Huawei Agile Controller-Campus Datasheet

The Agile Controller-Campus is a policy control system developed by Huawei for campus networks. It can centrally control user rights, quality of service (QoS), bandwidth, applications, and security policies over campus networks, making networks more agile for services.

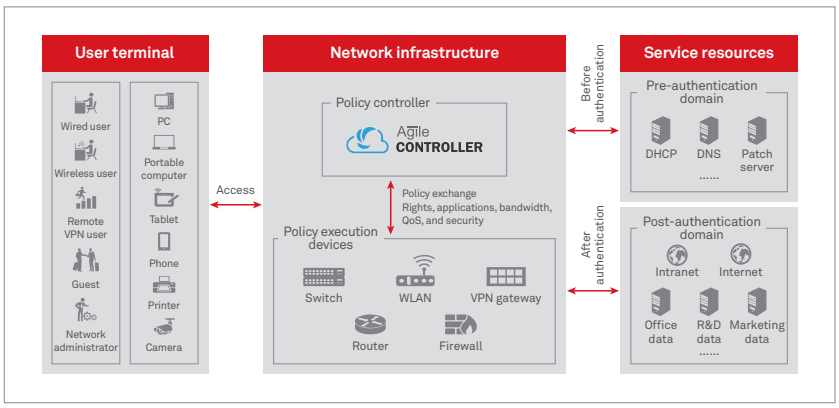
The Agile Controller-Campus provides unified network access and management for employees, guests, and device administrators, and is applicable in various sectors requiring identity authentication and authorization, including finance, government, education, healthcare, and hospitality.

Product Description

User terminals (information receivers) are not fixed in certain physical locations for services deriving from mobile office, bring your own device (BYOD), and wireless local area network (WLAN). These types of services pose the following challenges on statically configured traditional networks:

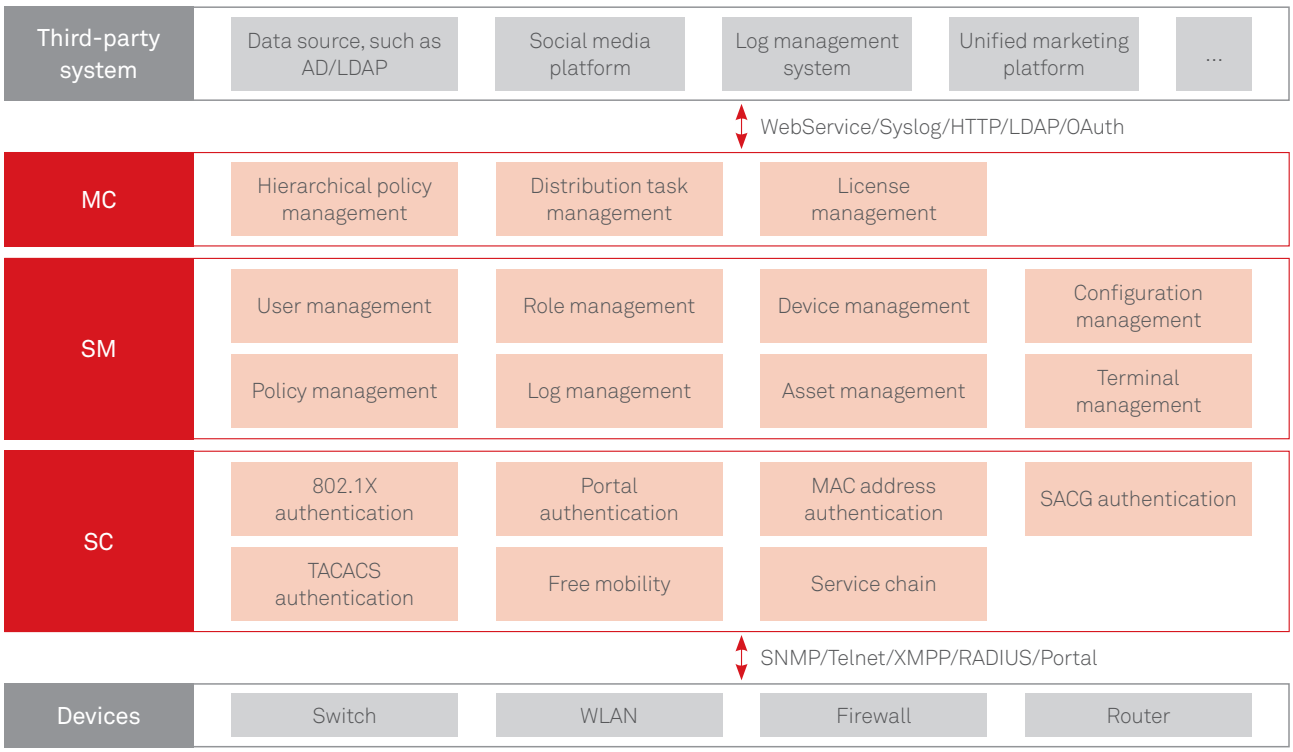
- How can a consistent experience be guaranteed for user terminals in different locations?
- How can user rights, QoS, bandwidth, applications, security, and other network policies be configured dynamically?
- Traditional networks enable users to be bound to physical interfaces whereby the administrator manually configures policies on the devices closest to users. In contrast, manual configuration cannot adapt to changes in user locations. To meet the requirements of mobile users, networks must support dynamic resource allocation and policy configuration; that is, network resources and policies must be able to migrate to users.

In Huawei Next-Generation Network Access Control (NAC) Solution, the Agile Controller-Campus provides unified network access and management for employees, guests, and device administrators, centrally controls user rights, QoS, bandwidth, applications, security, and other network policies, and implements enterprise service policies. This guarantees a good user experience and allows networks to provide more agile support for services.



Key Components

Using an open architecture design, the Agile Controller-Campus can interconnect with third-party network systems using northbound WebService, Syslog, HTTP, LDAP, or OAuth interfaces, and interconnect with network devices through southbound SNMP, Telnet, XMPP, RADIUS or Portal interfaces.



