How to Enable or Disable SMS Two Factor Authentication to the Cloud UI for your Organization

### Description

CloudControl provides Primary Administrators with the ability to enable or disable SMS Two Factor Authentication to the Cloud UI for their organization(s). When enabled, all users including the Primary Administrator trying to login to the Cloud UI will receive an SMS with a code, which they will have to enter in addition to their username/password to complete login.

**IMPORTANT:** the feature described in this guide article is specific to Two Factor Authentication for the Updated UI and is completely independent of the Client-to-Site VPN specific Multi-Factor Authentication feature described by [Introduction to Single-Factor and Multi-Factor VPN Authentication](#).

- Enable SMS Two Factor Authentication to the Cloud UI
- Disable SMS Two Factor Authentication to the Cloud UI

### Prerequisites:

1. The SMS Two Factor Authentication feature can only be enabled or disabled by the Primary Administrator.
2. SMS Two Factor Authentication applies to all account administrators. Therefore, the Phone Number field for both the Primary Administrator and every Sub-Administrator in the account must be populated with a valid SMS-enabled phone number prior to enabling this feature. For details on how to edit the phone number, see [How to Manage the Primary Administrator User and other Sub-Administrators as the Primary Administrator](#).

### Content / Solution:

1. **Click on the Compute button and select Account Management from the drop-down menu:**

   ![Unknown Attachment]

2. **The Account Management page will be displayed. Click on the Manage Two Factor Authentication button on the left side menu:**

   ![Account Management]

Enable SMS Two Factor Authentication to the Cloud UI
1. The Manage Two Factor Authentication dialog will be displayed. Click Confirm:

![Manage Two Factor Authentication](image)

Note: All users (Sub-Administrators) must have an SMS-enabled telephone in order to enable Two Factor Authentication.

2. The system will enable SMS Two Factor Authentication to the UI, and display a success message:

![Two Factor Authentication Enabled successfully for the Organization](image)

3. When logging into the Cloud UI, all users (including the Primary Administrator) will receive an SMS with a code which they will have to enter in addition to their username/password to complete login. For more details, see How to Log In to the Cloud UI When Two Factor Authentication with SMS is Enabled for your Organization

![CloudControl](image)

An SMS containing the verification code is being sent to *******930. Please enter the verification code to complete sign-in to Cloud Control.

**Verification Code:**

12345

**Sign-in**

Disable SMS Two Factor Authentication to the Cloud UI
1. The Manage SMS Two Factor Authentication dialog will be displayed. Click Confirm:

![Manage SMS Two Factor Authentication dialog]

2. The system will disable SMS Two Factor Authentication and display a success message:

![Success message]

Recently Updated

- How to Manage the Primary Administrator User and other Sub-Administrators as the Primary Administrator
- How to Create a Sub-Administrator using the CloudControl UI
- Introduction to Tagging, Tag Keys and Tag Values
- How to Manage Sub-Administrators for a SAML-Enabled Organization
- How to Create a Sub-Administrator for SAML-Enabled Organizations