Cisco Intersight OnPremises: Deployment, Verification and Troubleshooting

Contents

Introduction
Prerequisites
Requirements
IP Address and Hostname Requirements
Port Requirements
Connectivity Requirements
Supported Browsers
Software Compatibility
Components Used
Configure
Claiming a Device
Unclaim a device
Network Diagram
Configurations
Verify
Troubleshoot
Scenario 1
Scenario 2
APPENDIX A - BIND DNS Sample

Introduction

Cisco Intersight provides infrastructure management for Cisco Unified Compute System (Cisco UCS) and Cisco HyperFlex platforms. This platform offers an intelligent level of management that enables IT organizations to analyze, simplify, and automate their environments in more advanced ways than previous generations of tools.

Cisco Intersight Virtual Appliancedelivers the management features of Intersight for Cisco UCS and HyperFlex in an easy to deploy VMware OVA that allows you to control what system details leave your premises. The Virtual Appliance form factor enables additional data locality, security, or compliance needs that are not completely met by intersight.com.Cisco Intersight Virtual Appliancerequires a connection back to Cisco and Intersight services for updates and access required services for full functionality of intersight.com.Cisco Intersight Virtual Applianceis not intended for an environment where you operate data centers with no external connectivity.

This guide provides an overview of how to install and set up Cisco Intersight Virtual Appliance in your environment.

Contributed by Brian Morrissey and Mohammed Majid Hussain, Cisco CX Engineers.

Prerequisites

Understanding of UCS, DNS records

Requirements

TheCisco Intersight Virtual ApplianceOVA can be deployed on VMware ESXi 6.0 and higher. The following sections describe the various system requirements to install and deployCisco Intersight Virtual Appliance:

Item	System Requirements

Supported Hypervisors	VMware ESXi 6.0 and higher VMware vSphere Web Client 6.5 and higher
Storage	500 GB. Cisco recommends that you use thin provisioning to optimize disk storage usage.
RAM	32 GB
vCPU Cores	16

Note

Cisco Intersight Virtual Appliancesupports managing up to 2000 servers per deployment and deploying 50 service profiles.

IP Address and Hostname Requirements

Setting up Intersight Appliance requires an IP address and 2 hostnames for that IP address. The hostnames must be in the following formats:

- myhost.mydomain.com—A hostname in this format is used to access the GUI. This must be defined as anA record and PTR recordin DNS. The PTR record is required for reverse lookup of the IP address. If an IP address resolves to multiple hostnames, the first resolved hostname is used.
- dc-myhost.mydomain.com—Thedc-must be prepended to your hostname. This hostname must be defined as theCNAME of myhost.mydomain.com. Hostnames in this format are used internally by the appliance to manage device connections.

Attention

Ensure that the appropriate entries of typeA, CNAME, and PTR recordsexist in the DNS, as described above.

Port Requirements

The following table lists the ports required to be open for Intersight Appliance communication.

Port	Protocol	Description
443	TCP/UDP	This port is required for communication between: • Intersight Virtual Appliance and the users' web browser. • Intersight Virtual Appliance to and from the endpoint devices. • Intersight Virtual Appliance and the required hosted services (svc.ucs-connect.com OR svc.intersight.com). For more information about connectivity, seeConnectivity Requirements.
80	TCP	This port is required for communication between: • Intersight Virtual Appliance and the users' web browserfor initial monitoring of the appliance setup. • Upgrade of the device connector from Intersight cloud.For more information, seeDevice Connector Upgrade. • Port 80 is used as an HTTP proxy port. All other traffic on port 80 is redirected to port 443.

Connectivity Requirements

- Intersight Virtual Appliance must properly resolve svc.ucs-connect.com(intersight.com). If a proxy is required for an HTTPS connection to svc.ucs-connect.com, it can be configured in the device connector user interface.
- Ensure that there is no firewall between the appliance and the endpoint.
- Ensure thatCisco Intersight Virtual Appliancehas access to the following sites directly or through a proxy. For more information about setting up a proxy, seeCloud Connection. All the following URLs are accessed through HTTPS:svc.intersight.com—for the device connector to access Intersight servicescisco.com—For access to all Cisco URLsapi.cisco.com:443— for access to Cisco Software download sitetools.cisco.com:443—for access to Cisco Smart Licensing Manager

Supported Browsers

Cisco Intersight runs on the following minimum supported browser versions:

- Google Chrome 62.0.3202.94
- Firefox 57.0.1

- Safari 10.1.1

Software Compatibility

This section contains details about the minimum versions of the following software supported by the appliance:

Component	Minimum Supported Version
Cisco UCS Manager	3.2(1)
Cisco HyperFlex Connect and Data Platform	2.6
Cisco IMC	3.1(3) for M5 Servers 3.0(4) for M4 Servers For more information about the Cisco IMC Software requirements for the M4 and M5 Servers, see the Supported Systems sect Help Center. SeeTable 1for a complete list of the supported software and the required device connector versions.

Important

- Cisco Intersight Virtual Appliance does not support claiming or managing Cisco UCS Director.

Components Used

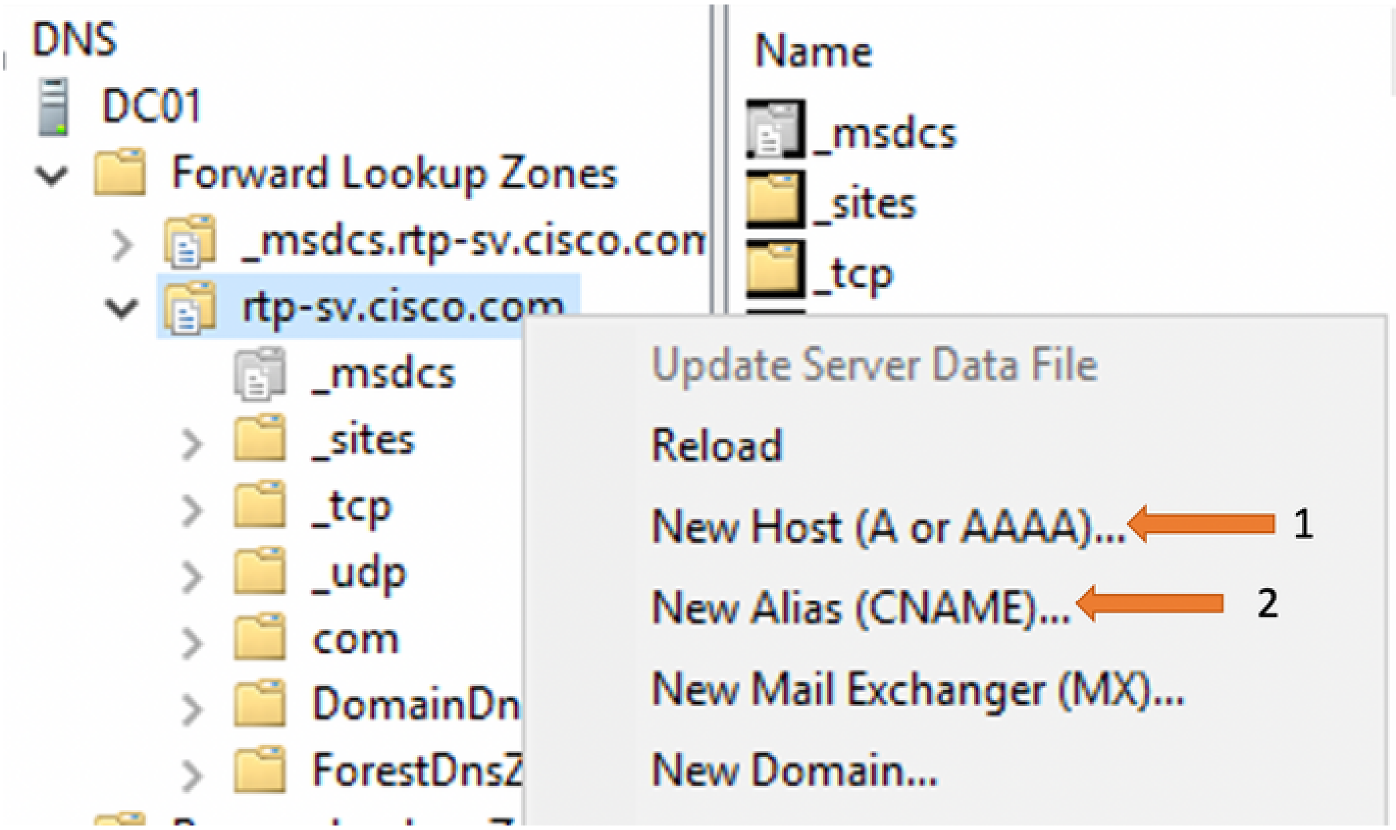
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

UCSM 4.0(1c)

Cisco Intersight Appliance 1.0.9-7

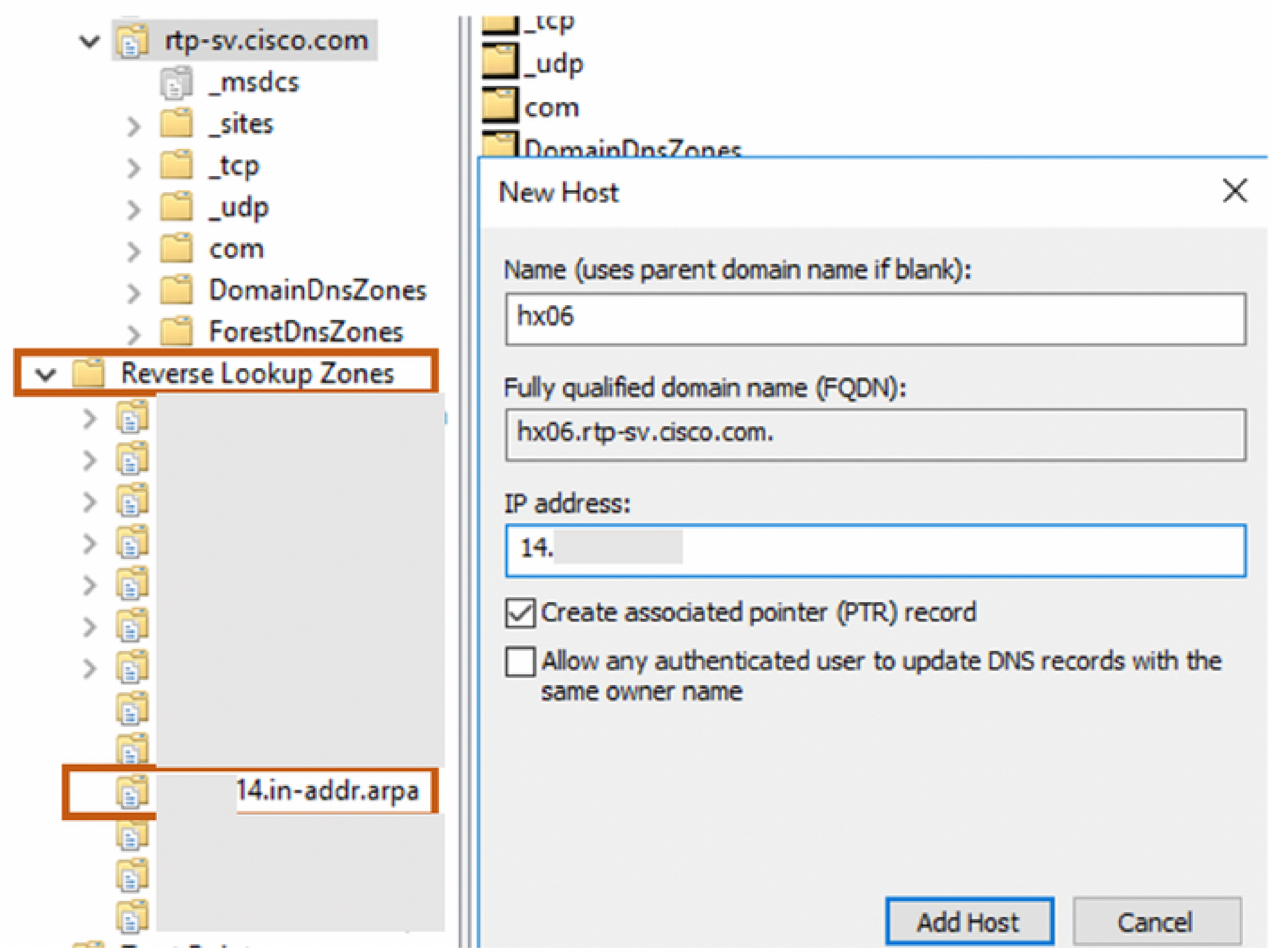
Configure

Configure DNS A record and CNAME



Make sure you have defined reverse lookup zone for the subnet in question.

