Identification and authentication permit legitimate callers while restricting unauthorized access

Access Control's identification and authentication functions analyze and validate all users dialing into the network. Features such as Calling Line ID (CLID) eliminate the possibility that a hacker gains access simply by guessing the password. Authentication capabilities then confirm a user's identity through a series of first tier password checks as well as analog and digital authentication protocols.

- Calling Line ID (CLID)
- Callback
- PAP and CHAP
- UNIX passwords
- TACACS, TACACS+ and Kerberos
- Third-party token cards: Security Dynamics' ACE/Server, Enigma Logic's SafeWord Server, AssureNet Pathways' Defender, Bellcore's S/Key, Cryptocard
- Analog and digital user authentication: SLIP, PPP Multilink PPP, Multilink Protocol Plus™ (MP+), terminal server and login user

Adaptable authorization rules regulate user access to network resources

Access Control offers a comprehensive yet flexible authentication mechanism that lets administrators customize user access rules. They can write rules to permit, limit or deny end user access based on source and destination IP addresses, type of protocol or type of application. Call filters help administrators maintain the connections that have legitimate data traffic and drop other calls after a predetermined period of inactivity.

- Data filters to limit access to specific hosts/networks
- Call filters to determine legitimate traffic
- UDP, TCP and ICMP protocols define authorization
- Applications using source/destination ports such as FTP, TFTP, PING, WWW control access
- Generic filters control non-IP protocols (IPX, NetBios)

Advanced resource management features deliver large-scale control over network infrastructure

Access Control gives network managers the tools to safely and completely manage the system resources on their network. They can assign additional bandwidth, pool IP addresses and send messages on user connections.

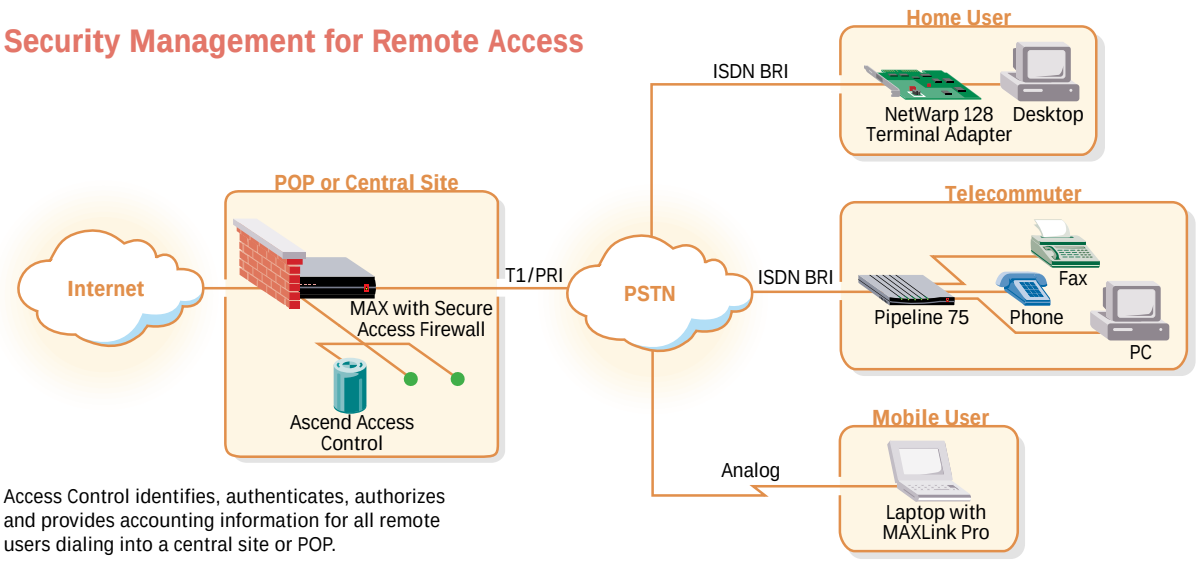
- Dynamic IP address assignment from an IP pool
- Static route assignment
- Banner messages for terminal server sessions
- Assignment of frame relay DLCIs
- Support for switched data services
- Password expiry
- Idle timeout

Access Control Manager simplifies configuration and management

Access Control Manager is an intuitive, user-friendly interface. With this Java-based application, network administrators have enterprise-wide control over the security and administrative functions of the network. Access Control Manager lists the attributes that can be added to a user profile on an individual basis.

