



## Products

Search:

[Download PDF version](#)

### UniGuard V.34/V.90

Secure console port access  
regardless of the status of the network

#### Features:

- o Centrally managed by CDI [DDM](#)
- o Operates with most tokens
- o RSA SecurID ready (no ACE server)
- o Self-contained Database (unlike RADIUS or TACACS+)
- o Available in multi-port versions [Port Authority](#)
- o Single or Triple DES Encryption with [UniGuard Client](#)
- o Available for use in [Demand Dial Routing](#)
- o [Cabling options](#) for ease of bulk install



#### The problem with RADIUS and TACACS+

Routers installed in the field are all connected to a network. When this network goes "down", the only way to reach the router is to dial into the console port for remote maintenance. This opens up a "back door" to the network which many network managers lock with RADIUS or TACACS+. The problem with these protocols is that they require the network to be functioning in order to contact the security server. This is in direct conflict with the purpose of the console port which is only used when the network is "down". Therefore, RADIUS and TACACS+ provide inadequate security for router console port protection.

#### The Solution

UniGuard-V34 connects directly to the console port and provides the highest level of protection regardless of the state of the network. This is done by maintaining an internal security database that is updated by a central database on an "as needed" basis. This internal database provides fast, reliable, two factor authentication every time a technician accesses the router. Full session level encryption can be enabled by using a CDI encryption modem at the technician end of the call.

#### How do I manage all these remote devices?

[DDM, Distributed Database Manager](#), can maintain an unlimited number of UniGuards and or Port Authority devices remotely from a single workstation. This eliminates the need to update each unit individually when there is a database change. This software program automatically maintains the database of each remote device and is capable of down-loading the entire database of units manually or automatically at preset times. Reports can also be extracted automatically.

#### What can I connect them to?

Anywhere you are afraid to put a non secure modem you can put a UniGuard with confidence! Examples include; Routers, Firewalls, PBX's, remote switches, remote monitoring stations, remote power stations, out of

band managers, backup sites, remote systems, and more! [Checkout our Cabling Options!](#)

[Download this diagram in PDF](#)



The above diagram shows a number of Technicians accessing the maintenance port of remote Routers, Firewalls, and PBX's, each connected to a UniGuard-V34 for authentication or possibly full encryption. The UniGuard Manager will automatically update all the remote UniGuards in the field.

#### **Remote Technician Access**

The technicians will be authenticated by the UniGuard-V34 and will have full Triple DES Encryption by the UniGuard's at the local NOC. They will then gain access to the appropriate Router Maintenance Port.

#### **The Security Administrator**

The Security Administrator needs only to maintain one database at the central site and adds or deletes technicians, as required, from the database. Third party maintenance companies often change the Field Technicians assigned to these Routers. All UniGuard-V34s can have their database automatically updated.

#### **DDM Distributed Database Manager**

The DDM is a powerful 32 bit NT application that can manage thousands of remote UniGuard and [Port Authority](#) devices in the field.

#### **Specifications**

#### **International Approval List**

Self contained modem .....Multitech 2834ZDX

---

Data Speeds.....	38.4K Single DES, 19.2K Triple DES, 115.2K baud clear text
Cryptographics.....	Single or Triple Des self synchronizing 8 byte cypher feedback with unique key for each session. Automatic generation and distribution of session keys. Automatic electronic Private key updates.
Mode switch.....	Encrypt/Bypass. Used to enable higher speed clear text communications or ensuring that the encryptor doesn't interfere with clear text communications. Other wise the unit will auto-detect encrypted sessions. Switch can be disabled from management center
Security Standards.....	Certified by NIST for X9.17 Financial institution key management.
Standards Compliance.....	FIPS46, FIPS 81, FIPS 140-1, ANSI X9.23, ANSI X9.17, X9.52
Internal Battery.....	Maintains set-up parameters and Keys in RAM.
Tamper switches .....	Erases Keys and all data in RAM if unit is opened.
Interface.....	RJ45 with RJ45 to DB9 and RJ45 to DB25 adapters.
Power supply.....	Wall mount 17.5 VAC CT International and 48VDC configs available
Size .....	1.5in H x 4.0in W x 6.5in L
Support.....	Toll free technical support. 1 year warranty on all parts including labor. Optional Extended Warranty Available

---

**Ordering Information**

- UG-V34** UniGuard V34, UniGuard with a built in V.34 33.6k modem and one host port.
- UG-01** UniGuard (no internal modem), contains one modem port and one host port.

**[UniGuard](#) | [UniGuard Client](#) | [UniGuard High Speed DDR](#)  
[48VDC Option](#) | [Power Control Module Option](#)**

©Copyright 2001, Communications Devices, Inc.