Define DNS A record as shown then click Add Host



New Host

Name (uses parent domain name if blank):
hx06

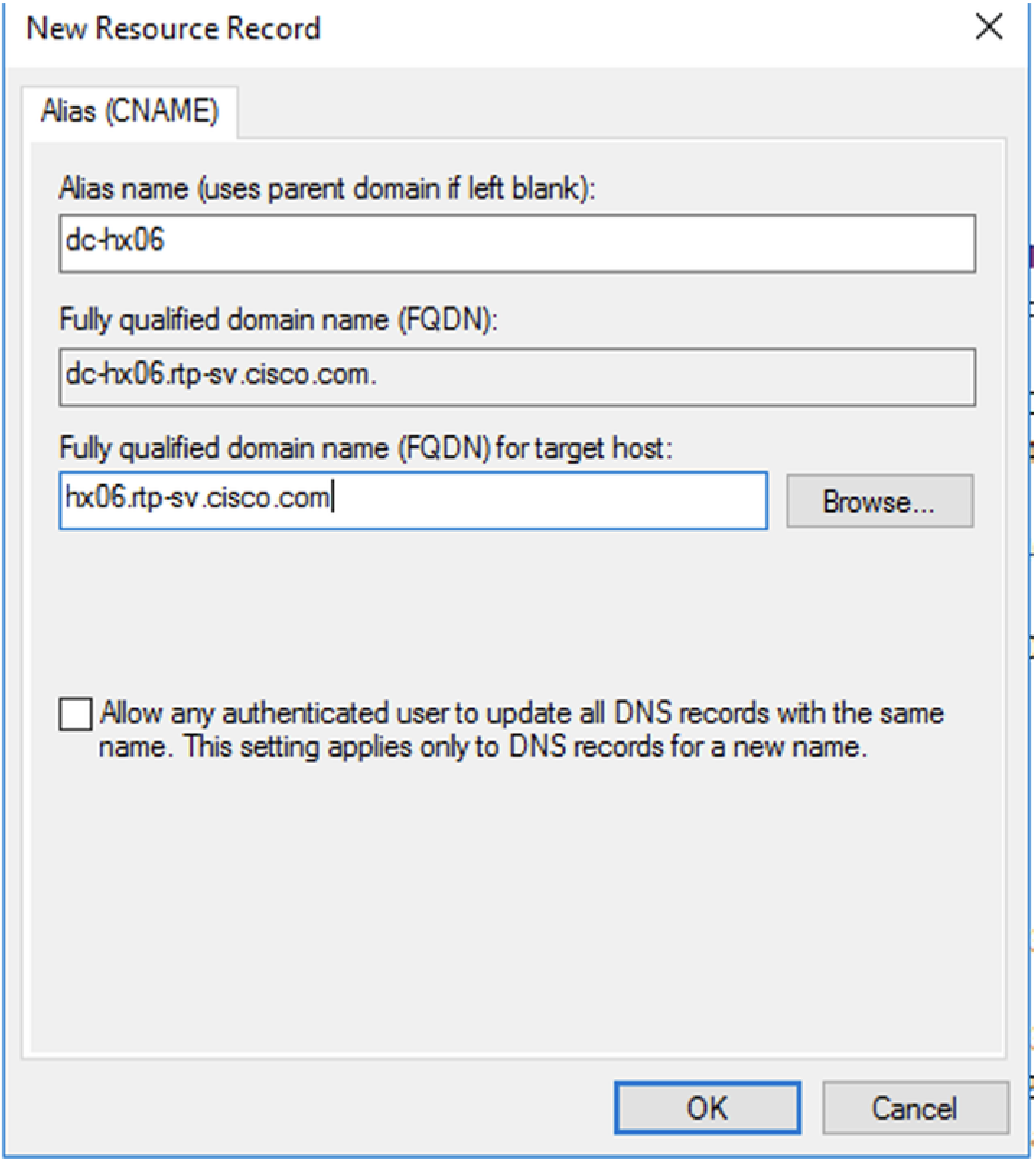
Fully qualified domain name (FQDN):
hx06.rtp-sv.cisco.com.

IP address:
14.[redacted]

☑ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

Define CNAME as shown



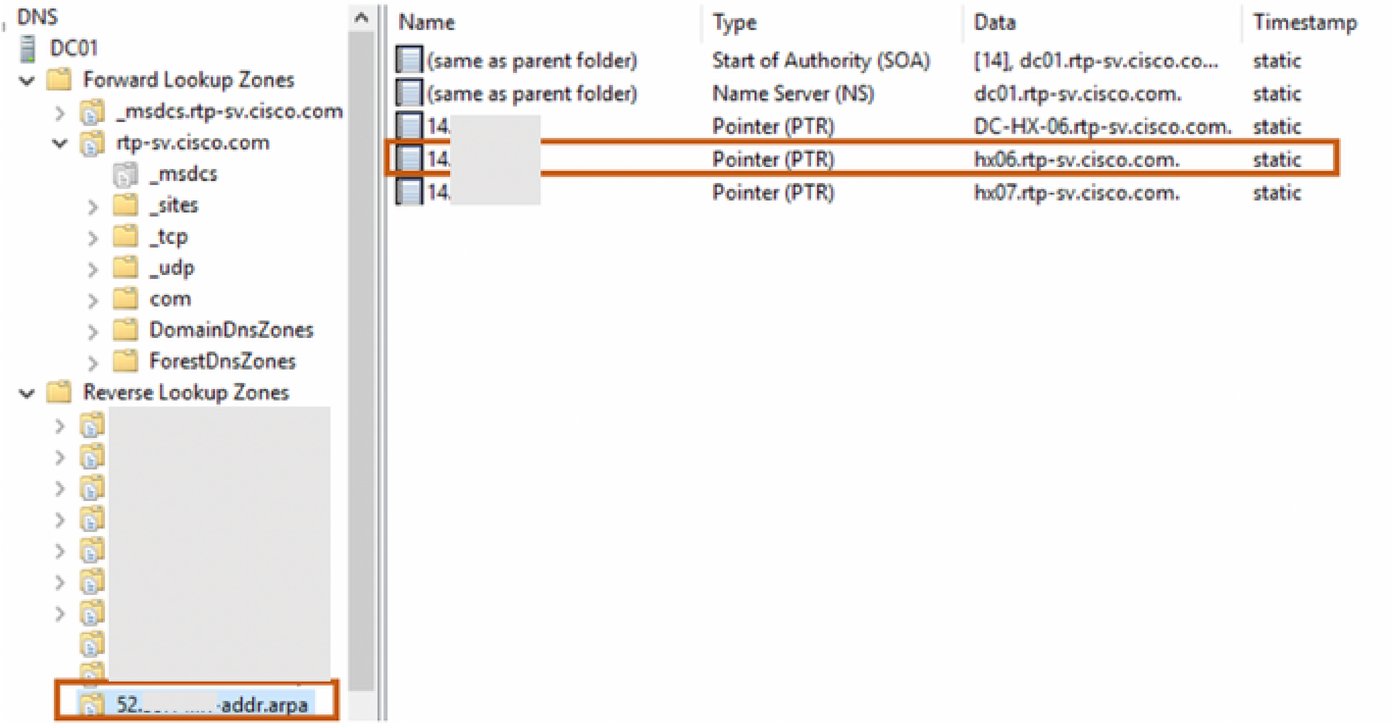
Alias name (uses parent domain if left blank): dc-hx06

Fully qualified domain name (FQDN): dc-hx06.rtp-sv.cisco.com.

Fully qualified domain name (FQDN) for target host: hx06.rtp-sv.cisco.com

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Verify that the PTR record is configured.

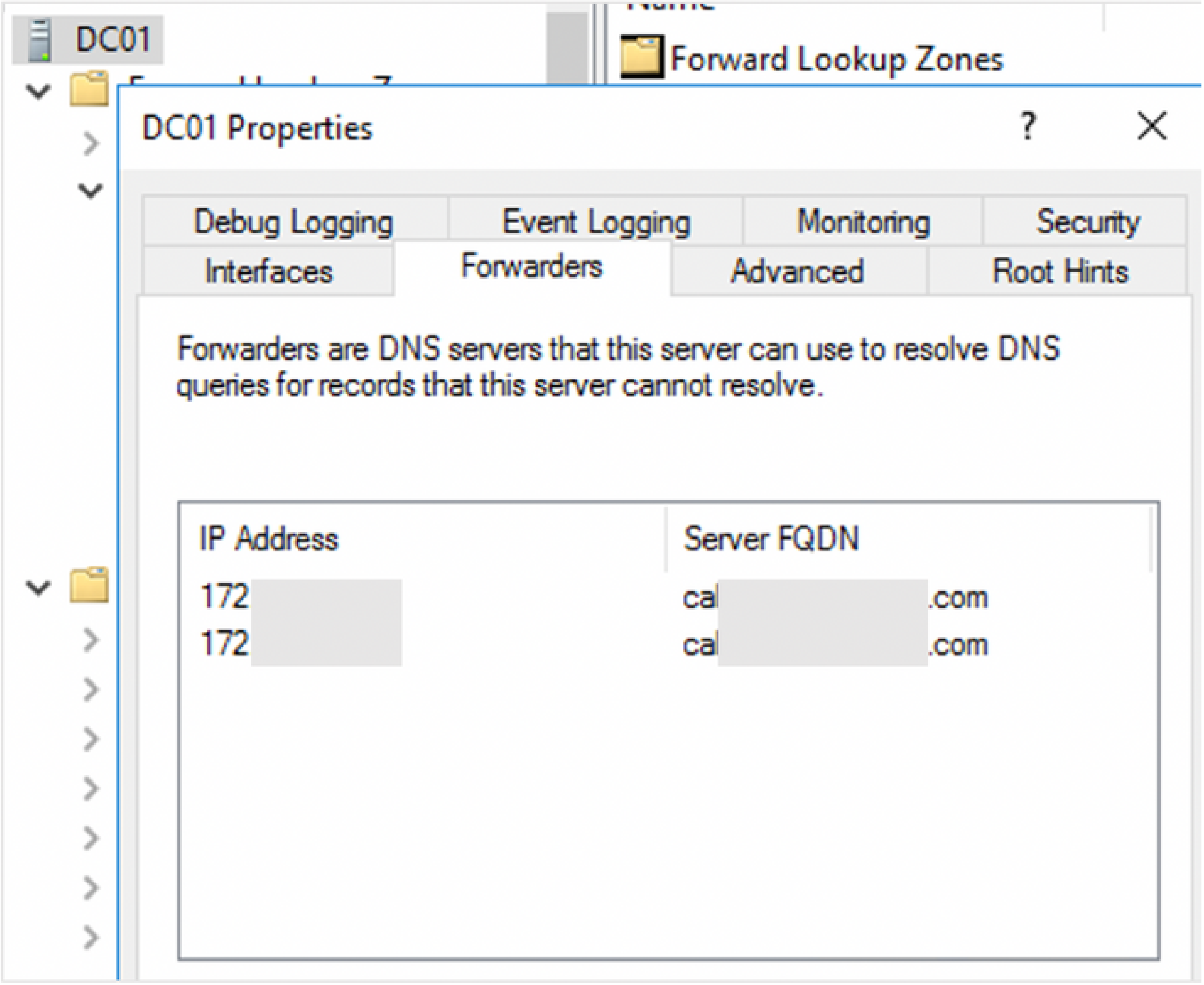


[redacted]

52.[redacted]-addr.arpa

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], dc01.rtp-sv.cisco.co...	static
(same as parent folder)	Name Server (NS)	dc01.rtp-sv.cisco.com.	static
14.[redacted]	Pointer (PTR)	DC-HX-06.rtp-sv.cisco.com.	static
14.[redacted]	Pointer (PTR)	hx06.rtp-sv.cisco.com.	static
14.[redacted]	Pointer (PTR)	hx07.rtp-sv.cisco.com.	static

Configure forwarders as necessary



Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

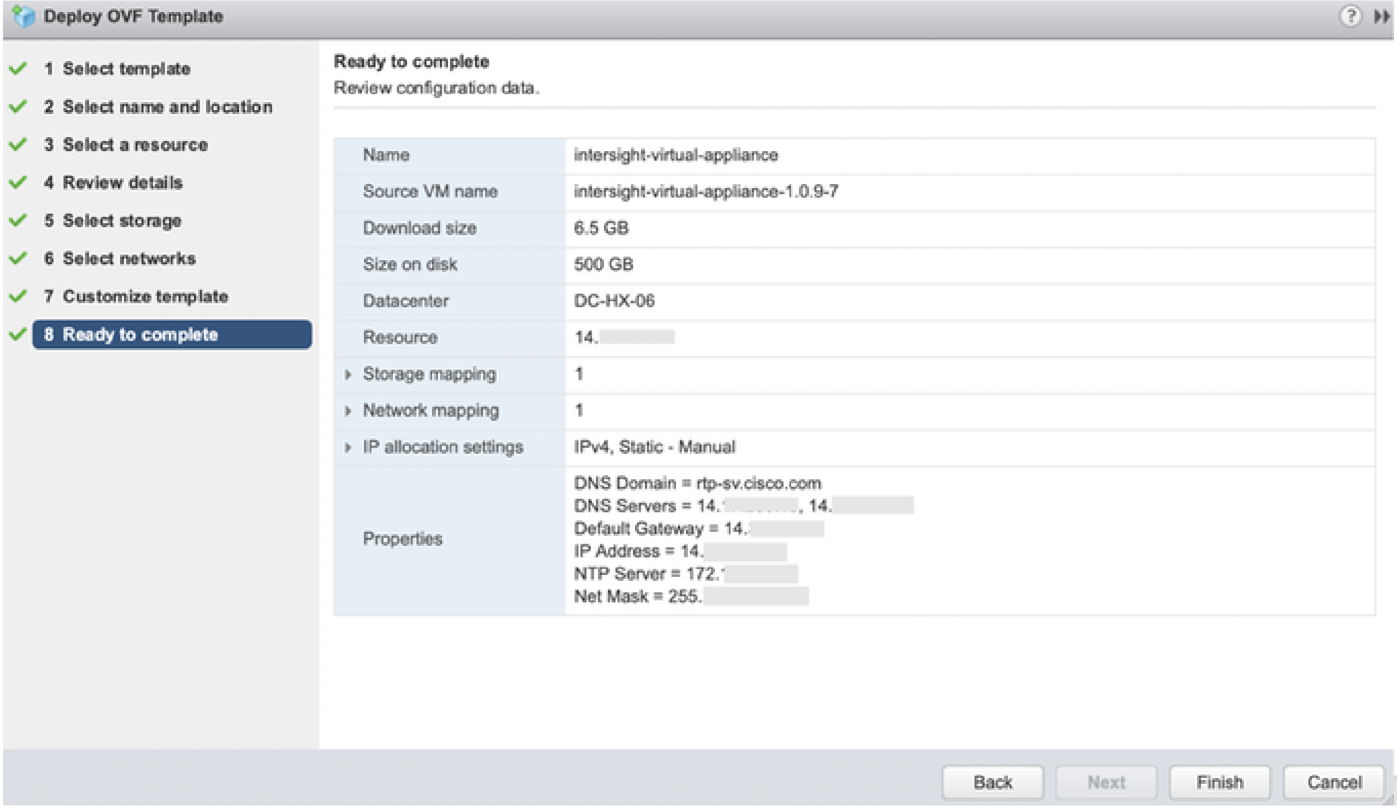
IP Address	Server FQDN
172[redacted]	ca[redacted].com
172[redacted]	ca[redacted].com

Once the DNS setting have been configured, proceed towards deploying the Intersight Appliance.