The Agile Controller-Campus adopts a hierarchical architecture design that is composed of Management Center (MC), Service Manager (SM), and Service Controller (SC). These components are described as follows:

- **MC:** Is responsible for uniformly distributing and managing hierarchical policies, distribution tasks, and licenses for the lower-level SM. One system has only one MC, available in the hierarchical deployment mode.
- **SM:** Performs service configuration and resource management, including user management, device management, configuration management, and log management. One system has only one SM.
- **SC:** Interconnects with network devices and performs authentication. One system supports multiple SCs, and new SCs can be added flexibly.

Benefits

Integrated Access

- Features integrated wired and wireless access and supports various authentication protocols, including 802.1X, Portal, MAC address, security access control gateway (SACG), and Terminal Access Controller Access Control System (TACACS).
- Provides unified network access and management for employees, guests, device administrators, and dumb terminals.
- Provides full lifecycle guest self-service and supports social media authentication.

Guaranteed User Experience

- Provides unified management on user rights, QoS, bandwidth, applications, and security policies.
- Supports scenario-based authentication and authorization, including the user account, time, location, terminal type, and access mode.

- Supports boarding management to automatically deliver terminal configurations and certificates, simplifying user access.

Improved Efficiency

- Supports matrix-based policy configuration to simplify network-wide policy planning.
- Supports drag-and-drop operations in graphical user interfaces (GUIs) to improve network operations and maintenance (O&M) efficiency.
- Supports the What You See Is What You Get (WYSIWYG) Portal editor and provides various system templates to enable marketing advertisements to be published in a timely manner.

Flexible and Open

- Features a flexible architecture design that supports distributed and hierarchical deployment modes.
- Features an all-round, reliable design to ensure consistent services.
- Features an open design, provides application programming interfaces (APIs) for secondary development, and supports interconnection with third-party systems.

Key Features

Access Management

Advances in Information and Communication Technologies (ICT) mean that enterprise users require network access from anywhere. However, enterprise information security is at risk when high numbers of mobile staff and partners frequently use their own terminals (such as laptops) to access the enterprise's local area networks (LANs). Unauthorized terminals may infect enterprise networks with viruses and, in worst case scenarios, phish trade secrets. In addition, the maturity of WLAN technologies and prevalence of intelligent terminals prompt many enterprises to open their intranets for guests and partners. In public areas (such as, shopping malls, hotels, exhibition halls, chain stores, scenic spots, business halls, and airport lounges), enormous advertising opportunities are created by the huge number of users accessing WLAN.

The access management component of the Agile Controller-Campus controls the network access for employees and guests, and implements unified access policy management. It also provides flexible authentication and authorization policies to meet the service control needs of different enterprises. In addition, it provides full lifecycle guest management, WYSIWYG page customization, and social media authentication. All these functions help enterprises simplify Wi-Fi management service and assist enterprises in advertising and marketing.

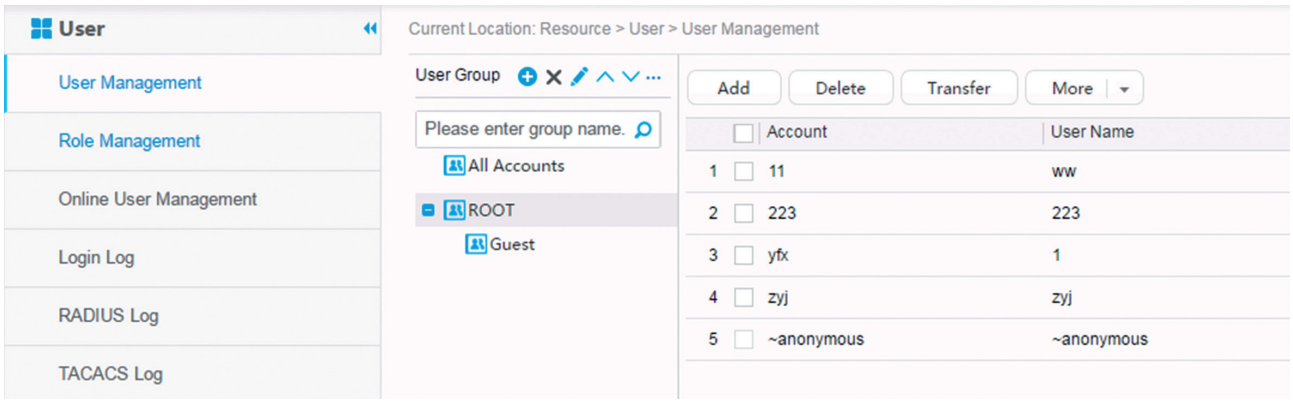
Comprehensive Access Authentication Modes for Different Application Scenarios

Authentication Mode	Characteristics	Application Scenarios
802.1X authentication	• Enables the 802.1X function on a switch or AC. • Implements Layer 2 isolation. • Complicates maintenance due to multiple authentication points. • Requires the switch to support 802.1X.	Applies to small, medium, and large campus networks with high security requirements. The Access Control component can associate with Huawei full-series Sx7 switches, routers, WLAN devices, and third-party standard 802.1X switches.
MAC address authentication	• Enables the switch or AC to automatically activate 802.1X or MAC address authentication for different terminals. • Authenticates terminals on the authentication server based on MAC addresses.	Applies to dumb terminals such as IP phones and printers.
Portal authentication	• Configures a combination of Portal and MAC address authentication on devices at the aggregation layer. Devices select authentication modes based on terminal type. The AC unifies wireless user authentication. • Makes clients optional on terminals based on service requirements. • Does not require access switches to support 802.1X.	Applies to small, medium, and large campus networks, especially in scenarios with no client installed. Associates with Huawei full-series Sx7 switches, AR routers, WLAN devices, and third-party CMCC Portal-supported devices.

