



システム設定の構成

- システム設定について (2 ページ)
- ユーザープロファイルの役割および権限 (2 ページ)
- システム 360 の使用 (3 ページ)
- システム 360 でのサービスの表示 (5 ページ)
- システムヘルスのモニターリング (6 ページ)
- Cisco DNA Center と Cisco ISE の統合 (41 ページ)
- データの匿名化 (44 ページ)
- 認証サーバとポリシーサーバの設定 (45 ページ)
- Cisco AI Network Analytics の設定 (49 ページ)
- 機械推論ナレッジベースの更新 (51 ページ)
- シスコアカウント (53 ページ)
- デバイスの可制御性 (59 ページ)
- SNMP プロパティの設定 (62 ページ)
- ICMP ping のイネーブル化 (63 ページ)
- イメージ配信サーバの設定 (63 ページ)
- PnP デバイス許可の有効化 (64 ページ)
- デバイスプロンプトの構成 (65 ページ)
- デバイス構成のバックアップ設定の構成 (66 ページ)
- デバイス構成をアーカイブする外部サーバーの構成 (66 ページ)
- クラウドアクセスキー (67 ページ)
- 整合性検証 (68 ページ)
- IP アドレスマネージャの設定 (71 ページ)
- Webex 統合の設定 (72 ページ)
- ThousandEyes の統合の構成 (73 ページ)
- デバッグログの設定 (73 ページ)
- ネットワークの再同期間隔の設定 (75 ページ)
- 監査ログの表示 (76 ページ)
- タスクを表示 (77 ページ)
- 高可用性のアクティブ化 (78 ページ)

- [統合設定の設定](#) (78 ページ)
- [ログインメッセージの設定](#) (79 ページ)
- [プロキシの設定](#) (80 ページ)
- [セキュリティに関する推奨事項](#) (81 ページ)
- [製品使用状況テレメトリの収集について](#) (102 ページ)
- [vManage プロパティの設定](#) (102 ページ)
- [アカウントのロックアウト](#) (103 ページ)
- [パスワードの有効期限切れ](#) (103 ページ)
- [IP アクセス制御](#) (104 ページ)

システム設定について

Cisco DNA Center の使用を開始するには、最初にシステム設定を構成して、サーバーがネットワークの外部と通信し、セキュアな通信の確保やユーザーの認証といった主要なタスクを実行できるようにする必要があります。システム設定を構成するには、この章で説明されている手順を使用します。



- (注) Cisco DNA Center の設定 (プロキシサーバーの設定を含む) の変更については、Cisco DNA Center GUI で実行する必要があります。IP アドレス、静的ルート、DNS サーバー、**maglev** ユーザーパスワードの変更については、CLI から `sudo maglev-config update` コマンドを使用して実行する必要があります。

ユーザープロファイルの役割および権限

Cisco DNA Center は、ロールベース アクセス コントロール (RBAC) をサポートします。ユーザープロファイルに割り当てられたロールは、ユーザーが実行する権限を持つ機能を定義します。Cisco DNA Center には、SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、および OBSERVER-ROLE の 3 つの主要なデフォルトユーザーロールがあります。

SUPER-ADMIN-ROLE は、ユーザーに幅広い機能を提供し、カスタムロールの作成やユーザープロファイルへの割り当てなど、Cisco DNA Center GUI ですべてのアクションを実行できるようにします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Cisco DNA Center GUI での機能が制限されます。

Cisco DNA Center でアクションを実行できない場合、それを許可しないロールがユーザープロファイルに割り当てられていることが原因である可能性があります。詳細については、システム管理者に確認するか、または [ロールベース アクセス コントロールの設定](#) を参照してください。

システム 360 の使用

[System 360] タブには、Cisco DNA Center に関する一目でわかる情報が表示されます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [System 360] の順に選択します。

ステップ 2 [System 360] ダッシュボードで、表示される次のデータメトリックを確認します。

[Cluster]

- [Hosts] : Cisco DNA Center ホストに関する情報を表示します。表示される情報には、ホストの IP アドレスと、ホストで実行されているサービスに関する詳細なデータが含まれます。ホストで実行されているサービスに関する詳細なデータを表示するには、[View Services] リンクをクリックします。

(注) ホスト IP アドレスの横には、カラーバッジが付きます。緑色のバッジは、ホストが正常であることを示します。赤色のバッジは、ホストが正常でないことを示します。

側面パネルには、次の情報が表示されます。

- [Node Status] : ノードのヘルスステータスが表示されます。
ノードヘルスが正常でない場合は、ステータスにカーソルを合わせると、トラブルシューティングのための追加情報が表示されます。
- [Services Status] : サービスのヘルスステータスが表示されます。1 つでもサービスがダウンしていると、ステータスは [Unhealthy] になります。
- [Name] : サービス名。
- [Appstack] : アプリケーションスタック名。
アプリケーションスタックは、疎結合されたサービスの集合です。この環境でのサービスは、要求が増えると自身のインスタンスを追加し、要求が減ると自身のインスタンスを解放する、水平方向にスケラブルなアプリケーションです。
- [Health] : サービスのステータス。
- [Version] : サービスのバージョン。
- [Tools] : サービスのメトリックとログを表示します。Grafana でサービスモニターリングデータを表示するには、[Metrics] リンクをクリックします。Grafana は、オープンソースのメトリック分析および可視化スイートです。サービスモニターリングデータを調べることで、問題をトラブルシューティングすることができます。Grafana の詳細については、<https://grafana.com/> を参照してください。[Logs] リンクをクリックすると、Kibana でサービスログが表示されます。Kibana は、オープンソースの分析および可視化プラットフォームです。サービスログを調べることで、問題をトラブルシューティングすることができます。Kibana の詳細については、<https://www.elastic.co/products/kibana> を参照してください。
- [High Availability] : HA が有効でアクティブであるかどうかが表示されます。

重要 Cisco DNA Center で HA が機能するためには 3 つ以上のホストが必要です。

- [Cluster Tools] : 次のツールにアクセスできます。
 - [Service Explorer] : アプリケーションスタックおよび関連付けられたサービスにアクセスします。
 - [Monitoring] : オープンソースメトリック分析および可視化スイートである Grafana を使用して、Cisco DNA Center コンポーネントの複数のダッシュボードにアクセスします。[Monitoring] ツールを使用して、メモリおよび CPU 使用率などの主要な Cisco DNA Center メトリックを確認および分析します。Grafana の詳細については、<https://grafana.com/> を参照してください。

(注) マルチホスト Cisco DNA Center 環境では、複数のホストによる Grafana データの重複が予想されます。
 - [Log Explorer] : Kibana を使用して Cisco DNA Center のアクティビティログとシステムログにアクセスします。Kibana は Elasticsearch と連動するように設計されたオープンソースの分析および可視化を実行するプラットフォームです。[Log Explorer] ツールを使用して、詳細なアクティビティログおよびシステムログを確認します。Kibana の左側にあるナビゲーションウィンドウで、[Dashboard] をクリックします。次に、[System Overview] をクリックしてすべてのシステムログを表示します。Kibana の詳細については、<https://www.elastic.co/products/kibana> を参照してください。

(注) デフォルトでは、Cisco DNA Center のすべてのロギングが有効になっています。
 - [Workflow] : 成功、失敗、保留中のステータスのマーキングを含む Cisco DNA Center インフラストラクチャタスクの詳細なグラフィカル表示を提供する、ワークフロービジュアライザにアクセスします。[Workflow] ツールを使用して、Cisco DNA Center タスクにおける障害の場所を特定します。

システム管理

- [Software Updates] : アプリケーションまたはシステムの更新のステータスが表示されます。[View] リンクをクリックすると、更新の詳細が表示されます。

(注) 更新には、その横にカラーバッジが付きます。緑色のバッジは、更新または更新に関連するアクションが正常に完了したことを示します。黄色のバッジは、使用可能な更新があることを示します。
- [Backups] : 最新のバックアップのステータスが表示されます。[View] リンクをクリックすると、すべてのバックアップの詳細が表示されます。

さらに、次のスケジュールバックアップのステータスも表示されます（またはスケジュールされているバックアップがないことを示します）。

(注) バックアップには、その横にカラーバッジが付きます。緑色のバッジは、バックアップが正常に完了したことをタイムスタンプとともに示します。黄色のバッジは、次のバックアップがまだスケジュールされていないことを示します。
- [Application Health] : 自動化および アシユアランス の健全性が表示されます。

- (注) アプリケーションの健全性には、その横にカラーバッジが付きます。緑色のバッジは、正常なアプリケーションであることを示します。赤色のバッジは、アプリケーションが正常でないことを示します。トラブルシューティングするには、[View] リンクをクリックします。

外部接続されたシステム

Cisco DNA Center によって使用されている外部ネットワークサービスに関する情報が表示されます。

- [Identity Services Engine (ISE)] : プライマリおよびセカンダリ Cisco ISE サーバーの IP アドレスとステータスを含む Cisco ISE 設定データを表示します。Cisco ISE と統合するように Cisco DNA Center を設定するには、[Configure] リンクをクリックします。
- [IP Address Manager (IPAM)] : IP アドレスマネージャの設定データと統合ステータスを表示します。IP アドレスマネージャを設定するには、[Configure] リンクをクリックします。
- [vManage] : vManage の設定データが表示されます。vManage を設定するには、[Configure] リンクをクリックします。

システム 360 でのサービスの表示

[System 360] タブは、Cisco DNA Center で実行されているアプリケーションスタックとサービスに関する詳細情報を提供します。この情報を使用して、特定のアプリケーションやサービスに関する問題のトラブルシューティングに役立てることができます。たとえば、アシュアランスに問題がある場合は、NDP アプリケーションスタックとそのコンポーネントサービスのモニターリングデータとログを表示できます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [System 360] の順に選択します。

ステップ 2 [System 360] タブの [Cluster Tools] 領域で、[Service Explorer] をクリックします。

ノードクラスタと関連サービスが新しいブラウザウィンドウにツリー型の構造で表示されます。

- ノードにカーソルを合わせると、ノードクラスタの正常性ステータスが表示されます。正常な状態のノードクラスタは緑色でマークされます。異常があるノードクラスタは赤色でマークされます。
- サービステーブルには、ノードに関連付けられているすべてのサービスが表示されます。マネージドサービスは「(M)」というマークで示されます。
- グローバルフィルタアイコンをクリックすると、サービステーブルのサービスをアプリケーションスタック名、サービス正常性ステータス ([Up]、[Down]、または [In Progress])、またはマネージドサービスかどうかに基づいてフィルタ処理できます。
- [Global Search] フィールドにサービス名を入力してサービスを検索できます。サービス名をクリックすると、関連付けられているノードでサービスが表示されます。

ステップ3 サービスをクリックして、サービス 360 ビューを起動します。次の詳細が表示されます。

- [Name] : サービス名。
- [Appstack] : アプリケーションスタック名。
- [Version] : サービスのバージョン。
- [Health] : サービスのステータス。
- [Metrics] : リンクをクリックすると Grafana のサービスモニターリングデータが表示されます。
- [Logs] : リンクをクリックすると Kibana のサービスログが表示されます。
- [Required Healthy Instances] : 正常なインスタンスの数が表示され、マネージドサービスであるかどうかを示されます。
- [Instances] : インスタンスをクリックすると詳細が表示されます。

ステップ4 テーブルにリストされているサービスを検索するには、[Search] フィールドにサービス名を入力します。

ステップ5 サービステーブルのサービスをアプリケーションスタック名、サービス正常性ステータス ([Up]、[Down]、または [InProgress])、またはマネージドサービスかどうかに基づいてフィルタ処理するには、フィルタアイコンをクリックします。

システムヘルスのモニターリング

[System Health] ページでは、Cisco DNA Center アプライアンスの物理コンポーネントの正常性をモニターし、発生する可能性がある問題を監視できます。この機能を有効にして実稼働環境で使用する方法については、以降のトピックを参照してください。

Cisco IMC 接続の確立

[System Health] ページを有効にするには、Cisco Integrated Management Controller (Cisco IMC) との接続を確立する必要があります。これにより、アプライアンスのハードウェアの正常性情報が収集されます。これを行うには、次の手順を実行します。



- (注) アプライアンスの Cisco IMC 接続設定を入力できるのは、SUPER-ADMIN-ROLE 権限を持つユーザーのみです。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [System Configuration] > [System Health] の順に選択します。

クラスターの各アプライアンスの IP アドレスが [Cisco DNA Center Address] 列に表示されます。

ステップ 2 Cisco IMC へのログインに必要な情報を設定します。

a) アプライアンスの IP アドレスをクリックします。

[Edit Cisco DNA Center Server Configuration] スライドインペインが開きます。

b) 次の情報を入力し、[Save] をクリックします。

- アプライアンスの Cisco IMC ポートに対して設定された IP アドレス。
- Cisco IMC にログインするために必要なユーザー名とパスワード。

c) 必要に応じて、クラスタの他のアプライアンスについてこの手順を繰り返します。

Cisco IMC 設定の削除

特定のアプライアンスに対して以前に設定された Cisco IMC 接続設定を削除するには、次の手順を実行します。



(注) これらの設定を削除できるのは、SUPER-ADMIN-ROLE 権限を持つユーザーのみです。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [System Configuration] > [System Health Notifications] の順に選択します。

ステップ 2 設定を削除するアプライアンスについて、[Actions] 列の [Delete] アイコン (🗑️) をクリックします。

ステップ 3 確認プロンプトで、[Ok] をクリックします。

システムイベント通知の登録

Cisco IMC との接続が確立されると、Cisco DNA Center は Cisco IMC からイベント情報を収集し、その情報を未処理のシステムイベントとして保存します。これらの未処理のイベントは、ルールエンジンによって処理され、システムヘルストポロジに表示されるシステムイベント通知に変換されます。『Cisco DNA Center Platform User Guide』の「Work with Event Notifications」で説明されている手順を完了することにより、これらの通知を、利用可能な形式のいずれかで受信することもできます。この手順を完了するときは、次のイベントを選択してサブスクライブしてください。

- 証明書の有効期限のイベント：
 - SYSTEM-CERTIFICATE
 - SYSTEM-NODE-CERTIFICATE
- 接続された外部システムのイベント：

- SYSTEM-EXTERNAL-CMX
- SYSTEM-EXTERNAL-IPAM
- SYSTEM-EXTERNAL-ISE-AAA-TRUST
- SYSTEM-EXTERNAL-ISE-PAN-ERS
- SYSTEM-EXTERNAL-ISE-PXGRID
- SYSTEM-EXTERNAL-ITSM
- ディザスタリカバリシステムのイベント：SYSTEM-DISASTER-RECOVERY
- 一般的なシステムのイベント：
 - SYSTEM-CIMC
 - SYSTEM-CONFIGURATION
 - SYSTEM-HARDWARE
 - SYSTEM-MANAGED-SERVICES



(注) マネージドサービスの場合、プローブ間隔（Cisco DNA Center が古いイベントをデータベースから削除するのにかかる時間）は60分です。マネージドサービスがダウンして再びアクティブになった場合、サービスが復元されたことをシステムの正常性GUIに反映するには、この時間がかかります。

- SYSTEM-SCALE-LIMITS

イベント通知情報

次の表に、Cisco DNA Center がシステム正常性通知メッセージを生成するときに提供される主要な情報を示します。

サブドメイン	タグ	インスタンス	状態	メッセージ
ドメイン：システム				
CPU	CPU	<node-hostname>:CPU-1	OK	Cisco DNA Center CPU-1 is working as expected on <node-hostname>
			NotOk	Cisco DNA Center CPU-1 has failed on <node-hostname>
			ディセーブル	Cisco DNA Center CPU-1 is disabled on <node-hostname>