Log in to VMware vSphere Web Client with administrator credentials.

Right-click on the host and select Deploy OVF Template.

Go through the wizard and review the details in the Ready to complete section

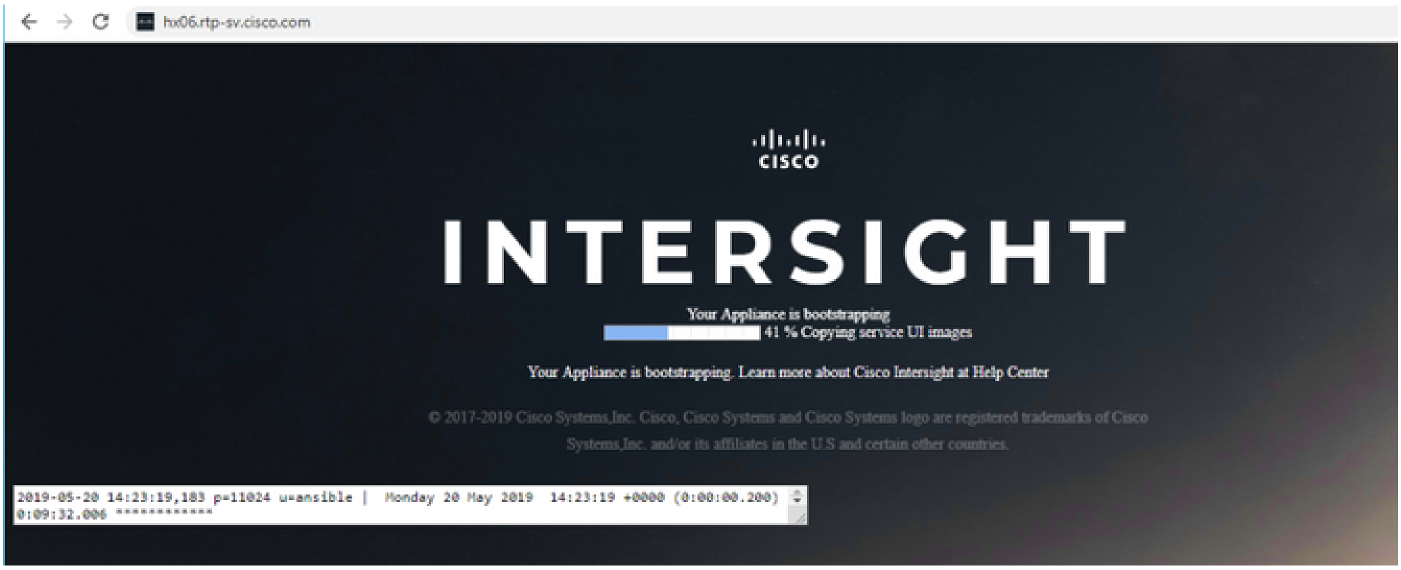


Ready to complete
Review configuration data.

Name	intersight-virtual-appliance
Source VM name	intersight-virtual-appliance-1.0.9-7
Download size	6.5 GB
Size on disk	500 GB
Datacenter	DC-HX-06
Resource	14.[redacted]
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual
Properties	DNS Domain = rtp-sv.cisco.com DNS Servers = 14.[redacted], 14.[redacted] Default Gateway = 14.[redacted] IP Address = 14.[redacted] NTP Server = 172.[redacted] Net Mask = 255.[redacted]

Specify the DNS name you configured earlier in the web browser and you should be able to monitor the progress of the deployment

You can click on the progress bar to view more details in the form of rolling log messages



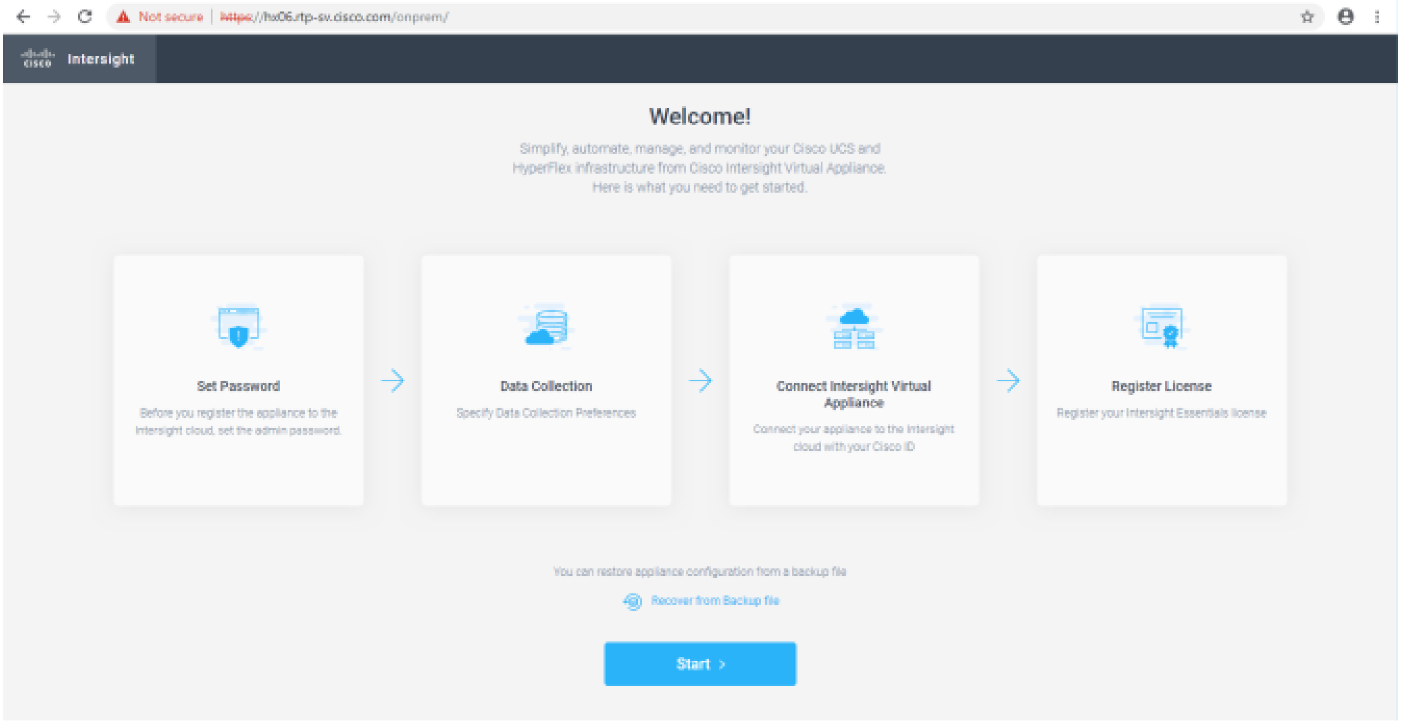
Your Appliance is bootstrapping
41 % Copying service UI images

Your Appliance is bootstrapping. Learn more about Cisco Intersight at Help Center

© 2017-2019 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries.

```
2019-05-20 14:23:19,183 p=11024 u=ansible |  Monday 20 May 2019  14:23:19 +0000 (0:00:00.200)
0:09:32.006 ************
```

After you install the Cisco Intersight Virtual Appliance OVA, go <<*http://your fqdn.com*>> to access the Initial Setup Wizard. The wizard enables you to complete the setup of the Intersight appliance. Use the following instructions to complete the setup



Welcome!

Simplify, automate, manage, and monitor your Cisco UCS and HyperFlex infrastructure from Cisco Intersight Virtual Appliance. Here is what you need to get started.

Set Password
Before you register the appliance to the Intersight cloud, set the admin password.

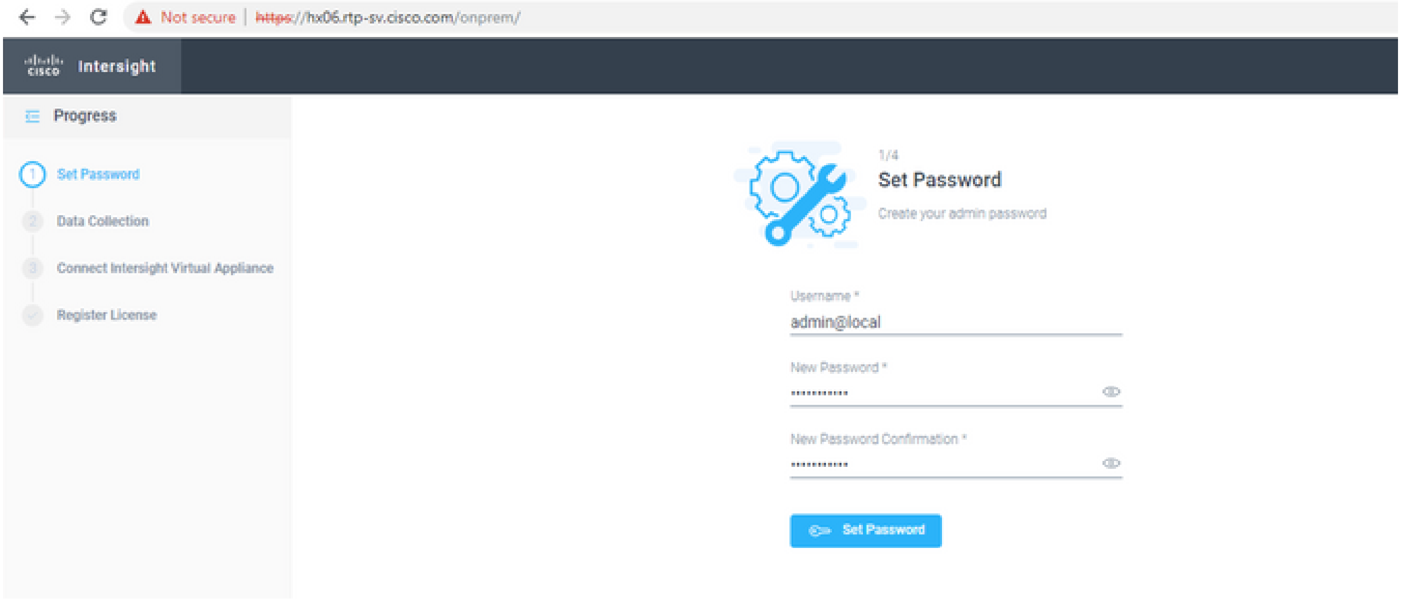
Data Collection
Specify Data Collection Preferences

Connect Intersight Virtual Appliance
Connect your appliance to the Intersight cloud with your Cisco ID

Register License
Register your Intersight Essentials license

You can restore appliance configuration from a backup file

Set Password—Before you register the appliance with Intersight, you must create an admin password. The password can contain 0-9, A-Z, a-z, and all special characters except a colon (:) and space. You must use the same password to log in to Intersight.



Not secure | https://hx06.rtp-sv.cisco.com/onprem/
cisco Intersight
Progress
1 Set Password
2 Data Collection
3 Connect Intersight Virtual Appliance
Register License

1/4
Set Password
Create your admin password

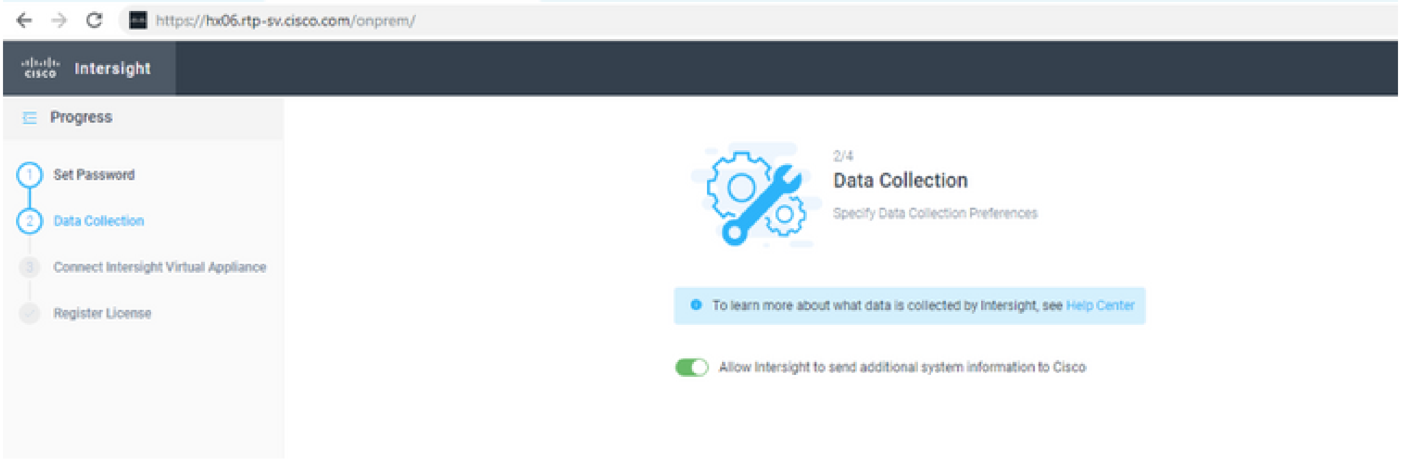
Username *
admin@local

New Password *
••••••••••••

New Password Confirmation *
••••••••••••

Data Collection—Specify your preference to allow Intersight to send additional system information to Cisco. This option is enabled by default.

