

## CypherManager Overview

**Senetas** designs and manufactures a range of encryption devices that protect data in motion by providing inline encryption at speeds up to 10Gbps. The units can be used on a broad range of networks for protocols such as ATM, SONET/SDH, Fibre Channel and Ethernet.

All Senetas encryptors are managed by a common element manager called CypherManager.

CypherManager provides secure local and remote management of the entire Senetas CN and CS encryptor range and also acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.

CypherManager is a Windows application that loads onto a PC and uses SNMPv3 to configure and manage the encryptor. The management session is secure and encrypted. Typically you would manage a unit via a dedicated RJ45 management port on the front panel, if desired you can use inband management to manage remote encryptors over the encrypted network itself.

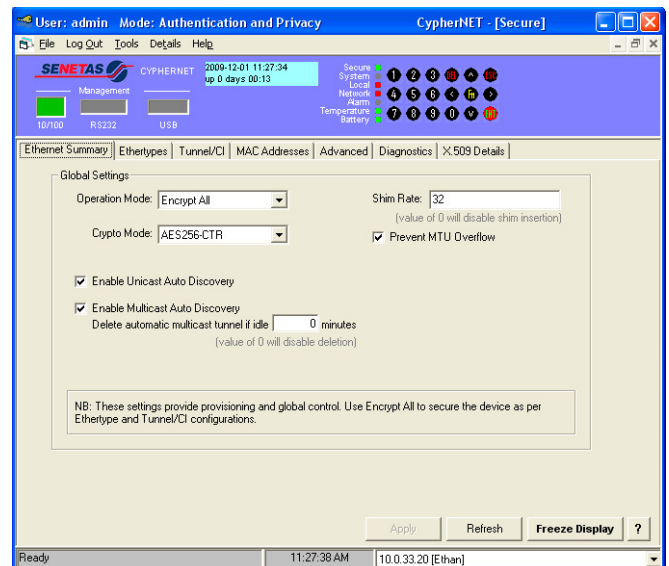
CypherManager manages all aspects of a distributed network including real-time status monitoring, configuration changes and certification.

CypherManager offers the following benefits:

- Purpose built graphical management tool
- Secure inband and out-of-band remote management using SNMPv3
- Automatically detects and manages every Senetas encryptor
- Real-time display
- Integrated certificate authority

A single CypherManager licence supports up to 10 encryptors with additional licenses available to extend this as required.

Senetas encryptors use SNMP traps to report events, alarms, etc., to a network management system such as OpenView or Tivoli, and CypherManager can itself monitor these traps. Encryptors maintain Audit logs (operator actions), Event logs (changes that occurred), and Alarm logs (error states). These logs can be viewed with CypherManager and saved and exported as files for archive and/or review.



In addition to providing configuration and monitoring functionality, CypherManager can be configured as the 'Certificate Authority' (CA) for the encryptors. Each encryptor must have a signed X.509 certificate so that units can establish trusted connections. Typically you would configure one copy of CypherManager on a secure PC as your Certificate Authority and then use it to certify all of the encryptors in the network. (Encryptors are tamper resistant and any attempt to physically access the unit will destroy all certification and key material such that the unit reverts to its factory uncertified state)

Encryptors can also be managed via a front panel 'craft' interface. This is an RS232 port that provides a Command Line Interface supporting a range of commands that provide similar functionality to CM. This interface does not provide certification functionality.

In the case of Ethernet encryptors, units can be configured as point-to-point or in multipoint mode with up to 509 units. Encryption is based on the AES algorithm with 256 bit keys, and automatic key updates change the data encryption key every 1-60 minutes (user defined). The encryption mode is CFB or Counter mode for units running at up to 1 Gbps, or Counter mode for 10 Gbps.

Senetas encryptors and the CypherManager solution have been accredited to the FIPS 140-2 and Common Criteria EAL4+ international security standards.

