How to Connect to a VPN with Single-Factor or Multi-Factor VPN Authentication

Description

This article describes how to connect to a secure client-to-site VPN in order to access your Cloud Servers on the CaaS infrastructure.

This action is necessary in order to access or administer your virtual servers via SSH or Windows Remote Desktop (RDP) protocols using the server's private IP address.

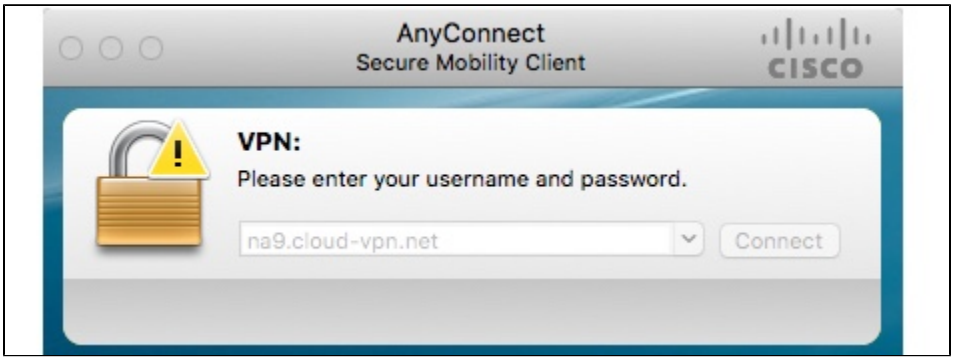
Please refer to How to Establish a Secure VPN Connection to Access your Cloud Network and Servers for the complete set of requirements and summary of steps and links to appropriate instructions.

Prerequisites:

1. To identify the VPN links relevant for your Organization please refer to: How to Establish a Secure VPN Connection to Access your Cloud Network and Servers
    a. Each link will be identified as requiring Single-Factor VPN Authentication or Multi-Factor VPN Authentication. For more information please refer to Introduction to Single-Factor and Multi-Factor Client-to-Site VPN Authentication.
2. Only users with the VPN role can connect to the VPN and access their Organization's cloud resources.
    a. To add the VPN Role to a user, see How to Manage the Primary Administrator User and other Sub-Administrators as the Primary Administrator
3. This article presumes that Cisco AnyConnect is already installed per the instructions at How to Download and Install the Cisco AnyConnect VPN Client.
4. Users of Organizations with Multi-Factor VPN Authentication enabled at the Geographic Region where they wish to connect to the VPN must be enrolled with Duo to connect to the VPN and must be prepared to provide a second-factor authentication approach and corresponding credentials. For more information please refer to:
    a. Introduction to Single-Factor and Multi-Factor Client-to-Site VPN Authentication
    b. How to Self-Enroll in Duo for Multi-Factor Authentication Access to Cloud VPN
    c. How to Manage VPN Authentication for an Organization using the VPN Access setting.
5. Each Primary Administrator or Sub-Administrator account is limited to two simultaneous Client-to-Site VPN connections.
    a. To create more Sub-Administrator accounts, see How to Create a Sub-Administrator using the CloudControl UI

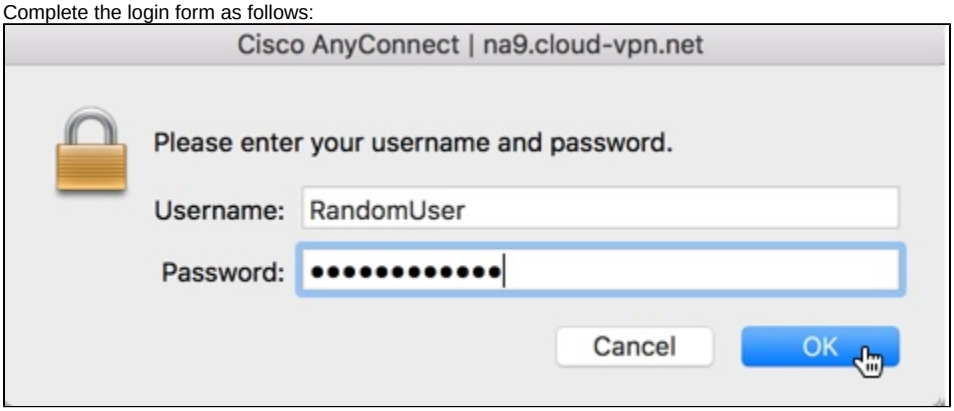
Content / Solution:

1. **How to connect to a VPN URL**
    a. **Launch Cisco AnyConnect and paste in a VPN URL copied from one of the links identified by the process described in How to Establish a Secure VPN Connection to Access your Cloud Network and Servers. Note that some operating systems will permit AnyConnect to launch directly from clicking a link in the CloudControl UI. Click "Connect".**



    b. **The next step(s) will vary depending on your Organization's VPN access setting (Introduction to Single-Factor and Multi-Factor Client-to-Site VPN Authentication).**
        i. If your organization has **Single-factor VPN Authentication** enabled:

1. Complete the login form as follows:

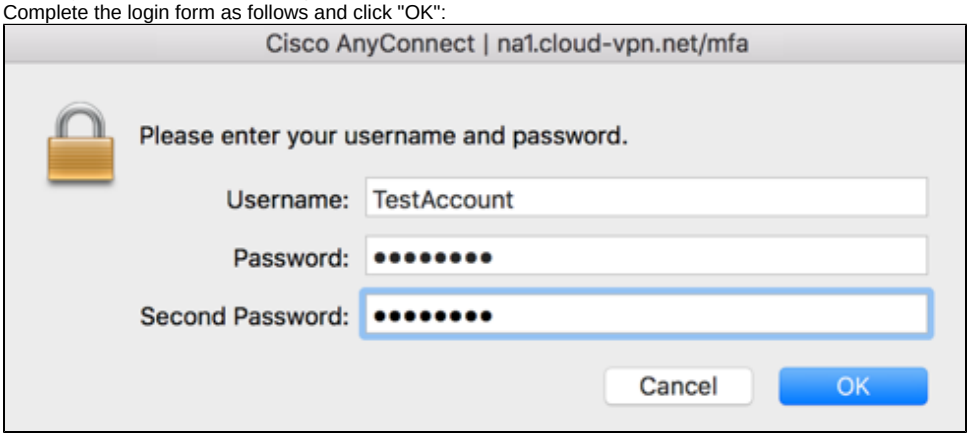


Username - Your CloudControl Username
Password - Your CloudControl Password

2. Click "OK" to connect to the VPN.

ii. If your organization has **Multi-factor VPN Authentication** enabled:

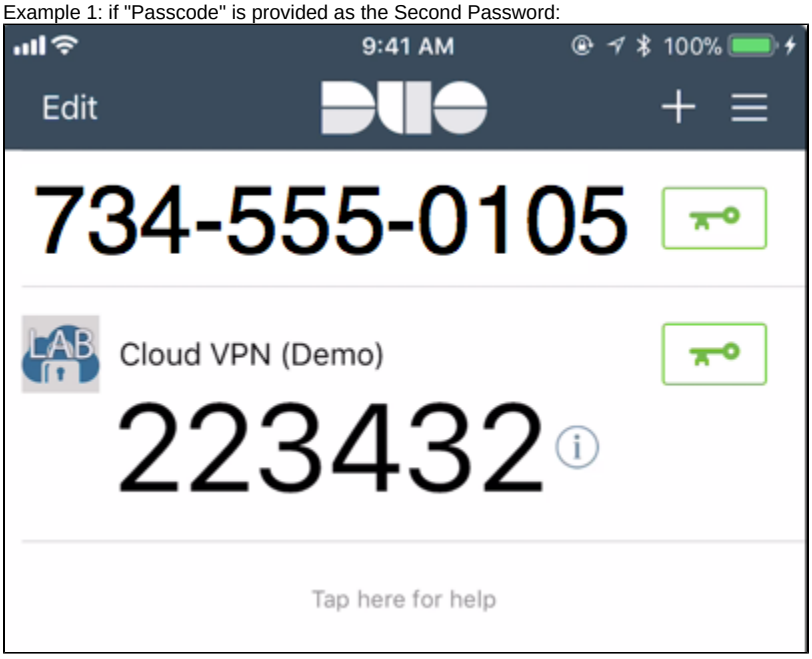
1. Ensure you are enrolled with Duo per How to Self-Enroll in Duo for Multi-Factor Authentication Access to Cloud VPN.
2. Complete the login form as follows and click "OK":