For more information about what data is collected by Intersight, see Data Collected from Intersight Virtual Appliance



https://hx06.rtp-sv.cisco.com/onprem/

Intersight

Progress

1 Set Password

2 Data Collection

3 Connect Intersight Virtual Appliance

Register License

2/4

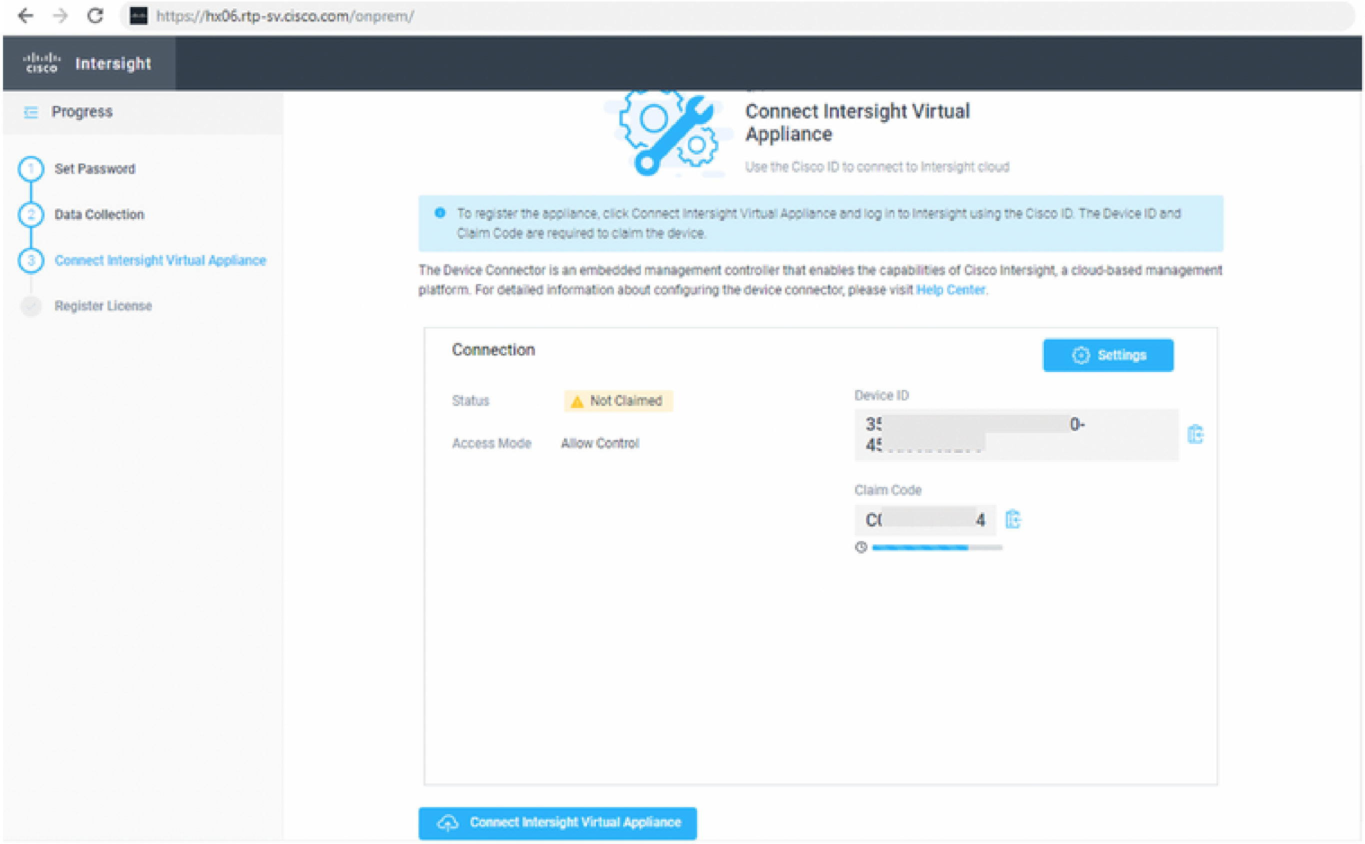
Data Collection

Specify Data Collection Preferences

To learn more about what data is collected by Intersight, see Help Center

Allow Intersight to send additional system information to Cisco

Connect Intersight Virtual Appliance—Click to connect Cisco Intersight Virtual Appliance to Intersight services using your Cisco ID. If you do not have a Cisco ID, you can create onehere



https://hx06.rtp-sv.cisco.com/onprem/

Intersight

Progress

1 Set Password

2 Data Collection

3 Connect Intersight Virtual Appliance

Register License

Connect Intersight Virtual Appliance

Use the Cisco ID to connect to Intersight cloud

To register the appliance, click Connect Intersight Virtual Appliance and log in to Intersight using the Cisco ID. The Device ID and Claim Code are required to claim the device.

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, please visit Help Center.

Connection

Settings

Status: Not Claimed

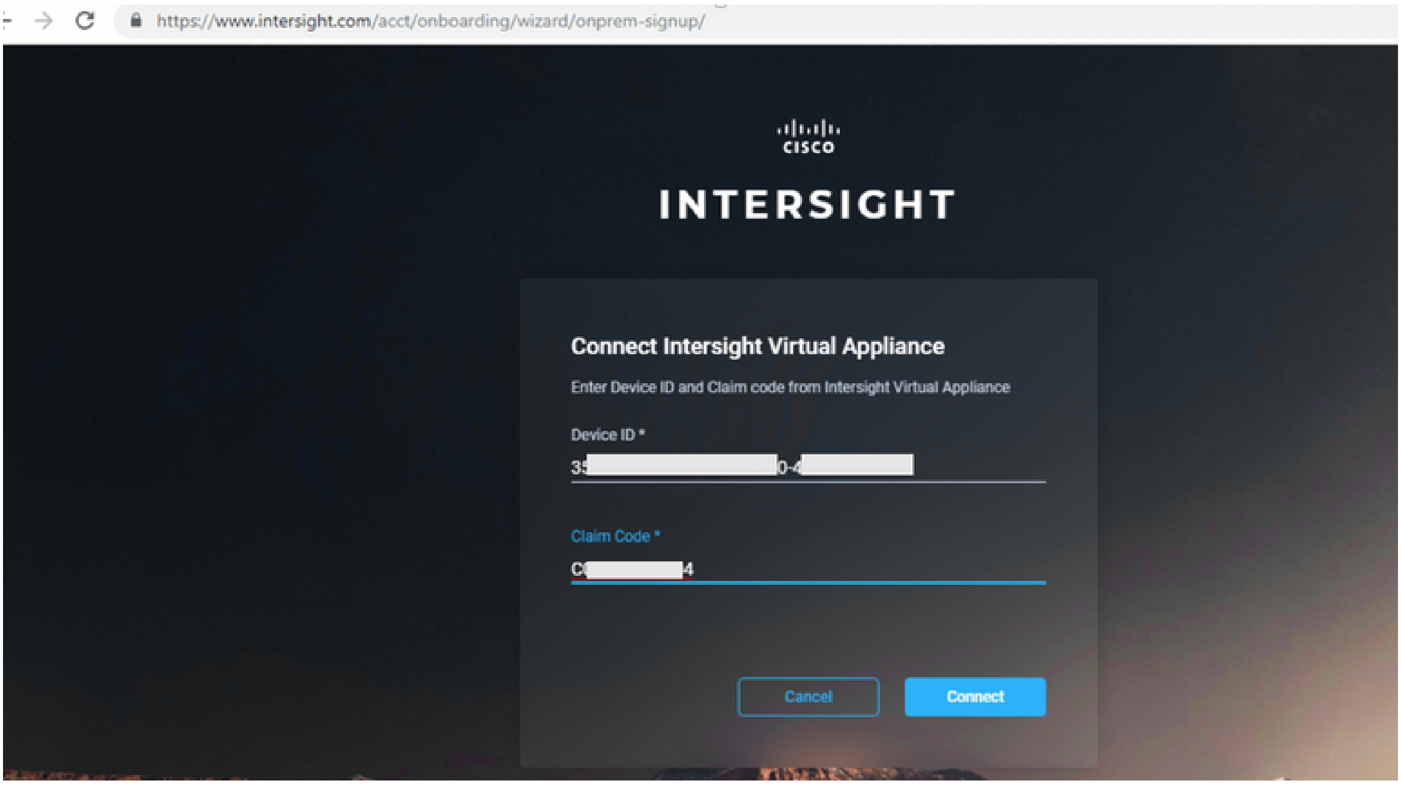
Access Mode: Allow Control

Device ID: 35[redacted]0- 45[redacted]

Claim Code: C[redacted]4

Connect Intersight Virtual Appliance

Specify the Device ID and the Claim Code from the Intersight Virtual Appliance



https://www.intersight.com/acct/onboarding/wizard/onprem-signup/

cisco

INTERSIGHT

Connect Intersight Virtual Appliance

Enter Device ID and Claim code from Intersight Virtual Appliance

Device ID *

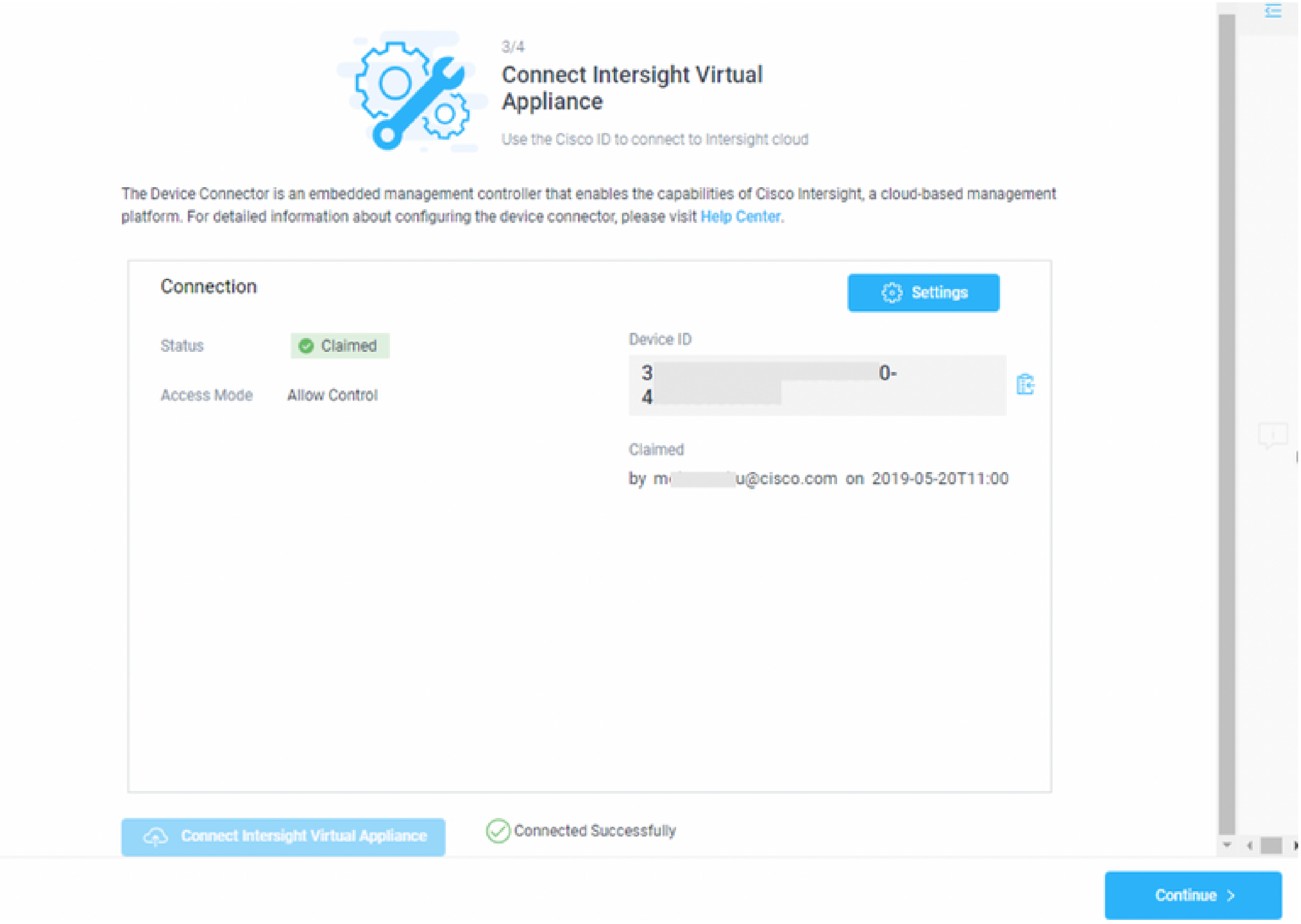
35[redacted]0-4[redacted]

Claim Code *

C[redacted]4

Cancel Connect

A successful claim should look like so



3/4

Connect Intersight Virtual Appliance

Use the Cisco ID to connect to Intersight cloud

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, please visit Help Center.

