cisco.



Cisco Cloud APIC and Intersight Device Connector

New and Changed Information 2 About Device Connector 2 About the Auto Update Option 2 Configuring the Intersight Device Connector 3 Claiming a Device Using the GUI 9 Revised: July 10, 2022

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior

Cisco APIC Release	Feature	Description		
25.0(4)	Initial release of this feature	Initial release of this feature.		

About Device Connector

Devices are connected to the Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Cisco Intersight service when you connect to Cisco Intersight. For more information on the **Auto Update** option, see About the Auto Update Option, on page 2.

About the Auto Update Option

This Auto Update option is enabled by default. We recommend that you leave the Auto Update option enabled.

When the **Auto Update** option is enabled, the Device Connector automatically initiates an upgrade after receiving an Upgrade message from the Cisco Intersight Cloud. During this time, the Device Connector checks if a Cisco Cloud APIC is being upgraded. If a Cisco Cloud APIC is being upgraded, then the Device Connector upgrade will be postponed to maximum of 24 hours, after which the Device Connector is upgraded regardless if a Cisco Cloud APIC is being upgraded. If there are no Cisco Cloud APICs being upgraded, then the Device Connector initiates its upgrade immediately. Likewise, the Cisco Cloud APIC upgrade pre-validation process verifies if the Device Connector is being upgraded when you initiate a Cisco Cloud APIC upgrade. In such a case, the upgrade page displays a corresponding warning message.

If a Device Connector upgrade is in progress, a message is displayed, saying that the DC upgrade is in progress and to wait until the DC upgrade is complete before triggering a Cloud APIC upgrade.

If the Cisco Cloud APIC pre-upgrade validation is unable to check the Device Connector upgrade status, the following message displays:

Could not check DC upgrade status

In this case, re-initiate the Cisco Cloud APIC upgrade. If the upgrade fails again with the same message, wait 1 or 2 minutes and try again.

If the **Auto Update** option is disabled and there is a new Device Connector software version available, you will be prompted in the Device Connector GUI page to update the software manually when new releases become available. In addition, the Device Connector can become out-of-date, which can affect the ability of the Device Connector to connect to Cisco Intersight.

Configuring the Intersight Device Connector

Procedure

Step 1

In the Cisco Cloud APIC GUI, navigate to Infrastructure > Intersight.

The Intersight Device Connector overview page appears.

You should see green dotted lines connecting **Device Connector** to **Internet** in the **Device Connector** graphic in this page.

Ŧ	Cloud APIC Azure	
Dashboard	Intersight Device Connector	Ø
Topology		•
Cloud Resources	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring visit Help Center	, the device connector, please
Application Management ~	Davias Connector	St Cattings C Batrach
Operations		tor vertings
C Infrastructure	ACCESS MODE ALLOW CONTROL Device ID	
System Configuration		ß
Inter-Region Connectivity	Claim Code	
Inter-Site Connectivity		ß
External Connectivity	Device Connector internet intersignin	
Intersight		
🖍 Administrative 🗸 🗸	Not Claimed	
	The connection to the Gisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new Open account and follow the guidance or go to the Targets page and click Claim a New Device for existing account.	
	1.0,9-1656	

- If you see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic, then your Intersight Device Connector is already configured and connected to the Intersight service, and the device is claimed.
- If you see yellow dotted lines and a caution icon connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Not Claimed** underneath the graphic, then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed. Follow these procedures to configure the Intersight Device Connector and connect to the Intersight service, and claim the device.
- **Note** If you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, go to Step 13, on page 7 to check the connections to troubleshoot the issue.
- **Step 2** Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

If there is a new Device Connector software version available and you do not have the **Auto Update** option enabled, you will see a message towards the top of the screen telling you that Device Connector has important updates available.

- If you do not want to update the software at this time, go to Step 3, on page 4 to begin configuring the Intersight Device Connector.
- If you would like to update the software at this time, click one of the two links in the yellow bar toward the top of the page, depending on how you would like to update the software:
 - Update Now: Click this link to update the Device Connector software immediately.

