



Network Time Protocol Setup

- [Authentication for the Controller and NTP/SNTP Server, on page 1](#)
- [Configuring the NTP/SNTP Server to Obtain the Date and Time \(GUI\), on page 1](#)
- [Configuring the NTP/SNTP Server to Obtain the Date and Time \(CLI\), on page 2](#)

Authentication for the Controller and NTP/SNTP Server

We highly recommend that controllers synchronize their time with an external NTP/SNTP server. We also recommend that you authenticate this connection to the NTP/SNTP server, as a best practice. By default, an MD5 checksum is used in this scenario.

Each NTP/SNTP server IP address is added to the controller database. The respective controller then attempts to poll an NTP/SNTP server from this database in the index order. The controller then obtains and synchronizes the current time at each user-defined polling interval, as well as following a reboot event. By default, the NTP polling interval is 600 seconds.

Guidelines and Restrictions on NTP

- When the time difference between the NTP server and the controller exceeds 1000s, the **ntpd** process exits and adds a panic message to the system log. In this situation, set the time on the controller manually.
- NTPv4 protocol is not supported in Cisco 2504 and 5508 Wireless Controllers.

Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI)

Procedure

- | | |
|---------------|--|
| Step 1 | Choose Controller > NTP > Server to open the NTP Servers page. |
| Step 2 | Click New to add a new NTP/SNTP Server. |
| Step 3 | (Optional) In the Server Index (Priority) field, enter the NTP/SNTP server index. |

The controller tries Index 1 first, then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP/SNTP server.

Step 4 Enter the server IP address.

You can enter an IPv4 or an IPv6 address or a fully qualified domain name (FQDN), which should meet the following criteria:

- Contains only a-z , A-Z, and 0-9 characters.
- Does not start with a dot (.) or a hyphen (-).
- Does not end with a dot (.).
- Does not have 2 consecutive dots (..).

Step 5 Enable or disable the NTP/SNTP Authentication.

Step 6 If you enable the NTP/SNTP Authentication, enter the Key Index.

Step 7 Click **Apply**.

Step 8 Delete an existing NTP server IP address or DNS server by hovering the cursor over the blue drop-down arrow for that server index and choose **Remove**.

Step 9 Confirm the deletion by clicking on **OK** in the dialog box.

Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI)

Use these commands to configure an NTP/SNTP server to obtain the date and time:

Procedure

- To specify the NTP/SNTP server for the controller, enter this command:
config time ntp server *index ip-address*
- (Optional) To specify the polling interval (in seconds), enter this command:
config time ntp *interval*
- To enable or disable NTP/SNTP server authentication, enter these commands:
 - **config time ntp auth enable *server-index key-index***—Enables NTP/SNTP authentication on a given NTP/SNTP server.
 - **config time ntp key-auth add *key-index md5 {ascii | hex} key***—Adds an authentication key. By default MD5 is used. The key format can be ASCII or hexadecimal.
 - **config time ntp key-auth delete *key-index***—Deletes authentication keys.
 - **config time ntp auth disable *server-index***—Disables NTP/SNTP authentication.
 - **show ntp-keys**—Displays the NTP/SNTP authentication related parameter.

- To delete an NTP server IP address or DNS server from the controller, enter this command:

config time ntp delete *NTP_server index*

