

**Agile Controller-Campus
V100R002C10**

Boarding Technology White Paper

Issue **01**
Date **2016-04-15**

Copyright © Huawei Technologies Co., Ltd. 2016. 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.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://e.huawei.com>

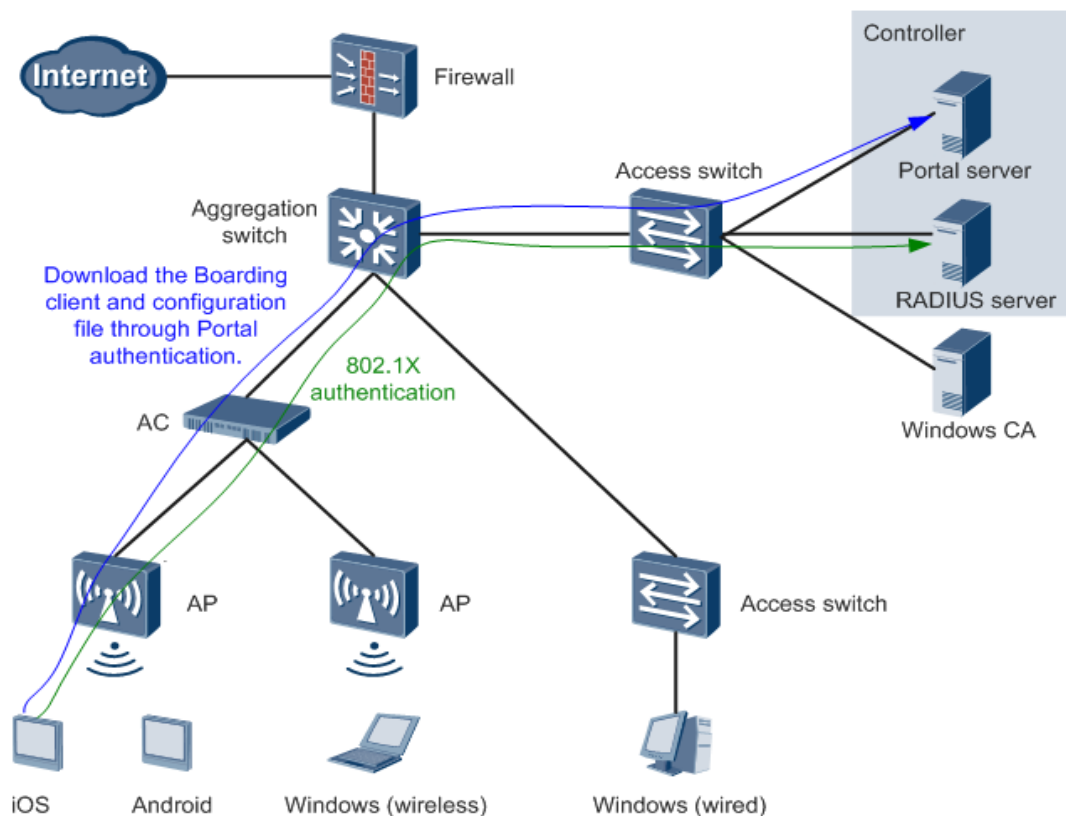
Contents

1 Boarding Necessity	1
2 Application Scenarios and Principles	3
2.1 Access a Network in Wireless mode Using a Terminal Running the Android or Windows OS.....	3
2.2 Accessing a Network in Wireless mode Using a Terminal Running the iOS.....	5
2.3 Accessing a Network in Wired mode Using a Terminal Running the Windows OS	6
3 Configuration Process.....	8

1 Boarding Necessity

When 802.1X authentication is used, users need to perform complex terminal configurations, especially when the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is used. A certificate needs to be downloaded and installed.

Boarding simplifies configurations for accessing a network using 802.1X authentication. Boarding provides network configuration tools for terminals running the Android and Windows OSs and configuration files for terminals running the iOS, enabling the automatic configuration of 802.1X access parameters.



The Boarding deployment scheme provides the following functions:

- Distribution of network configuration tools for terminals running the Android and Windows OSs, and configuration files for terminals running the iOS

The administrator deploys two service set identifiers (SSIDs). One is used for initializing the network and uses Portal authentication. The other one is used for service access and uses 802.1X authentication. If a user associates with the initialization SSID and accesses a web page, the user is redirected to the Portal authentication page.

The administrator has configured the download link of network configuration tools or configuration files on the Portal authentication page. The user can click the link to download a network configuration tool or configuration file.

