

How to Deploy the CloudGen Access Application With MDMs

https://campus.barracuda.com/doc/96012976/

Using a configuration profile, the administrator can pre-configure the macOS network stack with a VPN profile so that upon installation of CloudGen Access on end user devices, the user is not prompted to approve/accept installation of software or policies. This profile does *not* represent an MDM enrollment profile, and thus can only be deployed via MDM *after* a device has been enrolled.

The .mobileconfig configuration profile can be copied and pasted from this page, and can then be uploaded to any MDM solution to be used for deployment. Before deploying this profile to all of your managed devices, test it on a local machine as described below.

Using the Tamperproof feature

To use the <u>Tamperproof</u> feature mentioned below, you must use the CloudGen Access App version 2.2.0 or later. Deploying via MDM when using the <u>Tamperproof</u> feature requires using a specific .mobileconfig configuration profile and, in the case of macOS devices, a plist file is required as well. Both file types can be copied and pasted from this page and stored on your macOS or iOS devices.

Test the Configuration Profile On a Local macOS Device

- 1. Make sure the device **does not** have CloudGen Access installed.
- 2. If you are using the <u>Tamperproof</u> feature:
 - Copy and paste the contents of the macOS configuration file as shown in mobilconfigmacOSTamperproofsection of this article, and name the file .mobilconfig. Download this configuration profile to your test macOS device. If you are using Tamperproof, the mobilecconfig file is set to prevent uninstall of the VPN profile, and to make sure that the user cannot bypass web filtering by recreating a connection on the VPN when a connection is initiated.
 Skip to step 4.
- 3. If you are *not* using the Tamperproof feature, copy and paste the contents of the macOS configuration file as shown in <u>mobilconfigConfigurationNOTTamperproof</u>section of this article, and name the file .mobilconfig. Download this configuration profile to your test macOS device. **Skip to step 5.**
- 4. If you are using Tamperproof and macOS, you also need to copy and paste the <u>plistFileTamperproofmacOS</u> and store it under /Library/LaunchAgent s/. The plist file is used to restart the CloudGen Access app if it is closed. This file is not required for iOS.
- 5. Double-click on the .mobileconfig file and follow the installation instructions on screen. This profile is unsigned, so it will be marked accordingly as *Unsigned*:



Device Profiles					
Barracuda CloudGen 1 setting	Barracuda CloudGen Access - VPN Profile Barracuda Networks, Inc. Unsigned				
JumpCloud Tray App 1 setting	Description Barracuda CloudGen Access VPN Pro Installed Jul 14, 2021 at 4:53 PM	ofile			
	Settings VPN Service 127.0.0.1				
	DETAILS				
	VPN Service				
	Description Barracuda CloudGen Access				
	VPN Configuration VPN Type				
	VPN Remote Address 127.0.0.1				
	VPN Auth Method Deceword				

6. Check under **Settings > Network Preferences** for **Access** to show up as *Not Connected*.

	Network	Q Search
Loca	tion: Automatic	0
Wi-Fi Image: Connected Connected Image: Connected Bluetooth PAN Image: Connected	Status: Not Connected	
Thundethernet Not Connected USB 10/00 LAN Not Connected Display Ethernet Not Connected >	Server Address: 127.0.0.1 Account Name: Connect on dem	nand
Display FireWire Not Connected ThundeIt Bridge Not Connected Thundet Slot 1 Not Connected	Connect VPN Application: Access	
Access Not Connected	Show VPN status in menu bar	3
		Revert Apply

7. Open the App Store and install **Barracuda CG Access**.



	X	
🔍 barracuda og access 🛛 🕲	Barracuda CG Access Secure access to apps and web	
★ Discover	Fyde	
🕹 Arcade	39 ****	4.
A Create	23 Ratings	Ag
Work		
Play	What's New	Version Histor
The Develop	Thank you for using Barracuda CloudGen Access! This version contains several bug fixes and performance	1mo ag Version 1.3
Develop	inproteinente.	
Categories	Preview	
Updates 1		
	Access and	
	Security Unified	
	Colladarin Access the pulses mitigate accordy and compliance risk, increase productivity and experience	

8. After installation, check the Network Preferences again for Access. It should now be in *Connected* state and show as active.