- Enable Auto Update: Click this link to go to the General page, where you can toggle the Auto Update field to ON, which allows the system to automatically update the Device Connector software. See About the Auto Update Option, on page 2 for more information.
- **Step 3** Locate the **Settings** link to the right of the **Device Connector** heading and click the **Settings** link.

The Settings page appears, with the General tab selected by default.

Ŧ						
Dashboard Topology Cloud Resources Application Management V	Intersight Device Connector The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connectivity the device connectivity of the device connectivity	Ctor, please				
Operations Operations Infrastructure System Configuration Inter-Region Connectivity Inter-Site Connectivity External Connectivity Intersight dministrative	Settings	×				
	1.0.91656					

Step 4 In the **General** page, configure the following settings.

a) In the **Device Connector** field, determine if you want to allow communication between the device and Cisco Intersight.

The **Device Connector** option (enabled by default) allows you to claim the device and leverage the capabilities of Intersight. If it is disabled, no communication will be allowed to Intersight.

b) In the Access Mode field, determine if you want to allow Intersight the capability to make changes to this device.

Access Mode enables you to allow full read/write operations from the cloud or restrict changes made to this device from Intersight.

- The **Read-only** option ensures that no changes are made to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.
- The **Allow Control** option (selected by default) enables you to perform full read/write operations from the cloud, based on the features available in Cisco Intersight.
- c) In the Auto Update field, determine if you want to allow the system to automatically update the software.
 - Toggle ON to allow the system to automatically update the software.
 - Toggle OFF so that you manually update the software when necessary. You will be asked to manually update the software when new releases become available in this case.

See About the Auto Update Option, on page 2 for more information.

Step 5 When you have completed the configurations in the **General** page, click **Save**.

The Intersight Device Connector overview page appears again.

- **Step 6** Continue with the next steps of the configuration process, if necessary.
 - If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to Step 7, on page 5.
 - If you want to manage certificates with the Device Connector, go to Step 10, on page 6.
 - If you want to check the connections, go to Step 13, on page 7.
- **Step 7** If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, click **Settings**, then click **Proxy Configuration**.

The Proxy Configuration page appears.

F	Cloud APIC	C Azure	ଷ୍ ଚ୍ଚାର୍ ଓ ସ େହ୍	2							
Dashboard	Intersight Devi	ce Connector		0							
Topology	intersignt Devi										
Cloud Resources	The Device Connector is an embedde visit Help Center	d management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed informa	tion about configuring the device connector, please	9							
Application Management	Settings										
Operations	Settings		^								
🔿 Infrastructure 🔨 🔨	General										
System Configuration	Proxy Configuration	Configure proxy settings									
Inter-Region Connectivity	Certificate Manager	Enable Proxy									
Inter-Site Connectivity	Connection	[Cancel Save								
External Connectivity											
Intersight	1.0.9-1656										
🖌 Administrative											

Step 8 In the **Proxy Configuration** page, configure the following settings.

In this page, you can configure the proxy that the Device Connector will use to communicate with the Intersight cloud.

- **Note** The Device Connector does not mandate the format of the login credentials; they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name depends on the configuration of the HTTP proxy server.
- a) In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.

The Proxy Hostname/IP and Proxy Port fields appear.

Ŧ	cisco Cloud Al	PIC Azure		Q 🤊 🗩	000	
Dashboard	Intersight De	vice Connector				0
Topology	intersignit De					•
Cloud Resources	The Device Connector is an emb	edded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For	detailed inf	formation about configuring the	device connector, p	please
Application Management	Cottingo					
Operations	Settings					×
O Infrastructure	General					
System Configuration	Proxy Configuration	Configure proxy settings				
Inter-Region Connectivity	Certificate Manager	Enable Proxy		Provy Port *		
Inter-Site Connectivity	Connection	Proxy Hostname/IP *	0	0	0	
External Connectivity					1 - 65535	
Intersight		Authentication				
🖍 Administrative 🗸 🗸						
				Cancel	Save	
	1.0.9-1656					

- b) In the **Proxy Hostname/IP** field, enter a Proxy Hostname and IP Address.
- c) In the **Proxy Port** field, enter a Proxy Port.
- d) In the Authentication field, toggle the Authentication option to ON to configure the proxy authentication settings.