Connection

Settings

Status: Claimed

Access Mode: Allow Control

Device ID

3[redacted]0-
4[redacted]

Claimed

by m[redacted]u@cisco.com on 2019-05-20T11:00

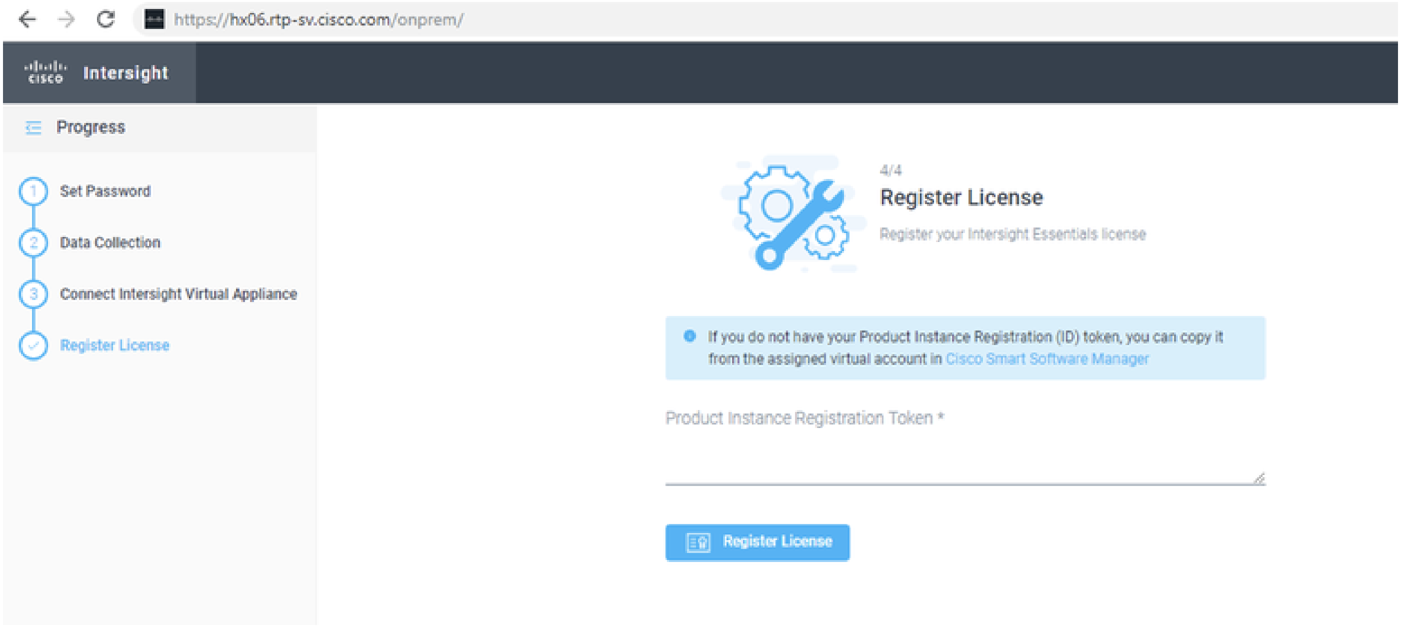
Connect Intersight Virtual Appliance

Connected Successfully

Continue >

Register License—Click Register License. Obtain a license registration token from Cisco Smart License Manager, and apply add the token to activate your license. The license registration process could take a few minutes to complete. For more information about registering your

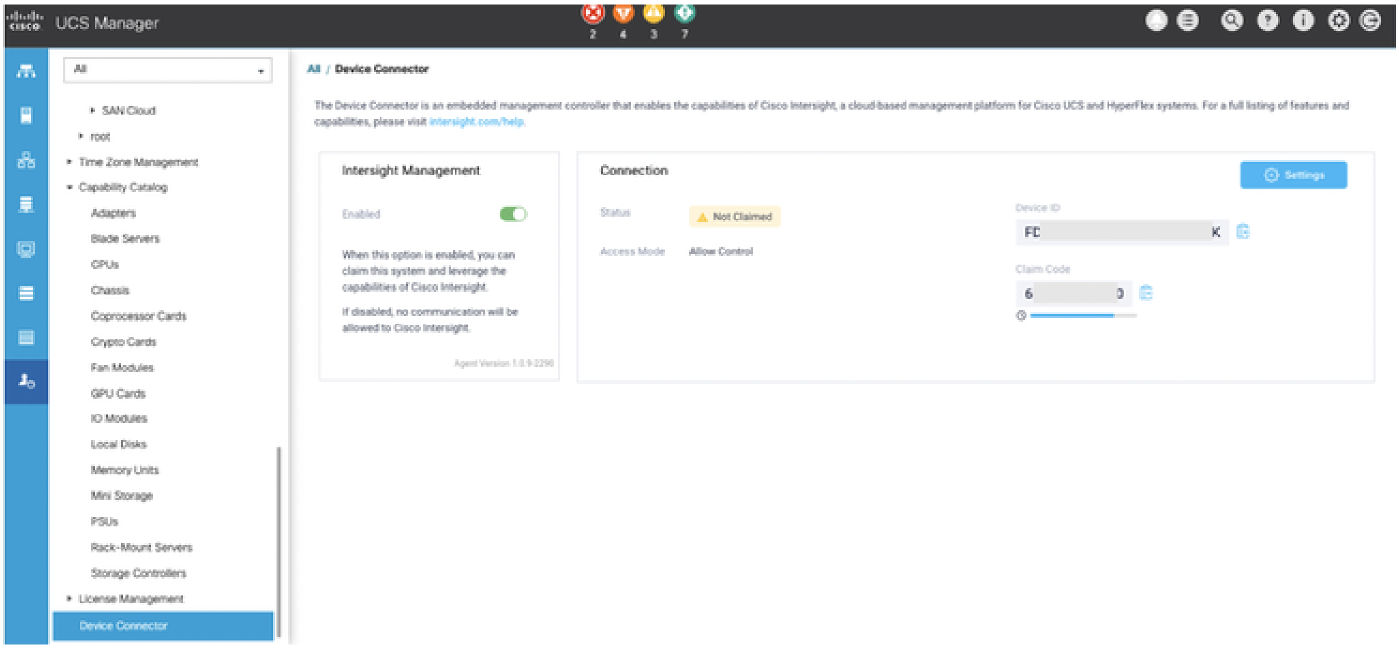
Intersight license, watch Activating Intersight License


https://hx06.rtp-sv.cisco.com/onprem/
Intersight
Progress
1 Set Password
2 Data Collection
3 Connect Intersight Virtual Appliance
Register License
4/4
Register License
Register your Intersight Essentials license
Register License

If you do not have your Product Instance Registration (ID) token, you can copy it from the assigned virtual account in Cisco Smart Software Manager

Product Instance Registration Token *

Claiming a Device



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform for Cisco UCS and HyperFlex systems. For a full listing of features and capabilities, please visit intersight.com/help.

Intersight Management

Enabled

When this option is enabled, you can claim this system and leverage the capabilities of Cisco Intersight.

If disabled, no communication will be allowed to Cisco Intersight.

Agent Version 1.0.9-2290

Connection

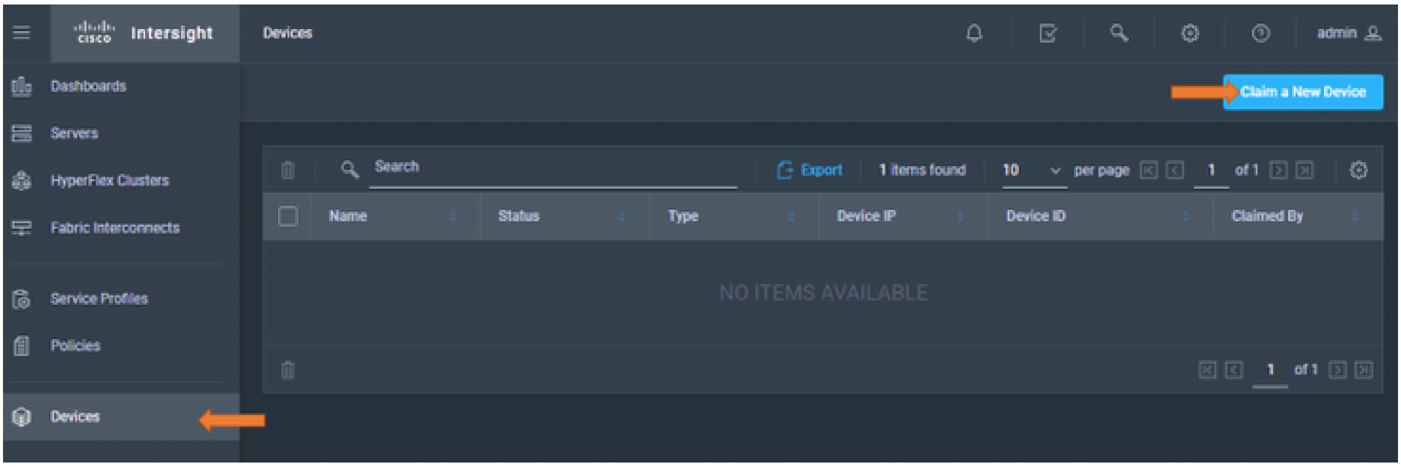
Status: Not Claimed

Access Mode: Allow Control

Device ID: FC[redacted]K

Claim Code: 6[redacted]0

From Intersight Dashboard>Devices, click Claim a New Device



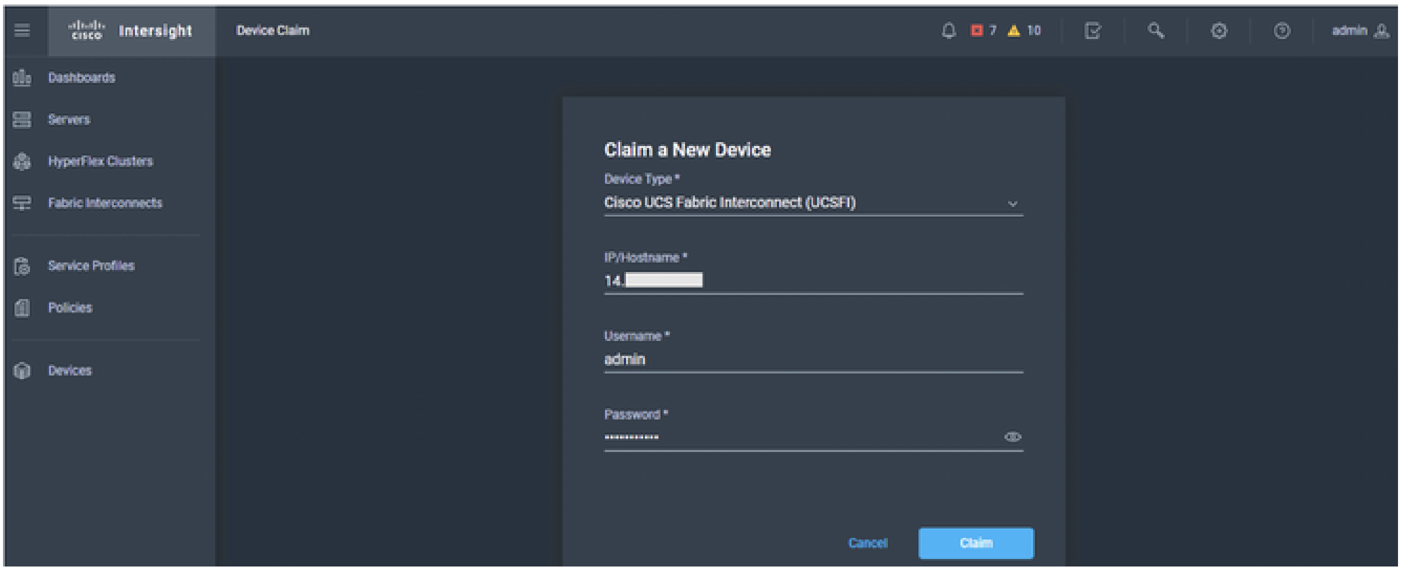
Select theDevice Typefrom the drop-down list.

You can select a Cisco UCS Fabric Interconnect, Integrated Management Controller or a HyperFlex Server.

Enter the IP/Hostname of the device you want to claim.

Enter the Username for the device. This user must have administrative privileges.

Enter the Password for the user and click Claim to initiate device claim.



Claim a New Device

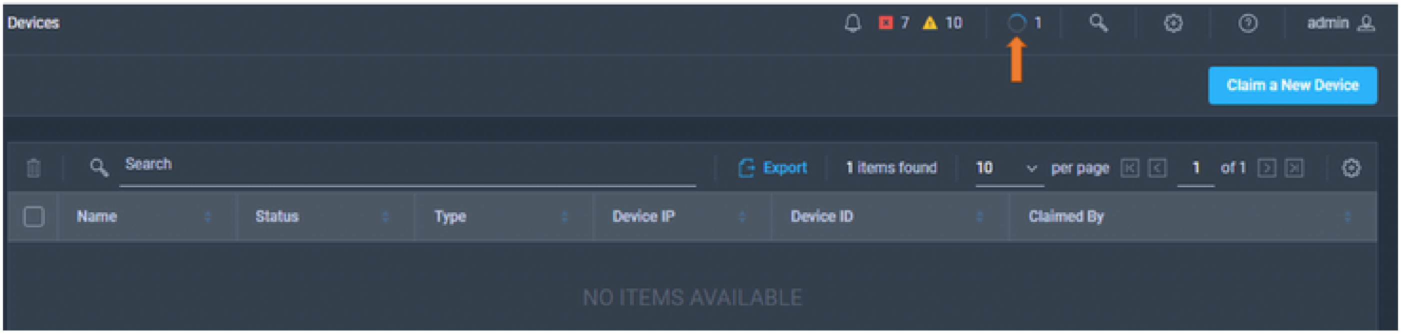
Device Type *
Cisco UCS Fabric Interconnect (UCSFI)

IP/Hostname *
14.[redacted]

Username *
admin

Password *
••••••••••••

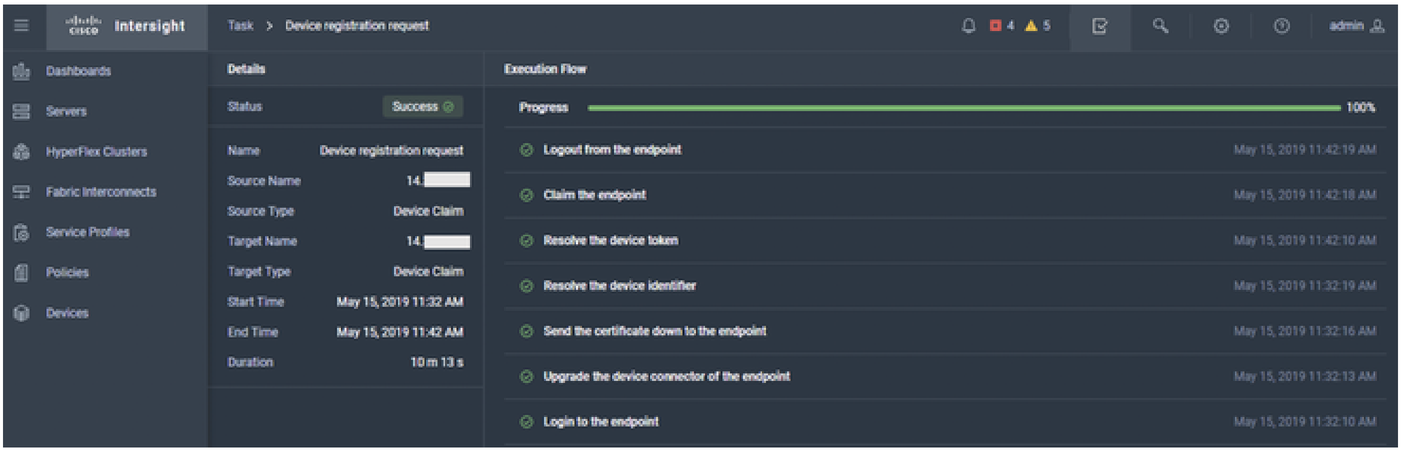
You can monitor the progress of the claim by clicking on the revolving circular icon



Name	Status	Type	Device IP	Device ID	Claimed By

NO ITEMS AVAILABLE

The device claim process could take a few minutes. If required, the Device Connector will be automatically upgraded as part of the process.