サブドメイン	タグ	インスタンス	状態	メッセージ
メモリ	メモリ	<node-hostname>:DIMM_A1	Ok	Cisco DNA Center RAM DIMM_A1 is working as expected on <node-hostname>
			NotOk	Cisco DNA Center RAM DIMM_A1 has failed on <node-hostname>
ディスク	Disk	<node-hostname>:Disk1	Ok	Cisco DNA Center Disk 2 is working as expected on <node-hostname>
			NotOk	Cisco DNA Center Disk 2 has failed on <node-hostname>
RAID コントローラ	RAIDController	<node-hostname>:Controller-1	Ok	Cisco DNA Center RAID VD-2 is working as expected on <node-hostname>
			NotOk	Cisco DNA Center RAID VD-2 has degraded on <node-hostname>
			ディセーブル	Cisco DNA Center RAID VD-2 is offline on <node-hostname>
ネットワークインターフェイス	NIC	<node-hostname>:nic-1	Ok	Cisco DNA Center network interfaces are working as expected
			NotOk	Cisco DNA Center: <x> network interfaces are missing for <node-hostname>: nic-1
PSU_FAN	PSU	<node-hostname>:psu-1	Ok	Cisco DNA Center power supply (PSU-1) is powered on and thermal condition is normal for <node-hostname>
			NotOk	Cisco DNA Center power supply (PSU-2) is powered off and thermal condition is critical for <node-hostname>

サブドメイン	タグ	インスタンス	状態	メッセージ
ディザスタリカバリ	DisasterRecovery	<disaster-recovery-hostname>	Ok	<ul style="list-style-type: none"> Disaster recovery cluster is up Disaster recovery failover succeeded to <site-name>
			Degraded	<ul style="list-style-type: none"> Disaster recovery failover triggered from <site-name> to site-name Disaster recovery failed while failing over to <site-name> Disaster recovery standby cluster on <site-name> is down; cannot failover Disaster recovery witness is down; cannot failover Disaster recovery replication halted; recovery point objective will be impacted Disaster recovery pause failed Disaster recovery route advertisement failed Disaster recovery IPSec communication failed
			NotOk	<ul style="list-style-type: none"> Disaster recovery configuration failed Disaster recovery failed to rejoin the standby system
プラットフォームサービス	ManagedServices	<hostname>:<name>	OK	Managed Service <service-name> is Running
			NOTOK	Managed Service <service-name> is Interrupted

サブドメイン	タグ	インスタンス	状態	メッセージ
スケール制限	wired_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wired clients exceeded 26250 (105% of limit)
			DEGRADED	The number of concurrent wired clients exceeded 21250 (85% of limit)
			注意\t	The number of concurrent wired clients exceeded 18750 (75% of limit)
	wireless_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wireless clients exceeded 18750 (75% of limit)
			DEGRADED	The number of concurrent wireless clients exceeded 21250 (85% of limit)
			注意\t	The number of concurrent wireless clients exceeded 18750 (75% of limit)
	wired_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wired devices exceeded 1050 (105% of limit)
			DEGRADED	The number of wired devices exceeded 850 (85% of limit)
			注意\t	The number of wired Devices exceeded 750 (75% of limit)
	wireless_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wireless devices exceeded 3800 (105% of limit)
			DEGRADED	The number of wireless devices exceeded 3400 (85% of limit)
			注意\t	The number of wireless devices exceeded 3000 (75% of limit)
interfaces	<hostname>:<name>	OK	OK	
		NOTOK	The number of interfaces exceeded 1140000000 (95% of limit)	
		DEGRADED	The number of interfaces exceeded 1020000000 (85% of limit)	
		注意\t	The number of interfaces exceeded 900000000 (75% of limit)	
ippools	<hostname>:<name>	OK	OK	
		NOTOK		

サブドメイン	タグ	インスタンス	状態	メッセージ	
				The number of IP pools exceeded 47500 (95% of limit)	
			DEGRADED	The number of IP pools exceeded 42500 (85% of limit)	
			注意\t	The number of IP pools exceeded 37500 (75% of limit)	
	netflows	<hostname>:<name>		OK	OK
				NOTOK	The number of Netflows exceeded 37500 (75% of limit)
				DEGRADED	The number of Netflows exceeded xxx (x% of limit)
				注意\t	The number of Netflows exceeded yyy (y% of limit)
	physical_ports	<hostname>:<name>		OK	OK
				NOTOK	The number of physical ports exceeded 50400 (95% of limit)
				DEGRADED	The number of physical ports exceeded 40800 (85% of limit)
				注意\t	The number of physical ports exceeded 36000 (75% of limit)
	policy	<hostname>:<name>		OK	OK
				NOTOK	The number of policies exceeded 23750 (95% of limit)
				DEGRADED	The number of policies exceeded 21250 (85% of limit)
				注意\t	The number of policies exceeded 18750 (75% of limit)
	security_group	<hostname>:<name>		OK	OK
				NOTOK	The number of security groups exceeded 3800 (95% of limit)
				DEGRADED	The number of security groups exceeded 3400 (85% of limit)
				注意\t	The number of security groups exceeded 3000 (75% of limit)
	sites	<hostname>:<name>		OK	OK
				NOTOK	The number of sites exceeded 475 (95% of limit)

サブドメイン	タグ	インスタンス	状態	メッセージ
			DEGRADED	The number of sites exceeded 425 (85% of limit)
			注意	The number of sites exceeded 375 (75% of limit)
	transient_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of transient clients exceeded 71250 (95% of limit)
			DEGRADED	The number of transient clients exceeded 63750 (85% of limit)
			注意	The number of transient clients exceeded 56250 (75% of limit)
ソフトウェアアップグレード	Upgrade	<hostname>:<name>	OK	Successfully finished downloading package <package-name> with version <package-version>
			NOTOK	Catalog package download failed for <package-name>
バックアップ	Backup	<hostname>:<name>	OK	Successfully completed backup
			NOTOK	Failed to backup
Restore	Restore	<hostname>:<name>	OK	Successfully restored
			NOTOK	Failed to restore configuration
ドメイン：接続性				
ISE	ISE_ERS	<Cisco-ISE-hostname>	Success	ISE AAA trust establishment succeeded for ISE server <ISE-server-details>
			Failed	ISE AAA trust establishment failed for ISE server <ISE-server-details>
ドメイン：統合				
IPAM	IPAM	<IPAM-hostname>	Ok	IPAM connection to Cisco DNA Center established. IPAM <IPAM-IP-address>.
			Critical	IPAM connection to Cisco DNA Center offline. IPAM <IPAM-IP-address>.

サブドメイン	タグ	インスタンス	状態	メッセージ
ISE	ISE_AAA	<Cisco-ISE-hostname>	アップ	ISE AAA trust establishment succeeded for ISE server. ISE <ISE-IP-address>
			ダウン	ISE AAA trust establishment failed for ISE server. ISE <ISE-IP-address>
CMX	CMX	<CMX-hostname>	serviceAvailable	CMX connection to Cisco DNA Center offline. CMX <CMX-IP-address>.
			serviceNotAvailble	CMX connection to Cisco DNA Center offline. CMX <CMX-IP-address>.
ITSM	ITSM	<ITSM-hostname>	アップ	ITSM connection to Cisco DNA Center offline. ITSM <ITSM-IP-address>.
			ダウン	ITSM connection to Cisco DNA Center offline. ITSM <ITSM-IP-address>.

システム正常性スケール番号

第2世代 Cisco DNA Center アプライアンスには、次のバージョンがあります。

- 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
- 44 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-U
- 56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
- 56 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-L-U
- 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
- 112 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-XL-U

システムヘルスにより、これらのアプライアンスがモニターされ、次の表に示されているネットワークコンポーネントが特定のしきい値を超えるたびに通知が生成されます。生成される通知の優先順位は、測定されたしきい値のパーセンテージによって異なります。

- しきい値の 75 % を超えると、情報（P3）通知が生成されます。
- しきい値の 85 % を超えると、警告（P2）通知が生成されます。
- しきい値の 95% を超えると、クリティカル（P1）通知が生成されます。



(注) すべてのアプライアンス（タイプに関係なく）について 1,000,000 件の通知が監査ログに保持され、1 年間保存されます。

ネットワークコンポーネント	44 コアアプライアンス	56 コアアプライアンス	112 コアアプライアンス
有線デバイス（ルータ、スイッチ、スタック、およびワイヤレスコントローラ）	1,000	2,000	5,000
ワイヤレスデバイス（アクセスポイントおよびセンサー）	4,000	6,000	18,000
インベントリの物理ポート	48,000	192,000	480,000
論理および物理インターフェイス	1,200,000	1,200,000	1,200,000
有線クライアント（同時）	25,000	40,000	40,000
ワイヤレスクライアント（同時）	25,000	40,000	60,000
一時的なクライアント	75,000	120,000	250,000
サイト	500	1,000	2,000
着信 NetFlow	27,500	60,000	120,000
IP プール	50,000	100,000	100,000
ポリシーマトリックスサイズ	25,000	25,000	25,000

システムトポロジの表示

[System Health] ウィンドウのトポロジには、ネットワークに接続された Cisco DNA Center アプライアンスと外部システム（Cisco Connected Mobile Experiences（Cisco CMX）や Cisco Identity Services Engine など）をグラフィック形式で表示できます（Cisco ISE）。このページから、ネットワーク上の問題があるコンポーネントや注意が必要なコンポーネントをすばやく特定できます。このページにアプライアンスと外部システムのデータを取り込むには、まず以降のトピックで説明するタスクを完了する必要があります。

- [Cisco IMC 接続の確立（6 ページ）](#)
- [システムイベント通知の登録（7 ページ）](#)

このページを表示するには、Cisco DNA Center GUI で [Menu] アイコン (≡) をクリックし、[System] > [System Health] の順に選択します。トポロジのデータは 30 秒間隔でポーリングされます。新しいデータを受信すると、そのデータがトポロジに自動的に反映されます。

次の点に注意してください。

- Cisco DNA Center は IPv6 をサポートするようになりました。IPv6 が有効になっているクラスタを表示すると、トポロジには、そのクラスタのエンタープライズ仮想 IP アドレスに関する次の情報も表示されます。

- [Pre] フィールド：16 ビットのプレフィックス
- [GID] フィールド：32 ビットのグローバル ID
- [Subnet] フィールド：16 ビットのサブネット値

クラスタのエンタープライズ仮想 IP アドレスの残りは、クラスタのトポロジアイコンのラベル付けに使用されます。

- IPv6 対応のクラスタは、やはり IPv6 対応の外部システムにのみ、接続してデータを取得することができます。
- 接続されているアプライアンスまたは外部システムに、有効期限が設定されている証明書がインストールされている場合は常に、トポロジで次のことが実行されます。
 - 証明書が 90 日以内に期限切れになるように設定されている場合、トポロジに警告が表示されます。
 - 証明書が 30 日以内に期限切れになるように設定されている場合は、トポロジにエラーが表示されて問題への注意が喚起されます。
- システムヘルスはハードウェア コンプライアンス チェックを定期的に行い、接続されているアプライアンスまたは外部システムが最小構成要件を満たしていない場合は常に、そのことを示します。たとえば、接続されている仮想ドライブに関してライトスルーキャッシュ書き込みポリシーが設定されていない場合、システムヘルスはトポロジを更新して、そのことを示します。
- 実稼働環境でディザスタリカバリが正常に機能している場合、システムヘルスは、メインサイトとリカバリサイトの両方のアプライアンスに関するハードウェア情報を提供します。以前は、メインサイトのアプライアンスに関してのみ、ハードウェア情報が提供されていました。

アプライアンスと外部システムの問題のトラブルシューティング

システム正常性のトポロジの画面では、注意が必要なネットワークコンポーネントがある場合、軽微な問題については ▲ アイコン、重大な問題については × アイコンで示されます。コンポーネントに関する問題のトラブルシューティングを開始するには、コンポーネントのトポロジアイコンにカーソルを合わせます。ポップアップウィンドウが開き、次の情報が表示されます。

- 問題が検出された日時を示すタイムスタンプ。
- Cisco DNA Center アプライアンスにインストールされている Cisco IMC ファームウェアのバージョン（アプライアンスのポップアップウィンドウの場合）。
- 問題の簡単な概要。

- 問題の現在の状態またはシビラティ（重大度）。
- 問題に関連するドメイン、サブドメイン、および IP アドレスまたはロケーション。

接続された外部システムに問題がある関連サーバーが 3 つ以上ある場合や Cisco DNA Center アプライアンスに問題があるハードウェアコンポーネントが 3 つ以上ある場合、それらの外部システムまたはアプライアンスのポップアップウィンドウを開くと、[More Details] リンクが表示されます。リンクをクリックするとスライドインペインが開き、該当するサーバーまたはコンポーネントのリストが表示されます。それらの各項目の [>] をクリックしてエントリを展開することで、特定の項目の情報を確認できます。

外部システムの接続に関する問題のトラブルシューティング

Cisco DNA Center が現在外部システムと通信できない場合は、次の手順を実行してそのシステムを ping し、到達できない理由をトラブルシューティングします。

始める前に

この手順を完了する前に、次の操作を実行します。

- 機械推論パッケージをインストールします。『[Cisco DNA Center Administrator Guide](#)』の「Download and Install Packages and Updates」を参照してください。
- 機械推論機能への書き込み権限を持つロールを作成し、この手順を実行するユーザーにそのロールを割り当てます。[Create a User Role] ウィザードでこのパラメータにアクセスするには、[Define the Access] ページの [System] 行を展開します。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Configure Role-Based Access Control」を参照してください。

-
- ステップ 1** [System Health] ウィンドウの右上部分から、[Tools] > [Network Ping] を選択して [Ping Device] ウィンドウを開きます。
- ウィンドウには、Cisco DNA Center が現在管理しているすべてのデバイスが一覧表示されます。
- ステップ 2** 到達可能性ステータスが [Reachable] であるデバイスのオプションボタンをクリックし、[Troubleshoot] リンクをクリックします。
- [Reasoner Inputs] ポップアップウィンドウが開きます。
- ステップ 3** [Target IP Address] フィールドに、到達できない外部システムの IP アドレスを入力します。
- ステップ 4** [Run Machine Reasoning] をクリックします。
- Cisco DNA Center で外部システムを ping すると、ダイアログボックスが表示されます。
- ステップ 5** [View Details] をクリックして、ping が成功したかどうかを確認します。
- ステップ 6** ping が失敗した場合は、[View Relevant Activities] リンクをクリックして [Activity Details] スライドインペインを開き、[View Details] アイコンをクリックします。

[Device Command Output] ポップアップウィンドウが開き、外部システムに到達できない原因として考えられる内容が一覧表示されます。

検証ツールの使用

検証ツールは、Cisco DNA Center アプライアンスハードウェアと接続された外部システムの両方をテストし、ネットワークに重大な影響を与える前に対処する必要がある問題を特定します。検証プロセスでは、次のような多数のチェックが行われます。

