



Steel-Belted Radius Software

Steel-Belted Radius is an award-winning RADIUS server that lets you consolidate the management of all your remote users, and enhance the security of your network.

By performing a powerful trio of functions — remote user authentication, authorization, and accounting — Steel-Belted Radius significantly alleviates your administrative burden. Now, you won't have to set up and maintain separate authentication databases on each remote access device on your LAN. Instead, let Steel-Belted Radius validate remote user names and passwords against a central database that you can easily administer. What's more, if you're already using NT/2000, NetWare, or UNIX for your LAN authentication, you can use the same database for your remote user authentication as well.

And, because Steel-Belted Radius works with the widest variety of remote access equipment and methods, it can manage users who connect via dial-up, the Internet, even VPNs tunnels. It even tracks and documents all remote access to your LAN.

Step up to the next level of remote access security and administration — with Steel-Belted Radius.

Centralize the Administration of all your Remote Users

Steel-Belted Radius is a complete implementation of the widely used IETF standards-track RADIUS (Remote Authentication Dial-In User Service) protocols. It acts as a security gateway to your LAN that performs the following functions:

- **Authentication** – validates any remote user's username and password against a central security database
- **Authorization** – for each new connection, provides information to the remote access device, such as what IP address to use, whether dialback is required, or which type of tunnel to set up
- **Accounting** – logs all remote connections, including user names and connection duration, for tracking and billing

Briefly, here's how Steel-Belted Radius works: When a remote user connects to the LAN via any remote access device (such as a remote access server, firewall, or router), that device communicates with Steel-Belted Radius to determine if the remote user is allowed to connect and, if so, what type of connection to establish. Steel-Belted Radius accepts or rejects the connection based on the results of the authentication, and responds with the necessary information authorizing a particular type of connection or service. The remote access device then establishes the user's connection. When the user logs off, the remote access device informs Steel-Belted Radius, which records an accounting transaction.

Works with any Combination of Remote Access Equipment and Methods

Steel-Belted Radius works with the remote access equipment and methods you already have in place on your network. Whether you have set up dial-in access via remote access servers, Internet access via firewalls, tunnel access via VPN routers — or any combination of these devices and methods — Steel-Belted Radius can manage the connections of all your remote users.

For example, you will be able to centralize the authentication, authorization, and accounting of:

- Dial-in users who connect via remote access servers from Cisco, Ascend, Bay Networks, Shiva, Ericsson, and others
- Internet users who connect via firewalls from Check Point, Raptor Systems, and others
- Tunnel/VPN users who connect via routers from Microsoft, New Oak Communications, VPNet, 3Com, and others
- Remote users who connect via outsourced remote access services from ISPs and other service providers

These are only examples; Steel-Belted Radius will work with any device that supports the RADIUS protocol.

And, Steel-Belted Radius supports a heterogeneous network, with remote access equipment from different vendors all interfacing with Steel-Belted Radius at once. Steel-Belted Radius automatically communicates with each device in the language it understands, based on dictionaries customized for each vendor that describe each vendor's extensions to the RADIUS protocol.

Choose Your Authentication Method

Not only does Steel-Belted Radius work with the widest variety of remote access equipment, it also offers the most methods for authenticating remote users.

In addition to Steel-Belted Radius's native database of users and their passwords, Steel-Belted Radius supports "pass-through" authentication to the security system you have already established for your LAN using NT Domains/Hosts, Windows 2000 Active Directory, NetWare NDS or Bindery, UNIX, or other means.

There are many reasons to use pass-through authentication to your OS database:

- You can use the same database to authenticate both LAN and remote users, saving you countless hours in administration
- You'll be able to authorize users for remote access simply by choosing names or groups from the information you've already set up in Windows NT/2000, Solaris, or NetWare
- Any changes you make in your LAN security database apply automatically to Steel-Belted Radius as well, so you can always be sure that remote users are authenticated based on the most up-to-date information
- Remote users can connect using the same user names and passwords as they use when they're on site



Steel-Belted Radius Software

Depending on its platform, Steel-Belted Radius performs pass-through authentication to:

- Microsoft NT Domains and Hosts/ Windows 2000 Active Directory
- UNIX user names and passwords
- NetWare NDS and Bindery users, groups, and organizational units

All versions of Steel-Belted Radius also support:

- Token-based authentication systems such as Security Dynamics ACE/Server, CryptoCard, and LeeMah's TraqNet 8000
- Proxy RADIUS authentication against a RADIUS server at another site which has the necessary database to perform authentication

In addition, Steel-Belted Radius running on Windows NT/2000 and Solaris can authenticate any remote user based on information stored in SQL databases from Informix, Oracle, and Sybase. Steel-Belted Radius for Windows NT/2000 also supports any ODBC-compliant database. Steel-Belted Radius:

- Works with your existing SQL table structure; no database redesign is likely to be necessary
- Can authenticate against one or more SQL databases, even if they're from different vendors
- Can simultaneously authenticate many users, for the fastest performance

Finally, Steel-Belted Radius for Windows NT/2000 and Solaris also supports authentication based on information in LDAP and TACACS+ databases. You can even combine any of these authentication methods, and specify the order each is checked to implement any policy you'd like.

Easily Manage Tunnel/VPN Authentication

Steel-Belted Radius can centralize the management and administration associated with VPN/tunnel access.

Steel-Belted Radius supports:

- All standard RADIUS tunneling attributes, as well as the vendor-specific attributes supported by many popular vendors
- MS-CHAP authentication, for full support of Microsoft RAS and PPTP connections
- Tunnel authorization based on username format (user@tunnel, tunnel#user), or the dialed number (DNIS)

Proxy RADIUS Creates Powerful Distributed Authentication Systems

Proxy RADIUS is a powerful feature of the RADIUS specification that permits one RADIUS server to pass authentication requests to another RADIUS server which has the necessary database to perform authentication.

Steel-Belted Radius fully supports proxy RADIUS; it can:

- Forward proxy RADIUS requests to other RADIUS servers
- Act as a target server that processes requests from other RADIUS servers
- Use DNS services to forward proxy RADIUS requests to other RADIUS servers (roaming)
- Pass accounting information to a target proxy RADIUS server, either the one that is performing the authentication, or a different one

You'll save countless hours in maintenance if you employ proxy RADIUS when you have multiple sites that remote users could potentially connect to; instead of storing everyone's authentication information on each possible server, you can simply store pointers to the appropriate authentication database.

RADIUS Accounting Makes Tracking and Billing Easy

Steel-Belted Radius logs all authentication transactions, so you'll be able to view the entire history of authentication requests and the responses that result. And, if your remote access device supports RADIUS accounting, you'll be able to track how long each user stays connected; you'll even have the security of being able to see exactly who's connected at any time and on which port.

Accounting data can easily be exported to spreadsheets, databases, and specialized billing software. Or, you can choose to log data directly to your SQL database.

System Requirements

Steel-Belted Radius is available in three versions.

- Steel-Belted Radius for Windows NT/2000 runs on an NT 4.0 or Windows 2000 workstation or server. It's administered from Windows NT or Windows 2000.
- Steel-Belted Radius for Solaris runs on Solaris 2.5.1, 2.6, and Solaris 7 running on SPARC or UltraSPARC. It's administered using a Java-based administration program that requires Netscape 4.03 or later, or Microsoft Internet Explorer 4 or later.
- Steel-Belted Radius for NetWare runs on a NetWare 3.12, 4.x, or 5.x server. It's administered from Windows 95 or Windows NT.
- Choose the LDAP Configuration Interface (LCI) add-on to configure Steel-Belted Radius from the command line.