Details

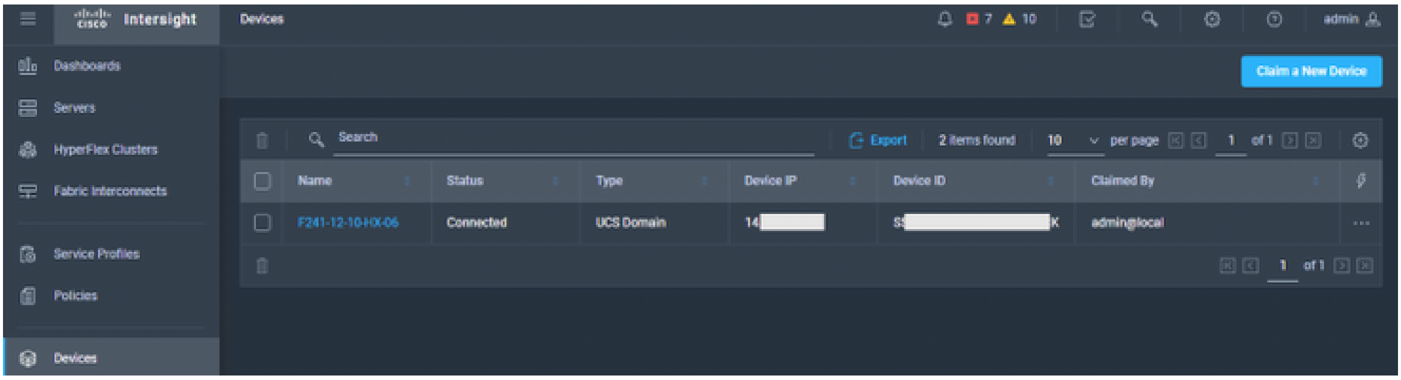
Status	Success
Name	Device registration request
Source Name	14.[redacted]
Source Type	Device Claim
Target Name	14.[redacted]
Target Type	Device Claim
Start Time	May 15, 2019 11:32 AM
End Time	May 15, 2019 11:42 AM
Duration	10 m 13 s

Execution Flow

Progress 100%

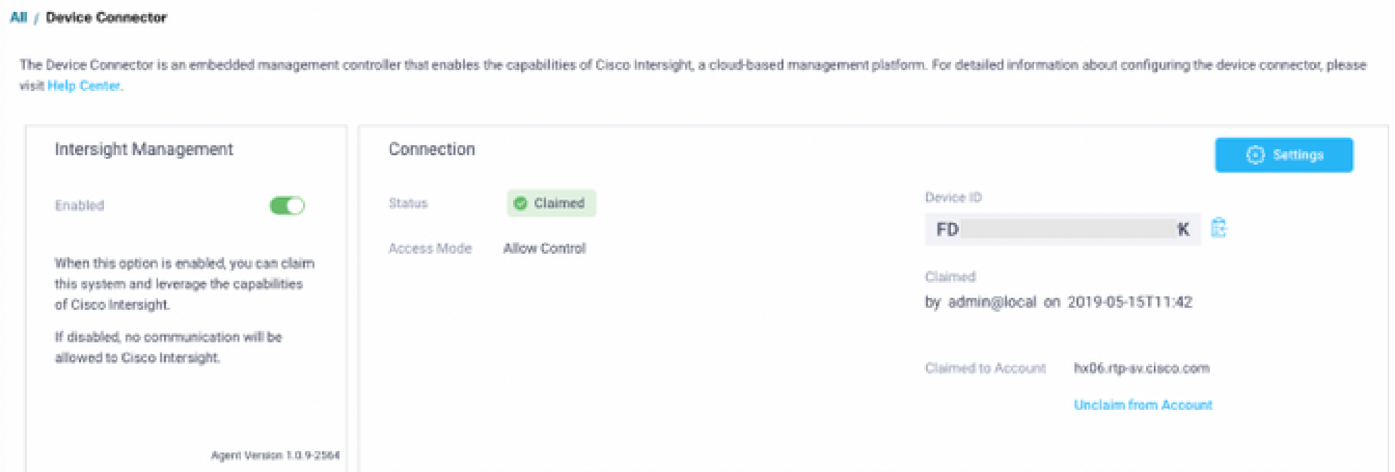
✓ Logout from the endpoint	May 15, 2019 11:42:19 AM
✓ Claim the endpoint	May 15, 2019 11:42:18 AM
✓ Resolve the device token	May 15, 2019 11:42:10 AM
✓ Resolve the device identifier	May 15, 2019 11:32:19 AM
✓ Send the certificate down to the endpoint	May 15, 2019 11:32:16 AM
✓ Upgrade the device connector of the endpoint	May 15, 2019 11:32:13 AM
✓ Login to the endpoint	May 15, 2019 11:32:10 AM

Once a device is successfully claimed, it would should up in the Devices section



Name	Status	Type	Device IP	Device ID	Claimed By
F241-12-10-HX-06	Connected	UCS Domain	14[redacted]	S[redacted]K	admin@local

We could also login to the UCSM (in this case) and verify the claim status



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, please visit Help Center.

Intersight Management

Enabled

When this option is enabled, you can claim this system and leverage the capabilities of Cisco Intersight.

If disabled, no communication will be allowed to Cisco Intersight.

Agent Version 1.0.9-2564

Connection

Status: Claimed

Access Mode: Allow Control

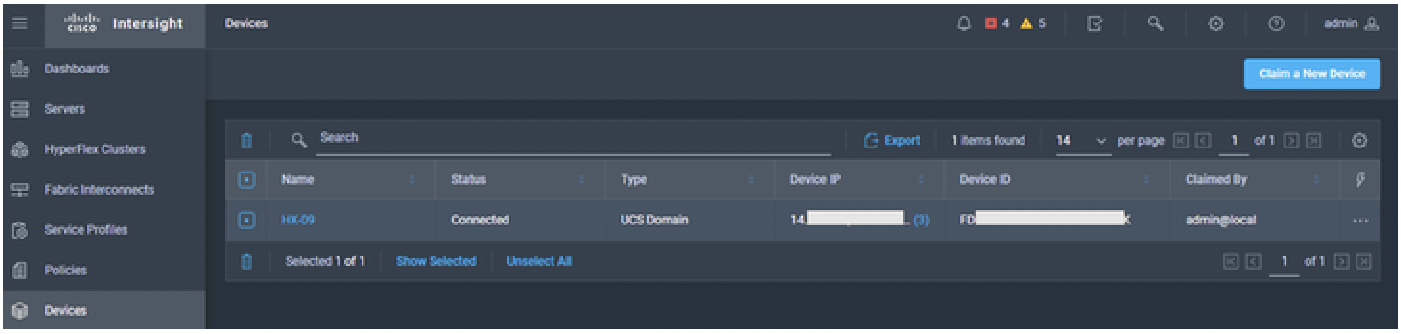
Device ID: FD[redacted]K

Claimed by admin@local on 2019-05-15T11:42

Claimed to Account: hx06.rtp-sv.cisco.com

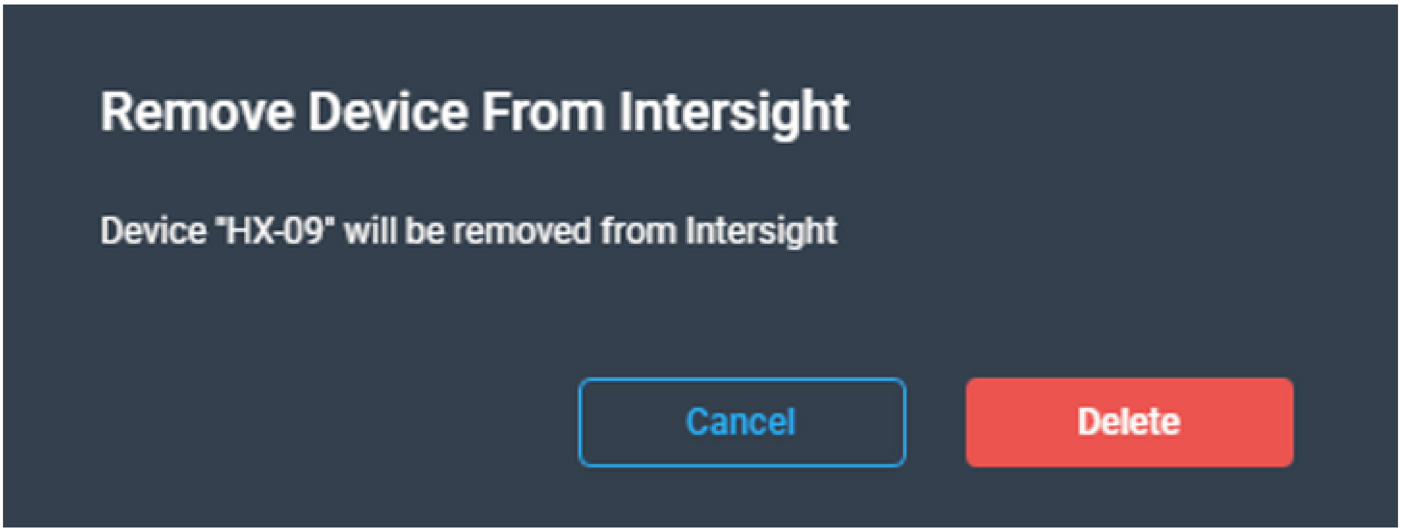
Unclaim a device

You can unclaim a device by selecting a device from Devices>Device Table view, and clicking Delete



Name	Status	Type	Device IP	Device ID	Claimed By
HX-09	Connected	UCS Domain	14[redacted] (3)	FD[redacted]K	admin@local

Click Delete to unclaim



Remove Device From Intersight

Device "HX-09" will be removed from Intersight

Network Diagram

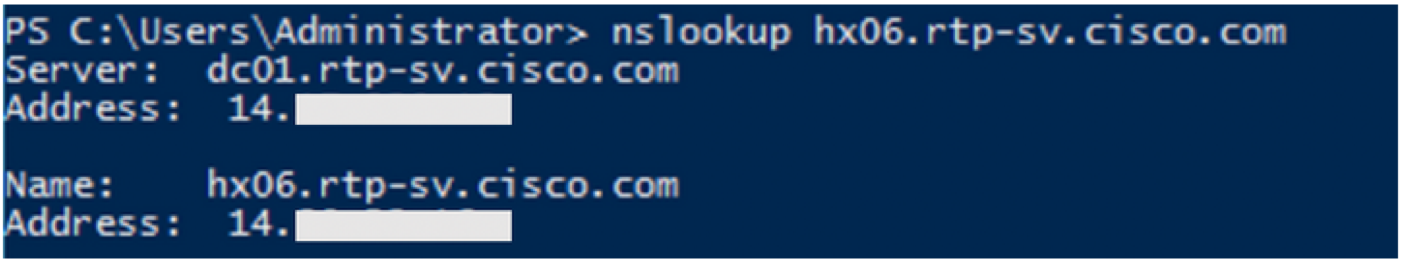
N/A

Configurations

N/A

Verify

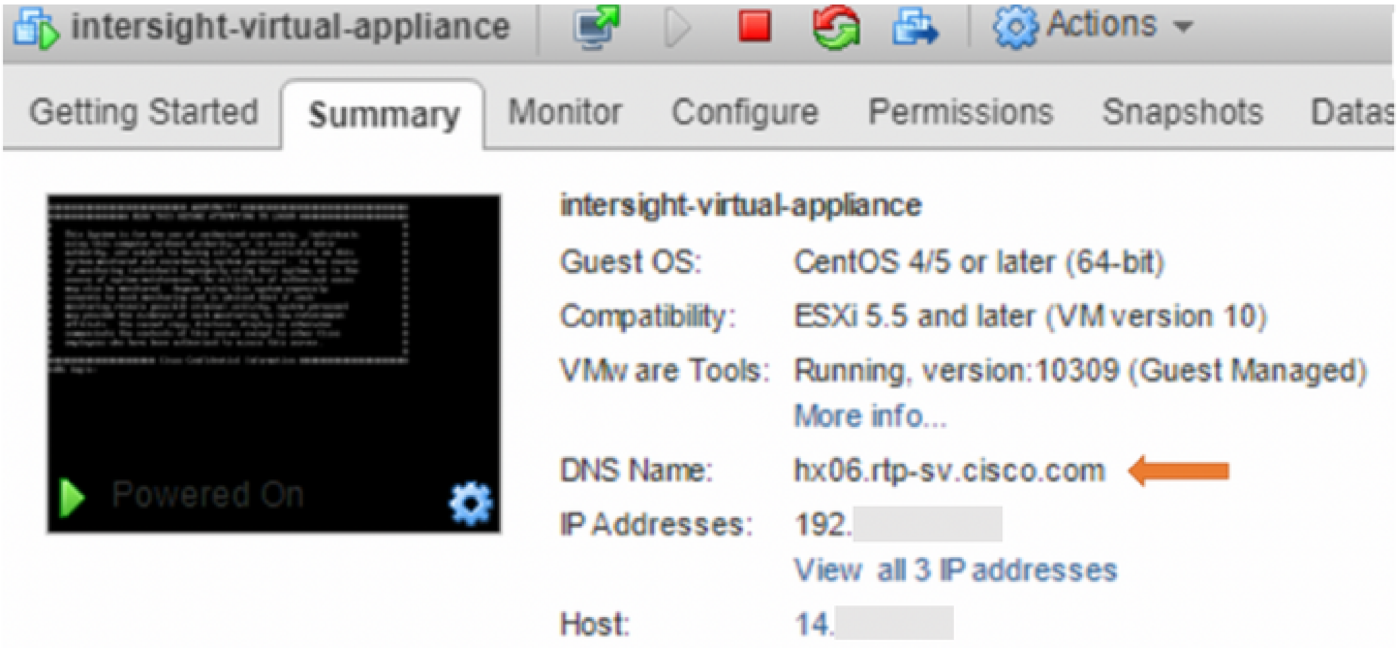
Confirm if your FQDN resolves to the IP address you specified



```
PS C:\Users\Administrator> nslookup hx06.rtp-sv.cisco.com
Server:  dc01.rtp-sv.cisco.com
Address:  14.[redacted]

Name:    hx06.rtp-sv.cisco.com
Address:  14.[redacted]
```

Click on the Intersight Appliance. Under the Summary tab you should be able to see the DNS name being resolved



intersight-virtual-appliance

Guest OS: CentOS 4/5 or later (64-bit)

Compatibility: ESXi 5.5 and later (VM version 10)

VMware Tools: Running, version:10309 (Guest Managed)

More info...