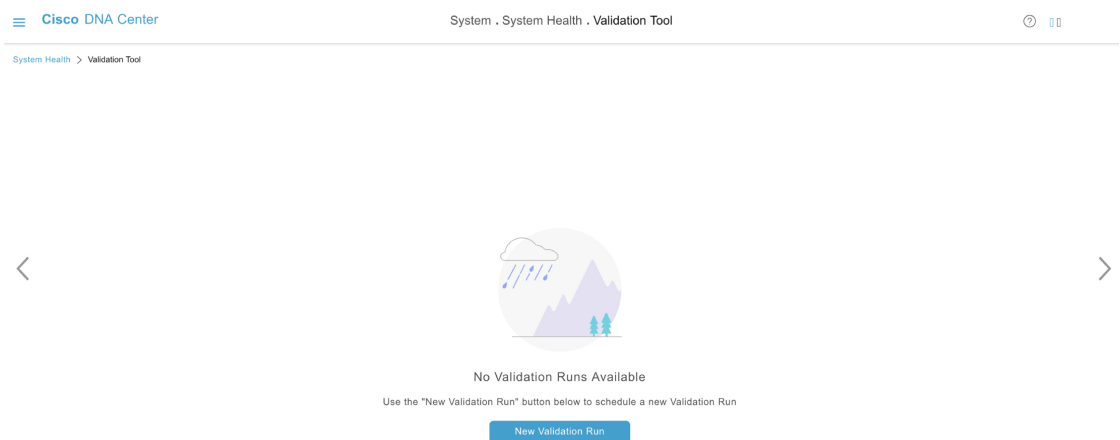
- ciscoconnectdna.com への接続機能（システムおよびパッケージの更新をダウンロードするため）。
- 期限切れの証明書の有無。
- アプライアンスハードウェアとバックエンドサービスの現在の状態。
- スケール番号のしきい値を超えたネットワークコンポーネント。

検証ツールにアクセスするには、次の手順を実行します。

1. メニューアイコン（☰）をクリックして、[System] > [System Health] をクリックして、[System Health] ページを開きます。
2. [Tools] ドロップダウンメニューから、[Validation Tool] を選択します。

検証ツールページの移動

[Validation Tool] ページの内容は、以前に完了した検証処理に関する情報があるかどうかによって異なります。Cisco DNA Center 情報がない場合、ページは次のようになります。



Cisco DNA Center に検証処理に関する情報がある場合、ページは次のようになります。

Validation Runs (7) As of: Jun 25, 2021 2:17 PM

① Search Table

② Add ④ Delete 0 Selected

<input type="checkbox"/>	Name	Description	Selected Set(s)	Status	Start Time	Duration	Actions
<input type="checkbox"/>	vr7		upgrade	Success	Jun 25, 2021 1:57 PM	104 ms	View Status ⑤
<input type="checkbox"/>	vr6		upgrade	Success	Jun 25, 2021 1:30 PM	104 ms	View Status
<input type="checkbox"/>	vr5		upgrade	Failed	Jun 25, 2021 12:42 PM	115 ms	View Status
③ <input type="checkbox"/>	vr4		upgrade	Success	Jun 25, 2021 5:00 AM	135 ms	View Status
<input type="checkbox"/>	vr3		upgrade	Failed	Jun 25, 2021 3:51 AM	274 ms	View Status
<input type="checkbox"/>	vr2		upgrade	Failed	Jun 25, 2021 3:43 AM	1 second(s)	View Status
<input type="checkbox"/>	vr1		upgrade	Partial Success	Jun 25, 2021 2:57 AM	5 second(s)	View Status

1-7 < 1 >

次の表に、[Validation Tool] ページを構成するコンポーネントと、検証処理に関する情報が利用可能な場合の機能を示します。

引き出し線	説明
1	[Search Table] フィールド：このページにリストされている検証処理をフィルタリングするための検索文字列を入力します。
2	[Add] ボタン：クリックして [New Validation Run] スライドインペインを開き、新しい処理のために必要な設定を入力します。詳細については、 検証処理の開始 (20 ページ) を参照してください。
3	[Validation Runs] テーブル：以前に完了した検証処理がリストされます。このテーブルには、処理ごとの名前、適用可能な検証セット、完了ステータスなどの情報が表示されます。次の点に注意してください。 <ul style="list-style-type: none"> デフォルトでは、処理は開始時刻順に並べられ、最新の処理が最初にリストされます。 現在進行中のすべての処理に対しては、期間はゼロと表示されます。
4	[Delete] ボタン：検証処理のチェックボックスをオンにした状態でこのボタンをクリックすると、処理が削除されます。次に [Warning] ダイアログボックスで [OK] をクリックして、削除を確定します。 (注) 進行中の処理は削除できません。
5	[View Status] リンク：特定の処理の詳細を表示します。詳細については、 検証処理の詳細の表示 (20 ページ) を参照してください。
6	[Refresh] ボタン：クリックすると、このページに表示されている情報が更新されます。

検証処理の開始

検証処理を開始するには、以下の手順を実行します。



(注) 一度に実行できる検証は1つだけです。検証処理がすでに進行中の場合は、完了するまで待つてから、別の処理を開始する必要があります。

ステップ 1 [Validation Runs] テーブルが表示されるかどうかに応じて、[Validation Tool] ウィンドウで次のいずれかを実行します。

- テーブルが表示されない場合は、以前の検証処理が削除されているか、検証処理がまだ完了していないことを意味します。[New Validation Run] をクリックします。
- [Validation Runs] テーブルが表示されたら、[Add] をクリックします。

[New Validation Run] スライドインペインが開きます。

ステップ 2 [Name] フィールドに、検証処理の名前を入力します。

入力する名前は一意で、英数字のみを使用してください。特殊文字は使用できません。

ステップ 3 (任意) [Description] フィールドに、これから開始する検証処理に関する簡単な説明を入力します。

説明は最大 250 文字まで入力できます。

ステップ 4 [Validation Set(s) Selection] エリアで、実行する検証セットのチェックボックスをオンにします。

検証セットを最大化して、実行するチェックを表示できます。

ステップ 5 [Run] をクリックします。

検証処理の詳細の表示

[Validation Run Details] スライドインペインから、選択した処理中に行われたチェック、チェックの完了ステータス、期間、およびその他の関連情報を表示できます。

The screenshot shows the 'Validation Run Details' window. On the left, a table lists validation runs. The selected run 'TEST_5185' is highlighted. The right pane shows details for this run, including its name, description, and status (Partial Success). Below this, a 'Result' section shows a table of validation checks.

Validation	Status	Duration	Message
Validating maglev parent catalog server settings [VERSION 1.0.90]	Success	12 ms	ParentCatalogServer https://www.wrong.com:443 configured
Validating maglev parent catalog server repository settings [VERSION 1.0.90]	Warning	9 ms	ParentCatalogServerRepository NOT configured

ここでは次の操作も実行できます。

- [Search Table] フィールドに、提供される情報をフィルタリングするための検索文字列を入力します。
- [Export] をクリックして、このペインの内容を .json ファイルとしてダウンロードします。
- [Copy] をクリックして、このペインの内容をコピーします。

検証セットの更新

検証セットは、Cisco DNA Center をアップグレードするたびに更新する必要があります。検証セットを手動で更新する必要がある場合は、次の手順を実行します。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [System Configuration] > [System Health] の順に選択します。

The screenshot shows the Cisco DNA Center interface. On the left, a navigation menu is open, listing various settings categories. 'System Health' is highlighted at the bottom of the menu. The main content area shows the 'System Health' page, which includes tabs for 'CIMC Configuration' and 'Validation Catalog'. The 'Validation Catalog' tab is active, displaying the text 'Update Cisco DNA Center with most recent Validation Catalog' and buttons for 'Download Latest' and 'Import'. Below this, there is a section for 'Validation Set Versions' with a table showing the current version as 1.0.90.

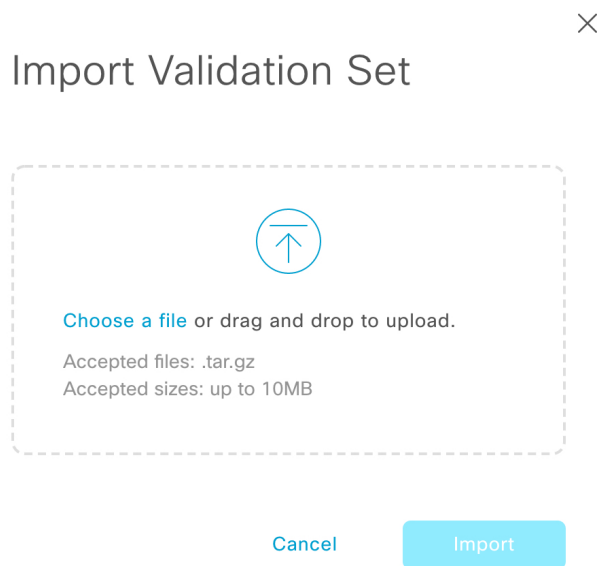
Validation Set Versions	
Upgrade Validation Set Version	1.0.90

ステップ 2 [Validation Catalog] タブをクリックします。

ステップ 3 [Download Latest] をクリックして、使用可能な最新の検証セットのローカルコピーをダウンロードします。

ステップ 4 検証セットを Cisco DNA Center にインポートします。

a) [Import] をクリックし、[Import Validation Set] ダイアログボックスを開きます。



b) 次のいずれかを実行します。

- [Choose a file] リンクをクリックして、インポートする .tar ファイルに移動します。
- 適切な .tar ファイルをデスクトップから強調表示された領域にドラッグアンドドロップします。

c) [インポート (**Import**)] をクリックします。

System Analyzer ツールの使用

トラブルシューティングが必要な問題が発生した場合は、System Analyzer ツールを使用してログファイルを取得できます。システムレベルのログファイルに加えて、Cisco SD-Access とソフトウェアイメージ管理 (SWIM) に固有のログファイルを取得できます。[System Analyzer] ツールにアクセスするには、次の手順を実行します。

1. メニューアイコンをクリックし、[System]>[System Health]の順に選択して[System Health] ウィンドウを開きます。
2. [Tools] ドロップダウンメニューから、[System Analyzer] を選択します。

このツールを使用する前に、次の点に注意してください。

- 管理者ユーザーのみが、システム分析の実行を開始し、結果のログファイルをダウンロードし、完了した実行を削除できます。すべてのユーザーは、選択した実行の[System Analysis Details] スライドインペインを開いて表示できます。
- System Analyzer ツールでは、Cisco DNA Center の GlusterFS ファイルシステムに 5 GB のディスク容量が必要です。
- Cisco DNA Center は、5 GB または過去 3 ヶ月分のシステム分析実行のいずれか小さい方を保存します。

- いずれかのストレージ制限に達すると、Cisco DNA Center は古い実行を 1 日 1 回削除します。また、新しい実行が開始される前に、古い実行も削除されます。
- ログファイル情報はトラブルシューティングにのみ役立つため、システム分析実行のデータはバックアップされません。
- HA が有効になっている展開では、実行の進行中にシステムヘルスサービスがダウンした場合、システムヘルスが再び起動した後に実行を再開する必要があります。
- ディザスタリカバリが有効になっている展開では、実行データはディザスタリカバリシステムのサイト全体にレプリケートされません。システムのアクティブサイトとスタンバイサイトは、独自の実行履歴を保持します。

[System Analyzer] ページをナビゲートする

[System Analyzer] ページの内容は、Cisco DNA Center に以前に完了した処理に関する情報があるかどうかによって異なります。情報がない場合、ページは次のようになります。

The screenshot shows the Cisco DNA Center interface for System Analyzer. At the top, there is a navigation bar with 'Cisco DNA Center' and 'System > System Health > System Analyzer'. Below the navigation bar, there is a message: 'No System Analysis Sets Available'. Underneath this message, there is a sub-message: 'Use the "New System Analyzer Run" button below to schedule a new System Analysis'. A blue button labeled 'New System Analyzer Run' is positioned below the text.

Cisco DNA Center に処理に関する情報がある場合、ページは次のようになります。

The screenshot shows the Cisco DNA Center interface for System Analyzer with a table of runs. The table has columns for Name, Description, Type, Status, Start Time, Duration, and Actions. There are three rows of data, each with a 'Details' link. The table is titled 'System Analyzer Runs (3)' and includes a search bar and action buttons (Add, Delete).

Name	Description	Type	Status	Start Time	Duration	Actions
sar3	System data	System	✓	Nov 1, 2021 3:21:00 PM	11 mins 57 secs	Details
sar2	SWIM data	SWIM	✓	Nov 1, 2021 3:20:39 PM	7 mins 7 secs	Details
sar1	Cisco SD-Access data	SDA	✓	Nov 1, 2021 3:20:15 PM	3 mins 34 secs	Details

次の表に、[System Analyzer] ページを構成するコンポーネントと、処理に関する情報が利用可能な場合の機能を示します。

引き出し線	説明
1	[Search Table] フィールド：このページにリストされている処理をフィルタリングするための検索文字列を入力します。
2	[Add] ボタン：クリックして [New System Analyzer Run] スライドインペインを開き、処理のために必要な設定を入力します。詳細については、 System Analyzer 処理の開始 (24 ページ) を参照してください。
3	[System Analyzer Runs] テーブル：現在進行中または以前に完了した処理をリストします。処理ごとに、名前、関連する Cisco DNA Center コンポーネント、処理の完了にかかった時間などの情報がテーブルに表示されます。 次の点に注意してください。 <ul style="list-style-type: none"> デフォルトでは、処理は開始時刻順に並べられ、最新の処理が最初にリストされます。 現在進行中のすべての処理に対しては、期間はゼロと表示されます。
4	[Delete] ボタン：処理のチェックボックスをオンにした状態で、[Delete] をクリックして削除します。 (注) 進行中の処理は削除できません。
5	[Details] リンク：特定の処理の詳細を表示します。詳細については、 System Analyzer 処理の詳細の表示 (25 ページ) を参照してください。
6	[Refresh] ボタン：クリックすると、このページに表示されている情報が更新されます。

System Analyzer 処理の開始

System Analyzer 処理を開始するには、次の手順を実行します。

ステップ 1 [System Analyzer Runs] テーブルが表示されているかどうかに応じて、[System Analyzer] ページで次のいずれかを実行します。

- テーブルが表示されない場合は、以前の処理が削除されているか、処理がまだ完了していないことを示します。[New System Analyzer Run] をクリックします。
- [System Analyzer Runs] テーブルが表示されたら、[Add] をクリックします。

[New System Analyzer Run] スライドインペインが開きます。

ステップ 2 [Name] フィールドに、処理の名前を入力します。

入力する名前は一意で、英数字のみを使用してください。特殊文字は使用できません。

ステップ 3 [Description] フィールドに、これから開始する処理に関する簡単な説明を入力します。

説明は最大 250 文字まで入力できます。

ステップ 4 (オプション) [Notes] フィールドに、処理に指定する追加情報 (最大 250 文字) を入力します。

ステップ 5 [Select a System Analyzer to run] エリアで、ログファイルを取得する Cisco DNA Center コンポーネントのラジオボタンをクリックします。

ステップ 6 [Run] をクリックします。

System Analyzer 処理の詳細の表示

[System Analysis Details] スライドインペインから、取得したログファイルの合計ファイルサイズや関連する Cisco DNA Center コンポーネントなど、選択した実行に関する追加情報を表示できます。実行中に問題が発生したログファイルも特定できます。

The screenshot displays the 'System Analyzer' interface. On the left, a table titled 'System Analyzer Runs (3)' lists three runs: sar3 (System data), sar2 (SWIM data), and sar1 (Cisco SD-Access). The 'System Analysis Details' panel for 'sar3' is open, showing the following information:

- Name: sar3
- Description: System data
- Notes: (empty)
- Type: System
- Overall Status: Success
- Start Time: Mon Nov 01 2021 15:21:00 GMT-0700 (Pacific Daylight Time)
- Duration: 11 mins 57 secs
- File Size: 50.25 MB

Below this, the 'Event Details' section shows a table of events:

Event	Status	Duration	Message
▼ sar3 log collection	Success	5 mins 11 secs	Log Collection Task Executed Successfully
	Success	0 secs	Collected logs for default
	Success	0 secs	Collected logs for dms
	Success	2 mins 3 secs	Collected logs for fusion

ここでは次の操作も実行できます。

- [Search Table] フィールドに、表示される情報をフィルタリングするための検索文字列を入力します。
- [Download] をクリックして、取得したログファイルを .tar.gz ファイルとしてダウンロードします。

システムトポロジ通知

次の表に、[System Health] ページのシステムトポロジに表示される Cisco DNA Center アプライアンスおよび接続された外部システムについてのさまざまな通知を示します。通知は対応するシビラティ (重大度) に応じてグループ化されています。

- シビラティ (重大度) 1 (エラー) : 無効化された RAID コントローラや故障した電源などの重大なエラーを示します。

- シビラティ（重大度）2（警告）：Cisco ISE サーバーとの信頼を確立できないなどの問題を示します。
- シビラティ（重大度）3（成功）：サーバーやハードウェアコンポーネントが想定どおりに動作していることを示します。



(注) アプライアンスのすべてのハードウェアコンポーネントが問題なく動作している場合は、各コンポーネントの個別の通知は表示されません。代わりに、[Cisco DNA Center Ok] という通知が表示されます。

表 1: Cisco DNA Center アプライアンスの通知

コンポーネント	シビラティ（重大度）1の通知	シビラティ（重大度）2の通知	シビラティ（重大度）3の通知
CPU	Processor CPU1 (SerialNumber - xxxxx) State is Disabled	Processor CPU1 (SerialNumber - xxxxx) Health is NotOk and State is Enabled	Processor CPU1 (SerialNumber - xxxxx) Health is Ok and State is Enabled
ディスク	Driver - PD1 State is Disabled	Driver - PD1 Health is Critical and State is Enabled	Driver - PD1 Health is Ok and State is Enabled
MemoryV1	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is NotOk	—	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is Ok
MemoryV2	Storage DIMM1 (SerialNumber - xxxxx) Status is NotOperable	—	Storage DIMM1 (SerialNumber - xxxxx) Status is Operable
NIC	NIC Adapter Card MLOM State is Disabled	NIC Adapter Card MLOM State is Enabled and port0 is Down	NIC Adapter Card MLOM State is Enabled and port0 is Up
電源モジュール	PowerSupply PSU1 (SerialNumber - xxx) State is Disabled	—	PowerSupply PSU1 (SerialNumber - xxx) State is Enabled
RAID	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) State is Disabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is NotOK and State is Enabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is OK and State is Enabled

表 2: 接続されている外部システムの通知

コンポーネント	シビラティ（重大度）1の通知	シビラティ（重大度）2の通知	シビラティ（重大度）3の通知
Cisco Connected Mobile Experiences (CMX) サーバー	—	There is a critical issue with the integrated CMX server.	CMX server is integrated and servicing.
IP アドレス管理 (IPAM) サーバー	There is a critical issue with the connected third-party IPAM provider	—	<ul style="list-style-type: none"> • A third-party IPAM provider is connected. • There is no third-party IPAM provider connected. • The third-party IPAM provider is currently synchronizing.
Cisco ISE : 外部 RESTful サービス (ERS)	—	ISE PAN ERS connection: ISE ERS API call unauthorized	ISE PAN ERS connection: ERS reachability with ISE - Success
Cisco ISE : 信頼性	—	ISE AAA Trust Establishment: Trust Establishment Error	ISE AAA Trust Establishment: Successfully established trust and discovered PSNs from PAN
IT サービス管理 (ITSM) サーバー	Servicenow connection health status is NOT up and running	—	Servicenow connection health status is up and running

Disk Utilization Event Notifications

システムヘルスは、システム内のノードごとのディスク使用率を監視し、これらのノードの使用率がネットワーク操作に影響を与える可能性のあるレベルに達すると通知を送信します。使用率が 75% を超えると、システムヘルスは警告通知を送信します。また、使用率が 85% を超えると、システムヘルスは重大な通知を送信します。これらの通知を設定およびサブスクライブするには、『[Cisco DNA Center Platform User Guide](#)』の「Work with Event Notifications」トピックを実行してください。この手順を完了するときは、必ず [System Performance: Filesystem Utilization] イベントを選択してサブスクライブしてください。

ディスク使用率の監視に関して、次の点に注意してください。

- バックアップファイルを復元または Cisco DNA Center をアップグレードすると、システムヘルスによってディスク使用率の監視が再開され、1 時間ごとに更新が収集されます。
- 3 ノードの HA デプロイメントでは、3 つのクラスタノードで構成されているすべてのパーティションが監視されます。生成される通知は、関連するパーティションに固有です。

- ディザスタリカバリが有効になっている展開では、システムヘルスはアクティブサイトとスタンバイサイトの両方でノードごとにディスク使用率を監視します。

推奨されるアクション

次の表に、システムの正常性のモニターリング時によく発生する一般的な問題と、それらの問題を修復するための推奨される処置を示します。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
Cisco ISE	外部 RESTful サービス (ERS) : 到達可能性	タイムアウトが発生する (Cisco ISE ERS API の負荷がしきい値を超えたことが原因と考えられる)。	<ul style="list-style-type: none"> • Cisco DNA Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。
		Cisco ISE との接続を確立できない。	<ul style="list-style-type: none"> • ファイアウォールが設定されているかどうかを確認します。 • Cisco DNA Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。
	ERS : 可用性	ERS API コールへの応答がない。	<ul style="list-style-type: none"> • インストールされている Cisco ISE のバージョンを確認します。 • Cisco ISE で ERS が有効になっているかどうかを確認します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable External RESTful Services APIs」を参照してください。
	ERS : 認証	Cisco ISE ERS API コールが許可されない。	AAA 設定のログイン情報と Cisco ISE のログイン情報が同じであるかどうかを確認します。
	ERS : 設定	Cisco ISE の証明書が変更されている。	Cisco DNA Center GUI で信頼を再確立します。詳細については、『 Cisco Identity Services Engine Administration Guide 』の「Enable PKI in Cisco ISE」を参照してください。
	ERS : 未分類または一般的なエラー	未定義の診断エラーが発生する。	

コンポーネント	サブコンポーネント	問題	推奨されるアクション
			<ol style="list-style-type: none"> 1. Cisco DNA Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。 3. 信頼を再確立します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable PKI in Cisco ISE」を参照してください。
	信頼：到達可能性	HTTPS 接続を確立できない。	AAA 設定のログイン情報と Cisco ISE のログイン情報が同じであるかどうかを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Cisco DNA Center エンドポイント URL に到達できない。	<ul style="list-style-type: none"> • Cisco DNA Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。
	信頼：設定	Cisco ISE 証明書チェーンが無効である。	<ul style="list-style-type: none"> • 必要に応じて、Cisco ISE 内部ルート CA チェーンを再生成します。詳細については、『Cisco Identity Services Engine Administration Guide』の「ISE CA Chain Regeneration」を参照してください。 • 内部 CA 証明書チェーンが Cisco ISE から削除されていないことを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Cisco DNA Center エンドポイント URL が禁止されている。	

コンポーネント	サブコンポーネント	問題	推奨されるアクション
			<ul style="list-style-type: none"> • URL を起動し、エンドポイントの /aaa/Cisco ISE/certificate ディレクトリにアクセスできるかどうかを確認します。 • Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっているかどうかを確認します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable External RESTful Services APIs」を参照してください。
	信頼：認証	Cisco ISE パスワードの期限が切れている。	<ul style="list-style-type: none"> • Cisco ISE 管理者パスワードを再生成します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Administrative Access to Cisco ISE」を参照してください。 • Cisco ISE GUI にログインできることを確認します。
	信頼：未分類または一般的なエラー	未定義の診断エラーが発生する。	<ol style="list-style-type: none"> 1. Cisco DNA Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。 3. 信頼を再確立します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable PKI in Cisco ISE」を参照してください。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
Cisco Connected Mobile Experiences (CMX) サーバー IP アドレス管理 (IPAM) サーバー IT サービス管理 (ITSM) サーバー	到達可能性	サーバーとの接続を確立できない。	該当するサーバーがダウンしていないかどうかを確認します。
	認証	サーバーにログインできない。	Cisco DNA Center で正しいログイン情報が設定されていることを確認します。
ハードウェア	ディスク	指定したハードウェアコンポーネントに問題がある。	問題のあるコンポーネントを交換します。
	ファン		
	電源モジュール		
	メモリ モジュール		
	CPU		
	ネットワークカード		
	RAID コントローラ		
ネットワークング	インターフェイスがない。	<ol style="list-style-type: none"> 1. Cisco IMC に接続します。 2. PID が UCSC-C220-M4、UCSC-C220-M4S、または DN1-HW-APL の場合は、次の手順を実行します。 <ol style="list-style-type: none"> 1. メインメニューから、[Compute] > [BIOS] > [Configure BIOS] を選択します。 2. [Advanced] タブをクリックします。 3. [LOM and PCIe Slots Configuration] を展開します。 4. 無効な mLOM を有効にして、ホストを再起動します。 3. その他すべての PID について、問題のあるコンポーネントを交換します。 	

コンポーネント	サブコンポーネント	問題	推奨されるアクション
System configuration	ハードウェア構成	Cisco DNA Center <IP_address> 仮想ドライブの書き込みキャッシュポリシーとしてライトバックを指定することはできません。書き込みポリシーはライトスルーである必要があります。	<ol style="list-style-type: none"> 1. Cisco IMC に接続します。 2. メインメニューから、[Storage] > [Raid Controller] を選択します。 3. [Virtual Drive] タブをクリックします。 4. 仮想ドライブを選択し、[Edit] を右クリックします。書き込みポリシーがライトスルーでない場合は、仮想ドライブを更新します。書き込みポリシーはライトスルーである必要があります。
システムリソース	ストレージ	指定したマウントディレクトリに空きがない。	<ul style="list-style-type: none"> • 現在のディレクトリから不要なデータを削除して記憶域を解放します。 • 記憶域が多い新しいマウントディレクトリを指定します。

サポートされている REST API

システムヘルスでは、次の表に示す REST API がサポートされています。これらの API のいずれかを実行するには、API のパスに次の URL を追加します。

<https://CDNAC-server-IP-address/api/v1/API-path>

Method	API パス	説明
GET	diagnostics/system/health	接続されているすべての Cisco DNA Center アプライアンスと外部システムの最新の正常性関連イベントが表示されます。
	diagnostics/system/health?summary=true	シビラティ（重大度）が最も高い最新の正常性イベントが表示されます。
	diagnostics/system/health?domain=DNAC-Appliance	接続されているアプライアンスのすべてのハードウェアイベントが表示されます。
	diagnostics/system/health?domain=Integrations&subdomain-AAA Trust Establishment	すべての統合および AAA 信頼の確立イベントが表示されます。
	diagnostics/system/health?limit=5	最新の 5 つの正常性関連イベントが表示されます。
	diagnostics/system/performance	接続されたアプライアンスのパフォーマンス情報が要約され、過去 15 分間の平均が表示されます。
	diagnostics/system/performance?range=now-1h	過去 1 時間の重要業績評価指標（KPI）メトリックが表示されます。
	diagnostics/system/performance?range=now-1d	過去 1 日間の KPI メトリックが表示されます。
	diagnostics/system/performance?range=now-1w	過去 1 週間の KPI メトリックが表示されます。
	diagnostics/system/performance?function=max	指定した期間の最大値、現在値が表示されます。デフォルトは平均値です。
	diagnostics/system/nodes/performance?range=now-1d	過去 1 日間の接続された各アプライアンスの KPI メトリックが表示されます。
	diagnostics/system/performance?kpi=cpu,memory	デフォルトの期間（15 分）の CPU およびメモリ使用率が表示されます。
	diagnostics/system/nodes/performance/history?kpi=cpu	デフォルト期間の指定された KPI の履歴メトリックが表示されます。複数の KPI を指定する場合は、カンマで区切ります。
	diagnostics/system/nodes/performance/history?kpi=cpu&range=now-1d	過去 1 日間の指定された KPI の履歴メトリックが表示されます。
	/system/health/summary/	最新の重大クラスタイベントが表示されます。クラスタイベントには、すべてのハードウェアコンポーネントと外部サブシステムのイベントが含まれます。
	/system/health/externalsubsystems/subdomain	指定されたサブドメインの最新のイベントが表示されます。有効なサブドメイン値は、IPAM、ISE、CMX、および ITSM です。

Method	API パス	説明
	/system/health/hardware	最新の重大なハードウェアイベントが表示されます。
	/system/health/hardware/hardware_component	指定されたハードウェアコンポーネントの最新のイベントが表示されます。有効なハードウェアコンポーネントの値には、CPU、RAID、MEMORY、POWER、NIC、および DISK があります。
	/diagnostics/system/health/externalsubsystems/ISE	この API によって提供される出力は、接続されている Cisco ISE サーバーの現在の状態によって異なります。この出力の例については、 サンプル API 出力 (35 ページ) を参照してください。
	/diagnostics/system/health/externalsubsystems/IPAM	この API によって提供される出力は、接続されている Cisco Prime Network Registrar IP アドレスマネージャ (IPAM) の現在の状態によって異なります。この出力の例については、 サンプル API 出力 (35 ページ) を参照してください。

サンプル API 出力

次の表に、/diagnostics/system/health/externalsubsystems/ISE または /diagnostics/system/health/externalsubsystems/IPAM API を実行したときに表示される出力の例を示します。

/diagnostics/system/health/externalsubsystems/ISE の出力例
シナリオ : Cisco ISE サーバーが Cisco DNA Center と統合されていません。
Output: <pre>{ "DNAC-Cluster": { "Status": "Warning", "TooltipInfo": "No data available" } }</pre>