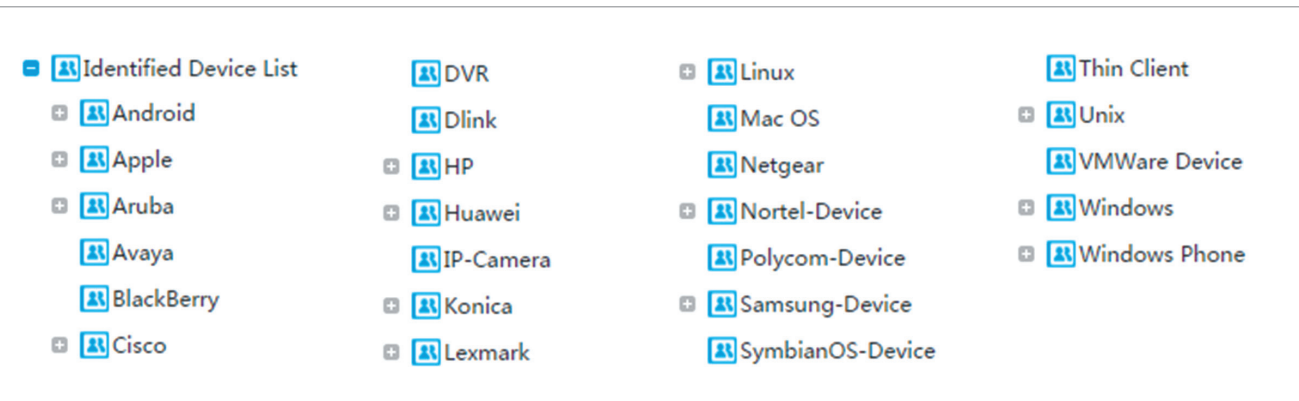
Context-Awareness Authentication and Authorization, Implementing Refined Policy Control

Dimension	Description	Example
Who	User identity	Administrative personnel, ordinary employees, VIP users, guests
Where	Access location	R&D area, non-R&D area, home
When	Access time	On-duty time, off-duty time, work days
Whose	Device source	Enterprise devices, BYOD devices
What	Device type	Windows, Linux, iOS, Android
How	Access mode	Wired, wireless, VPN, Internet

Satisfying Complex Enterprise Requirements with Two-dimensional (User Group + Role) User Management



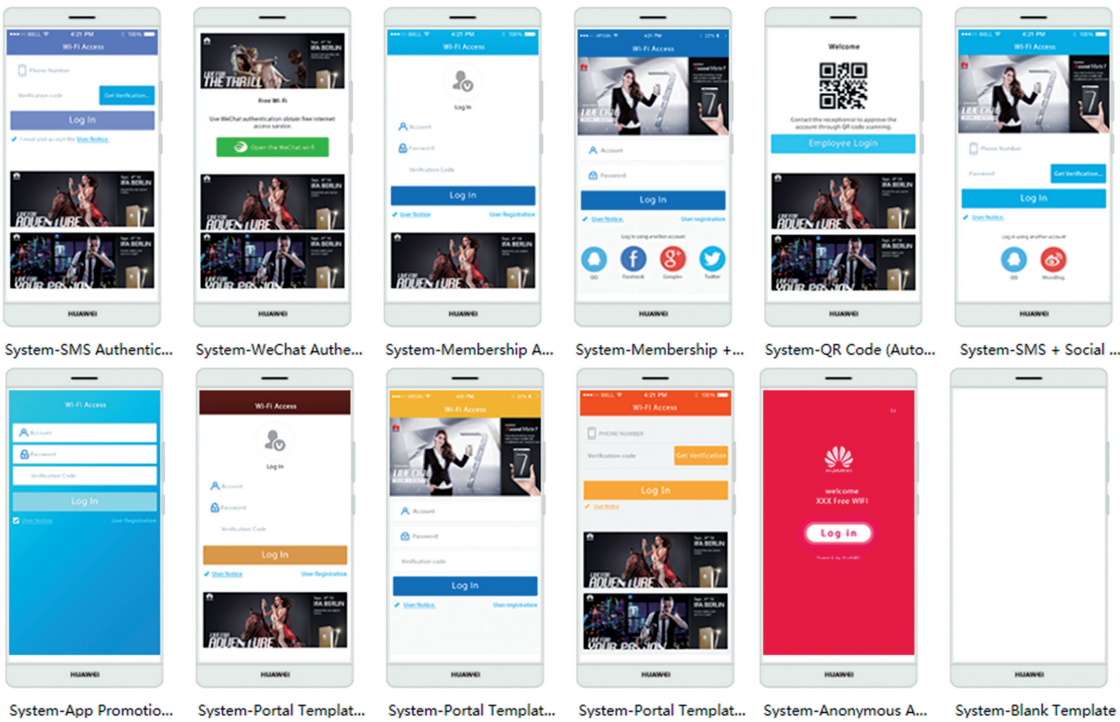
Intelligent Terminal Identification for Rights Control on BYOD Terminals



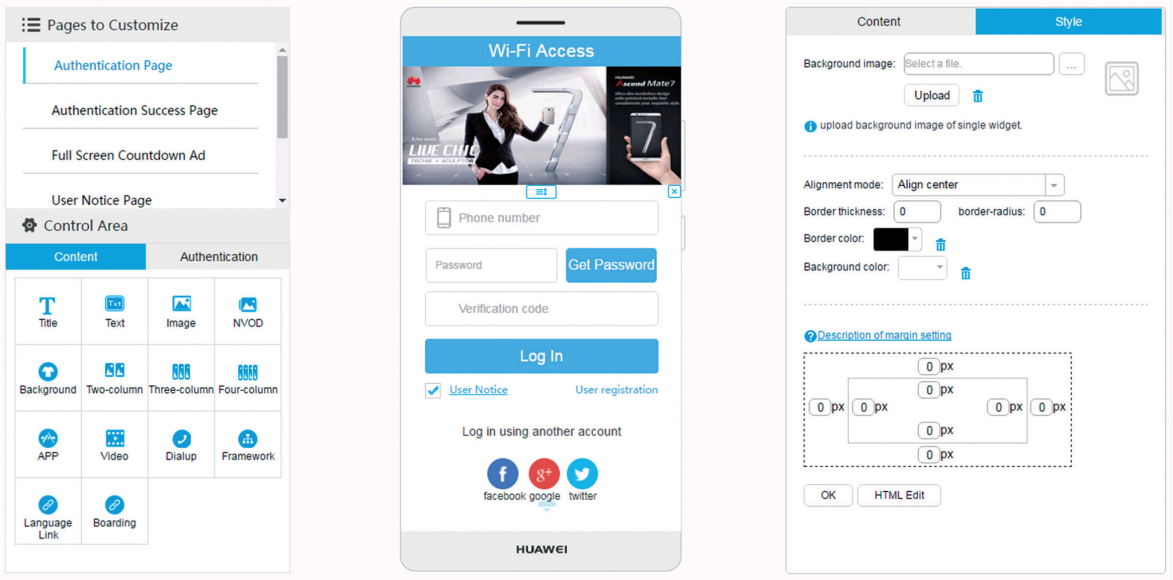
Full Lifecycle Guest Self-Service, Meeting On-demand Requirements of Enterprises