		Network		Barracuda CloudGen Access
	Loca	ation: Automatic	٥	OVERVIEW
• Wi-Fi Connected	(î•	Status: Connected		
Access Connected		Connect Time: 00:00:30 IP Address: 192.0.2.1	Sent: Received:	S O
Bluetooth PAN Not Connected	*			
Thundethernet		Server Address: 127.0.0.1		

Deploy Using Your MDM

- 1. Make sure that your have enrolled your device for MDM before proceeding (check your MDM provider for device enrollment instructions).
- To create an MDM policy for CloudGen Access, use the payload respective to the target OS from <u>The .mobileconfig Configuration Profiles for macOS and iOS</u> section below. **Be sure to choose the correct config file(s) as instructed above,** depending on whether or not you want to use the <u>Tamperproof</u> feature for user devices.
- Upload the configuration to the MDM provider in use. Each provider has its own method of inputting the content of this payload, so follow your provider's instructions. For example, both Jamf and JumpCloud MDM providers sign the profile payload before pushing them to target devices.
- 4. Create an MDM policy to use **Barracuda CG Access** from the App Store to push to the device.
- 5. Apply both policies to the target group of devices.

Important:

- Make sure that the custom CloudGen Access network profile is installed **before** the app is installed on the device. If installed after the app is installed, there will temporarily be two VPN configurations shown in **Network Preferences** until the machine is rebooted or the app is restarted.
- Upon uninstallation, make sure to **first** uninstall the app **and then** remove the custom



CloudGen Access configuration profile. Removing the CloudGen Access MDM profile will remove the *Access* VPN configuration that it installed in the first place.

The .mobileconfig Configuration Profiles for macOS and iOS

The .mobileconfig Configuration Profile for macOS - NOT using the Tamperproof Feature

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>PayloadContent</key>
        <array>
                <dict>
                        <key>OnDemandMatchAppEnabled</key>
                        <false/>
                        <key>PayloadDescription</key>
                        <string>Configures Barracuda CloudGen Access VPN
profile.</string>
                        <key>PayloadDisplayName</key>
                        <string>Barracuda CloudGen Access</string>
                        <key>PayloadIdentifier</key>
                        <string>com.apple.vpn.managed.190B5F98-6340-4B70-
B2CE-11913B298611</string>
                        <key>PayloadOrganization</key>
                        <string>Barracuda Networks, Inc.</string>
                        <key>PayloadType</key>
                        <string>com.apple.vpn.managed</string>
                        <key>PayloadUUID</key>
                        <string>190B5F98-6340-4B70-B2CE-11913B298611</string>
                        <key>PayloadVersion</key>
                        <integer>1</integer>
                        <key>Proxies</key>
                        <dict/>
                        <key>UserDefinedName</key>
                        <string>Access</string>
                        <key>VPN</key>
                        <dict>
```



```
<key>AuthenticationMethod</key>
                                <string>Password</string>
                                <key>OnDemandEnabled</key>
                                <false/>
                                <key>ProviderBundleIdentifier</key>
<string>com.fyde.guardian.macos.extension</string>
                                <key>ProviderType</key>
                                <string>packet-tunnel</string>
                                <key>RemoteAddress</key>
                                <string>127.0.0.1</string>
                        </dict>
                        <key>VPNSubType</key>
                        <string>com.fyde.guardian.macos</string>
                        <key>VPNType</key>
                        <string>VPN</string>
                        <key>VPNUUID</key>
                        <string>4812F41C-374A-4859-9106-1D881205A63E</string>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Barracuda CloudGen Access VPN Profile</string>
        <key>PayloadDisplayName</key>
        <string>Barracuda CloudGen Access - VPN Profile</string>
        <key>PayloadIdentifier</key>
        <string>543CC1DE-AC7A-4227-B45B-2055ACDD0AF4</string>
        <key>PayloadOrganization</key>
        <string>Barracuda Networks, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>D337E9D4-40FB-4602-8284-F4AEBB298439</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
</plist>
```

The .mobileconfig Configuration Profile for iOS - NOT using the Tamperproof Feature

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
```