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ : Cisco ISE サーバーが Cisco DNA Center に統合されており、正常に機能しています。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Ok",
    "Group": "ISE",
    "Label": {
      "hostname": "ISE-60-38.example.com",
      "ip": "172.28.80.37"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "-429109689",
        "tenantId": "TNT0",
        "severity": 3,
        "timestamp": "1591072373412",
        "source": "ISE ERS Client",
        "actualState": "",
        "description": "ISE PAN ERS connection : ERS reachability with ISE - Success",
        "group": "ISE",
        "family": "External Subsystem",
        "drUsability": "No",
        "state": "SUCCESS",
        "eventInstanceIdentity": {
          "subDomain": "ISE",
          "domain": "Connectivity",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
          "type": "SYSTEM",
          "tags": "ISE_ERS",
          "event_instance_id": {
            "component": "primary",
            "hostname": "ISE-60-38.example.com",
            "ip": "172.28.80.37"
          }
        }
      }
    ]
  }
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：警告ステータスを持つ Cisco ISE イベントが発生しました。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Warning",
    "Group": "ISE",
    "Label": {
      "hostname": "pi-system-200.example.com",
      "ip": "10.197.73.213"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "-440073227",
        "tenantId": "TNT0",
        "severity": 2,
        "timestamp": "1591072804646",
        "source": "AAA Trust Establishment",
        "actualState": "",
        "description": "ISE AAA Trust Establishment : Trust Establishment - Error-IP/FQDN not reachable",
        "group": "ISE",
        "family": "External Subsystem",
        "drUsability": "No",
        "state": "FAILED",
        "eventInstanceIdentity": {
          "subDomain": "ISE",
          "domain": "Integrations",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-ISE-AAA-TRUST",
          "type": "SYSTEM",
          "tags": "ISE_AAA",
          "event_instance_id": {
            "hostname": "pi-system-200.example.com",
            "component": "primary",
            "ip": "10.197.73.213"
          }
        }
      }
    ]
  }
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：接続された Cisco ISE サーバーで外部 RESTful サービス（ERS）が無効になっています。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Warning",
    "Group": "ISE",
    "Label": {
      "hostname": "csg-nscg-0861.example.com",
      "ip": "10.63.107.41"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "-915009445",
        "tenantId": "TNT0",
        "severity": 2,
        "timestamp": "1591357663101",
        "source": "ISE ERS Client",
        "actualState": "",
        "description": "ISE PAN ERS connection : Timeout elapsed",
        "group": "ISE",
        "family": "External Subsystem",
        "state": "FAILED",
        "eventInstanceIdentity": {
          "subDomain": "ISE",
          "domain": "Connectivity",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
          "type": "SYSTEM",
          "tags": "ISE_ERS",
          "event_instance_id": {
            "hostname": "csg-nscg-0861.example.com",
            "component": "primary",
            "ip": "10.63.107.41"
          }
        }
      }
    ]
  }
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：接続された Cisco ISE サーバーで ERS が有効になっています。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Ok",
    "Group": "ISE",
    "Label": {
      "hostname": "csg-nscg-0861.example.com",
      "ip": "10.30.148.52"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "-915009445",
        "tenantId": "TNT0",
        "severity": 3,
        "timestamp": "1591359643926",
        "source": "ISE ERS Client",
        "actualState": "",
        "description": "ISE PAN ERS connection : ERS reachability with ISE - Success",
        "group": "ISE",
        "family": "External Subsystem",
        "state": "SUCCESS",
        "eventInstanceIdentity": {
          "subDomain": "ISE",
          "domain": "Connectivity",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
          "type": "SYSTEM",
          "tags": "ISE_ERS",
          "event_instance_id": {
            "hostname": "csg-nscg-0861.example.com",
            "component": "primary",
            "ip": "10.30.148.52"
          }
        }
      }
    ]
  }
}
```

/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ：Cisco Prime Network Registrar IPAM が Cisco DNA Center に接続されていません。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Warning",
    "TooltipInfo": "No data available"
  }
}
```

/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ : IPAM が Cisco DNA Center に接続されており、正常に機能しています。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Ok",
    "Group": "IPAM Integration",
    "Label": {
      "hostname": "",
      "ip": "192.168.101.72"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "1328761079",
        "tenantId": "TNT0",
        "severity": 3,
        "timestamp": "1591072639889",
        "source": "INFOBLOX: https://192.168.101.72",
        "actualState": "",
        "description": "A third-party IPAM provider is connected.",
        "group": "IPAM",
        "family": "External Subsystem",
        "drUsability": "No",
        "state": "OK",
        "eventInstanceIdentity": {
          "subDomain": "IPAM Integration",
          "domain": "Integrations",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-IPAM",
          "type": "SYSTEM",
          "tags": "IPAM",
          "event_instance_id": {
            "hostname": "",
            "ip": "192.168.101.72"
          }
        }
      }
    ]
  }
}
```


/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ：IPAM が Cisco DNA Center に接続されており、エラーが発生しました。

Output:

```
{
  "DNAC-Cluster": {
    "Status": "Error",
    "Group": "IPAM Integration",
    "Label": {
      "hostname": "",
      "ip": "192.168.101.72"
    },
    "Family": "ExternalSystems",
    "Id": 1,
    "TooltipInfo": [
      {
        "_id": "1328761079",
        "tenantId": "TNT0",
        "severity": 1,
        "timestamp": "1591363687041",
        "source": "INFOBLOX: https://192.168.101.72",
        "actualState": "",
        "description": "There is a critical issue with the connected third-party IPAM provider.",
        "group": "IPAM",
        "family": "External Subsystem",
        "state": "CRITICAL",
        "eventInstanceIdentity": {
          "subDomain": "IPAM Integration",
          "domain": "Integrations",
          "namespace": "SystemRawEvent",
          "id": "SYSTEM-EXTERNAL-IPAM",
          "type": "SYSTEM",
          "tags": "IPAM",
          "event_instance_id": {
            "hostname": "",
            "ip": "192.168.101.72"
          }
        }
      }
    ]
  }
}
```

Cisco DNA Center と Cisco ISE の統合

Cisco ISE には、Cisco DNA Center に関して次の3つの使用例があります。

1. Cisco ISE はユーザー、デバイス、クライアント認証用の AAA（「トリプル A」と発音）サーバーとして使用できます。アクセスコントロールポリシーを使用していない場合、または Cisco ISE をデバイス認証用の AAA サーバーとして使用していない場合は、Cisco ISE のインストールおよび設定は不要です。
2. アクセスコントロールポリシーは Cisco ISE を使用してアクセス制御を適用します。アクセスコントロールポリシーを作成および使用する前に、Cisco DNA Center と Cisco ISE を統合します。このプロセスでは、特定のサービスを用いて Cisco ISE をインストールして

設定し、Cisco DNA Center で Cisco ISE の設定を行う必要があります。Cisco DNA Center を用いた Cisco ISE のインストールと設定の詳細については、[Cisco DNA Center 設置ガイド](#)を参照してください。

3. ネットワークでのユーザー認証に Cisco ISE を使用している場合、Cisco ISE を統合するためにアシュアランスを設定します。この統合により、有線クライアントの詳細（ユーザー名やオペレーティングシステムなど）をアシュアランスで確認できるようになります。詳細については、[Cisco DNA Assurance ユーザガイド](#)の「Cisco DNA Center の Cisco ISE 設定について」を参照してください。

Cisco ISE が正常に登録され、Cisco DNA Center で信頼性が確立されると、Cisco DNA Center は Cisco ISE と情報を共有します。Cisco ISE を使って AAA サーバーとして構成されたサイトに割り当てられた Cisco DNA Center デバイスのインベントリデータは Cisco ISE に伝達されます。さらに、Cisco DNA Center におけるそれらの Cisco DNA Center デバイスに対するすべての更新（デバイス クレデンシャルなど）も Cisco ISE を変更によって更新します。

Cisco ISE を使って AAA サーバーとしてサイトに関連付けられている Cisco DNA Center デバイスが想定どおり Cisco ISE に伝達されない場合、Cisco DNA Center は一定期間待機した後、自動的に再試行します。この後続の試行は、Cisco ISE への最初の Cisco DNA Center デバイス プッシュが、ネットワークの問題、Cisco ISE のダウンタイム、またはその他の自動訂正可能なエラーが原因で失敗した場合には行われます。Cisco DNA Center は、デバイスの追加または Cisco ISE へのデータの更新を再試行することで、Cisco ISE との最終的な一貫性の確立を試みます。ただし、Cisco ISE へのデバイスまたはデバイスデータの伝達が、Cisco ISE 自体による拒否が原因で入力検証エラーとして失敗した場合、再試行は行われません。

Cisco ISE について RADIUS の共有秘密を変更しても、Cisco ISE が Cisco DNA Center を更新する際にその変更は反映されません。Cisco DNA Center の共有秘密を Cisco ISE と一致するように更新するには、新しいパスワードで AAA サーバーを編集します。Cisco DNA Center は新しい証明書を Cisco ISE からダウンロードし、Cisco DNA Center を更新します。

Cisco ISE は既存のデバイス情報を Cisco DNA Center と共有しません。Cisco DNA Center が Cisco ISE 内のデバイスに関する情報を認識するには、そのデバイスに Cisco DNA Center と同じ名前を付ける必要があります。Cisco DNA Center と Cisco ISE は、デバイスのホスト名変数を通じて、この統合用に固有のデバイスを識別します。



-
- (注) Cisco DNA Center インベントリ デバイスを Cisco ISE に伝達し、変更を更新するプロセスはすべて Cisco DNA Center 監査ログにキャプチャされます。Cisco DNA Center と Cisco ISE 間のワークフローに問題がある場合は、Cisco DNA Center GUI で監査ログの情報を確認します。
-

Cisco DNA Center は、プライマリ管理者 ISE ノードと統合されています。Cisco DNA Center から Cisco ISE にアクセスする場合は、このノードと接続します。

Cisco DNA Center は 15 分ごとに Cisco ISE をポーリングします。Cisco ISE サーバーがダウンした場合、Cisco DNA Center に Cisco ISE サーバーが赤色（到達不能）で表示されます。

Cisco ISE サーバーに到達不能な場合、Cisco DNA Center はポーリングを 15 秒に増やし、その後 30 秒、1 分、2 分、4 分といった具合に、最大ポーリング時間の 15 分になるまで倍増してい

きます。Cisco DNA Center は 15 分間隔でのポーリングを 3 日間継続します。Cisco DNA Center は接続が復活しない場合、ポーリングを停止し、Cisco ISE サーバーのステータスを [信頼できない (Untrusted)] に更新します。この場合、Cisco DNA Center と Cisco ISE サーバー間の信頼関係を再確立する必要があります。

次の追加要件と推奨事項を確認して、Cisco DNA Center と Cisco ISE の統合を確認してください。

- Cisco DNA Center と Cisco ISE の統合はプロキシサーバー経由ではサポートされていません。プロキシサーバーを使用して設定されている Cisco ISE がネットワークにある場合、そのプロキシサーバーを使用しないように Cisco DNA Center を設定します。設定するにはプロキシサーバーの IP アドレスをバイパスします。
- Cisco DNA Center と Cisco ISE の統合は、現在、Cisco DNA Center 仮想 IP アドレス (VIP) 経由ではサポートされていません。Cisco DNA Center にエンタープライズ CA 発行の証明書を使用している場合は、サブジェクトの別名 (SAN) 拡張内にある Cisco DNA Center のすべてのインターフェイスの IP アドレスが Cisco DNA Center 証明書に含まれていることを確認します。Cisco DNA Center が 3 ノードクラスタの場合、3 ノードの全インターフェイスの IP アドレスが、Cisco DNA Center 証明書の SAN 拡張に含まれている必要があります。
- Cisco ISE での管理者レベルのアクセス権が必要です。
- Cisco ISE の管理者ユーザーのパスワードの有効期限を無効にします。または、期限が切れる前に、パスワードを忘れずに更新します。詳細については、『[Cisco Firepower Threat Defense Virtual for Microsoft Azure Quick Start Guide](#)』を参照してください。
- Cisco ISE 証明書が変更された場合は、Cisco DNA Center を更新する必要があります。更新するには、AAA サーバー (Cisco ISE) を編集し、パスワードを再入力して保存します。これにより、Cisco DNA Center は新しい管理証明書の証明書チェーンを Cisco ISE からダウンロードし、Cisco DNA Center を更新します。Cisco ISE を HA モードで使用し、管理者証明書がプライマリまたはセカンダリ管理ノードで変更された場合は、Cisco DNA Center を更新する必要があります。
- Cisco DNA Center は、pxGrid 経由で接続するように、自身の証明書、および Cisco ISE の証明書を設定します。pxGrid に対する別の証明書を使用して、別の pxGrid クライアント (Firepower など) に接続することもできます。これらの接続が、Cisco DNA Center および Cisco ISE の pxGrid 接続と干渉することはありません。
- RADIUS のシークレットパスワードは変更できます。シークレットパスワードは、[System]> [Settings] > [External Services] > [Authentication and Policy Servers] で Cisco ISE を AAA サーバーとして設定する際に指定しています。シークレットパスワードを変更するには、[Design] > [Network Settings] > [Network] の順に選択し、[Change Shared Secret] リンクをクリックします。これにより、Cisco ISE は、Cisco DNA Center によって管理されているネットワークデバイスに接続するとき、新しいシークレットパスワードを使用するようになります。
- 分散 Cisco ISE クラスタでは、各ノードは PAN (管理)、MnT (監視とトラブルシューティング)、PSN (ポリシーサービス) などの特定の機能のみを実行します。PAN ノードでは

管理証明書のみを使用し、PSN ノードでは EAP 認証証明書のみを使用することができます。ただし、この構成により pxGrid の Cisco DNA Center と Cisco ISE の統合が妨げられません。したがって、Cisco ISE プライマリ PAN ノードで EAP 認証証明書の使用を有効にすることをお勧めします。

- Cisco DNA Center は、CRL 配布ポイント（CDP）および Online Certificate Status Protocol（OCSP）による証明書失効チェックをサポートしています。統合中に、Cisco DNA Center はポート 9060 で Cisco ISE 管理証明書を受信し、その Cisco ISE 管理証明書内の CDP および OCSP URL に基づいてその有効性を検証します。CDP（CRL のリストを含む）と OCSP の両方が設定されている場合、Cisco DNA Center は OCSP を使用して証明書の失効ステータスを確認し、OCSP URL にアクセスできない場合は CDP にフォールバックします。CDP に複数の CRL がある場合、Cisco DNA Center は最初の CRL に到達できない場合は、次の CRL に接続します。ただし、JDK PKI Oracle のバグにより、すべての CRL エントリはチェックされません。

プロキシは証明書の検証ではサポートされていません。Cisco DNA Center はプロキシなしで CRL および OCSP サーバーに接続します。

- 証明書の OCSP および CRL エントリはオプションです。
- LDAP は、証明書検証用のプロトコルとしてサポートされていません。CDP または AIA 拡張に LDAP URL を含めないでください。
- Cisco DNA Center から CDP および OCSP のすべての URL に到達できる必要があります。到達不能な URL が原因で、統合の失敗など、統合エクスペリエンスの低下が生じる可能性があります。

データの匿名化

Cisco DNA Center では、有線エンドポイントとワイヤレスエンドポイントのデータを匿名化できます。ユーザー ID やデバイスのホスト名など、有線エンドポイントとワイヤレスエンドポイントの個人を特定できる情報をスクランブル化できます。

[Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 1 メニューアイコン（☰）をクリックして、[System] > [Settings] > [Trust & Privacy] > [Anonymize Data] の順に選択します。

[Anonymize Data] ウィンドウが表示されます。

ステップ 2 [Enable Anonymization] チェックボックスをオンにします。

ステップ 3 [保存 (Save)] をクリックします。

匿名化を有効にすると、デバイス検索時に、MAC アドレス、IP アドレスなどの匿名以外の情報しか指定できなくなります。

認証サーバとポリシーサーバの設定

Cisco DNA Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center および Cisco ISE が統合されていることを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
 - AAA サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
 - AAA サーバーで Cisco DNA Center の属性名を定義します。
 - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、以下の点を確認してください。
 - Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『[Cisco DNA Center Compatibility Matrix](#)』を参照してください。Cisco ISE のインストールについては、[Cisco Identity Services Engine インストールおよびアップグレードガイド \[英語\]](#) を参照してください。
 - スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。



(注) pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：
 - Cisco DNA Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。



(注) PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

- 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、[Work Centers] > [Trustsec] > [Trustsec Servers] > [Trustsec AAA Servers] でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名 (SAN) のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の SAN フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。



(注) Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、[Cisco Cloud APIC リリースノート \[英語\]](#) を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [External Services] > [Authentication and Policy Servers]。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address] : AAA サーバの IP アドレス。
- [Shared Secret] : デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address] : Cisco ISE サーバーの IP アドレス。
- [Shared Secret] : デバイス認証のキー。
- [Username] : Cisco ISE に HTTPS 経由でログインするために使用するユーザー名。
- [Password] : Cisco ISE HTTPS ユーザー名のパスワード。

(注) ユーザー名とパスワードは、ネットワーク管理者に属する ISE 管理者アカウントである必要があります。

- [FQDN] : Cisco ISE サーバーの完全修飾ドメイン名 (FQDN) 。

(注)

- Cisco ISE ([Administration] > [Deployment] > [Deployment Nodes] > [List]) で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
- 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名 (CN) または Subject Alternative Name (SAN) と一致する必要があります。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

たとえば、Cisco ISE サーバーの FQDN は *ise.cisco.com* である可能性があります。

- [Virtual IP Address (es)] : Cisco ISE ポリシーサービスノード (PSN) が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

ステップ5 [Advanced Settings] をクリックして、設定を構成します。

- [Connect to pxGrid] : pxGrid 接続を有効にするには、このチェックボックスをオンにします。

Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Cisco DNA Center システムを認証するために Cisco ISE に送信) 、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局 (CA) によって生成されていること (そうでない場合、pxGrid 認証は失敗します) 。

- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。
- [Protocol] : [TACACS] と [RADIUS] (デフォルト)。両方のプロトコルを選択できます。
注目 ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design] > [Network Settings] > [Network]**で Cisco ISE サーバーを TACAS サーバーとして設定できません。
- [Authentication Port] : AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port] : AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port] : デフォルトの TACACS ポートは 49 です。
- [Retries] : 接続の試行が中止される前に、Cisco DNA Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- [Timeout] : 接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

(注) 必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Cisco DNA Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、[Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ :

- [Authentication and Policy Servers] ウィンドウ : 「進行中」
- [System 360] ウィンドウ : 「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ :

- [Authentication and Policy Servers] ウィンドウ : 「アクティブ」
- [System 360] ウィンドウ : 「プライマリ使用可能」 および 「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により [FAILED] と表示されている場合は、[Retry] をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

Cisco AI Network Analytics の設定

この手順では、Cisco AI Analytics 機能を有効にして、ネットワークデバイスからのネットワークイベントのデータとインベントリ、サイト階層、およびトポロジのデータを Cisco AI Cloud にエクスポートします。

始める前に

- Cisco DNA Center 用の Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認してください。AI ネットワーク分析 アプリケーションは、Cisco DNA Advantage ソフトウェアライセンスに含まれています。
- AI Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。アプリケーションの更新のダウンロードとインストールを参照してください。
- ネットワークまたは HTTP プロキシが、次のクラウドホストへのアウトバウンド HTTPS (TCP 443) アクセスを許可するように設定されていることを確認します。
 - [api.use1.prd.kairos.ciscolabs.com] (米国東部地域)
 - [api.euc1.prd.kairos.ciscolabs.com] (EU 中央地域)

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
[AI ネットワーク分析] ウィンドウが表示されます。

AI Network Analytics

Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Configure

Recover from a config file ⓘ

ステップ 3 次のいずれかを実行します。

- アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。
 1. [Recover from a config file] をクリックします。
[Restore AI ネットワーク分析] ウィンドウが表示されます。

2. 表示されたエリアにコンフィギュレーション ファイルをドラッグアンドドロップするか、ファイルシステムからファイルを選択します。
3. [Restore] をクリックします。

Cisco AI Network Analytics の復元には数分かかる場合があります、その後、[Success] ダイアログボックスが表示されます。

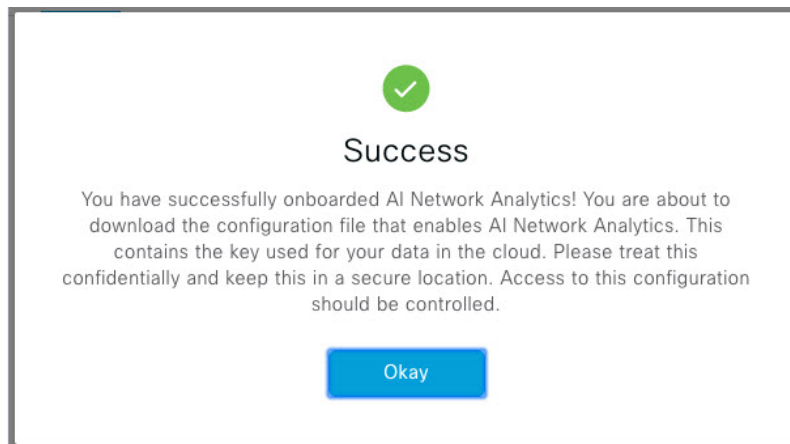
- Cisco AI Network Analytics を初めて設定する場合は、次の手順を実行します。

1. [Configure] をクリックします。
2. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。

[Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。

3. [Next] をクリックします。
[terms and conditions] ウィンドウが表示されます。
4. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。

Cisco AI Network Analytics が有効になるまでに数分かかる場合があります、その後、[Success] ダイアログボックスが表示されます。



ステップ 4 [Success] ダイアログボックスで [Okay] をクリックします。

AI ネットワーク分析 ウィンドウが表示され、[Enable AI Network Analytics] トグルボタン が表示されます。

ステップ 5 (推奨) AI ネットワーク分析 ウィンドウで、[Download Configuration] ファイルをクリックします。

クライアント証明書の更新

AIエージェントは、X.509クライアント証明書を使用してAIクラウドへの認証を実行します。証明書は、AIクラウドへのテナントのオンボーディング時にAIクラウドCAによって作成および署名され、3年間有効です（2021年8月に1年に短縮）。有効期限が切れる前に、クラウド接続が失われないようにクライアント証明書を更新する必要があります。証明書の自動更新メカニズムが導入されています。このメカニズムでは、更新後に証明書を手動でバックアップする必要があります。新しいCisco DNA Centerを復元または移行する場合は、バックアップが必要です。

更新後、すべてのAI分析ウィンドウ（ピア比較、ヒートマップ、ネットワーク比較、トレンドおよびインサイト）に通知が表示され、新しいAIネットワーク分析構成をバックアップするように指示されます。

ディセーブル Cisco AI Network Analytics

Cisco AI Network Analytics のデータ収集を無効にするには、次のように AI Network Analytics 機能を無効にする必要があります。

-
- ステップ 1** メニューアイコン（☰）をクリックして、[System] > [Settings]の順に選択します。
 - ステップ 2** [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
各機能のチェックマーク（）は、その機能が有効になっていることを示します。チェックボックスがオフの場合（）、機能は無効になっています。
 - ステップ 3** [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします（）。
 - ステップ 4** [Update] をクリックします。
 - ステップ 5** Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center (TAC) に連絡してサポートリクエストをオープンします。
 - ステップ 6** （オプション） 以前の設定が間違っていて配置されている場合は、[Download configuration file] をクリックします。
-

機械推論ナレッジベースの更新

機械推論ナレッジパックは、機械推論エンジン（MRE）がセキュリティの問題を特定し、根本原因の自動分析を改善するために使用する、段階的なワークフローです。これらのナレッジパックは、より多くの情報を受信しながら継続的に更新されます。機械推論ナレッジベースは、これらのナレッジパック（ワークフロー）のリポジトリです。最新のナレッジパックにアクセスするために、機械推論ナレッジベースを毎日自動更新するように Cisco DNA Center を設定することもできれば、手動更新を実行することもできます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings]の順に選択します。

ステップ 2 [External Services] まで下にスクロールし、[Machine Reasoning Knowledge Base]を選択します。
[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。

- [INSTALLED] : インストールされている機械推論ナレッジベースパッケージのバージョンとインストール日が表示されます。

機械推論ナレッジベースの新しいアップデートがある場合は、[Machine Reasoning Knowledge Base] ウィンドウに [AVAILABLE UPDATE] 領域が表示され、アップデートの [Version] と [Details] が示されます。

- [AUTO UPDATE] : 機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。
- [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] : 自動構成を実行できる CX Cloud と Cisco DNA Center を統合します。この統合により、Cisco DNA Center のセキュリティアドバイザリ ツールからデバイスの強化された脆弱性検出が直接提供されます。

ステップ 3 (推奨) [AUTO UPDATE] チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。

[Next Attempt] 領域に、次回の更新の日付と時刻が表示されます。

自動更新は、Cisco DNA Center がクラウドの機械推論エンジンに正常に接続されている場合にのみ実行できます。

ステップ 4 機械推論ナレッジベースを Cisco DNA Center で手動で更新するには、次のいずれかを実行します。

- [AVAILABLE UPDATES] の下にある [Update] をクリックします。[Success] ポップアップウィンドウが表示され、更新のステータスが表示されます。
- 機械推論ナレッジベースをローカルマシンに手動でダウンロードして Cisco DNA Center にインポートします。次の手順を実行します。

1. [Download] をクリックします。

[Opening mre_workflow_signed] ダイアログボックスが表示されます。

2. ダウンロードしたファイルを開くか、ローカルマシンの目的の場所に保存して、[OK] をクリックします。

3. [Import] をクリックして、ダウンロードした機械推論ナレッジベースをローカルマシンから Cisco DNA Center にインポートします。

ステップ 5 [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの Cisco CX Cloud の連携を有効にします。

ステップ 6 [Security Advisories Settings] エリアで、[RECURRING SCAN] トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。

ステップ 7 [CISCO CX CLOUD] トグルボタンをクリックして、Cisco CX Cloud を有効または無効にします。

シスコアカウント

シスコのクレデンシャルの設定

Cisco DNA Center の Cisco のクレデンシャルを設定できます。Cisco のクレデンシャルは、シスコの顧客またはパートナーとして制限付きの場所にアクセスするために、シスコの Web サイトのログインに使用するユーザー名とパスワードです。



- (注) 次の手順を使用して、Cisco DNA Center 用に設定された Cisco のクレデンシャルは、ソフトウェアイメージや更新プログラムをダウンロードするために使用されます。Cisco のクレデンシャルはまた、セキュリティのために、このプロセスによって暗号化されます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。

- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Cisco Accounts] > [Cisco.com Credentials] の順に選択します。
- ステップ 2** シスコユーザー名およびパスワードを入力してください。
- ステップ 3** [Save] をクリックします。

cisco.com のログイン情報がソフトウェアとサービスに対して設定されます。

シスコのクレデンシャルのクリア

Cisco DNA Center に対して現在設定されている cisco.com のログイン情報を削除するには、次の手順を実行します。



- (注)
- ソフトウェアのダウンロードやデバイスのプロビジョニングに関連するタスクを実行する際、[cisco.com](#)のログイン情報が設定されていないと、タスクの開始前にログイン情報を入力するように求められます。入力したログイン情報を保存してCisco DNA Center全体で使用するには、表示されたダイアログボックスで[Save for Later]チェックボックスをオンにします。それ以外の場合は、これらのタスクを実行するたびにログイン情報を入力する必要があります。
 - この手順を完了すると、エンドユーザーライセンス契約 (EULA) の承認が取り消されます。EULA の承認を再入力する方法については、[ライセンス契約書の受諾 \(62 ページ\)](#)を参照してください。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。

- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Cisco Accounts] > [Cisco.com Credentials] の順に選択します。
- ステップ 2** [Clear] をクリックします。
- ステップ 3** 表示されたダイアログボックスで、[Continue] をクリックして操作を確定します。

接続モードの設定

接続モードは、Cisco DNA Center と連携するネットワーク内のスマート対応デバイスと Cisco Smart Software Manager (SSM) の間の接続を管理します。異なる接続モードを設定するには、SUPER-ADMIN アクセス権限が必要です。

- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Cisco Accounts] > [SSM Connection Mode] の順に選択します。
- 次の接続モードを使用できます。
- 直接
 - オンプレミス CSSM
 - スマートプロキシ

- ステップ 2** Cisco SSM クラウドへの直接接続を有効にするには、[Direct] を選択します。

ステップ 3 組織のセキュリティを高める必要がある場合は、[On-Prem CSSM] を選択します。オンプレミスオプションでは、Cisco SSM クラウドでライセンスを管理する際に、インターネットで直接接続する代わりに Cisco SSM 機能のサブセットにアクセスできます。

- a) [On-Prem CSSM] を有効にする前に、サテライトがネットワークサイトに展開されて稼働していることを確認してください。

サテライトが FQDN で設定されている場合、サテライト FQDN の Call Home 設定が IP アドレスの代わりにプッシュされます。

- b) [On-Prem CSSM Host]、[Smart Account Name]、[Client ID]、および [Client Secret] の詳細を入力します。スマートアカウント名にスペースやアンダースコアを使用しないでください。

クライアント ID とクライアントシークレットを取得する方法については、『[Cisco Smart Software Manager On-Prem User Guide](#)』を参照してください。

- c) [Test Connection] をクリックして Cisco SSM 接続を検証します。
d) [Save] をクリックしてから [Confirm] をクリックします。
e) 変更した SSM で再登録が必要なデバイスがある場合は、[Need to Re-Register Devices] ダイアログボックスが表示されます。ダイアログボックスで [OK] をクリックします。
f) [Tools] > [License Manager] > [Devices] のウィンドウで、再度登録するデバイスを選択し、[Finish Connection Mode Changes] をクリックします。
g) [Resync Devices] ダイアログボックスで、次の手順を実行します。

- [Smart Account] を入力します。
- [Virtual Account] を入力します。
- [Now] をクリックしてすぐに再同期を開始するか、[Later] をクリックして特定の時間に再同期をスケジュールします。
- [Resync] をクリックします。

[Recent Tasks] ウィンドウには、デバイスの再同期ステータスが表示されます。

ステップ 4 [Smart Proxy] を選択し、Cisco DNA Center を介して Cisco SSM クラウドにスマート対応デバイスを登録します。このモードでは、デバイスを Cisco SSM クラウドに直接接続する必要はありません。Cisco DNA Center は、デバイスからの要求を自身を介して Cisco SSM クラウドにプロキシします。

Call Home 設定をデバイスにプロビジョニングするときに、サテライトが FQDN で設定されている場合、IP アドレスの代わりにサテライトの FQDN がプッシュされます。

プラグアンドプレイの登録

Cisco DNA Center を、Cisco Plug and Play (PnP) Connect のコントローラとして、リダイレクトサービス用に Cisco スマートアカウントに登録できます。これにより、Cisco PnP Connect クラウドポータルから Cisco DNA Center の PnP に、デバイスインベントリを同期することができます。

始める前に

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

スマートアカウントで、特定の機能の実行を許可するロールがユーザーに割り当てられます。

- スマートアカウント管理者ユーザーは、すべてのバーチャルアカウントにアクセスできます。
- ユーザーは、割り当てられたバーチャルアカウントにのみアクセスできます。

ステップ 1 メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Cisco Accounts] > [PnP Connect]** の順に選択します。

PnP 接続プロファイルのテーブルが表示されます。

ステップ 2 **[Register]** をクリックして、バーチャルアカウントを登録します。

ステップ 3 [バーチャルアカウントの登録 (Register Virtual Account)] ウィンドウで、設定したスマートアカウントが [スマートアカウントの選択 (Select Smart Account)] ドロップダウンリストに表示されます。[Select Virtual Account] ドロップダウンリストからアカウントを選択できます。

ステップ 4 必要な [IP] または [FQDN] オプションボタンをクリックします。

ステップ 5 コントローラの IP アドレスまたは FQDN (完全修飾ドメイン名) を入力します。

ステップ 6 プロファイル名を入力します。指定した設定を使用して、選択したバーチャルアカウントのプロファイルが作成されます。

ステップ 7 [Use as Default Controller Profile] チェックボックスをオンにして、この Cisco DNA Center コントローラを Cisco PnP Connect クラウドポータルにデフォルトコントローラとして登録します。

ステップ 8 [登録 (Register)] をクリックします。

PnP イベント通知の作成

イベント通知を作成することで、プラグアンドプレイ (PnP) イベントが Cisco DNA Center で発生するたびに通知を受け取ります。サポートされているチャンネルを設定し、イベント通知を作成するには、『[Cisco DNA Center Platform User Guide](#)』の「Work with Event Notifications」トピックを参照してください。

次の PnP イベントへのイベント通知を作成してください。

Event Name	イベント ID	説明
デバイスの追加に失敗しました。	NETWORK-TASK_FAILURE-3-008	デバイスは、単一または一括インポートでは追加されません。単一または一括インポートによってデバイスを追加すると、エラーが発生します。

Event Name	イベント ID	説明
デバイスの追加に成功しました。	NETWORK-TASK_COMPLETE-4-007	単一または一括インポートによってデバイスが正常に追加されました。
デバイスはエラー状態です。	NETWORK-ERROR_1-002	デバイスは エラー 状態になります。
デバイスはプロビジョニング状態です。	NETWORK-INFO_4-003	デバイスは プロビジョニング 状態になります。
デバイスがオンボーディング状態でスタックします。	NETWORK-TASK_PROGRESS-2-006	デバイスが 15 分以上オンボーディング状態でスタックしています。
デバイスが請求を待っています。	NETWORK-INFO_2-001	デバイスは 未請求 の状態になり、プロビジョニングの準備ができています。
スマートアカウントの同期に失敗しました。	NETWORK-TASK_FAILURE-1-005	一部のデバイスでスマートアカウントの同期に失敗しました。
スマートアカウントの同期に成功しました。	NETWORK-TASK_COMPLETE-4-004	一部のデバイスで、スマートアカウントの同期に成功しました。

スマートアカウントの設定

シスコスマートアカウントのログイン情報は、スマートライセンスアカウントに接続する目的で使用されます。ライセンスマネージャツールは、権限付与とライセンス管理のために、このスマートアカウントの詳細なライセンス情報を使用します。

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

-
- ステップ 1** [System]メニューアイコン (☰) をクリックして、> [Settings] > [Cisco Accounts] > [Smart Account]。
- ステップ 2** [Add] ボタンをクリックします。スマートアカウントのログイン情報を入力するように求められます。
- スマートアカウントのユーザー名およびパスワードを入力します。
 - [Save] をクリックします。スマートアカウントが設定されます。

- ステップ3** 選択したスマートアカウントの名前を変更するには、[Change]をクリックします。Cisco SSMクラウドでスマートライセンスアカウントへの接続に使用されるスマートアカウントを選択するように促されます。
- ドロップダウンリストから [Smart Account] を選択します。
 - [Save] をクリックします。
- ステップ4** [View all virtual accounts] をクリックし、そのスマートアカウントに関連付けられているすべてのバーチャルアカウントを表示します。
- (注) シスコアカウントは複数のスマートアカウントとバーチャルアカウントをサポートしていません。
- ステップ5** (オプション) スマートライセンス対応デバイスをバーチャルアカウントに自動登録する場合、[Auto register smart license enabled devices] チェックボックスをオンにします。スマートアカウントに関連付けられているバーチャルアカウントのリストが表示されます。
- ステップ6** 必要なバーチャルアカウントを選択します。スマートライセンス対応デバイスがインベントリに追加されるたびに、選択したバーチャルアカウントに自動的に登録されます。
- ステップ7** ライセンスを取得したスマートアカウントユーザーとそれに関連する履歴データを削除する場合は、[Delete historical information] をクリックします。
- [Delete Historical Data] スライドインペインには、ライセンスを取得したスマートアカウントユーザーが表示されます。また、Cisco DNA Center に現在存在していない既存のスマートアカウントも表示されますが、それらの履歴データは引き続き利用できます。
- ステップ8** [Smart Account list] エリアで、削除するスマートアカウントの横にあるチェックボックスをオンにします。
- ステップ9** [削除 (Delete)] をクリックします。
- ステップ10** 次の確認ウィンドウで、[Delete] をクリックします。
- ステップ11** (オプション) [Delete the associated license historical information] チェックボックスをオンにして、関連するライセンスの履歴情報を削除します。

スマートライセンス

シスコスマートライセンスは、シスコポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。製品アクティベーションキー (PAK) は不要です。
- **管理の統合**：My Cisco Entitlements (MCE) は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。

- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります (software.cisco.com)。

シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

始める前に

- スマートライセンスを有効にするには、Cisco クレデンシャルを設定し（「[シスコのクレデンシャルの設定 \(53 ページ\)](#)」を参照）、Cisco SSM で Cisco DNA Center ライセンス規則をアップロードする必要があります。
- スマートライセンスは、[System] > [Settings] > [Cisco Accounts] > [SSM Connection Mode] が [On-Prem CSSM] の場合はサポートされません。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Cisco Accounts] > [Smart Licensing] の順に選択します。

デフォルトでは、[Smart User] と [Smart Domain] の詳細が表示されます。

ステップ 2 登録するバーチャルアカウントを [Search Virtual Account] ドロップダウンリストから選択します。

ステップ 3 [登録 (Register)] をクリックします。

ステップ 4 登録が正常に完了したら、[View Available Licenses] リンクをクリックして、Cisco DNA Center の使用可能なライセンスを確認します。

デバイスの可制御性

デバイスの可制御性とは、Cisco DNA Center におけるいくつかのデバイス層機能の同期状態を徹底するシステムレベルのプロセスです。この目的は、Cisco DNA Center がデバイスを管理するのに必要なネットワーク設定の導入を支援することです。ディスカバリを実行したり、インベントリにデバイスを追加したり、デバイスをサイトに割り当てたりすると、ネットワークデバイスに変更が加えられます。

デバイスにプッシュされる設定を表示するには、[Provision > Inventory] に移動し、[Focus] ドロップダウンリストから [Provision] を選択します。[Provision Status] 列の [See Details] をクリックします。



-
- (注) Cisco DNA Center によりデバイスが設定または更新されると、トランザクションが監査ログにキャプチャされ、変更の追跡と問題のトラブルシューティングに使用できます。
-

下記のデバイス設定がデバイスの可制御性の一部として有効になります。

- デバイス検出
 - [SNMP Credentials]
 - [NETCONF Credentials]
- インベントリへのデバイスの追加
 - Cisco TrustSec (CTS) クレデンシヤル



(注) [Global] サイトが Cisco ISE で AAA として設定されている場合のみ、Cisco TrustSec (CTS) クレデンシヤルがインベントリ中にプッシュされます。それ以外の場合は、CTS が Cisco ISE で AAA として設定されている場合に「サイトへの割り当て」中にデバイスにプッシュされます。

- デバイスのサイトへの割り当て
 - コントローラ証明書
 - SNMP トラップサーバ定義
 - Syslog サーバ定義
 - NetFlow サーバ定義
 - Wireless Service Assurance (WSA)
 - IPDT の有効化

デバイスの可制御性はデフォルトで有効です。デバイスの可制御性を有効にたくない場合は、手動で無効にします。詳細については、[デバイスの可制御性の設定 \(61 ページ\)](#) を参照してください。

デバイスの可制御性が無効の場合、ディスカバリ実行時やデバイスのサイトへの割り当て時に、上述のクレデンシヤルや機能が Cisco DNA Center で設定されることはありません。

次のような状況により、デバイスの可制御性によってデバイスにネットワーク設定が適用されるかどうかが決まります。

- **デバイス検出** : SNMP と NETCONF クレデンシヤルがまだデバイスに存在しない場合は、この設定が検出プロセス中に適用されます。
- **インベントリ内のデバイス (Device in Inventory)** : 初期インベントリ収集が正常に終了すると、IPDT がデバイスで設定されます。

以前のリリースでは、次の IPDT コマンドが設定されていました。