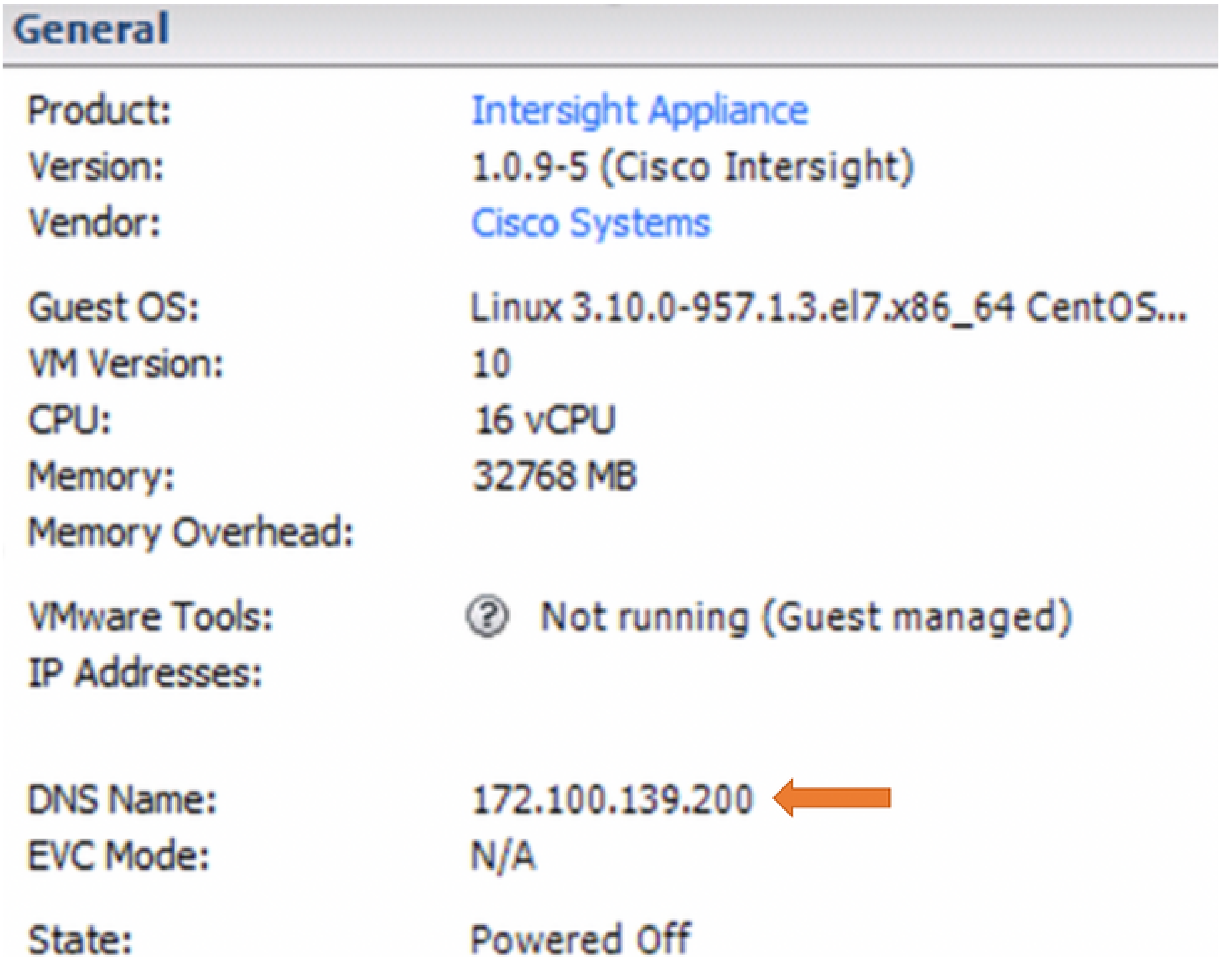
DNS Name: hx06.rtp-sv.cisco.com

IP Addresses: 192.[redacted]

View all 3 IP addresses

Host: 14.[redacted]

If DNS resolution wasn't successdul, it would look something like this:



Product: Intersight Appliance

Version: 1.0.9-5 (Cisco Intersight)

Vendor: Cisco Systems

Guest OS: Linux 3.10.0-957.1.3.el7.x86_64 CentOS...

VM Version: 10

CPU: 16 vCPU

Memory: 32768 MB

Memory Overhead:

VMware Tools: Not running (Guest managed)

IP Addresses:

DNS Name: 172.100.139.200

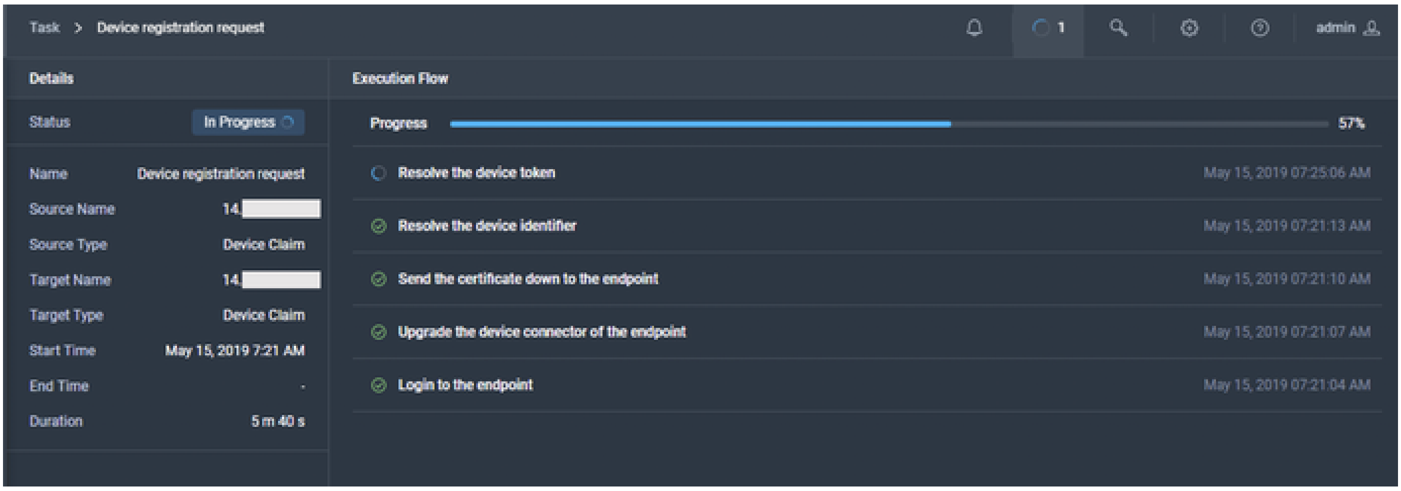
EVC Mode: N/A

State: Powered Off

Troubleshoot

Scenario 1

If the progress bar (under device registration) on the appliance looks hung or fails, give UCSM a look and see what it reports



Details

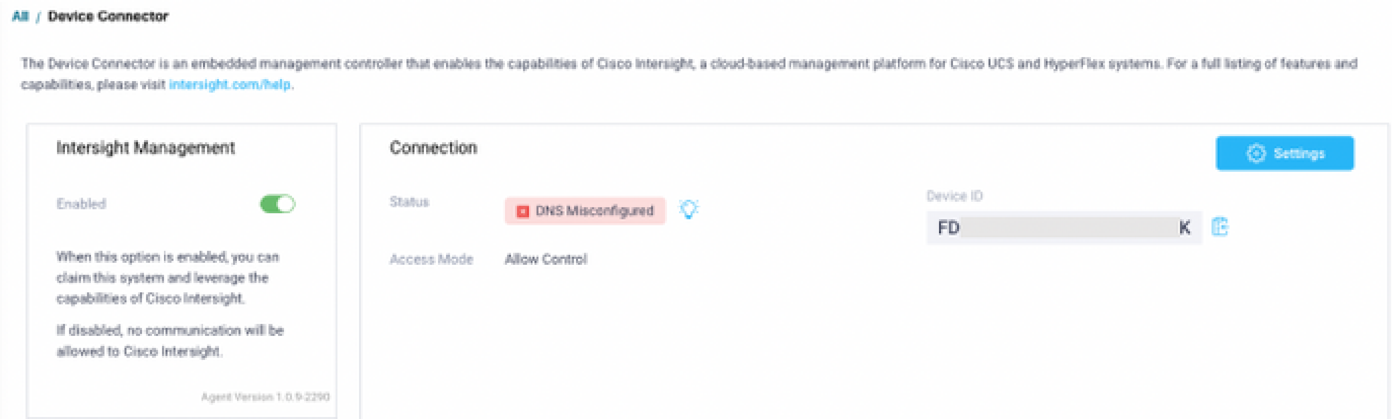
Status	In Progress
Name	Device registration request
Source Name	14.[redacted]
Source Type	Device Claim
Target Name	14.[redacted]
Target Type	Device Claim
Start Time	May 15, 2019 7:21 AM
End Time	-
Duration	5 m 40 s

Execution Flow

Progress 57%

○ Resolve the device token	May 15, 2019 07:25:06 AM
✓ Resolve the device identifier	May 15, 2019 07:21:13 AM
✓ Send the certificate down to the endpoint	May 15, 2019 07:21:10 AM
✓ Upgrade the device connector of the endpoint	May 15, 2019 07:21:07 AM
✓ Login to the endpoint	May 15, 2019 07:21:04 AM

The UCSM reports that the Connection hasn't completed yet as there is a DNS Misconfiguration



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform for Cisco UCS and HyperFlex systems. For a full listing of features and capabilities, please visit intersight.com/help.

Intersight Management

Enabled ●

When this option is enabled, you can claim this system and leverage the capabilities of Cisco Intersight.

If disabled, no communication will be allowed to Cisco Intersight.

Agent Version 1.0.9-2290

Connection

Status: DNS Misconfigured

Access Mode: Allow Control

Device ID: FD[redacted]K

Let us look at the device_connector.log

/var/sysmgr/sam_logs/device_connector.log

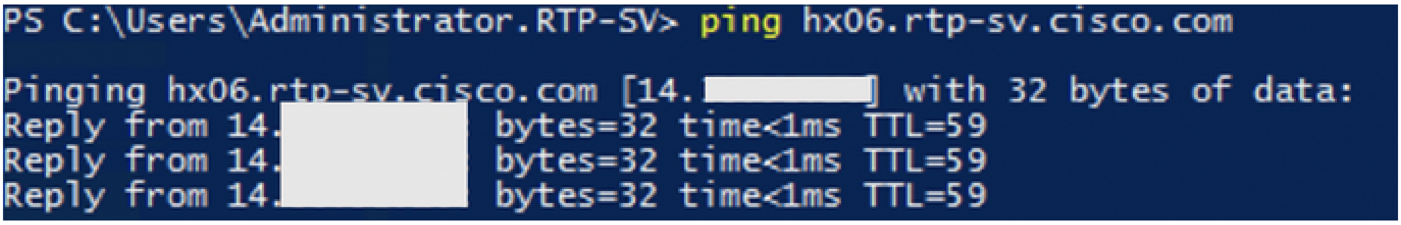
```
2019-05-15T15:34:40.643Z error base/connector.go:1477 Error in round trip {"traceId": "DC791e24a496bf9aec1c79f4c1b41cfb39", "error": "dial tcp: lookup dc-hx06.rtp-sv.cisco.com on 14.xx.xx.xx:53: no such host"}
2019-05-15T15:34:40.643Z error base/connector.go:413 Connection error {"traceId": "DC791e24a496bf9aec1c79f4c1b41cfb39", "error": "DNS Misconfigured: Error during dns lookup: lookup dc-hx06.rtp-sv.cisco.com on 14.xx.xx.xx:53: no such host"}
2019-05-15T15:36:10.171Z error base/rest_interface.go:268 security token is nil {"traceId": "DC7c3714b0a2d1f910e838086cd339c7f8"}
```

The logs indicate that there is some misconfiguration with the DNS settings.