- GUI with point-and-click configurator
- User profile templates simplify adding new users
- User-configurable templates simplify managing user files

Security Management for Remote Access



Access Control identifies, authenticates, authorizes and provides accounting information for all remote users dialing into a central site or POP.

Detailed accounting functions facilitate billing and analysis of user activity

Access Control collects and organizes information about dial-up sessions to bill customers, analyze resource utilization patterns and charge back departments or projects. The accounting feature collects detailed session information that is used to manage user access and activity.

- Day/time stamped information
- Duration of call and network usage
- Type of connection (analog/digital) and data rate
- Extensive call diagnostics (call termination codes)
- Realtime call tracking
- User profile information

Support for standard database servers and operating systems protects investments and ensures interoperability

Support for a wide range of operating systems means that Access Control can be integrated into a network without making an additional investment in infrastructure. Because Access Control is ODBC-compliant, administrators can rapidly retrieve data for authentication from a centralized user management system using databases such as Sybase or Oracle. Statistics can be collected and forwarded to the ODBC-compliant database for easy report generation.

- UNIX platforms: SunOS 4.1.4 (Solaris 1.1.2), IBM AIX 4.1, Solaris 2.5.1 (Intel/Sparc), Windows NT, HP UX 10.x (PA RISC)
- Other ODBC-compliant databases: Oracle 7, Sybase System 11, IBM DB2, Informix

Proxy-RADIUS establishes secure connections for VPNs and corporate Intranets

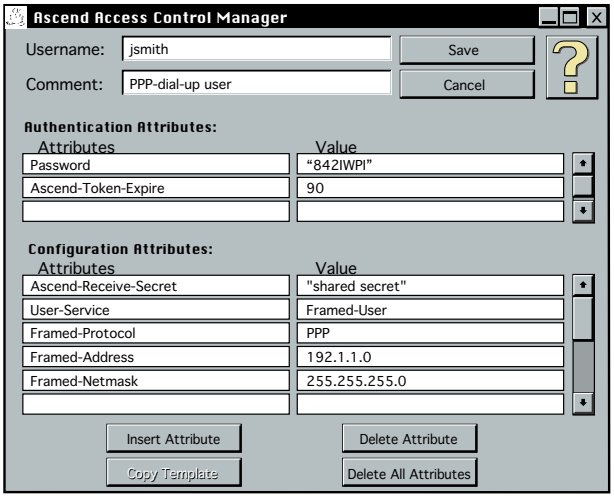
The Proxy-RADIUS functionality within Access Control facilitates the setup and management of VPNs by corporations and ISPs. It typically resides at the central site of a network service provider while another authentication server such as Access Control resides at the corporate network. Together, they authenticate users. After successful authentication, Access Control facilitates establishing a tunnel to the corporate network for Virtual Private Networking.

- Proxy-RADIUS in conjunction with Point to Point Tunneling Protocol (PPTP) and Ascend Tunneling Management Protocol (ATMP) establishes a tunnel
- Access Control is compatible with a wide range of authentication servers such as RADIUS, TACACS, TACACS+ and Kerberos
- Realm-based (domain name) authentication

Ascend Intranet Authentication consolidates security management for Intranets

When the Ascend Intranet Authentication feature within Access Control is used in VPN/Intranet applications, the need for a separate authentication server at the corporate site is eliminated. Corporations can use the authentication server located at their service provider's central office while still managing and maintaining their own user information.

- Eliminates the need for multiple authentication servers
- Enables companies to manage their own user information on the service provider's database
- Username
- Password
- User profile



Access Control Manager

Access Control Manager gives administrators enterprise-wide control over the security and administrative functions of the network.