- Automatic application for certificates

A user enters the account and password on a terminal, and initiates a request for identity authentication to the Agile Controller-Campus server. After the identity authentication succeeds, the Agile Controller-Campus applies for a user certificate from the Windows CA server and sends the certificate to the terminal.

- Automatic configuration for the network access

A user can automatically obtain 802.1X access configurations predefined by the administrator. After 802.1X configuration is complete according to the predefined parameters, the user can associate with the service access SSID to access a network through 802.1X authentication.

2 Application Scenarios and Principles

2.1 Access a Network in Wireless mode Using a Terminal Running the Android or Windows OS

2.2 Accessing a Network in Wireless mode Using a Terminal Running the iOS

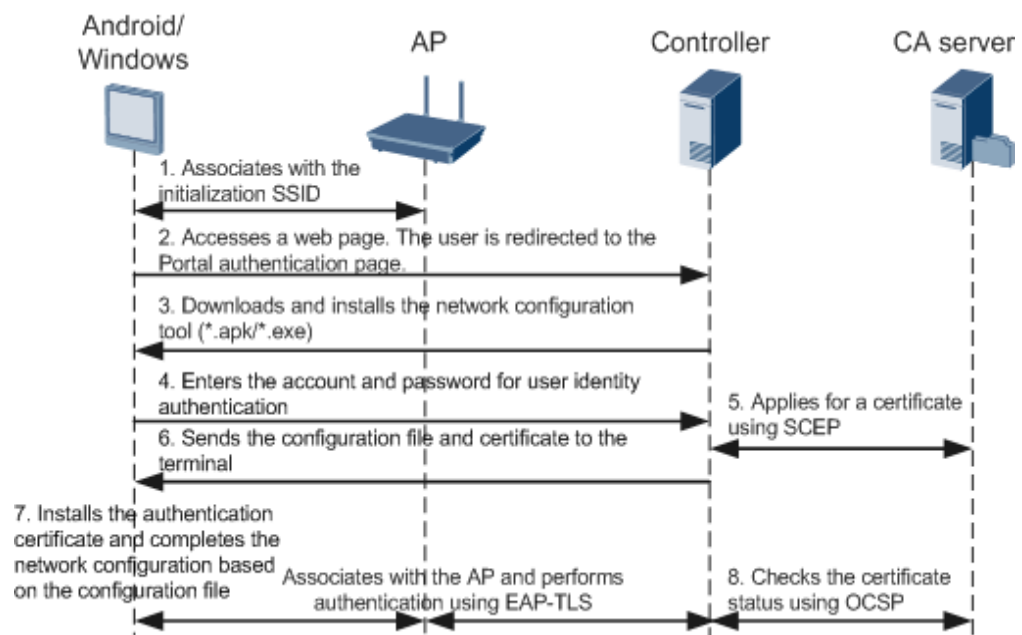
2.3 Accessing a Network in Wired mode Using a Terminal Running the Windows OS

2.1 [Access a Network in Wireless mode Using a Terminal Running the Android or Windows OS](#)

2.2 [Accessing a Network in Wireless mode Using a Terminal Running the iOS](#)

2.3 [Accessing a Network in Wired mode Using a Terminal Running the Windows OS](#)

2.1 Access a Network in Wireless mode Using a Terminal Running the Android or Windows OS



1. A user uses a terminal running the Android or Windows OS to access a wireless network and associates with the initialization SSID.
2. The user accesses a web page. The Agile Controller-Campus checks whether the terminal runs the Android or Windows OS based on the useragent parameter carried in the HTTP request packet, and then redirects the user to the Portal authentication page.
3. If the terminal runs the Android OS, the user can download the network configuration tool (in the format of *.apk) on the Portal authentication page and install the tool. If the terminal runs the Windows OS, the user can download the network configuration tool (in the format of *.exe) on the Portal authentication page and install the tool.

The administrator needs to define Portal authentication pages and page push policies on the server, providing download links of network configuration tools in formats of .apk and .exe for terminals running the Android and Windows OSs.

The administrator only needs to define a Portal authentication page for terminals running the Android and Windows OSs.

4. A user enters the account and password on the configuration tool and initiates a request for identity authentication to the Agile Controller-Campus server.

After the user identity authentication succeeds, the configuration tool automatically completes 802.1X certificate authentication and network access processes.



