Agile Controller-Campus Brief Brochure

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.

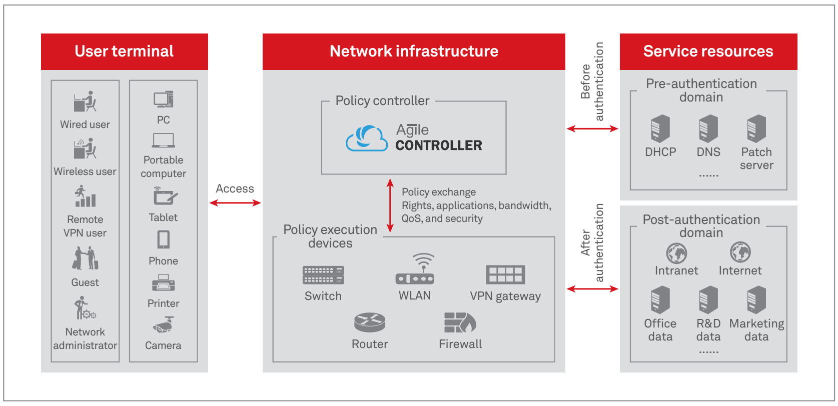
The Agile Controller-Campus provides unified network access and management for employees, guests, and device administrators, and is applicable in various sectors requiring identity authentication and authorization, including finance, government, education, healthcare, and hospitality.

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:

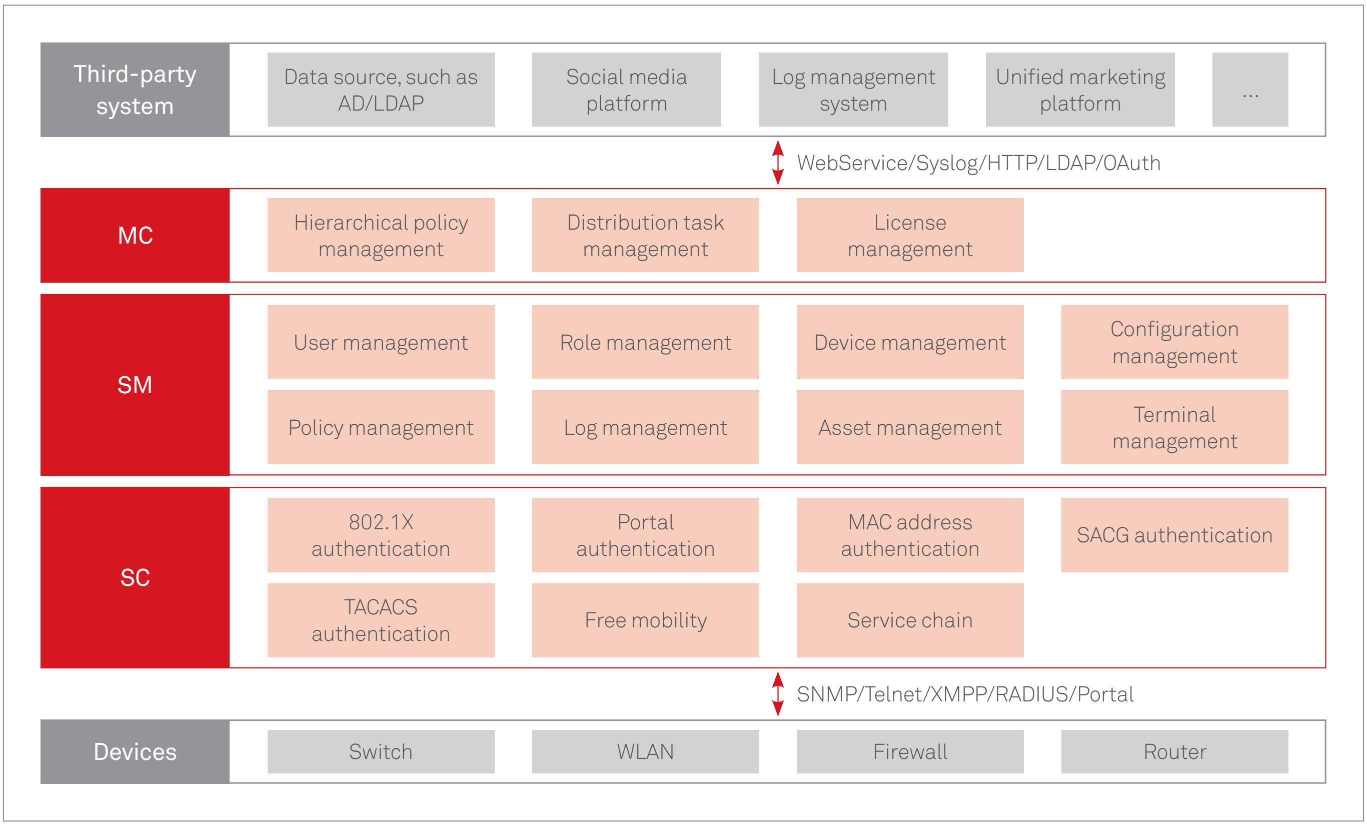
- How can a consistent experience be guaranteed for user terminals in different locations?
- How can user rights, QoS, bandwidth, applications, security, and other network policies be configured dynamically?
- Traditional networks enable users to be bound to physical interfaces whereby the administrator 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.

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.

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.

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.

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.

Item	Description
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.
	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.

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.

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.

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.