



KEYNET Network Security Manager



Secure, Centralized, Cipher X® Network Security Device Management System

The KEYNET Network Security Manager simplifies the configuration and management a global networks of TCC's Cipher X 7210, 7211, and 7220 Network Security Devices. With an intuitive user interface and automated polling of alarms and logs, a network expert is not needed for trusted key and device management.

Centralized Management

KEYNET provides centralized key and device management of a global network of Cipher X family of Network Security Devices. All device configurations including security policies are intuitively managed with a user-friendly interface. Automatic polling of alarms and logs monitor device status. KEYNET also securely generates, stores and distributes middle and high-layer encryption keys to ensure the critical security of the network.

Cipher X Encryption

The wire speed Cipher X 7210, 7211, and 7220 devices provide strategic-level communications security for global networks. They integrate seamlessly into existing or new networks without impacting network performance. The Cipher X family provides performance from 100 Mb/s to 10 Gb/s and is highly flexible, supporting a vast number of network configurations and a wide range of network security requirements.



Cipher X 7211 Encryptor



Multiple Layers of Protection

The KEYNET Network Security Manager consists of a Windows 7 ultimate rack mount server and 1RU tamper-proof hardware-based security vault. The security vault is outside the Windows environment and generates and deploys the middle and upper level keys used in TCC's three-tier symmetric key management hierarchy.

KEYNET securely communicates with all Cipher X Network Security Devices using SNMP with TCC's secure extensions. Additionally, device management is user authenticated to provide control and traceability of changes. Two levels of role-based security are provided: crypto officers have full control capabilities, while operators are restricted to monitoring privileges.

Benefits

- Easy to use, centralized management platform
- Automated key and device management requires little human interaction
- Hardware-based security vault protects highly critical keys
- Multiple layers of protection
- User-authenticated device configuration and deployment for traceability
- Manages remote software updates
- Simple provisioning and management of security policies
- Intuitive user-friendly interface
- Network expert not needed to manage network security

KEYNET Network Security Manager

KEYNET Network Security Manager

Flexible Network Configurations and Security Policies

KEYNET configures and monitors the robust Cipher X Family security policy enforcement engine. Policies indicate how data is treated in the encryptors, including: pass through, cipher or block. Policies are based on a wide range of configurable parameters such as VLAN tags, L2/3 source and destination addresses, L3/4 protocol and port numbers. The flexibility of the Cipher X's security policy engine provides wide-ranging support of network configurations and security requirements, while KEYNET simplifies their provisioning and management. Simple policy entries in KEYNET establish the policies without complex router reconfiguration required.



Status	ID	Device Name	Last Poll	Poll Result	Last CSM	CSM Result	IP Address	Inband IP	Ping Result
Success	1	Unit1	4/19/2013 4:02:51 PM	Success	4/11/2013 9:48:51 AM	Success	192.168.10.1	192.168.10.1	Reply from 192.168.10.1: bytes=32
No Changes	2	Unit2	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:48:59 AM	Success	192.168.10.2	192.168.10.2	Reply from 192.168.10.2: bytes=32
No Changes	6	Unit6	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:47:19 AM	Success	192.168.10.6	192.168.10.6	Reply from 192.168.10.6: bytes=32
No Changes	7	Unit7	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:49:14 AM	Success	192.168.10.7	192.168.10.7	Reply from 192.168.10.7: bytes=32
No Changes	10	Unit10	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:48:59 AM	Success	192.168.10.10	192.168.10.10	Reply from 192.168.10.10: bytes=32
No Changes	12	Unit12	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:48:07 AM	Success	192.168.10.12	192.168.10.12	Reply from 192.168.10.12: bytes=32
No Changes	15	Unit15	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:47:27 AM	Success	192.168.10.15	192.168.10.15	Reply from 192.168.10.15: bytes=32
No Changes	16	Unit16	4/19/2013 4:04:53 PM	No Changes	4/11/2013 9:48:43 AM	Success	192.168.10.16	192.168.10.16	Reply from 192.168.10.16: bytes=32

Unit: CX7211: L/Unit1

The Unit ID, IP Address and FPS Mode controls are not saved to the device but must match the device's values. Click "Save to KeyNet" to save the Initial Unit Setup.

Initial Unit Setup

Required for Communication: Unit Name: Unit1

Unit ID: 1 Description: Unit 1

IP Address: 192.168.10.1 Polling Interval (1-60 min): 5

FPS Mode: Disabled

Enable Management of This Device

Other Basic Unit Configuration

Unit Serial #: ECD003187 IP Traffic: Process

Public Mgt. State: PublicReadOnly Non-IP Traffic: Bypass

Throughput: 100 MB

Buttons: Poll Device, Save to KeyNet, Save to Device, Close

CX7211: L/Unit1

Unit | Security | NMEK Schedule | Status | Logs | Diagnostics | Multicast | Protocol Table | Unit Time | Version

Last Status Update: 4/19/2013 3:59:46 PM

Unit Up Time: 4:30:42 Hours

Unit Battery: Good

Reason for Last Reboot: Snmp Initiated

Warning Status Flags (DSCF)