Phase	Options
Registration	• Registration-free • Self-service guest registration • Account creation by administrator
Approval	• Automatic approval • Administrator approval • Receptionist approval • Approval through email activation • Receptionist approval (QR code scanning)
Distribution	• SMS (SMS modem and SMS gateway) • Email • Web
Authentication	• Authentication-free • Account and password authentication • Passcode authentication • Mobile phone verification code authentication • QR code authentication • Social media authentication
Audit and deregistration	• User login and logout audit • Automatic deregistration after expiration • Scheduled account deletion

Various, Exquisite System Templates to be Selected Based on Scenarios



WYSIWYG Portal Editor, Reducing Skill Requirements for Page Customization

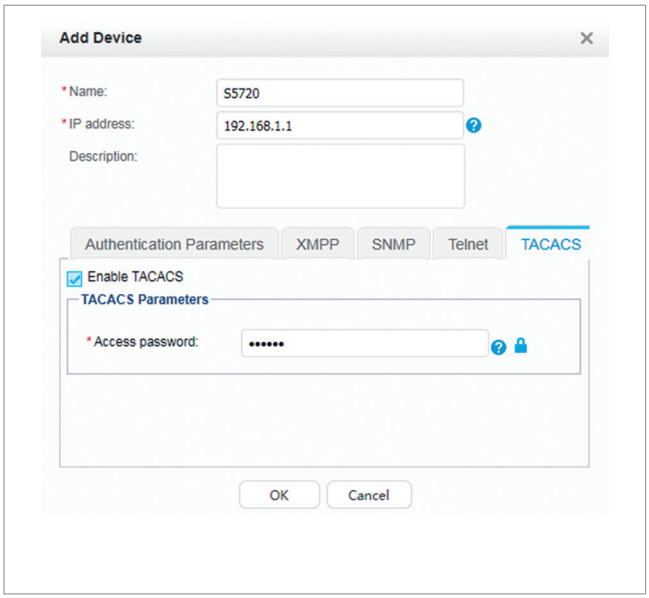


TACACS Management

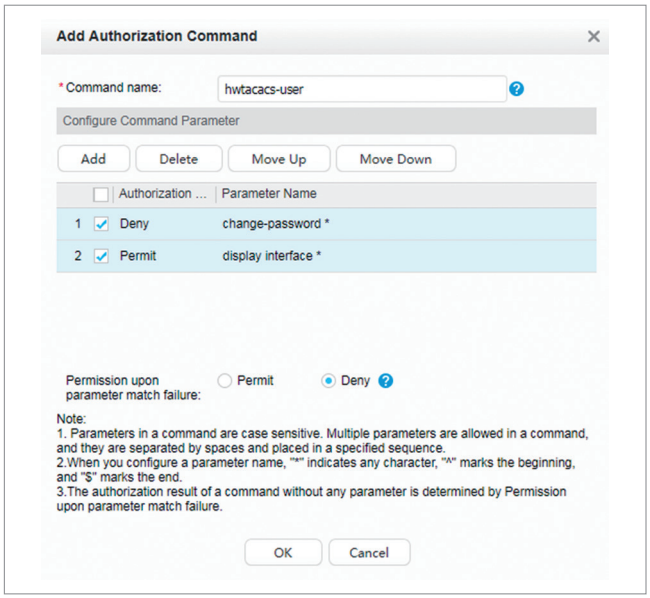
As networks expand and the number of devices increases, network administrators require a standard, clear, and unified network O&M to guarantee consistent services. TACACS authentication can authenticate common users logging in through 802.1X or Portal, and administrative users logging in through serial port, Telnet, SSH, or FTP. TACACS authorization can authorize common access users and administrative users. In addition, it can authorize each command line configured by administrators.

The TACACS Manager of the Agile Controller-Campus uniformly verifies all administrative users attempting to access devices, offers fine-grained authorization of configuration commands on each device, and audits and traces configuration changes of network devices.

Verification on Network Administrators Accessing Devices



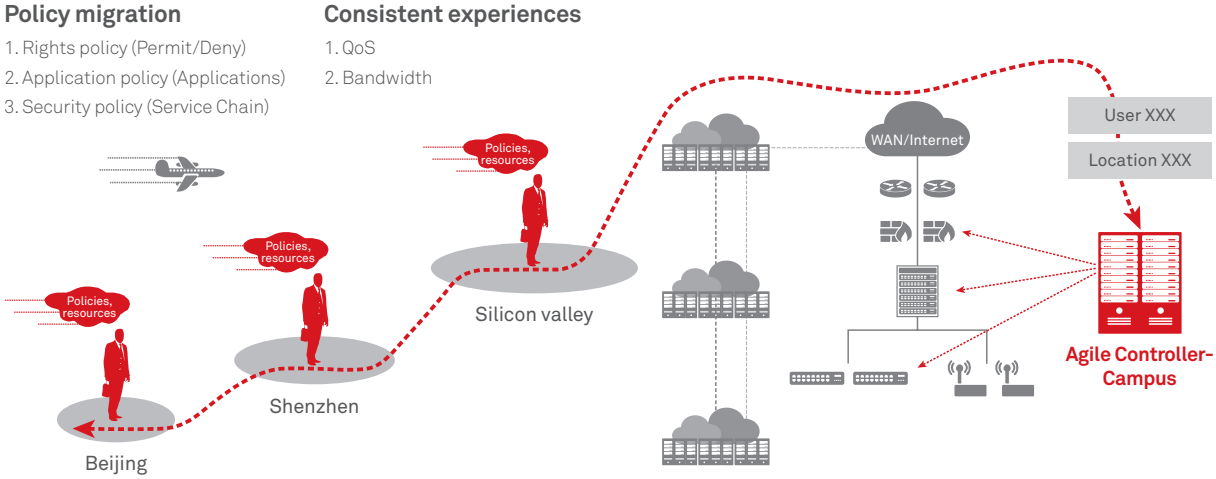
Fine-grained Authorization for Command Lines



