

# HUAWEI UMA Full Product Datasheet



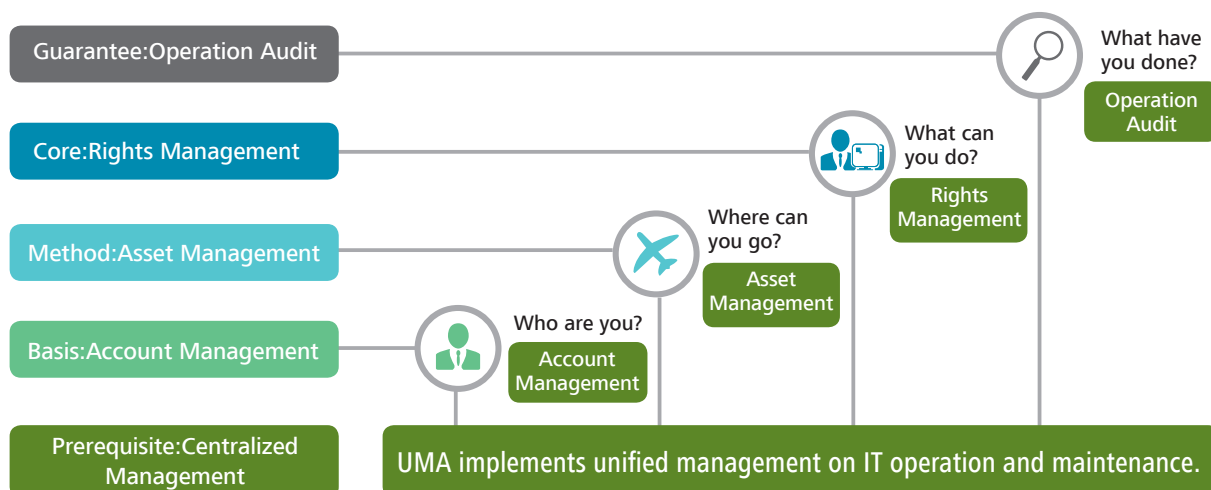
# HUAWEI UMA

## Brief Product Datasheet



### Product Overview

HUAWEI Unified Maintenance Audit (UMA) system centrally manages, monitors, and audits operations of all operation and maintenance (O&M) personnel in an enterprise, reducing internal O&M risks of network devices, servers, databases, and service systems to perfect enterprise IT management systems. In addition, the UMA meets related audit regulations and standards.



HUAWEI UMA serves as a unified management platform for enterprise IT O&M operations. It prevents unordered connections between humans (operators) and hosts (operated objects) and separates management data streams from service data streams. By centrally managing user operations and behaviors, HUAWEI UMA enables comprehensive account management, asset management, permission management, and operation audit, building a standardized and orderly network and controlling resource use behaviors.

## Product Features

### Account management

- User management: Management of users by group for simplified permission assignment
- Batch user import: Import of specified formats of user information in batches
- Open extended authentication system: The open, flexible, and scalable authentication system structure supports local static password authentication and third-party authentication modes including Radius, dynamic password card, PKI, and AD domain

### Asset management

- Device management: Management of devices by group for simplified permission assignment
- Device import: Import of specified formats of device configuration information in batches
- Device types: Support for routers, switches, security devices, servers, databases, and service systems from multiple vendors
- Account password management: Auto-fill and periodic change of device account passwords for centralized management

### Permission management

- Permission level settings: HUAWEI UMA assigns different permissions to different types of users. Supported user types are super administrator, asset administrator, permission administrator, password administrator, audit administrator, and user.
- Central permission management: User permissions on device assets are centrally managed. Group permission assignment is supported for simplified management.
- Access control: Access control policies can be based on user, device IP address, login IP address, device account, date, time, command set, idle time, or any combination of these parameters.

### Operation audit

- Protocols and applications: HUAWEI UMA supports character terminals (SSH and Telnet), graphic terminals (RDP, VNC, X11), web applications (HTTP and HTTPS), file transfer protocols (FTP and SFTP), database management tools, KVM, and self-defined enterprise applications.

