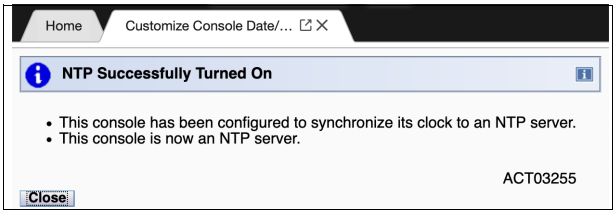

Figure 8-10 NTP Successfully Turned On

Consideration: If more than one NTP server is defined, you cannot specify which server is the primary server. The NTP service on the HMC takes any defined NTP server and tries to contact it. If it succeeds, that server is used as the time source until either the server in question is no longer available or the console is rebooted. If it cannot communicate with that server, it tries another in the list.

The check box on the Configure NTP Setting window is used only for actions in the **Select Action** list, and not for setting a primary or preferred NTP server.

8.4.2 NTP Broadband Authentication (optional)

HMC supports NTP Broadband Authentication. Configure the (optional) NTP Authentication if your HMC requires it. NTP server authentication provides an increased level of security in the following situations:

- When using a proxy to access outside network

  NTP requests are User Datagram Protocol (UDP) socket packets, so they cannot pass through the proxy. The proxy must be configured as an NTP server to get to target servers on the internet.

- When using a firewall

  NTP requests can pass through the firewall. If you use a firewall to access an outside NTP server, use the HMC authentication to ensure untampered time stamps.

Two authentication methods are supported for NTP:

- Symmetric key (NTP V3-V4) authentication

  Symmetric key encryption uses the same key for both encryption and decryption. When the HMC is acting as the client, the symmetric key index that is specified on each NTP server definition must be present in the key file. The specified key index, key type, and the key string must align with the specified key information of the target server. Likewise, if the HMC is acting as a server, the client specified key information must match the same key index on the server. Symmetric key supports Network Address Translation (NAT).

- Autokey (NTP V4) authentication

  Autokey uses public key cryptography. The key generation for the HMC NTP is done by clicking **Generate Local Host Key** on the Autokey Configuration window. Clicking this button issues the **`ntp-keygen`** command, which generates the specific key and certificate for this system. Autokey authentication is not available with a NAT firewall.