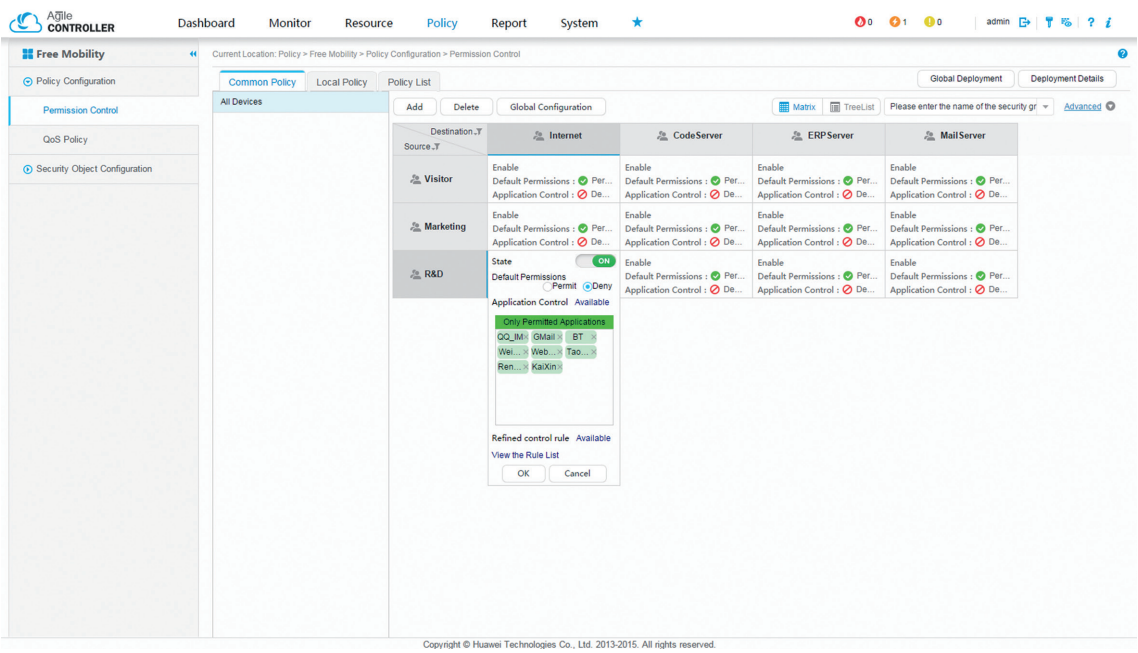
Free Mobility Management

With the popularity of mobile office and BYOD applications, users need to access enterprise networks from HQ, branches, and even on business trips. Employees of different roles start to work in the same area, physical locations of terminals are no longer fixed, and users frequently handle business on their own terminals. Additionally, guests and partners access the intranet, resulting in an increasing number of user types as well as intranet security risks. In this case, isolation is necessary. It becomes a common concern for enterprises to ensure consistent QoE for users who access networks using different terminals at different places and to isolate the users for security.

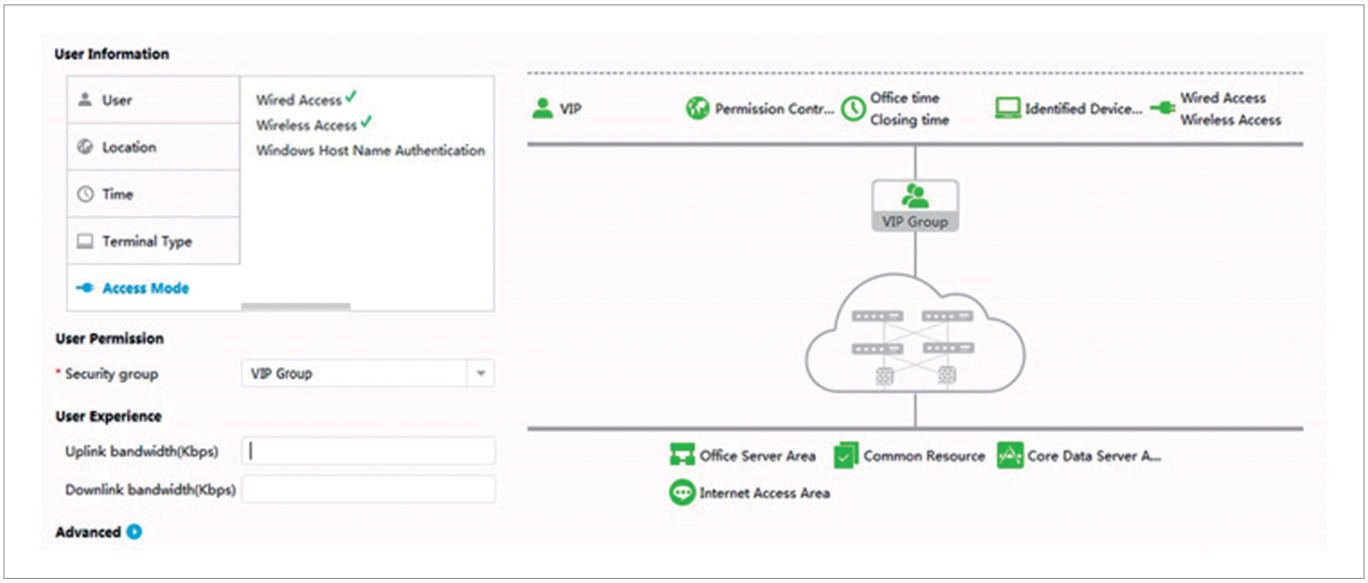
The free mobility management component of the Huawei Agile Controller works with Huawei agile switches, NGFWs, or SVN gateways to provide a brand-new policy orchestration matrix, implementing unified planning and automatic deployment of rights, applications, bandwidth, QoS, and security policies based on security groups. Users can then receive a consistent service experience when they move on the network.



