

Enabling SNTP Authentication on 200, 300, & 500 Series Managed Switches

Objective:

On a network switch, system time can be set manually by the user, dynamically from an SNTP server, or synchronized from the PC running the GUI interface associated with Cisco. If an SNTP server is chosen, the manual time settings are overwritten when communications with the server are established. The SNTP Authentication page enables configuration of the keys that are used when connecting to an SNTP server. The authentication key is created on the SNTP server in a separate process that depends on the type of SNTP server you are using.

The objective of this article is to show you how to enable SNTP Authentication on the SG200, SG300 and SG500 Series switches for SNTP Network Time Synchronization.

Note: In order to enable SNTP Authentication, the SNTP mode must have already been selected. Please refer to [Setting the System Time on Dynamically from a SNTP Server on 200, 300, & 500 Series Managed Switches](#) for further assistance.

Applicable Devices:

- Cisco Small Business 200 Series Managed Switches
- Cisco Small Business 300 Series Managed Switches
- Cisco Small Business 500 Series Managed Switches

Software Versions:

- 1.3.0.59

Setting the System Time:

Step 1. Log in to the web configuration utility. The default username is “cisco” and the default password is “cisco”.

Step 2. Navigate to **Administration > Time Settings > SNTP Authentication**. The *SNTP Authentication* page opens:

Authentication Key ID	Authentication Key	Trusted Key
0 results found.		

Step 3. Check the **Enable** checkbox next to *SNTP Authentication*.

SNTP Authentication

SNTP Authentication: Enable

Apply Cancel

Step 4. Click **Apply**.

SNTP Authentication

SNTP Authentication: Enable

Apply Cancel

Step 5. Select **Add** to add a new SNTP Authentication Key.

SNTP Authentication

Success.

SNTP Authentication: Enable

Apply Cancel

SNTP Authentication Key Table

<input type="checkbox"/>	Authentication Key ID	Authentication Key	Trusted Key
0 results found.			

Add... Delete

The *Add SNTP Authentication* window opens:

Authentication Key ID: (Range: 1 - 4294967295)

Authentication Key: User Defined (Encrypted)

User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

Apply Close

Step 6. Enter the Identification Number in the *Authentication Key ID* field.

Authentication Key ID: (Range: 1 - 4294967295)

Authentication Key: User Defined (Encrypted)

User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

Apply Close

Step 7. Select the desired radio button for the Authentication Key and enter the key name in

the field provided.

Authentication Key ID: 12345 (Range: 1 - 4294967295)

Authentication Key: User Defined (Encrypted)
 User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

Apply Close

The options are as follows:

- User Defined (Encrypted) – Provides encryption between the client and server
- User Defined (Plaintext) – No encryption between client and server.

Step 8. (Optional) Check the **Enable** checkbox if you want the device to receive synchronization information only from an SNTP server using this authentication key.

Authentication Key ID: (Range: 1 - 4294967295)

Authentication Key: User Defined (Encrypted)
 User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

Apply Close

Step 9. Click **Apply** to save settings.

Authentication Key ID: (Range: 1 - 4294967295)

Authentication Key: User Defined (Encrypted)
 User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

Apply Close