Device Rebooted User Database Changed Configuration Change

Warning Logs/Taps

Fatal Logs: 0

Error Logs: 0

Warning Logs: 0

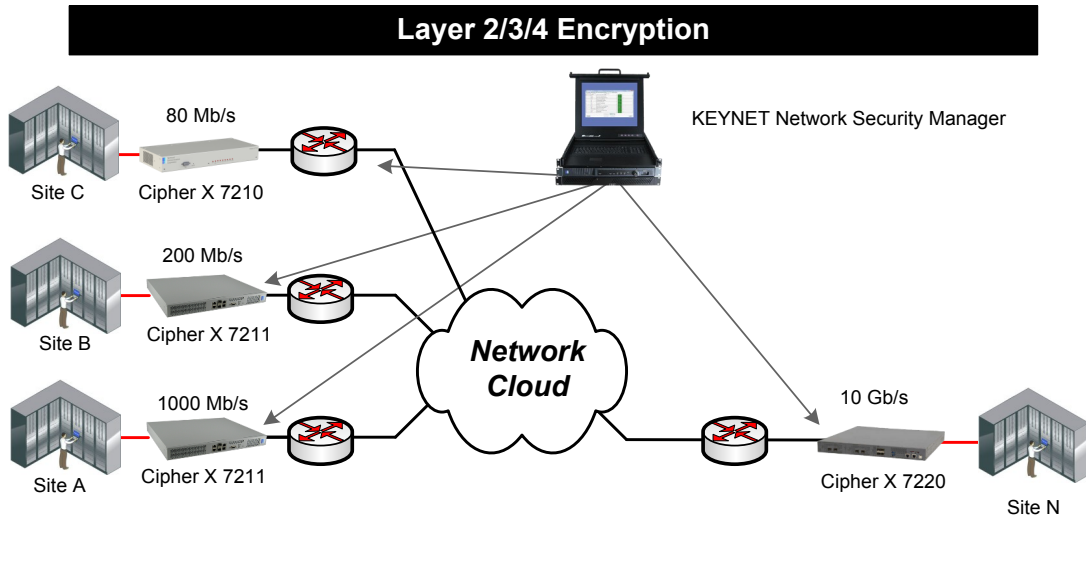
Buttons: Save to Device, Close

CX7211: L/Unit1

Filter By: Facility: Priority: Ordering: Newest Logs First

Log Source	Time (Local)	Device Time (Local)	Source	Facility	Priority	Log Message
L/Unit1	4/19/2013 4:01:53 PM	4/19/2013 4:01:53 PM	KeyNet	CSM	Debug	No mismatched KEKs/MACs, KEK change function returning without changing...
L/Unit1	4/19/2013 4:00:53 PM	4/19/2013 4:00:53 PM	KeyNet	CSM	Debug	No past due KEK bank change, will still check KEKs
L/Unit1	4/19/2013 4:00:52 PM	4/19/2013 4:00:52 PM	KeyNet	CSM	Debug	No past due KEK bank change, will still check KEKs
L/Unit1	4/19/2013 3:59:52 PM	4/19/2013 3:59:52 PM	KeyNet	CSM	Debug	No mismatched KEKs/MACs, KEK change function returning without changing...
L/Unit1	4/19/2013 3:59:52 PM	4/19/2013 3:59:52 PM	KeyNet	CSM	Debug	No past due KEK bank change, will still check KEKs
L/Unit1	4/19/2013 3:59:47 PM	4/19/2013 3:59:47 PM	KeyNet	SNMP	Debug	DevTimeStampFromDevice: 735449137, KeyNetQueueTimeTemp: 735449137
L/Unit1	4/19/2013 3:59:47 PM	4/19/2013 3:59:47 PM	KeyNet	SNMP	Debug	DevTimeStampFromDevice: 735449137, KeyNetQueueTimeTemp: 735449137
L/Unit1	4/19/2013 3:59:46 PM	4/19/2013 3:59:46 PM	KeyNet	SNMP	Debug	DevTimeStampFromDevice: 735297976, KeyNetQueueTimeTemp: 735297976
L/Unit1	4/19/2013 3:59:46 PM	4/19/2013 3:59:46 PM	KeyNet	SNMP	Debug	DevTimeStampFromDevice: 735297976, KeyNetQueueTimeTemp: 735297976
L/Unit1	4/19/2013 3:59:46 PM	4/19/2013 3:59:46 PM	KeyNet	General	Debug	Retained reader lock
L/Unit1	4/19/2013 3:59:46 PM	4/19/2013 3:59:46 PM	KeyNet	General	Debug	Computed device's counters against previous counters. Flag results: Current P...

Buttons: Refresh, Restore Default Column Widths, Log Messages At or Above Level, Log SQL Server Detail, Archive Acknowledged, Save to Device, Close



For more than 50 years, Technical Communications Corporation has specialized in superior-grade secure communications systems and customized solutions, supporting our CipherONE® best-in-class criteria, to protect highly sensitive voice, data and video transmitted over a wide range of networks. Government entities, military agencies and corporate enterprises in over 115 countries have selected TCC's proven security to protect their communications.

