Configuring Administrator Usernames and Passwords

- Finding Feature Information, page 1
- Information About Configuring Administrator Usernames and Passwords, page 1
- Configuring Administrator Usernames and Passwords, page 2
- Examples: Administrator Usernames and Passwords Configuration, page 4
- Additional References for Administrator Usernames and Passwords, page 5
- Feature History and Information For Performing Administrator Usernames and Passwords Configuration, page 6

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the controller.

Strong Passwords

You can set strong administrator passwords such as encrypted passwords with ASCII keys for the administrator user for managing access points.

Use the following guidelines while creating strong passwords:

- There should be at least three of the following categories—lowercase letters, uppercase letters, digits, and special characters.
- The new password should not be the same as that of the associated username and the username should not be reversed.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be **cisco**, **ocsic**, **admin**, **nimda**, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".
- The maximum number of characters accepted for the username and password is 32.

Encrypted Passwords

You can set three types of keys for the password:

- Randomly generated key—This key is generated randomly and it is the most secure option. To export the configuration file from one system to another, the key should also be exported.
- Static key—The simplest option is to use a fixed (static) encryption key. By using a fixed key, no key management is required, but if the key is somehow discovered, the data can be decrypted by anyone with the knowledge of that key. This is not a secure option and it is called obfuscation in the CLI.
- User defined key—You can define the key by yourself. To export the configuration file from one system to another, both systems should have the same key configured.

Configuring Administrator Usernames and Passwords

SUMMARY STEPS

1. **configure terminal**
2. **wireless security strong-password**
3. **username** *admin-username* **password {0** *unencrypted_password* **| 7** *hidden_password* **|** *unencrypted_text***}**
4. **username** *admin-username* **secret {0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text* **| 5** *MD5 encrypted_secret_text* **| LINE}**
5. **ap mgmtuser username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}secret {0** *unencrypted password* **| 8** *AES encrypted password* **}**
6. **ap dot1x username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}**
7. **end**
8. **ap name apname mgmtuser username** *username***password** *password* **secret** *secret _text*
9. **ap name apname dot1x-user** *username* **password** *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	**wireless security strong-password** **Example:** `Controller(config)# wireless security strong-password`	Enables strong password policy for the administrator user.
Step 3	**username** *admin-username* **password {0** *unencrypted_password* **| 7** *hidden_password* **|** *unencrypted_text***}** **Example:** `Controller(config)# username adminuser1 password 0 QZsek239@`	Specifies a username and password for an administrator. The administrator can configure the controller and view the configured information.
Step 4	**username** *admin-username* **secret {0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text* **| 5** *MD5 encrypted_secret_text* **| LINE}** **Example:** `Controller(config)# username adminuser1 secret 0 QZsek239@`	Specifies the secret for the administrator.
Step 5	**ap mgmtuser username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}secret {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `Controller(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!`	Specifies administrator username and password for managing all of the access points configured to the controller. You can also include the secret text to perform privileged access point management. **Note** If your password is not strong enough to fulfill the strong password policy, then the password is rejected with a valid error message. For example, the following password is rejected because it is not a strong password. `Controller# ap mgmtuser username cisco password 0 abcd secret 0 1234`
Step 6	**ap dot1x username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `Controller(config)# ap dot1x username cisco password 0 Qwci12@`	Specifies the 802.1X username and password for managing all of the access points configured to the controller.

	Command or Action	Purpose
Step 7	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**ap name apname mgmtuser username** *username***password** *password* **secret** *secret _text* **Example:** `Controller# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$`	Configures the administrator username, password, and secret text for managing a specific access point that is configured to the controller.
Step 9	**ap name apname dot1x-user** *username* **password** *password* **Example:** `Controller# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!`	Configures the 802.1X username and password for a specific access point.

Examples: Administrator Usernames and Passwords Configuration

This example shows how to configure administrator usernames and passwords with the strong password policy in configuration mode:

```
Controller# configure terminal
Controller(config)# wireless security strong-password
Controller(config)# username adminuser1 password 0 QZsek239@
Controller(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
Controller(config)# ap dot1x username cisco password 0 Qwci12@
Controller# end
```

This example shows how to configure administrator usernames and passwords for an access point in global EXEC mode:

```
Controller# wireless security strong-password
Controller# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Controller# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Controller# end
```

Additional References for Administrator Usernames and Passwords

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Administrator Usernames and Passwords Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.