<dict></dict>	
<key>PayloadCon⁻</key>	tent
<array></array>	
<dict></dict>	
	<key>OnDemandMatchAppEnabled</key>
	<false></false>
	<pre><kev>PavloadDescription</kev></pre>
	<pre><string>Configures Barracuda CloudGen Access VPN</string></pre>
profile /strings	String-configures barracuda croudden Access vin
profice.	<pre>ckovsPavlaadDicplavNamo</pre>
	<key>PaytoauDisplayName</key>
	<pre><string>Barracuda cloudGen Access</string></pre>
	<key>Payloadidentifier</key>
	<string>com.apple.vpn.managed.190B5F98-6340-4B/0-</string>
B2CE-11913B298611 <td>1g></td>	1g>
	<key>PayloadOrganization</key>
	<string>Barracuda Networks, Inc.</string>
	<key>PayloadType</key>
	<string>com.apple.vpn.managed</string>
	<key>PayloadUUID</key>
	<pre><string>190B5F98-6340-4B70-B2CE-11913B298611</string></pre>
	<key>PayloadVersion</key>
	<integer>1</integer>
	<kev>Proxies</kev>
	<pre><dict></dict></pre>
	<pre><kev>llserDefinedName</kev></pre>
	<pre><string>Access</string></pre>
	<pre> <</pre>
	<hr/>
	<pre><ure></ure></pre>
	<pre><key>AuthenticationMethod</key> <pre></pre></pre>
	<string>Passworu</string>
	<key>UnDemandEnabled</key>
	<false></false>
	<key>ProviderBundleldentifier</key>
<string>com.fyde.guardia</string>	an.ios.extension
	<key>ProviderType</key>
	<string>packet-tunnel</string>
	<key>RemoteAddress</key>
	<string>127.0.0.1</string>
	<key>VPNSubType</key>
	<string>com.fyde.guardian.ios</string>
	<key>VPNType</key>
	<string>VPN</string>
	<key>VPNUUID</key>
	<pre><string>4812F41C-374A-4859-9106-1D881205A63F</string></pre>
7 410 6	



```
</array>
        <key>PayloadDescription</key>
        <string>Barracuda CloudGen Access VPN Profile</string>
        <key>PayloadDisplayName</key>
        <string>Barracuda CloudGen Access - VPN Profile</string>
        <key>PayloadIdentifier</key>
        <string>543CC1DE-AC7A-4227-B45B-2055ACDD0AF4</string>
        <key>PayloadOrganization</key>
        <string>Barracuda Networks, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>2D042D06-9981-46BB-BE0A-A5FBC0631A5D</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
</plist>
```

The .mobileconfig Configuration Profile for macOS - USING the Tamperproof Feature

xml version="1.0" end</th <th>coding="UTF-8"?></th>	coding="UTF-8"?>
plist PUBLIC</td <td>"-//Apple//DTD PLIST 1.0//EN"</td>	"-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/[DTDs/PropertyList-1.0.dtd">
<plist version="1.0"></plist>	
- <dict></dict>	
<key>PayloadCor</key>	ntent
<array></array>	
<dict></dict>	
	<key>OnDemandMatchAppEnabled</key>
	<false></false>
	<key>PayloadDescription</key>
	<string>Configures Barracuda CloudGen Access VPN</string>
profile.	
	<key>PayloadDisplayName</key>
	<string>Barracuda CloudGen Access</string>
	<key>PayloadIdentifier</key>
	<string>com.apple.vpn.managed.190B5F98-6340-4B70-</string>
B2CE-11913B298611 <td>ing></td>	ing>
	<key>PayloadOrganization</key>
	<string>Barracuda Networks, Inc.</string> <key>PavloadType</key>



```
<string>com.apple.vpn.managed</string>
                        <key>PayloadUUID</key>
                        <string>2C0D7638-6071-4ECB-A8D1-CAFAD3F8E679</string>
                        <key>PayloadVersion</key>
                        <integer>1</integer>
                        <key>UserDefinedName</key>
                        <string>Access</string>
                        <key>VPN</key>
                        <dict>
                                <key>AuthenticationMethod</key>
                                <string>Password</string>
                                <key>OnDemandEnabled</key>
                                <integer>1</integer>
                                <key>OnDemandRules</key>
                                <array>
                                        <dict>
                                                 <key>Action</key>
                                                 <string>Connect</string>
                                                 <key>InterfaceTypeMatch</key>
                                                 <string>WiFi</string>
                                        </dict>
                                </array>
                                <key>ProviderBundleIdentifier</key>
<string>com.fyde.guardian.macos.extension</string>
                                <key>ProviderType</key>
                                <string>packet-tunnel</string>
                                <key>RemoteAddress</key>
                                <string>127.0.0.1</string>
                        </dict>
                        <key>VPNSubType</key>
                        <string>com.fyde.guardian.macos</string>
                        <key>VPNType</key>
                        <string>VPN</string>
                        <key>VPNUUID</key>
                        <string>4812F41C-374A-4859-9106-1D881205A63E</string>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Barracuda CloudGen Access VPN Profile</string>
        <key>PayloadDisplayName</key>
        <string>Barracuda CloudGen Access - VPN Profile</string>
        <key>PayloadIdentifier</key>
        <string>543CC1DE-AC7A-4227-B45B-2055ACDD0AF4</string>
        <key>PayloadOrganization</key>
        <string>Barracuda Networks, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
```



```
<false/>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>A4797083-FC34-4D22-B622-A386141FDAD2</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>RemovalDate</key>
<date>2024-03-21T15:37:24Z</date>
</dict>
</dict>
```