So we could verify a few more things to figure out where the misconfiguration could be

Ping the hostname you defined, as the A record on your DNS.

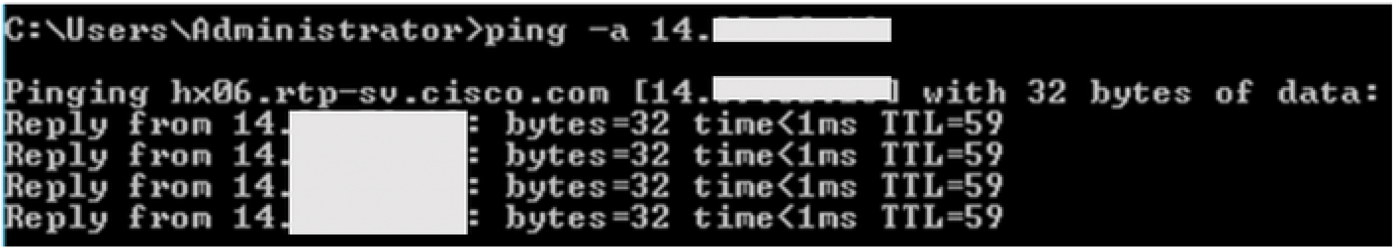
In this case, it does respond, so that was set correctly



```
PS C:\Users\Administrator.RTP-SV> ping hx06.rtp-sv.cisco.com

Pinging hx06.rtp-sv.cisco.com [14.[redacted]] with 32 bytes of data:
Reply from 14.[redacted] bytes=32 time<1ms TTL=59
Reply from 14. bytes=32 time<1ms TTL=59
Reply from 14. bytes=32 time<1ms TTL=59
```

Use Ping -a <IP_Address> to verfiy if the resolution occurs, this is to confirm that a PTR record exists

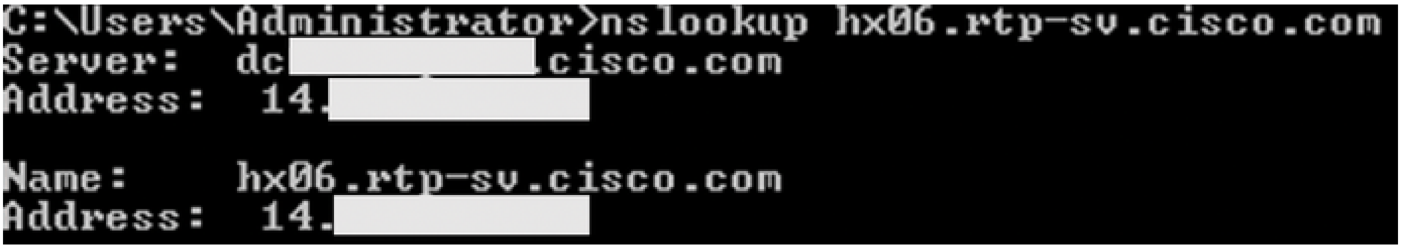


```
C:\Users\Administrator>ping -a 14.[redacted]

Pinging hx06.rtp-sv.cisco.com [14.[redacted]] with 32 bytes of data:
Reply from 14.[redacted]: bytes=32 time<1ms TTL=59
Reply from 14.[redacted]: bytes=32 time<1ms TTL=59
Reply from 14.[redacted]: bytes=32 time<1ms TTL=59
Reply from 14.[redacted]: bytes=32 time<1ms TTL=59
```

Let us get the nslookup output for both the A record and the CNAME for clues on where we would need to look in the DNS settings

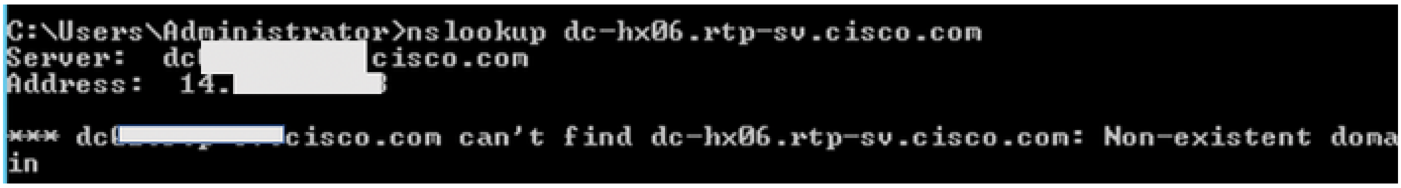
The A record does resolve, so that was set correctly



```
C:\Users\Administrator>nslookup hx06.rtp-sv.cisco.com
Server:  dc[redacted].cisco.com
Address:  14.[redacted]

Name:    hx06.rtp-sv.cisco.com
Address:  14.[redacted]
```

The CNAME doesn't resolve, which would indicate that the CNAME was either not set or was misconfigured



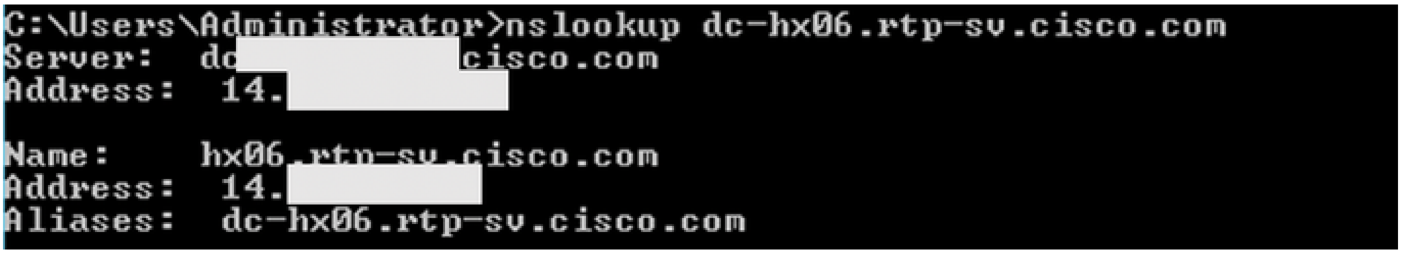
```
C:\Users\Administrator>nslookup dc-hx06.rtp-sv.cisco.com
Server:  dc[redacted]cisco.com
Address:  14.[redacted]

*** dc[redacted]cisco.com can't find dc-hx06.rtp-sv.cisco.com: Non-existent doma
in
```

Solution

In this scenario, CNAME wasn't configured on the DNS server. Once done, the error went away and registration was successful

The nslookup for the CNAME now resolves.

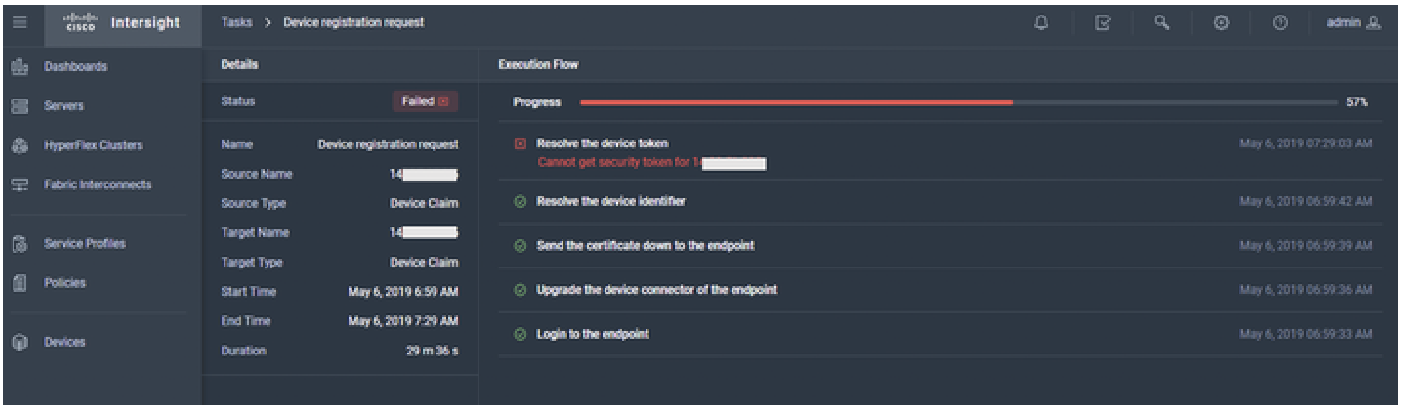


```
C:\Users\Administrator>nslookup dc-hx06.rtp-sv.cisco.com
Server:  dc[redacted]cisco.com
Address:  14.[redacted]

Name:    hx06.rtp-sv.cisco.com
Address:  14.[redacted]
Aliases:  dc-hx06.rtp-sv.cisco.com
```

Scenario 2

The device claim has failed



Details

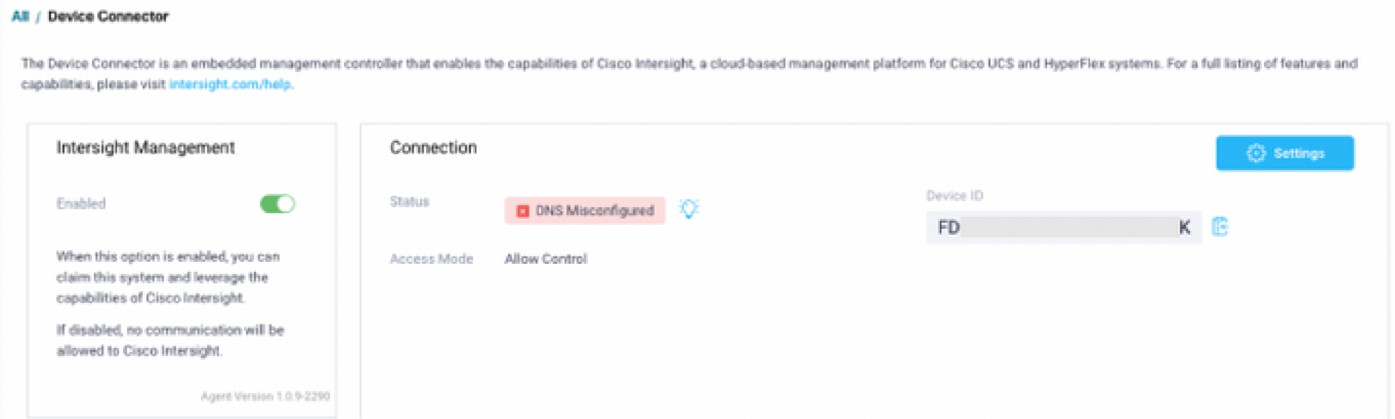
Status	Failed
Name	Device registration request
Source Name	14[redacted]
Source Type	Device Claim
Target Name	14[redacted]
Target Type	Device Claim
Start Time	May 6, 2019 6:59 AM
End Time	May 6, 2019 7:29 AM
Duration	29 m 36 s

Execution Flow

Progress 57%

Resolve the device token Cannot get security token for 1[redacted]	May 6, 2019 07:29:03 AM
Resolve the device identifier	May 6, 2019 06:59:42 AM
Send the certificate down to the endpoint	May 6, 2019 06:59:39 AM
Upgrade the device connector of the endpoint	May 6, 2019 06:59:36 AM
Login to the endpoint	May 6, 2019 06:59:33 AM

The UCSM reports that the Connection hasn't completed yet as there is a DNS Misconfiguration



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform for Cisco UCS and HyperFlex systems. For a full listing of features and capabilities, please visit intersight.com/help.

Intersight Management

Enabled

When this option is enabled, you can claim this system and leverage the capabilities of Cisco Intersight.

If disabled, no communication will be allowed to Cisco Intersight.

Agent Version 1.0.9-2290

Connection

Status: DNS Misconfigured

Access Mode: Allow Control

Device ID: FD[redacted]K

Lets us look at the device_connector.log

var/sysmgr/sam_logs/device_connector.log

```
2019-05-06T09:13:28.312Z info base/types.go:282 Failed to resolve proxy hostname
2019-05-06T09:13:28.312Z error base/connector.go:1477 Error in round trip {"error": "dial tcp:
lookup dc-hx06.rtp-sv.cisco.com on 172.xx.xx.xx:53: no such host"}
2019-05-06T09:13:28.312Z error base/connector.go:413 Connection error {"error": "DNS
Misconfigured: Error during dns lookup: lookup dc-hx06.rtp-sv.cisco.com on 172.xx.xx.xx:53: no
such host"}
```

Solution

Incorrect DNS IP Address was specified on UCSM. Once that was corrected, the device was claimed successfully.

APPENDIX A - BIND DNS Sample

/etc/named.conf

```
options {
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "rtp-sv.local" {
        type master;
        file "/etc/named/zone/rtp-sv.local";
};

zone "177.6.206.in-addr.arpa" {
        type master;
        file "/etc/named/zone/206.6.177";
};


include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

/etc/named/zone/rtp-sv.local

```
$TTL 3D
@       IN      SOA     rtp-sv.local. root.rtp-sv.local. (
                        199609206       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds
                NS      rtp-sv.local.
                NS      ns2.rtp-sv.local.
                MX      10 rtp-sv.local.  ; Primary Mail Exchanger
                TXT     "RTP-sv local"
```

```
localhost       A       127.0.0.1

intersight      A       206.xx.xx.xx

ns              A       206.xx.xx.xx
www             A       207.xx.xx.xx

dc-intersight   CNAME   intersight.rtp-sv.local.
mail            CNAME   land-5.com.
```

/etc/named/zone/206.xx.xx.

```
$TTL 3D
@               IN      SOA     rtp-sv.local. root.rtp-sv.local. (
                                199609206       ; Serial
                                28800   ; Refresh
                                7200    ; Retry
                                604800  ; Expire
                                86400)  ; Minimum TTL
                        NS      rtp-sv.local.
                        NS      ns2.rtp-sv.local.
;
;       Servers
;
1       PTR     intersight.rtp-sv.local.
2       PTR     www.rtp-sv.local.
2       PTR     ns.rtp-sv.local.
```