- Audit log playback, monitoring, interruption, and query: All audit logs are recorded in the unit of session. A session can be played back as a whole or from a certain command statement. Connected sessions can be monitored in real time and interrupted. Users can input command names to search for sessions.
- Character terminal audit: HUAWEI UMA supports intelligent semantic-level command capturing, which audits the full process of user operations. Command capturing and identification are not affected by the types of terminals used by customers. The UMA ensures complete and accurate audit on any client and any type of terminal and supports audit of all function keys. Users can online edit multiple lines of ultra-long commands generated after function key operations are captured.
- Graphic terminal audit: HUAWEI UMA records audit logs on graphic terminals in data formats without frame loss, reducing the required amount of recorded log data. Audit logs are played back in videos through real-time calculation. The videos have no frame loss and support seeking, fast-forward, and fast-rewind. Keyboard commands on graphic terminals can also be audited.
- Database operation audit: Database operations can be played back, and submitted SQL statements and results are recorded.
- Graphic application interaction audit: Audit logs are played back in videos through real-time calculation. The videos have no frame loss and support seeking, fast-forward, and fast-rewind. Keyboard commands on graphic terminals can also be audited.
- File transfer audit: The audit of file transfer and clipboard operations can be enabled or disabled on demand.
- Automatic system audit: The login and configuration of all system accounts are audited and recorded by the system.
- Audit report: Default audit reports are provided. Alternatively, users can develop audit reports.





## Highlights

### Comprehensive account management mechanism

- After back-end system accounts are automatically filled in, each O&M engineer manages one account only to eliminate the risks caused by borrowing multiple accounts.
- Functions such as periodic modification, encrypted transfer, and backup/download are provided for service systems, reducing the workload of password maintenance.

### All-around recording of IT O&M

- O&M of various operations including command line characters, graphical operations, text input, database operations, and KVM operations are recorded in the forms of text and video.
- Fine-grained query prevents malicious O&M by accurately identifying the person responsible for certain operations.

### Pioneering technologies

- APPBOX allows users to extend various O&M applications without the need to install any client plug-in on the target device.
- OCR image identification technology summarizes graphical operations in text and intelligently identifies operations to avoid watching an entire video, facilitating fast query and audit.

### Industry-leading hardware architecture

- The UMA hardware is based on Huawei-developed T3000 platform that provides redundant hot-swappable fans and power supplies, delivering high reliability and telecom-level operating.
- Clustered deployment enables access of thousands of devices and provides load balancing and robust reliability.

## Customer Benefits

### Standardized O&M operation management

- The UMA serves as a uniform O&M access management and resource control platform that provides a uniform access portal and centralized permission control. The platform uniformly manages access and maintenance of various systems, including account management, authentication, and permission assignment. The permission-specific access control at the network layer and application layer enhances system security.
- Unified and standardized maintenance relieves administrative pressure and improves work efficiency.

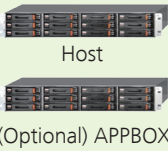
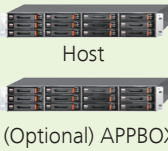
### Reduced resource risks

- The UMA uses a bastion host to prevent unauthorized and insecure terminals from directly accessing core resources, as well as reduce impacts of Trojan, spyware, and internal security risks on core resources.
- The UMA guards against external risks by standardizing third-party maintenance and system integrators' onsite operations.
- Operation records are helpful in accident tracking and liability assessment.