Innovative, Matrix-based Policy Management, Simplifying Network-wide Policy Planning



Brand-new, 5W1H-based Fast Authorization, Allowing for Easier O&M

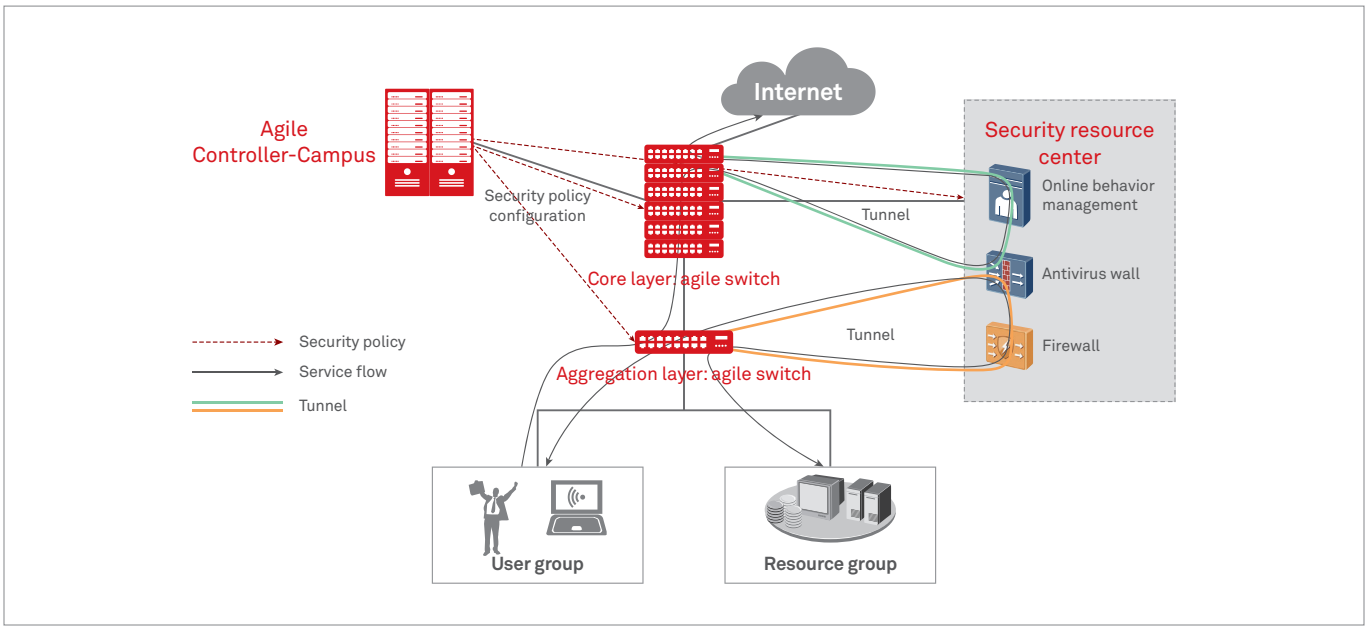


Graphical, Multi-level QoS Policy Configuration, Ensuring Consistent Service Experience for Users

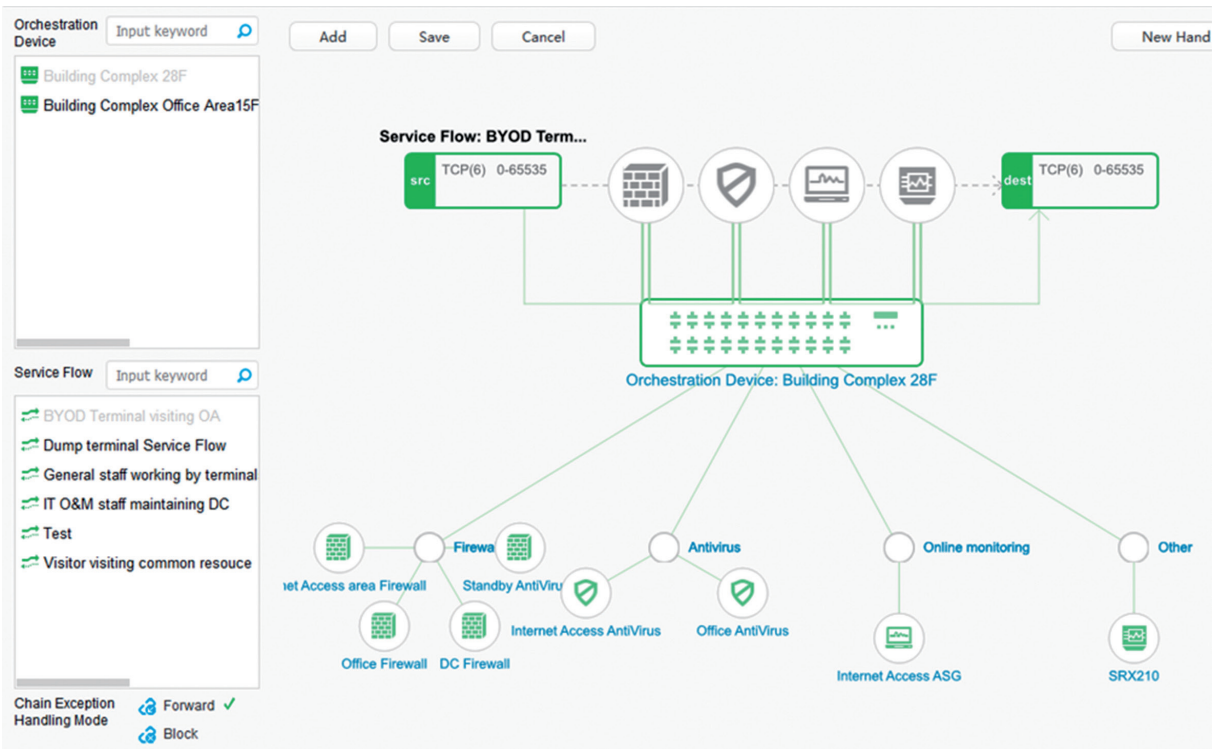
Service Chain Management

Traditional security solutions used on enterprise campus networks and data center networks define network borders. Security devices such as firewalls, anti-DDoS, antivirus (AV) software, the intrusion prevention system (IPS), and data loss prevention (DLP) devices are deployed on borders with different security levels. As networks expand, users connect to networks using more diverse access methods. Traditional security deployment results in the investment of enterprises increasing exponentially. In addition, many customers calculate the number of security devices they need to purchase based on data usage that is two to five times that during peak-hours. However, high-performance security devices, such as firewalls, IPS, and anti-DDoS have low resource utilization, which wastes resources.