The .mobileconfig Configuration Profiles for iOS - USING the Tamperproof Feature

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>PayloadContent</key>
        <array>
                <dict>
                        <key>PayloadDescription</key>
                        <string>Configures Barracuda CloudGen Access VPN
profile.</string>
                        <key>PayloadDisplayName</key>
                        <string>Barracuda CloudGen Access</string>
                        <key>PayloadIdentifier</key>
                        <string>com.apple.vpn.managed.190B5F98-6340-4B70-
B2CE-11913B298611</string>
                        <key>PayloadOrganization</key>
                        <string>Barracuda Networks, Inc.</string>
                        <key>PayloadType</key>
                        <string>com.apple.vpn.managed</string>
                        <key>PayloadUUID</key>
                        <string>A7B29D29-6CA5-4343-A41A-D2DBEB7BDEE1</string>
                        <key>PayloadVersion</key>
                        <integer>1</integer>
                        <key>UserDefinedName</key>
                        <string>Barracuda Access VPN</string>
                        <key>VPN</key>
                        <dict>
                                <key>AuthenticationMethod</key>
                                <string>Password</string>
```



```
<key>OnDemandEnabled</key>
                                <integer>1</integer>
                                <key>OnDemandUserOverrideDisabled</key>
                                <integer>1</integer>
                                <key>ProviderBundleIdentifier</key>
<string>com.fyde.guardian.ios.extension</string>
                                <key>ProviderType</key>
                                <string>packet-tunnel</string>
                                <key>RemoteAddress</key>
                                <string>127.0.0.1</string>
                        </dict>
                        <key>VPNSubType</key>
                        <string>com.fyde.guardian.ios</string>
                        <key>VPNType</key>
                        <string>VPN</string>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Barracuda CloudGen Access VPN Profile</string>
        <key>PayloadDisplayName</key>
        <string>Barracuda CloudGen Access - VPN Profile</string>
        <!-- identifier for profiles command -->
        <key>PayloadIdentifier</key>
        <string>543CC1DE-AC7A-4227-B45B-2055ACDD0AF4</string>
        <key>PayloadOrganization</key>
        <string>Barracuda Networks, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <!-- uuid for profiles command -->
        <key>PayloadUUID</key>
        <string>E6CB1F7E-1083-439C-91EA-DD782BCCBDC7</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>RemovalDate</key>
        <date>2024-03-21T15:37:24Z</date>
</dict>
</plist>
```



The . plist file for macOS USING the Tamperproof Feature

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>KeepAlive</key>
    <true/>
    <key>Label</key>
    <string>com.barracuda.cga</string>
    <key>LimitLoadToSessionType</key>
    <string>Aqua</string>
    <key>ProgramArguments</key>
    <array>
        <string>open</string>
        <string>--wait-apps</string>
        <string>/Applications/Access.app</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
```

Using MDM

The process described here uses the example of JumpCloud, which is similar to Jamf and other MDM providers. First, import the custom profile by either uploading the .mobileconfig profile, or by copying the content from the .mobileconfig profile payload shown above into the provided MDM user interface.