### Compliant with related regulations

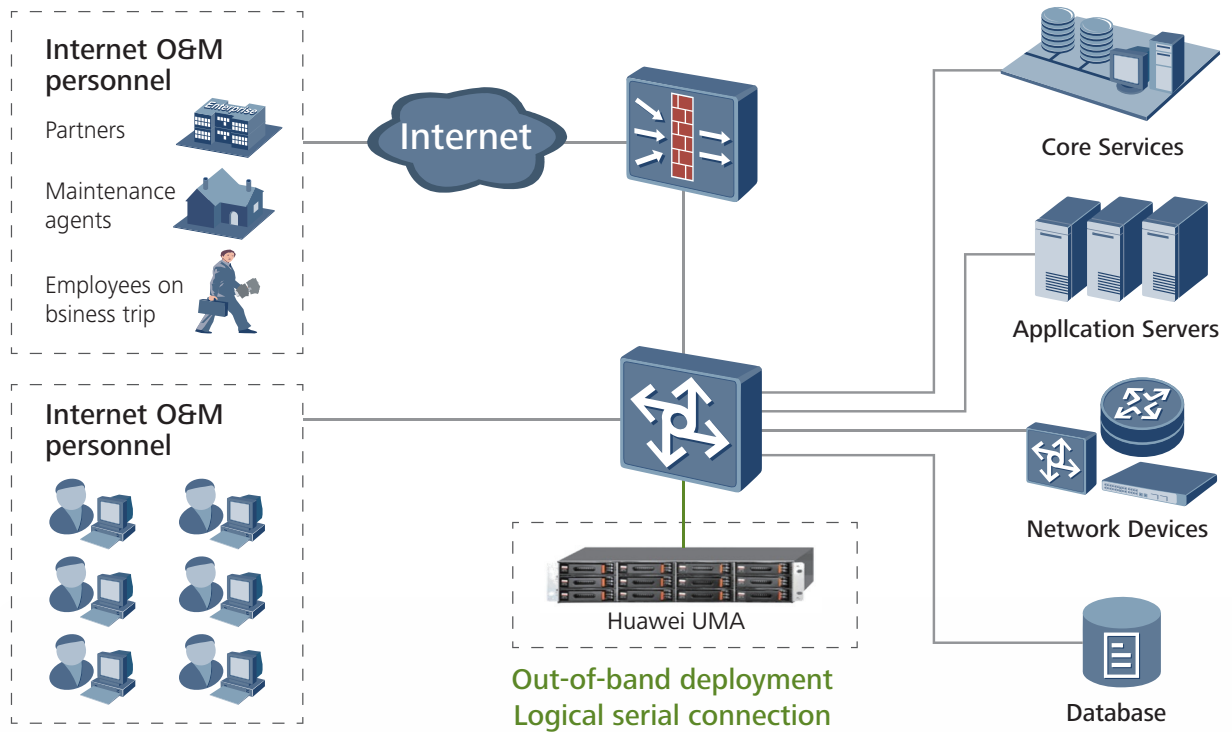
- The UMA complies with laws and regulations such as IT internal control guidelines, the SOX, and the COBIT.
- Audit reports and original O&M logs are available for supervision institutions.
- The UMA perfects customers' IT internal control and audit systems to help ensure a successful IT audit.