The Username and Password fields appear.

Ē	cisco Cloud AF					Q 0				
Dashboard	Intersight De	vice Connector						0		
Topology	intersignt De									
Cloud Resources	The Device Connector is an embe visit Help Center	added management controller that enables the capab	ilities of Cisco Intersight, a cloud-ba	sed management platform.	For detailed inf	ormation about configuring	the device connector, p	lease		
Application Management	Cattings									
Operations	settings							~		
🔿 Infrastructure 🔨 🔨	General									
System Configuration	Proxy Configuration	 Configure proxy settings 								
Inter-Region Connectivity	Certificate Manager	Enable Proxy				Draw Port #				
Inter-Site Connectivity	Connection	Proxy Hostname/IP *			0	0	0			
External Connectivity							1 - 65535			
Intersight		Authentication								
🖍 Administrative 🗸 🗸		Username *) Password			• •			
						Cancel	Save			
	1.0.9-1656									

e) Enter a proxy username and password for authentication.

Step 9 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

The Intersight Device Connector overview pages appears again.

If you want to make manage certificates with the Device Connector, go to the next step.

Step 10If you want to manage certificates with the Device Connector, click Settings, then click Certificate Manager.The Certificate Manager page appears.

Ē	cisco Cloud Al				9	♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥	1
Dashboard	Intersight De	vice Connecto	r				6
Topology	intersigne De						
Cloud Resources	The Device Connector is an embry visit Help Center	edded management controller that ena	bles the capabilities of Cis	sco Intersight, a cloud-based management	platform. For detailed information about o	configuring the device connector, plea	se
Application Management	~						
Derations	Settings						×
⊖ Infrastructure	General						
System Configuration	Proxy Configuration	 Import transparent prox 	y certificate				
Inter-Region Connectivity	Certificate Manager	Trusted Certificates			(requires Base64 encoded	i certificate) 💽 Import	
Inter-Site Connectivity	Connection	Name	In Use	Issued By	Expires		
External Connectivity		Amazon Root CA 1	à Yes	Amazon Root CA 1	Jan 16, 2038 4:00 PM	۲	
Intersight		Cisco Root CA 2048	No No	Cisco Root CA 2048	May 14, 2029 1:25 PM	۲	
1º Administrative	~						
	1.0.9-1656					Close	

Step 11 In the **Certificate Manager** page, configure the following settings.

By default, the device connector trusts only the built-in svc.ucs-connect.com certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in svc.ucs-connect.com certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device or not.

Click **Import** to import a CA signed certificate. The imported certificates must be in the *.pem (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of Trusted Certificates and if the certificate is correct, it is shown in the In-Use column.

View these details for a list of certificates that are used to connect to svc.ucs-connect.com (intersight.com):

- Name—Common name of the CA certificate.
- In Use—Whether the certificate in the trust store was used to successfully verify the remote server.
- Issued By—The issuing authority for the certificate.
- Expires—The expiry date of the certificate.

Delete a certificate from the list of Trusted certificates. However, you cannot delete bundled certificates (root+intermediate certificates) from the list. The lock icon represents the Bundled certificates.

Step 12 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

The Intersight Device Connector overview pages appears again.

Step 13 Determine if you want to check the connection.