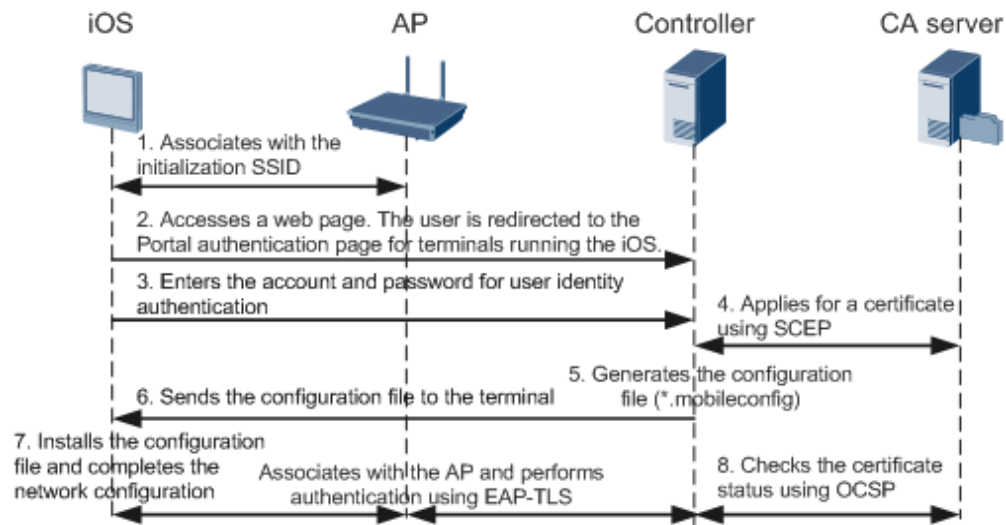
NOTE

The Boarding client on a PC running the Windows OS supports authentication using a domain account, requiring no account and password.

5. After the user identity authentication succeeds, the Agile Controller-Campus uses the Simple Certificate Enrollment Protocol (SCEP) to apply for a certificate from the Windows CA server.
6. The Agile Controller-Campus sends the configuration file that contains the applied certificate and network access parameters defined by the administrator to the terminal.
7. The terminal automatically installs the received certificate and completes the 802.1X configuration based on the configuration file. After that, the terminal automatically associates with the service access SSID and can access the Internet.
8. The user can use the Online Certificate Status Protocol (OCSP) to check whether a user certificate is revoked. If a user certificate is revoked from the Windows CA server, the certificate is invalid and the user cannot not access the network.

The user can also check the root certificate and Certificate Revocation List (CRL) to verify whether a user certificate is revoked.

2.2 Accessing a Network in Wireless mode Using a Terminal Running the iOS



1. A user uses a terminal running the iOS to access a wireless network and associates with the initialization SSID.
2. The user accesses a web page. The Agile Controller-Campus checks whether the terminal runs the iOS based on the useragent parameter carried in the HTTP request packet, and then redirects the user to the Portal authentication page.

The administrator needs to define a Portal authentication page and page push policies for terminals running the iOS, providing download links of configuration files for terminals running the iOS.



NOTE

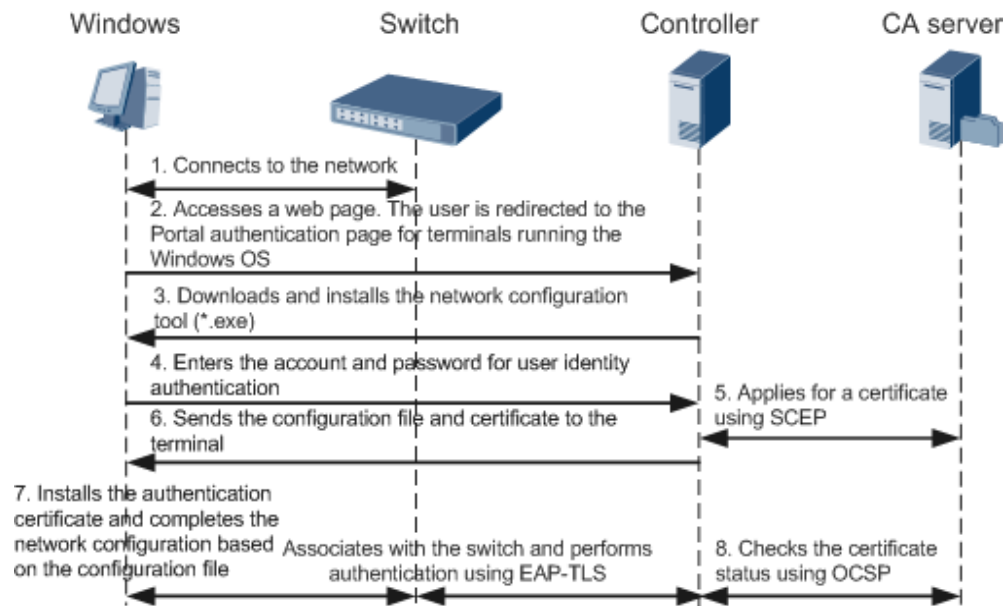
Configuration files of the iOS system use the mobileconfig format defined by Apple, which comply with Apple's security protocols.