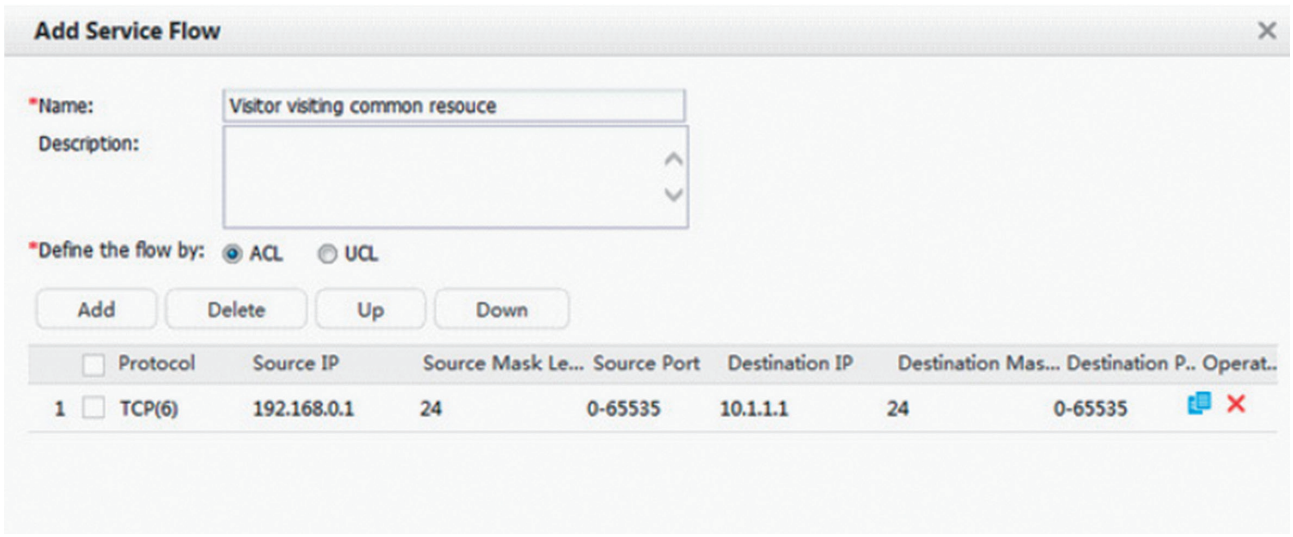
The service chain management component of the Agile Controller-Campus permits the resource pooling of physical security devices, screens specific physical forms and locations, and creates a security resource center. It sends traffic to the security resource center according to service requirements, where the traffic is inspected and processed. This increases the usage of physical resources and reduces network construction costs.



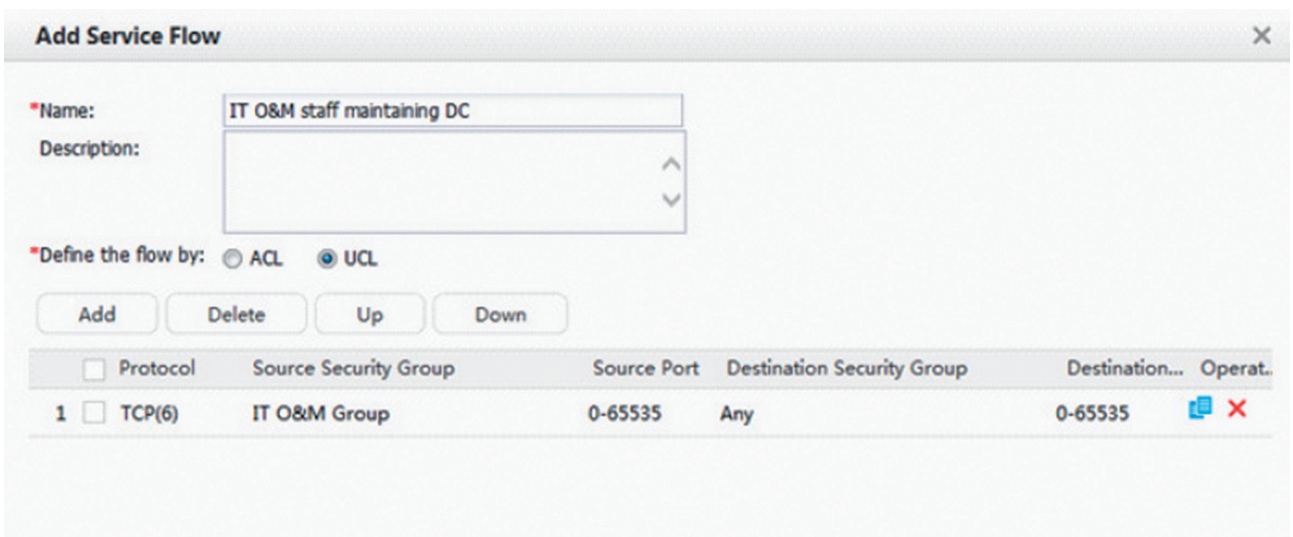
Physical Security Resource Virtualization and Service Flow-based Resource Scheduling, Providing In-depth Security Protection
Graphical Policy Orchestration, Implementing Differentiated Traffic Import Policies for Different Services



Service Chain Creation by Service Flow, Service Flow Definition by Source and Destination IP Addresses, Source and Destination Port Numbers, and Protocol



Service Chain Creation by Service Flow, Service Flow Definition by Source and Destination User Groups, Source and Destination Port Numbers, and Protocol