You might want to navigate to the **Connection** page to troubleshoot connection issues, such as if you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, as shown in the following figure:

F		cisco Cloud APIC 🔥 Azure	◎ ● ● ◎ ● ● ●
Dashboard		Intersight Device Connector	0
Topology		Intersight Device Connector	•
Cloud Resources	~	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the de	vice connector, please visit Help Center
Application Management	~	Device Connector	🛞 Settings 🛛 💭 Refresh
Operations	~	ACCESS MODE ALLOW CONTROL	Davies ID
C Infrastructure	^		Bendenb
System Configuration			
Inter-Region Connectivity		□ · · · · · · · · · · · · · · · · · · ·	
Inter-Site Connectivity		Device Connector Interruet Retry Connection Intersight	
External Connectivity			
Intersight		Intersiont DNS Resolve Error	
1º Administrative	~	DNS appears to be configured, but unable to resolve the DNS name of Intersight. Intersight may be in maintenance	
		For more diagnostic information, please check the connection tool. Open Settings	
		Remediations	
		Verify the DNS server IP addresses configured are valid Open Settings	
		Verify the DNS servers are reachable from Device Connector.	
		1.0.9-1056	

In that case, navigate to the **Connections** page by clicking on **Open Settings** in the **Device Connector** graphic, or by clicking **Settings**, then clicking **Connections**.

The **Connections** page appears.

F	Cloud APIC 🔥 Azure							
Dashboard	ersight Device Connector							
Topology								
Cloud Resources	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, platform with Hein Center	lease						
Application Management	Entiron							
Operations	setungs	*						
🔿 Infrastructure 🔨 🤨	General Charles and the Charles and Charle							
System Configuration	Proxy Coniguration Cileck Connection Last Cileck Run Filme -							
Inter-Region Connectivity	Connection							
Inter-Site Connectivity								
External Connectivity	1.0.9-1056							
Intersight								
🖍 Administrative 🗸 🗸								

Click **Check Connection** to check the connections, then use the information provided in the page to address any connection issue that you might have.

Ŧ	cisco Cloud AP	Q 💿 🛛 🕸 Q 💶								
Dashboard	Intersight Dev	tersight Device Connector								
Topology	intersignt Dev									
Cloud Resources ~	The Device Connector is an embed visit Help Center	led management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed	information about configuring the device connector, please							
Application Management ~	Sattinge									
Operations	Settings		*							
⊖ Infrastructure ∧	General									
System Configuration	Proxy Configuration	Check Connection Last Check Run Time a few seconds ago								
Inter-Region Connectivity	Certificate Manager	The connection check was successful								
Inter-Site Connectivity	Connection	Results	View All Details							
External Connectivity		O DNS Resolution	View Details							
Intersight		⊘ TCP Connection	View Details							
🖍 Administrative 🗸 🗸		O TLS Connection	View Details							
		⊘ Bandwidth Test	View Details							
			Close							
	1.0.9-1656									

Click Close when you're finished with this page.

What to do next

Claim the device using the instructions provided in Claiming a Device Using the GUI, on page 9.

Claiming a Device Using the GUI

Before you begin

Configure the Cisco Intersight Device Connector information from the Cisco Cloud APIC site using the instructions provided in Configuring the Intersight Device Connector, on page 3.

Procedure

Step 1	Navigate to the Cisco Intersight cloud site:						
	https://www.intersight.com						
Step 2	Enter the necessary information to log into the Cisco Intersight cloud site.						
Step 3	Select the appropriate account and role, if necessary.						
	The Profiles page appears.						
Step 4	Navigate to Admin > Targets.						
	The Targets page appears.						

≡	cisco Intersight	ADMIN > Targets				٩	⊵ q,	0 0) (&
×	CONFIGURE ^								Claim a New Target
	Profiles	* All Targets ⊚ +							
	Pools		1 Filter				0 items found	10 v per page	• K < 0 of 0 > ≫
ē	ADMIN ^	Connection 2	lop large X						
	Targets								
		Name		Status		Claimed Time		Claimed By	
									K < 0 of 0 > X

Step 5 Click Claim a New Target.

The Select Target Type page appears.