- **Username** - Your CloudControl Username
- **Password** - Your CloudControl Password
- **Second Password** - Use one of the following options:

Enter	To
A Passcode	Log in using a passcode either generated with Duo Mobile, sent via SMS, Generated by your hardware token, or provided by an Administrator. Examples: 123456 or 1456789
Push	Push a login request to your device (if you have Duo Mobile installed on your iPhone, Android, Windows Phone, or BlackBerry device). Just review the request and tap "Approve" to log in
Phone	Authenticate via a phone callback
SMS	Get a new batch of SMS passcodes. Note: Your login attempt will fail - log in again with one of the new passcodes.

Example 1: if "Passcode" is provided as the Second Password:

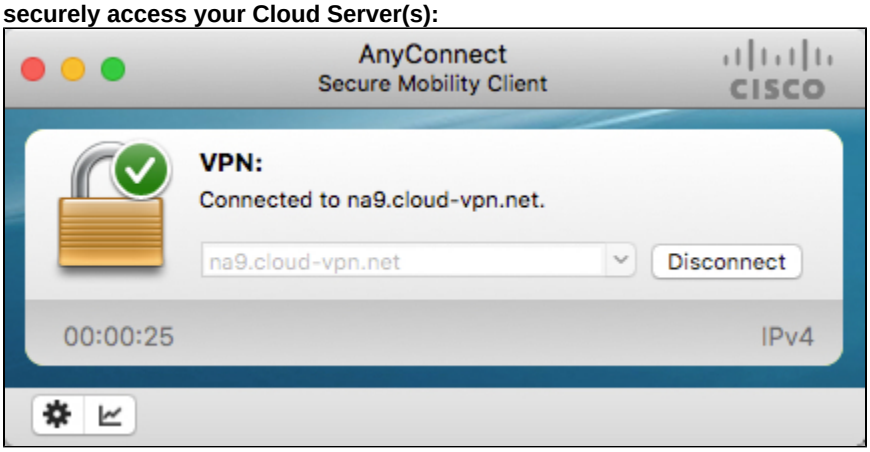


Example 2: if "Phone" is provided as the Second Password, the Duo service will call the phone number provided when you enrolled with the service and will allow the connection process to proceed when the call is answered and an acknowledging keypress is provided. For a full list of Duo approach prompts please see How to Self-Enroll in Duo for Multi-Factor Authentication Access to Cloud VPN.

i.

We have successfully tested Push, Passcode, SMS and Phone for the Authentication.

c. **You will be connected to the VPN. You can now connect to your Cloud Networks (MCP 1.0) and Cloud Network Domains (MCP 2.0) using SSH or Microsoft Windows Remote Desktop Connection (RDC) to securely access your Cloud Server(s):**



Note: Click "Disconnect" to disconnect the VPN connection.

Download of AnyConnect Not Required Each Time It Is Used

Once the Cisco AnyConnect is installed on your local machine, you do not have to use the links in the Admin UI to connect to the VPN or install it again. You also have the option of launching the Cisco AnyConnect VPN Client locally from your machine and enter the appropriate VPN URL to connect to the VPN. Geographic Region and Data Center VPN addresses are available as described above as well as in the Data Center details screen as described in How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location

Recently Updated

- Navigating the Home Page

- How to Create a Detailed Usage Report
- How to Create a Summary Usage Report
- How to Manage Snapshot Long-Term Retention
- How to Manage Snapshot Replication on a Cloud Server