Specification List

Item	Description
Authentication management	Supports 802.1X, Portal, MAC address, and SACG authentication.
	Supports PAP, CHAP, EAP-MD5, EAP-PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS-PAP, and EAP-PEAP-GTC identity authentication protocols.
	Supports anonymous authentication, account authentication, certificate authentication, AD/LDAP authentication, third-party database authentication, and RADIUS relay authentication.
	Supports two-factor authentication (user name and password + mobile phone verification code).
	Supports social media authentication (Facebook, Twitter, Google+, WeChat, QQ, and Sina Weibo).
	Supports an escape mechanism. When an AD/LDAP server breaks down, users directly pass authentication.
Authorization management	Supports authorization based on user groups, accounts, roles, SSIDs, time ranges, terminal IP addresses, terminal device groups, access device groups, and terminal compliance check results.
	Supports authorization based on the dynamic ACLs, static ACLs, VLANs, user groups, and security groups.
	Supports online duration control to limit the one-time online duration and accumulated online duration of terminals.
Terminal identification	Supports the following terminal identification modes: Simple Network Management Protocol (SNMP), User-Agent, DHCP, and MAC organizationally unique identifier (OUI).
	Supports various terminal types such as PCs, smart phones, tablets, dumb terminals, IP phones, and printers.
	Supports Windows, Linux, macOS, Android, iOS, and Windows Phone operating systems.
	Identifies information about vendors such as Huawei, Samsung, Apple, HTC, and Lenovo.
Boarding management	Automatically delivers 802.1X configurations (EAP-TLS or EAP-PEAP) to terminals.
	Interworks with the Windows CA server to deliver certificates.
	Provides network access policies by terminal type and user group.
	Supports automatic device registration, manual report of device loss, and restriction on lost devices.
	Supports terminals running Windows, Android, and iOS operating systems.
TACACS management	Verifies the identity of network administrators before they access devices.
	Supports fine-grained authorization for command lines.
Guest service	Provides guest self-services such as account registration, password changes, and automatic login settings.
	Supports automatic approval, administrator or employee approval, and approval by QR code scanning.
	Distributes accounts and passwords through SMS messages, emails, or on the web page.
	Supports account and password authentication, smartphone verification code authentication, authentication through QR code scanning, and social media authentication.
	Allows users to set the account validity period and automatic account clearing.
Page customization	Allows users to select a system template based on scenarios and provides a page customization wizard.
	Supports customization of pages for PCs, tablets, and mobile phones. Customized pages include the authentication page, authentication success page, user notice page, registration page, registration success page, and full-screen advertisement page.
	Allows users to edit texts, images, videos, near video on demand (NVOD), apps, and WYSIWYG dial-up control.
	Supports domain-based management, which allows administrators to create and manage their own Portal pages.
	Supports multi-language templates, including English, simplified Chinese, traditional Chinese, German, Spanish, Portuguese, and French.

Item	Description
	Supports page pushing based on SSIDs, locations (MAC addresses), time ranges, terminal types, and guest access modes.
Free mobility	Supports security group-based authorization and deployment of rights, applications, bandwidth, QoS, and security policies based on security groups.
	Works with agile switches, NGFW firewalls, and SVN gateways to ensure unified policy deployment.
	Supports hierarchical QoS guarantee and schedules security group traffic based on queues.
	Supports global and local policies, and separate policy deployment for a single device.
	Supports separate policy deployment by VPN in the BGP/MPLS VPN networking.
Service chain	Defines service flows by IP 5-tuple information and security group.
	Supports service chain orchestration in GUIs, which allows specified service flow to be directed to the specified security device for processing.
Report management	Predefines common report templates and security trend reports, such as the online user information report.
	Supports user-defined reports or reports obtained from the security center.
Hierarchical management	Allows lower-layer servers to register to the superior MC and switches from the MC to the lower-layer nodes to view detailed information.
Fault diagnosis	Supports quick fault location by tracing RADIUS, Portal, or change-of-authorization (CoA) events.
	Provides fault diagnosis, troubleshooting suggestions, and automatic repair for network-side and client faults.
Performance specifications	One server can manage a maximum of 20,000 online terminals.
	One system can manage a maximum of 100,000 online terminals.
Network deployment	Supports deployment on physical servers.
	Supports deployment on VMs running VMware 5.5.
	Supports centralized, distributed, and hierarchical deployment modes.

Running Environment

The Agile Controller-Campus supports physical server deployment and VM deployment solutions.

Platform	Configuration Requirements of Physical Server	Configuration Requirements of VM
Windows	CPU: 2 x 8 cores 2.1 GHz (E5-2620 V4) Memory: 32 GB Hard disk: 2 x 600 GB Network adapter: 4 x GE NICs	CPU: 3 x 8 cores 2.1 GHz, exclusive mode Memory: 48 GB Hard disk: 2 x 600 GB Network adapter: 4 x GE NICs
Linux-single node	CPU: 2 x 8 cores 2.1 GHz (E5-2620 V4) Memory: 32 GB Hard disk: 2 x 600 GB Network adapter: 4 x GE NICs	CPU: 3 x 8 cores 2.1 GHz, exclusive mode Memory: 48 GB Hard disk: 2 x 600 GB Network adapter: 4 x GE NICs
Linux-HA	CPU: 2 x 8 cores 2.1 GHz (E5-2620 V4) Memory: 32 GB Hard disk: 2 x 600 GB + disk array Network adapter: 6 x GE NICs	CPU: 3 x 8 cores 2.1 GHz, exclusive mode Memory: 48 GB Hard disk: 2 x 600 GB + disk array Network adapter: 6 x GE NICs

The Agile Controller-Campus supports the Windows and Linux operating systems.

Platform	Software	Optional Environment	Remarks
Windows	Operating system	Windows Server 2012 R2 Standard 64-bit	Recommended
		Windows Server 2008 R2 Standard 64-bit	
	Database	SQL Server 2012 R2 Standard 64-bit	Recommended
		SQL Server 2008 R2 Standard 64-bit	
Linux	Operating system	SUSE Linux 11 SP3 64-bit	
	Database	Oracle 11G R2	

Ordering Information

Item	Quantity	Remarks
1.1 Software		
Access Control Function	1	Optional
Terminal Access Management Licenses	Incremental	Increments of 50, 200, 500, 1000, 2000, 5000, 10000, and 50000
TACACS Management Function	1	Optional
Free Mobility Function	1	Optional
Service Chain Function	1	Optional
1.2 Hardware Server (Optional)		
RH2288H Rack Server	1-N	Optional
S2600T Disk Array	1-N	Optional. The disk array is applicable in the Linux HA solution.