≡	cisco Intersight	ADMIN > Targets > Claim a New	r Target							2
×	CONFIGURE ^			Select Target Type						
	Policies Pools		Filters	Q. Search						
ē	ADMIN ^		Available for Claiming	Compute / Fabric						
	Targets		Categories All Gourd	Cisco UCS Server (Standaione) Cisco UCS Domain (Intersight Managed)	Cisco UCS Domain (UCSM Managed)		M			
			Compute / Fabric Hyperconverged	citado cisco UCS C890			I			
			Orchestrator	Platform Services						
			Platform Services	Cisco Intersight Appliance Cisco Intersight Assist	Intersight	workload Engi	☆ ne			
				Cloud						
				Cloud						
				Orchestrator			-			
		Cancel							Start	



=	cisco Intersight	ADMIN > Targets > Claim a New Target) () () () () () () () () () () () () ()
×	CONFIGURE ^	Select Target Type	
	Profiles		
	Policies	Filters Q, Search	
ē	ADMIN ^	Available for Claiming Network	
	Tatyets	Categories Article Cisco APIC Cisco Cloud APIC Cisco Clou	
		Compute / Fabric Hyperconverged Cisco Nexus Bashboard	
		Orchestrator Platform Services	
		Cancel	Start

Step 7 Click the **Cisco Cloud APIC** button, then click **Start**.

The Claim Cisco Cloud APIC Target page appears.

	cisco Intersight	ADMIN > Targets > Claim a New Target	© © &
	CONFIGURE ^ Profiles Policies Pools	Claim Cisco Cloud APIC Target To claim your target, provide the Device ID, Claim Code and select the appropriate Resource Groups.	
ē	ADMIN ^		
	Targets	Device ID * O	<u> </u>
		< Back Cancel	Claim

Step 8 In the Cisco Cloud APIC site, navigate back to **Infrastructure** > **Intersight**.

The Intersight Device Connector overview page appears.

Step 9 From the Cisco Cloud APIC site, copy the values in the **Device ID** and **Claim Code** fields, then paste them into the proper fields in the **Claim a New Device** page in the Cisco Intersight cloud site.

For each area in the Cisco Cloud APIC site, click the clipboard next to that field to copy the information into the clipboard, then paste it into the proper fields in the **Claim a New Device** page in the Cisco Intersight cloud site.

Ŧ	cisco Cloud APIC Azure	Q o d () 🔅 P 💶
Dashboard	Intersight Device Connector	Ø
Topology		Ŭ
Cloud Resources	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed inform visit Help Center	nation about configuring the device connector, please
Application Management ~	Davias Connector	St Pattings C Patroch
Operations		137 Gettings V Kerrean
C Infrastructure	ACCESS MODE ALLOW CONTROL	evice ID
System Configuration		
Inter-Region Connectivity		laim Code
Inter-Site Connectivity		B
External Connectivity	Dence Connector internet intersigni (9
Intersight		
🖍 Administrative 🗸 🗸	Not Claimed	
	The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Targets page and click Claim a New Device for existing account.	

Step 10 In the Cisco Intersight cloud site, claim the Cisco Cloud APIC target.

After you paste the Cisco Cloud APIC values in the **Device ID** and **Claim Code** fields in the Cisco Intersight cloud site, click **Claim** in the bottom right area of the page.

≡	cisco Intersight	ADMIN > Targets > Claim a New Target		₽ ₽ ९ © ©	۵
×	CONFIGURE ^		Claim Cisco Cloud APIC Target		
	Profiles		To claim your target, provide the Device ID, Claim Code and select the appropriate Resource Groups		
	Policies		● 451		
	Pools	Davies ID K	Claim Pada I		
(Ē	ADMIN ^				
	Targets				
4					
		< Back Cancel			Claim

The Targets page appears again, with the Cisco Cloud APIC shown in the table and Connected in the Status column.

≡	داندان Intersight	ADMIN > Targets	Q Q Q Q A
×	CONFIGURE ^		Claim a New Target
	Profiles	¥ All Tarrets @ +	
	Policies	Add Filter G	Export 1 items found 10 v per page 🔣 🔇 1 of 1 🕞 河
	Pools	Connection % Too Taroe %	
喠	ADMIN ^	© Connected 1	
	Targets		
Į.		Name Status Type Claimed	Time 💠 Claimed By 💠 🖗
		ACI-Cloud-Fabric-1 © Connected Cisco Cloud APIC a few set	conds ago ····
			K < 1 of 1 > N

Step 11 Go back to the **Intersight Device Connector** page in the Cisco Cloud APIC GUI and verify that Cisco Intersight successfully claimed the system.

