

UCrypt®

UCrypt® Monitoring Server



The demand for efficiency & reduced operating costs are clear. Operators require centralized control of their video services delivery. The UCrypt® monitoring server provides quick access to real-time information such as the health & status of all deployed UCrypt devices. It acts as a central site & information repository that NOC personnel, anywhere, can access.

The UCrypt monitoring servers use syslog forwarding, SNMP, & HTTPS protocols, all using a customizable rule/trigger creation capability. This allows for the creation of rules for alerts based on combinations & timing of various syslog, SNMP or HTTPS events. These rules & triggers are based on ATX Networks' years of experience with field deployed UCrypt devices & on feedback from MSOs. These go beyond SNMP alerts interpreted individually & truly help NOC personnel manage their systems across their footprint.

MSOs can define how they want to receive information & who receives it. With the UCrypt monitoring server, devices can be grouped & sub-categorized to correspond to an MSO's organization scheme. Whether it is by region, by system, or another method, MSOs have the flexibility to monitor their UCrypts in a similar manner to their other deployed hardware. They can also configure the UCrypt monitoring server to provide customized reports based on that information.

User tracking & alert notifications are an important part of the capabilities of the UCrypt monitoring server. The system allows for the creation of multiple user accounts, so actions can be logged & tracked by user. It also enables specific users to be sent customized email alerts based on the received alert.

Yet another benefit of the UCrypt monitoring server is its flexible deployment on various platforms. MSOs can install the UCrypt monitoring server as a virtual machine* on their supplied servers (such as generic data center servers) or, if preferred, ATX can provide dedicated server hardware as part of the solution.



Features

Robust Monitoring & Alerting

- Real-time snapshot of system health
- Continuous monitoring of all deployed UCrypts
- Dashboard-based design for easy notification

Advanced Rule & Trigger Creation

- Default rules & triggers based on extensive in-field experience
- Beyond individual SNMP alerts
- Customizable rules for creating alerts using syslog, SNMP or HTTPS events

Flexible & Configurable

- Can be installed on a virtual machine, on a supplied server, or purchased with dedicated server hardware
- Custom & pre-configured reports
- Group & categorize units to correspond to the organization's deployment scheme

The screenshot shows the 'Monitoring Server Status' page. It features a table with columns: 'Instance ID / Host Address', 'Host / IP / Hardware', 'Site Name / Address / Location', 'Firmware / Config Version', 'Event Details', 'Account # / Account Name', and 'Hub ID / Management Area'. The table lists several devices, some with active alerts highlighted in red. Navigation tabs at the top include STATUS, EVENTS, PROFILES, and SYSTEM.

The screenshot shows the 'Profiles, Triggers and Notifications' page. It includes a table of 'Trigger Scripts' with columns for 'Profile', 'Product', and 'Trigger Scripts'. Below this is a table of 'Alert Rules' with columns for 'Trigger Scripts', 'Error Type', 'Trigger', 'Notification Type', and 'Alert Details'. The interface includes tabs for PROFILES, TRIGGERS, and NOTIFICATIONS.

The screenshot shows the 'System Configuration' page. It contains several sections: 'Network Configuration' (Configure Network, Configure Syslog Forwarding, Configure Trap Destination Server), 'User and LDAP Configuration' (Configure Users, Configure LDAP), 'System Location' (Physical Location, System Date), 'System Status' (OS Release, System Date, System Time, System Time, System Time, System Time), and 'License' (License Key, License Key, License Key). The page includes various input fields and buttons for configuration.

* When configured as a virtual machine, the UCrypt monitoring server requires the following minimum server resources:

PROCESSOR: 6 Cores (2.6 GHz)
RAM: 8 Gigabytes (GB)
HARD DISK SPACE: 120 GB
OPERATING SYSTEM: CentOS 7.0

Any use of the UCrypt product, directly or indirectly, for the decryption and unauthorized reproduction of content that constitutes or may constitute copyright infringement or otherwise infringes on the proprietary rights of any third party is expressly prohibited. No user of UCrypt shall use UCrypt for any purpose or in any manner which, directly or indirectly, violates the law, violates the proprietary rights of any other party, or aids in any unlawful act or undertaking including, without limitation, laws governing data privacy, international data transmission, and export of technology or data. Any multiple systems operator or other similar party ("MSO") will use the UCrypt product in strict compliance with all applicable laws and in compliance with any agreement in effect between the MSO and a content provider. In no event shall ATX Networks Corp. or any of its affiliates be liable to an MSO, any end user of the UCrypt product, or any other third party, for any claims arising out of or related to any use or misuse of the UCrypt product in contravention of this disclaimer. It is the express obligation of an MSO to convey this disclaimer to any other end user of the UCrypt product.

UCrypt® is a registered trademark of ATX in the United States and/or other countries. Products or features contained herein may be covered by one or more U.S. or foreign patents. Other non-ATX product and company names mentioned in this data sheet are the property of their respective companies..

© 2019 by ATX Networks Corp. and its affiliates (collectively "ATX Networks Corp."). All rights reserved. This material may not be published, broadcast, rewritten, or redistributed. Information in this document is subject to change without notice.
Rev. 11/19 (ANW1219)



ATX Networks

Tel: 289.204.7800 | Toll-Free: 866.YOUR.ATX | support@atx.com