Specifications

Analog and Digital User Authentication	SLIP, PPP, Multilink PPP, Multilink Protocol Plus (MP+), login user, PAP, CHAP
User Identification	Calling Line ID (CLID), Callback security
User Authentication	User name, password, UNIX password, Kerberos
Token Card Security	Security Dynamics, AssureNet Pathways, Enigma Logic, Bellcore S/Key, Cryptocard
Per User Authorization	Data filters, call filters, generic filters, immediate telnet
Accounting	Username, NAS-identifier, NAS-port, IP address, authenticating server, session-ID, DNIS, framed protocol, connection date/time, duration of connection, start/stop, input/out put octets, input/output packets, data rate
Resource Management	Dynamic IP address assignment, static route, banner messages, assignment of frame relay DLCI, routing or bridging, extensive switched data services, password expiry, idle timeout
Intranet/VPN features	Proxy RADIUS, Ascend Intranet Authentication, the Ascend dictionary
ODBC-compliant Database Support	Sybase, Oracle, Informix, centralized management of user and accounting information
Access Control Compatibility	Ascend's MAX product family, any RADIUS-compliant network access server
Supported Platforms	Sun OS 4.1.4, Solaris 2.5.1, HP UX 10.x, IBM AIX 4.1, Windows NT

Ascend's Remote Networking Products

GRF™ Family
GRF products are high-performance IP switches that let network service providers cost-effectively and reliably offer network access and backbone services.

MAX™ Family
The MAX family of high-density, multiprotocol WAN access switches provide access to central sites or the Internet over high-speed access lines such as frame relay over ISDN PRI, channelized T1/E1 and ISDN BRI lines.

Pipeline® Family
Pipeline products are Ethernet-to-ISDN bridges/routers that connect remote users in small or home offices to backbone networks and/or the Internet.

Multiband™ Family
Multiband bandwidth on demand controllers are designed for videoconferencing and multimedia applications and let users dial up bandwidth in increments of 56/64 kbps up to 4 mbps.

NetWarp™ Family
NetWarp products are high-performance ISDN terminal adapters that enable PC users to access the Internet or a remote LAN using the full 128 kbps of an ISDN BRI line.

Security Family
Ascend's Security family incorporates the dynamic firewall technology in Secure Access products with Access Control's comprehensive security management system to deliver iron-clad, end-to-end security for the entire network.

Ascend's Services

Ascend Advantage Service℠
Ascend Advantage Services offers a comprehensive selection of installation, maintenance, remote support and per-incident services for customers of Ascend's remote networking products .

* Depending on model and configuration

Ascend Communications, Inc.

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502
United States
Tel: 510.769.6001
Fax: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

European Headquarters
Rosemount House
Rosemount Avenue
West Byfleet
Surrey KT14 6NP
United Kingdom
Tel: +44 (0) 1932.350.115
Fax: +44 (0) 1932.350.199

Asia Pacific Headquarters
Level 14 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07
Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Ascend Communications, Inc. is a leading, worldwide provider of remote networking solutions for corporate central sites, Internet Service Providers' points of presence, remote offices, mobile workers, and telecommuters. Ascend develops, manufactures, markets, sells and supports products which utilize bandwidth on demand to extend existing corporate networks for applications such as remote LAN access, Internet access, telecommuting, SOHO connectivity and videoconferencing/multimedia access. Detailed information on Ascend products, news announcements, seminars, service and support is available on Ascend's home page at the World Wide Web site http://www.ascend.com.

Ascend is headquartered at 1701 Harbor Bay Parkway, Alameda, California 94502.
Phone: 800/621-9578; Fax 510/747-2300
E-mail: info@ascend.com.

Ascend markets the Access Control, GRF, MAX, Multiband, Pipeline, NetWarp and Security families of products. Ascend products are available in more than 30 countries worldwide.

Access Control™, GRF™, MAX™, MaxLink Pro™, Multiband™, Multilink Protocol Plus™, NetWarp™, Pipeline® and Secure Access™ are trademarks of Ascend Communications, Inc. Ascend Advantage Services℠ is a servicemark of Ascend Communications, Inc. Other trade names mentioned in this publication belong to their respective owners.
U.S. Patent No.5,231,649

Specifications are subject to change without notice.

© Copyright 1996
Ascend Communications, Inc.

01-38

10-96

ASCEND

Remote Networking Solutions That Work.™

ISO 9001 REGISTERED