## Product Specifications

Model	UMA Standard Edition	UMA Enterprise Edition
Intended customer	Small- and medium-sized enterprises	Large-sized enterprises
Hardware appearance	 <p>Host (Optional) APPBOX</p>	 <p>Host (Optional) APPBOX</p>
Host specifications	Height: standard 2 U rack CPU: 1 x Intel quad-core E5-2403 Memory: 1 x 8 GB Power supply and fan: 1+1 redundant power supplies and fans System disk: 2 x 300 GB SAS in RAID 1 mode Data disk: 2 x 2 TB SATA in RAID 1 mode (scalable to 12 x 2 TB) Network ports: onboard 6 x GE ports (scalable to 14 GE ports)	Height: standard 2 U rack CPU: 2 x Intel quad-core E5-2403 Memory: 2 x 8 GB Power supply and fan: 1+1 redundant power supplies and fans System disk: 2 x 300 GB SAS in RAID 1 mode Data disk: 2 x 2 TB SATA in RAID 1 mode (scalable to 12 x 2 TB) Network ports: onboard 8 x GE ports (scalable to 14 GE ports)
APPBOX specifications	Height: standard 2 U rack CPU: 1 x Intel quad-core E5-2403 Memory: 1 x 8 GB Power supply and fan: 1+1 redundant power supplies and fans System disk: 2 x 300 GB SAS in RAID 1 mode Data disk: 2 x 2 TB SATA in RAID 1 mode (scalable to 12 x 2 TB) Network ports: onboard 4 x GE ports (scalable to 14 GE ports)	Height: standard 2 U rack CPU: 1 x Intel quad-core E5-2403 Memory: 1 x 8 GB Power supply and fan: 1+1 redundant power supplies and fans System disk: 2 x 300 GB SAS in RAID 1 mode Data disk: 2 x 2 TB SATA in RAID 1 mode (scalable to 12 x 2 TB) Network ports: onboard 4 x GE ports (scalable to 14 GE ports)
Concurrent connections	Character terminal: 500 Graphic terminal: 200	Character terminal: 1000 Graphic terminal: 300
Number of managed devices	50/100/200/300	500/1000/more (clustering)
Types of managed devices	Router, Switch, Firewall, Windows/Linux/Unix Servers	
Types of managed applications	UMA host supports: <ul style="list-style-type: none"> <li>• Character terminals such as telnet and SSH</li> <li>• Graphic terminals such as RDP, X11, and VNC</li> </ul> APPBOX supports: <ul style="list-style-type: none"> <li>• Web-based operations such as HTTP and HTTPS</li> <li>• Databases including Oracle, DB2, Sybase, SQLServer, Informix, MySQL, and PostgreSQL</li> <li>• Remote graphic control tools including pcAnywhere, Radmin, DameWare, ESXI, and AS400</li> <li>• KVMs including Avocent, Ranitan, and ATEN</li> <li>• Other private O&amp;M systems such as U2000 network management system</li> </ul>	
User management	<ul style="list-style-type: none"> <li>• User permission level setting, account lifecycle management, user group, and batch user import</li> </ul>	
Authentication management	<ul style="list-style-type: none"> <li>• Local authentication, Radius authentication, AD domain authentication, certificate authentication, and open extended authentication system</li> </ul>	
Device management	<ul style="list-style-type: none"> <li>• Management at device, device group, and device account levels</li> <li>• Single modification, periodic authentication, and automatic fill-in and delivery of account passwords</li> </ul>	
Permission management	<ul style="list-style-type: none"> <li>• Permission is granted to users by device IP, protocol type, or account password.</li> <li>• Devices are accessible to administrators who have permission to manage the devices.</li> <li>• Permission assignment by device group or user group</li> </ul>	
Security audit	<ul style="list-style-type: none"> <li>• Playback of command-line operations, graphics and videos, keyboard commands, and operation logs</li> <li>• Summary of graphic operations in text for intelligent operation identification</li> <li>• Risky command policy creation and automatic identification and interruption of risky command execution</li> <li>• Real-time monitoring and interruption of user operations</li> </ul>	
Deployment mode	<ul style="list-style-type: none"> <li>• Out-of-band deployment with no change to original network structure</li> <li>• Single-host, dual-host, clustered, and tiered deployment</li> </ul>	

## Application Scenario

Deploying the UMA system enables centralized management of an enterprise's O&M operations without change to original network topology and impact on service data streams.



- Deployment mode: The UMA is physically deployed out of band and works as a logical gateway.
- Deployment requirement: The UMA's IP address is reachable to accessed devices.
- Reliability: Dual-host hot-backup, clustering, and tiered deployment modes are supported.







**Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

**Trademark Notice**

 , HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd. Other trademarks, product, service and company names mentioned are the property of their respective owners.

**General Disclaimer**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO.,LTD.  
Huawei Industrial Base  
Bantian Longgang  
Shenzhen 518129,P.R.China  
Tel: +86 755 28780808

[www.huawei.com](http://www.huawei.com)