You will see green-dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic.

Ŧ		Q 🔊 🔍 🕽 🏵 🗨 💶
💿 Dashboard	Intersight Device Connector	0
Topology		0
Cloud Resources	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform connector please visit Hein Center	n. For detailed information about configuring the device
Application Management ~	Davies Comparison	C Detroit
Operations	Device connector	çes settings 🕤 Kerresn
O Infrastructure	ACCESS MODE ALLOW CONTROL	Device ID
System Configuration		
Inter-Region Connectivity		Claimed to Account
Inter-Site Connectivity		CloudAPIC-admin O
External Connectivity	bence connector intener intener	
Intersight		
🖍 Administrative 🗸 🗸	Claimed	
	1.0.9-1656	

Note You may have to click **Refresh** in the **Intersight Device Connector** page in the Cloud APIC GUI to update the information in the page to the current state.

If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight Device Connector** page in the Cisco Cloud APIC GUI and click that link.

A popup page appears, asking you to confirm that you want to unclaim the device.



WARNING! This device will be unclaimed from Intersight

When possible, you should unclaim this device from the Intersight portal.

Unclaiming the device will delete device configuration data from your Intersight account. The endpoint will continue to retain these configured settings and will be managed locally from the device. For more information, click here.



Click Unclaim again to confirm that you want to unclaim this device.

• In the Intersight Device Connector page in the Cisco Cloud APIC GUI, the status changes to Not Claimed.

Ŧ		cisco Cloud APIC Azure	Q O D () & ? 1
Dashboard		Intersight Device Connector	0
Topology			•
Cloud Resources	~	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed in visit Helio Canter	formation about configuring the device connector, please
Application Management	~	Davies Composter	C altre C ates
Operations	~	Device Connector	(3) Setungs (3) Kerresn
C Infrastructure	^	ACCESSINGLE ALLOW CONTROL	Device ID
System Configuration			E .
Inter-Region Connectivity			Claim Code
Inter-Site Connectivity			E .
External Connectivity		Device Connector Internet Intersignt	0
Intersight			
1º Administrative	\sim	Not Claimed	
		The connection to the Olsco Intersight Portal is successful, but device is still not claimed. To claim the device open Claco Intersight, create a new open account and follow the guidance or go to the Targets page and click. Claim a New Device for existing account.	
		1.0.9-1630	

• In the Targets page in the Cisco Intersight cloud site, the status changes to Unclaimed.

≡	،،ا،،،ا،، دוدده Intersight	ADMIN	N > Targets					٩	_ ⊡ _ ¢		0	<u>ه</u>
×	CONFIGURE ^										Claim a New	Target
	Profiles	* A	× All Targets ⊙ +									
	Pools			Add Filter					1 items found	10 v per page		
Ō	ADMIN ^	Con	nection X Unclaimed 1	Top Targe X								
	Targets											
			Name		Status	Туре		Claimed Time		Claimed By		
					O Unclaimed	Cisco CAPIC		5 minutes ago				
			Belected 1	of 1 Show Selected								

You can then click the box next to the Cisco Cloud APIC in the **Targets** page in the Cisco Intersight cloud site and click the trashcan icon to delete that target, if necessary.

Note You can also unclaim the device and delete the target in a single step, without having to perform any actions in the Cisco Cloud APIC GUI, by clicking the box next to the Cisco Cloud APIC in the **Targets** page in the Cisco Intersight cloud site and then clicking the trashcan icon.

A popup page appears, asking you to confirm that you want to unclaim the device.



Click **Unclaim** again to confirm that you want to unclaim this device.

© 2022 Cisco Systems, Inc. All rights reserved.

cisco.

Americas Headquarters Cisco Systems, Inc. San Jose, CA 95134-1706 USA Asia Pacific Headquarters CiscoSystems(USA)Pte.Ltd. Singapore Europe Headquarters CiscoSystemsInternationalBV Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.