- 1. Follow your MDM provider's instructions to set up the custom configuration profile by first uploading the .mobileconfig file to the MDM.
- After saving, on the client, go into Settings→Profiles to look for the CloudGen Access VPN profile
 - it show up as Verified when pushed through the MDM (your MDM provider should sign the
 profile using the APNS certificate you configured in their portal when setting up the MDM).



Device Profiles	Democrate Old	
Barracuda CloudGen 1 setting	Barracuda Cid Barrac	udgen Access - VPN Profile
JumpCloud Agent Se	Description	Barracuda CloudGen Access VPN Profile
- Setting	Signed	MDM Vendor: JUMPCLOUD INC.
JumpCloud MDM Set 1 setting	Installed	Jul 16, 2021 at 1:29 PM
JumpCloud Tray App 1 setting	Settings	VPN Service
MDM Enrollment Prof 2 settings		127.0.0.1
	DETAILS	
	VPN Service	
	Description	Barracuda CloudGen Access
	VPN Configuration Type	VPN
	VPN Remote Address	127.0.0.1

3. Open Settings→Network to verify that a new VPN configuration is there with the name Access. It should be in the Not Connected state since the CloudGen Access app has yet to be installed.

	Network	Q Search
Loc	ation: Automatic	0
 Wi-Fi Connected Bluetooth PAN Not Connected Thundethernet Not Connected USB 10/00 LAN Not Connected 	Status: Not Connected Server Address: 127.0.0.1 Account Name:	
Display Ethernet Not Connected Display FireWire Not Connected ThundeIt Bridge Not Connected	Connect on de	mand
Thundet Slot 1 Not Connected Access Not Connected	VPN Application: Access	
+ - &~	Show VPN status in menu bar	? Revert Apply

4. After the CloudGen Access app is installed, it uses this pre-configured configuration profile instead of creating its own so that this VPN will show as *Connected* as soon as CloudGen Access is started.



		Network					OVERVIEN	N
	Location:	Automatic		٥			10	
• Wi-Fi Connected	<u></u>	Status: C	onnected					
Access Connected		Connect Time: 00 IP Address: 19	0:00:43 92.0.2.1	Sent: Received:				
Bluetooth PAN Not Connected	8						$\langle \checkmark \langle $	
Thundethernet Not Connected	~~>	Server Address: 1 Account Name:	27.0.0.1		-			
USB 10/00 LAN Not Connected	~~>		Connect on	demand				
Display Ethernet Not Connected	\leftrightarrow		Disconnect					(3)
 Display FireWire Not Connected 	` 2	VPN Application: A	Access			Network	Device	Anomalies
 ThundeIt Bridge Not Connected 	$\langle \cdot \rangle$							
Thundet Slot 1 Not Connected		Show VPN status in r	nenu bar		2		Check nov	v
+ - *						Last chec	k Jul 14. 2021 4:49	PM (manual)

5. In order to remove the Cloudgen Access VPN configuration from the device, make sure CloudGen Access is uninstalled beforehand.

Note: If you want to keep CloudGen Access on the machine, make sure to quit the app first before removing the MDM profile, because the VPN configuration is in use. After that, as soon as Cloudgen Access is restarted, it will configure a VPN Configuration.

Pushing an MDM profile to a machine that already has CloudGen Access installed

If a machine already has CloudGen Access installed when you push the new MDM profile, you will temporarily see an *Access* configuration as well as an *Access 1* configuration as duplicates in *Settings→Network*. This is not a problem; the app will continue to work and the second *Access* VPN disappears as soon as you restart Cloudgen Access, or upon a reboot. Only one Access VPN Configuration will remain on the machine.



Figures

- 1. Unsigned VPN Profile.png
- 2. Network_VPN_Conifguration.png
- 3. AppStoreBarracudaCGAccess.png
- 4. CGA Connected.png
- 5. MDM_BarracudaCloudGenAccess_Configuration_Profile.png
- 6. Network_VPN_Conifguration.png
- 7. CloudGenAccess_using_VPN_Config.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.