The administrator needs to define a Portal authentication page and authentication success page for terminals running the iOS.

3. A user enters the account and password on the Portal authentication page and initiates a request for identity authentication to the Agile Controller-Campus server.
4. After the user identity authentication succeeds, the Agile Controller-Campus uses SCEP to apply for a certificate from the Windows CA server.
5. The Agile Controller-Campus integrates the applied certificate and configuration parameters for 802.1X network access into a configuration file (in the format of *.mobileconfig).
6. After the user passes identity authentication, the authentication success page is displayed, where the user can download the configuration file (in the format of *.mobileconfig).
7. After the configuration file is installed, the certificate is installed, and 802.1X network configurations are complete. The user can associate with the service access SSID to access the Internet.
8. The user can use the Online Certificate Status Protocol (OCSP) to check whether a user certificate is revoked. If a user certificate is revoked from the Windows CA server, the certificate is invalid and the user cannot not access the network.

The user can also check the root certificate and Certificate Revocation List (CRL) to verify whether a user certificate is revoked.

2.3 Accessing a Network in Wired mode Using a Terminal Running the Windows OS



1. A user accesses a wired network using a terminal running the Windows OS.
2. The user accesses a web page. The Agile Controller-Campus checks whether the terminal runs the Windows OS based on the useragent parameter carried in the HTTP request packet, and then redirects the user to the Portal authentication page configured for terminals running the Windows OS.
3. The user downloads the network configuration tool (in the format of *.exe) on the Portal authentication page and installs the tool.

The administrator has predefined a Portal authentication page and page push policies on the server, providing a download link of the network configuration tool in the format of .exe for terminals running the Windows OS.

The administrator only needs to define a Portal authentication page for terminals running the Windows OS.

4. A user enters the account and password on the configuration tool and initiates a request for identity authentication to the Agile Controller-Campus server.

After the user identity authentication succeeds, the configuration tool automatically completes 802.1X certificate authentication and network access processes.

NOTE

The Boarding client on a PC running the Windows OS supports authentication using a domain account, requiring no account and password.

5. After the user identity authentication succeeds, the Agile Controller-Campus uses the Simple Certificate Enrollment Protocol (SCEP) to apply for a certificate from the Windows CA server.
6. The Agile Controller-Campus sends the configuration file that contains the applied certificate and network access parameters defined by the administrator to the terminal.
7. The terminal automatically installs the received certificate and completes the 802.1X configuration based on the configuration file. After that, the user performs 802.1X certificate authentication. After the authentication succeeds, the user can access the Internet.

8. The user can use the Online Certificate Status Protocol (OCSP) to check whether a user certificate is revoked. If a user certificate is revoked from the Windows CA server, the certificate is invalid and the user cannot not access the network.

The user can also check the root certificate and Certificate Revocation List (CRL) to verify whether a user certificate is revoked.

3 Configuration Process

1. Deploy the Windows CA server.
The Windows CA server only supports Windows Server 2008 Enterprise or Windows Server 2008 R2 Enterprise OS.
2. Configure the WLAN device (AC) or switch.
 - Accessing a Network in Wireless Mode
Configure two SSIDs on the AC to provide Portal and 802.1X access services respectively.
 - Accessing a Network in Wired Mode
Only 802.1X authentication needs to be configured on the authentication switch. Run the dot1x url command to specify the URL for downloading the Windows network configuration tool.

```
[Switch] dot1x url http://SC_IP:8080
```



NOTE

The URL of the Portal page on the Agile Controller-Campus is http://SC_IP:8080. A Portal page is pushed based on the OS type and an HTTPS page is automatically displayed.

3. Choose **Policy > Permission Control > Boarding Management > Quick Start**, configure Boarding management based on the wizard.