```
ip device tracking
ip device tracking probe delay 60
ip device tracking probe use-svi
```

インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
ip device tracking maximum 65535
```

現在のリリースでは、新しく検出されたデバイスに対して次の IPDT コマンドが設定されます。

```
device-tracking tracking
device-tracking policy IPDT_POLICY
tracking enable
```

インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
device-tracking attach-policy IPDT_POLICY
```

- **グローバルサイト内のデバイス**：デバイスが正常に追加、インポート、または検出されると、Cisco DNA Center はデフォルトでデバイスを [Managed] 状態にして [Global] サイトに割り当てます。グローバル サイト用の SNMP サーバ、Syslog サーバ、および NetFlow コレクタ設定が定義済みの場合でも、デバイス上のこれらの設定を変更 Cisco DNA Center しません。
- **サイトに移動されたデバイス**：デバイスを [Global] サイトから、SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が定義済みの新しいサイトに移動させると、Cisco DNA Center ではデバイスのこれらの設定が新しいサイト用に定義された設定に変更されます。
- **サイトから削除されたデバイス**：デバイスをサイトから削除する場合、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が削除されません。
- **削除されるデバイス Cisco DNA Center**：デバイスを Cisco DNA Center から削除し、[Configuration Clean-up] チェックボックスがオンにすると、SNMP サーバ、Syslog サーバ、および NetFlow コレクタ設定はデバイスから削除されます。
- **別のサイトに移動したデバイス**：たとえばサイト A からサイト B にデバイスを移動させると、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が、サイト B に割り当てられた設定に置き換えられます。
- **サイトテレメトリの変更の更新**：デバイスの可制御性の範囲内にある設定に対する変更は、デバイスのプロビジョニング中、またはテレメトリ設定の更新アクションの実行時にネットワークデバイスに適用されます。

デバイスの可制御性の設定

デバイスの可制御性は、Cisco DNA Center でデバイスを管理するために必要なネットワーク設定の展開を支援します。



- (注) デバイスの可制御性を無効にすると、[Device Controllability] ページに記載されているログイン情報または機能は、ディスカバリ時または実行時にデバイスに設定されません。

デバイスの可制御性はデフォルトで有効です。デバイスの可制御性を手動で無効にするには、次の手順を実行します。

ステップ1 メニューアイコン (☰) をクリックして、[System]>[Settings]>[Device Settings]>[Device Controllability]。

ステップ2 [Enable Device Controllability] チェックボックスをオフにします。

ステップ3 [Save] をクリックします。

ライセンス契約書の受諾

ソフトウェアをダウンロードする前、またはデバイスをプロビジョニングする前に、エンドユーザーライセンス契約 (EULA) に同意する必要があります。



(注) cisco.com のログイン情報をまだ設定していない場合は、先に進む前に、[Device EULA Acceptance] ウィンドウで設定するように求められます。

ステップ1 メニューアイコン (☰) をクリックして、[System]>[Settings]>[Device Settings]>[Device EULA Acceptance] の順に選択します。

ステップ2 [Cisco End User License Agreement] リンクをクリックし、EULA を読みます。

ステップ3 [I have read and accept the Device EULA] チェックボックスをオンにします。

ステップ4 [Save] をクリックします。

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定することができます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールの概要](#)を参照してください。

ステップ1 メニューアイコン (☰) をクリックして、[System]>[Settings]>[Device Settings]>[SNMP] の順に選択します。

ステップ2 次のフィールドを設定します。

- **再試行回数 (Retries)** : 許容されるデバイス接続の最大試行回数。有効な値は 1 ~ 3 です。デフォルトは 3 です。
- **[Timeout]** : タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ~ 300 秒です。デフォルトは 5 秒です。

ステップ3 [保存 (Save)] をクリックします。

ステップ4 (オプション) デフォルトの設定に戻すには、[Reset] をクリックしてから [Save] をクリックします。

ICMP ping のイネーブル化

Internet Control Message Protocol (ICMP) ping が有効になっていて、FlexConnect モードで到達不能なアクセスポイントがある場合、Cisco DNA Center は ICMP を使用して 5 分ごとにそれらのアクセスポイントに ping を実行し、到達可能性を強化します。

次の手順では、ICMP ping を有効にする方法について説明します。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Device Settings] > [ICMP Ping] の順に選択します。

ステップ2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにします。

ステップ3 [Save] をクリックします。

イメージ配信サーバの設定

イメージ配信サーバは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように最大3つの外部イメージ配信サーバを設定できます。また、新しく追加されたイメージ配信サーバに1つ以上のプロトコルを設定できます。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Device Settings] の順に選択します。

ステップ2 [Device Settings] ドロップダウンリストから、[Image Distribution Servers] を選択します。

ステップ3 [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバのホスト、ユーザー名、SFTP、SCP、および接続に関する詳細が表示されます。

ステップ4 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server] slide-in pane が表示されます。

ステップ5 イメージ配信サーバについて、次の項目を設定します。

- [Host] : イメージ配信サーバのホスト名または IP アドレスを入力します。
- [Root Location] : ファイル転送にルートディレクトリを使用する場合は、[Use root directory for file transfers] チェックボックスをオンにします。それ以外の場合は、[Use root directory for file transfers] チェックボックスをオフにしてルートの場所を入力します。

(注) Cisco AireOS コントローラの場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [SFTP and SCP] 領域を展開します。
- [Username] : イメージ配信サーバーへのログインに使用されるユーザー名を入力します。ユーザー名には、サーバーの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [Password] : イメージ配信サーバーへのログインに使用されるパスワード。
- [ポート番号] : イメージ配信サーバーが実行されているポート番号を入力します。

ステップ 6 [Save] をクリックします。

ステップ 7 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTP の暗号方式として弱い暗号方式 (SHA1 ベースの暗号など) しかサポートされていないため、Cisco DNA Center でソフトウェアイメージの管理やワイヤレスアシュアランスの設定を行うには、ワイヤレスコントローラからの SFTP 接続に対して SFTP 互換モードを有効にする必要があります。Cisco DNA Center の SFTP サーバーでは、弱い暗号方式のサポートを最大 90 日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

- a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。
- b) [Compatibility Mode] slide-in pane で [Compatibility Mode] チェックボックスをオンにして期間 (1 分~90 日) を入力します。
- c) [Save] をクリックします。

ステップ 8 (オプション) 設定を編集するには、[Action] 列で対応するイメージ配信サーバーの [Edit] アイコンをクリックし、[Edit] ウィンドウで必要な変更を行って [Save] をクリックします。

ステップ 9 (任意) イメージ配信サーバーを削除するには、[Action] 列で対応するイメージ配信サーバーの横にある [Delete] アイコンをクリックし、[Delete] をクリックします。

PnP デバイス許可の有効化

次の手順では、デバイスで許可を有効にする方法について説明します。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Device Settings] の順に選択します。

ステップ 2 [Device Settings] ドロップダウンリストから [PnP Device Authorization] を選択します。

(注) デフォルトでは、デバイスは自動的に許可されます。

ステップ 3 [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。

ステップ 4 [Save] をクリックします。

デバイスプロンプトの構成

Cisco DNA Center ではユーザー名とパスワードのカスタムプロンプトを作成できます。カスタムプロンプトを使用してデバイスに関する情報を収集するように、ネットワーク内のデバイスを構成できます。

カスタムプロンプトの作成

ステップ 1 メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Device Settings] > [Device Prompts]**の順に選択します。

[Device Prompts] ウィンドウが表示されます。

ステップ 2 [Create Custom Prompt] をクリックします。

[Create Custom Prompt] スライドインペインが表示されます。

ステップ 3 ユーザー名のカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[username] を選択します。
2. [Prompt Text] フィールドに、正規表現 (Regex) でテキストを入力します。
3. [Save] をクリックします。

ステップ 4 パスワードのカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[password] を選択します。
2. [Prompt Text] フィールドに、正規表現 (Regex) でテキストを入力します。
3. [Save] をクリックします。

(注) [Device Prompts] ウィンドウにカスタムプロンプトが表示されます。ユーザー名とパスワードのカスタムプロンプトを 8 つまで作成できます。

ステップ 5 カスタムプロンプトを必要な順序でドラッグアンドドロップします。

(注) Cisco DNA Center は、カスタムプロンプトの順序を維持し、プロンプトをコンマ区切り値としてデバイスに渡します。最上位のカスタムプロンプトの優先度が高くなります。

ステップ 6 編集アイコンをクリックして、カスタムプロンプトを編集します。

ステップ 7 カスタムプロンプトを削除するには、削除アイコンをクリックします。

- (注) ユーザー名のプロンプトとパスワードのプロンプトには、一意の正規表現が必要です。同じまたは類似の正規表現を作成すると、デバイスで認証の問題が発生します。

デバイス構成のバックアップ設定の構成

Cisco DNA Center は、デバイスの実行構成の定期的なバックアップを実行します。バックアップの日時と、デバイスごとに保存できる構成ドリフトの合計数を選択できます。



- (注) デフォルトでは、構成のバックアップは毎週日曜日の午後 11 時 30 分 (UTC タイムゾーン) にスケジュールされます。

-
- ステップ 1** メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Configuration Archive]** を選択します。
- ステップ 2** **[Configuration Archive]** ウィンドウで、**[Internal]** タブをクリックします。
- ステップ 3** **[Number of config drift per device]** ドロップダウンリストをクリックし、デバイスごとに保存する構成ドリフトの数を選択します。

デバイスごとに 7 ~ 50 の構成ドリフトを保存できます。保存される構成ドリフトの合計には、デバイスのすべてのラベル付き構成が含まれます。

- (注) デフォルトでは、デバイスごとに保存される構成ドリフトの数は 15 です。

- ステップ 4** バックアップの日時を選択します。
- 選択したバックアップの日時は、ネットワークに展開された Cisco DNA Center クラスターのタイムゾーンに基づきます。
- ステップ 5** **[Save]** をクリックします。
- バックアップは、スケジュールした後にアクティビティセンターで表示できます。
- ステップ 6** **[External]** タブをクリックして、デバイス構成をアーカイブするための外部サーバーを構成します。詳細については、[デバイス構成をアーカイブする外部サーバーの構成 \(66 ページ\)](#) を参照してください。

デバイス構成をアーカイブする外部サーバーの構成

デバイスの実行コンフィギュレーションをアーカイブするための外部 SFTP サーバーを構成できます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Configuration Archive] を選択します。

ステップ 2 [Configuration Archive] ウィンドウで、[External] タブをクリックします。

ステップ 3 [Add] をクリックして、[External Repository] を追加します。

(注) 追加できる SFTP サーバーは 1 つだけです。

ステップ 4 [Add New External Repository] スライドインペインで、次の詳細を入力します。

- a) [Host] : ホストの IP アドレスを入力します。
- b) [Root Location] : ルートフォルダの場所を入力します。
- c) [Server Protocol] : SFTP サーバーのユーザー名、パスワード、ポート番号を入力します。
- d) [Backup Format] を選択します。

- [RAW] : 実行コンフィギュレーションがすべて公開されます。すべての機密設定とプライベート設定は、バックアップデータでマスク解除されます。パスワードを入力して、バックアップファイルをロックします。

(注) ファイルのパスワードは Cisco DNA Center に保存されません。SFTP サーバー上のファイルにアクセスするには、パスワードを覚えておく必要があります。

- [Sanitized (Masked)] : 実行コンフィギュレーションの機密設定とプライベート設定の詳細がマスクされます。

パスワードは、RAW バックアップ形式を選択した場合にのみ適用されます。

- e) バックアップサイクルをスケジュールします。

バックアップの日付、時刻、タイムゾーン、およびバックアップの繰り返し間隔を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 SFTP サーバーの詳細を編集するには、[Action] 列の編集ボタンをクリックします。

ステップ 7 SFTP サーバーを削除するには、[Action] 列の下にある削除ボタンをクリックします。

クラウドアクセスキー

Cisco DNA Center に Cloud Device Provisioning Application パッケージをインストールしたら、クラウドアクセスキーを登録できます。システムでは、複数のクラウドアクセスキーがサポートされています。各キーは、そのクラウドアクセスキーを使用して検出された AWS インフラストラクチャのコンストラクトまたはリソースをすべて含む個別のクラウドプロファイルとして使用されます。クラウドアクセスキーを追加すると、AWS VPC インベントリ収集が自動的にトリガーされます。そのクラウドアクセスキーの VPC インベントリ収集で検出されたリソースが AWS インフラストラクチャで構築され、CSR および ワイヤレスコントローラのクラウドプロビジョニングで表示して使用できます。

始める前に

- Amazon Web Services (AWS) コンソールからアクセスキー ID と秘密鍵を取得します。
- AWS マーケットプレイスで CSR または ワイヤレスコントローラ 製品に登録し、ターゲットリージョンのイメージ ID を確認します。
- AWS での HA フェールオーバー時に CSR で使用するキーペアを特定します。そのリージョンの CSR をプロビジョニングする際は、このキーペアの名前を Cisco DNA Center のリストから選択します。
- AWS での HA フェールオーバー時に CSR で使用する IAM ロールを特定します。CSR をプロビジョニングする際は、この IAM ロールを Cisco DNA Center のリストから選択します。
- Cisco DNA Center と AWS の間の HTTPS REST API を介した通信に使用するプロキシを設定します。[プロキシの設定 \(80 ページ\)](#) を参照してください。
- eNFV アプリの Cloud Connect 拡張機能は、Cloud Device Provisioning Application パッケージを別途展開することで有効になります。このパッケージは、デフォルトでは Cisco DNA Center の標準インストールに含まれていません。カタログサーバーからパッケージをダウンロードしてインストールする必要があります。詳細については、[アプリケーションの更新のダウンロードとインストール](#)を参照してください。

-
- ステップ 1** メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Cloud Access Keys]** の順に選択します。
- ステップ 2** **[Add]** をクリックします。
- ステップ 3** **[Access Key Name]** を入力し、**[Cloud Platform]** をドロップダウンリストから選択します。AWS コンソールから取得した **[Access Key ID]** と **[Secret Key]** を入力します。
- ステップ 4** **[Save and Discover]** をクリックします。
-

次のタスク

- クラウドアクセスキーを追加すると、AWS VPC インベントリ収集が自動的にトリガーされます。クラウドプラットフォームとの同期には数分かかります。インベントリ収集は、デフォルトの間隔で実行するようにスケジュールされています。
- クラウドインベントリ収集が正常に完了すると、**[Provision]** セクションの **[Cloud]** タブに、収集した AWS VPC インベントリのビューが表示されます。

整合性検証

整合性検証 (IV) では、主要なデバイスデータに対する、デバイス侵害の可能性を示す予期しない変更または無効な値を監視します (該当する場合)。この目的は、シスコデバイスに対する

る不正な変更の検出時間を大幅に短縮することで、侵害の影響を最小限に抑えることにあります。



- (注) このリリースでは、IV で Cisco DNA Center にアップロードされたソフトウェアイメージの整合性検証チェックを実行します。整合性検証チェックを実行するために、IV サービスは、Known Good Value (KGV) ファイルをアップロードする必要があります。

KGV ファイルのアップロード

セキュリティの整合性を提供するために、真正かつ有効なソフトウェアを実行しているものとしてシスコデバイスを検証する必要があります。現在、シスコデバイスには、真正なシスコソフトウェアを実行しているかどうかを判別するための参照ポイントがありません。IV では、収集されたイメージ整合性データをシスコソフトウェアの KGV と比較するためのシステムを使用します。

シスコは、その多くの製品の KGV が含まれる KGV データファイルを生成および発行しています。この KGV ファイルは標準の JSON 形式であり、シスコによって署名され、他のファイルとともに単一の KGV ファイルにバンドルされ、シスコの Web サイトから入手できます。KGV ファイルは、次の場所に掲載されています。

https://tools.cisco.com/cscrd/security/center/files/trust/Cisco_KnownGoodValues.tar

KGV ファイルは IV にインポートされ、ネットワークデバイスから取得した整合性の測定を検証するために使用されます。



- (注) デバイス整合性の測定値は IV に提供され、IV 内で完全に使用されます。IV と cisco.com の間の接続は必要ありません。KGV ファイルを保護された環境にエアギャップ転送し、IV にロードできます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [External Services] > [Integrity Verification] の順に選択します。

ステップ 2 現在の KGV ファイル情報を確認します。

- [File Name] : KGV tar ファイルの名前。
- [Imported By] : KGV ファイルをインポートした Cisco DNA Center ユーザー。自動的にダウンロードされる場合、値は [System] です。
- [Imported Time] : KGV ファイルがインポートされた時刻。

- [Imported Mode] : ローカルまたはリモートのインポートモード。
- [Records] : 処理されたレコード。
- [File Hash] : KGV ファイルのファイルハッシュ。
- [Published] : KGV ファイルの発行日。

ステップ 3 KGV ファイルをインポートするには、次のいずれかの手順を実行します。

- KGV ファイルをローカルにインポートするには、[Import New from Local] をクリックします。
- KGV ファイルを [cisco.com](https://tools.cisco.com) からインポートするには、[Import Latest from Cisco] をクリックします。

(注) [Import Latest from Cisco] オプションでは、ファイアウォール設定は必要ありません。ただし、ファイアウォールがすでに設定されている場合は、<https://tools.cisco.com> への接続のみを開く必要があります。

ステップ 4 [Import Latest from Cisco] をクリックした場合は、[cisco.com](https://tools.cisco.com) への接続が行われ、最新の KGV ファイルが自動的に Cisco DNA Center にインポートされます。

(注) <https://tools.cisco.com> へのセキュアな接続は、Cisco DNA Center とそのプロキシ（初回セットアップ時に設定された場合）に追加された証明書を使用して行われます。

ステップ 5 [Import New from Local] をクリックした場合は、[Import KGV] ウィンドウが表示されます。

ステップ 6 次の手順のいずれかを実行してローカルにインポートします。

- ローカル KGV ファイルを [Import KGV] フィールドにドラッグアンドドロップします。
- [Click here to select a KGV file from your computer] をクリックして、ご使用のコンピュータ上のフォルダから KGV ファイルを選択します。
- [Latest KGV file] リンクをクリックし、最新の KGV ファイルをダウンロードしてから、そのファイルを [Import KGV] フィールドにドラッグアンドドロップします。

ステップ 7 [Import] をクリックします。

KGV ファイルが Cisco DNA Center にインポートされます。

ステップ 8 インポートが完了したら、UI で現在の KGV ファイル情報を検証し、ファイルが更新されたことを確認します。

IV は、Cisco DNA Center が展開されてから 7 日後に最新の KGV ファイルを [cisco.com](https://tools.cisco.com) からシステムに自動的にダウンロードします。自動ダウンロードは 7 日ごとに継続されます。KGV ファイルをローカルシステムに手動でダウンロードして、Cisco DNA Center にインポートすることもできます。たとえば、金曜日に新しい KGV ファイルが使用可能になり、自動ダウンロードが 7 日ごと（月曜日）に行われる場合は、手動でダウンロードできます。

次の KGV 自動ダウンロード情報が表示されます。

- [Frequency] : 自動ダウンロードの頻度。
- [Last Attempt] : KGV スケジューラが最後にトリガーされた時間。

- [Status] : KGV スケジューラの最後の試行のステータス。
- [Message] : ステータスメッセージ。

次のタスク

最新の KGV ファイルをインポートしたら、[Design] > [Image Repository] を選択して、インポートされたイメージの整合性を表示します。



- (注) すでにインポートされたイメージが検証不能ステータス（物理または仮想）である場合は、KGV ファイルをインポートした効果を [Image Repository] ウィンドウで確認できます。さらに、将来のイメージインポートでも、新しくアップロードした KGV を検証のために参照します（該当する場合）。

IP アドレスマネージャの設定

Cisco DNA Center を外部 IP アドレスマネージャ（IPAM）と通信するように設定できます。Cisco DNA Center を使用して、IP アドレスプールの作成、予約、または削除を行うと、Cisco DNA Center はその情報を外部 IPAM に伝達します。

始める前に

- 外部 IP アドレスマネージャがすでに設定され、動作している必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、[System] > [Settings] > [External Services] > [IP Address Manager] の順に選択します。

ステップ 2 [Server Name] フィールドに、IPAM サーバーの名前を入力します。

ステップ 3 [Server URL] フィールドに、IPAM サーバーの URL または IP アドレスを入力します。

証明書がこのサーバーに対して信頼されていないことを示す警告アイコンとメッセージが表示されます。信頼証明書を IPAM から直接インポートするには、次の手順を実行します。

- a) 警告アイコンをクリックします。

[Certificate Warning] ダイアログボックスが表示されます。

- b) 証明書の発行者、シリアル番号、および有効期限を確認します。
c) 情報が正しい場合は、チェックボックスをクリックして Cisco DNA Center による IP アドレスへのアクセスを許可し、信頼できない証明書をトラストプールに追加します。
d) [許可 (Allowed)] をクリックします。

ステップ 4 [Username] および [Password] フィールドに、IPAM ログイン情報を入力します。

ステップ5 [Provider] ロップダウンリストからプロバイダーを選択します。

(注) [BlueCat] をプロバイダとして選択した場合は、自分のユーザーに、BlueCat アドレスマネージャの API アクセスが許可されていることを確認します。1 人または複数のユーザーの API アクセスを設定する方法に関する詳細については、**BlueCat** のマニュアルを参照してください。

Cisco DNA Center を連邦情報処理標準 (FIPS) モードの BlueCat と統合するには、BlueCat 9.3.0 を使用します。

ステップ6 [View] ドロップダウンリストから、デフォルトの IPAM ネットワークビューを選択します。専用ビューが 1 つ設定されている場合、[default] のみがドロップダウンリストに表示されます。ネットワークビューが IPAM で作成され、IP アドレスプールのコンテナとして使用されます。

ステップ7 [保存 (Save)] をクリックします。

次のタスク

証明書が正常に追加されたことを確認するには、[System] > [Settings] > [Trust & Privacy] > [Trustpool] に移動します。



(注) トラストプールでは、証明書はサードパーティの信頼できる証明書として参照されます。

[System] > [System 360] に移動し、外部 IP アドレスマネージャ設定が正常に完了したことを確認します。

Webex 統合の設定

Cisco DNA Center はクライアント 360 の Webex 会議セッション情報を提供します。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [External Services] > [Webex Integration] の順に選択します。

ステップ2 [Authenticate to Webex] をクリックします。

ステップ3 [Cisco Webex] ポップアップウィンドウで、電子メールアドレスを入力し、[Sign In] をクリックします。

ステップ4 パスワードを入力し、[Sign In] をクリックします。

Webex 認証が正常に完了します。

ステップ5 [Default Email Domain for Webex Meetings Sign-In] で、Webex ユーザーの電子メールアドレスドメインを入力し、[Save] をクリックします。

Webex ドメインは組織全体に適用され、ドメインを使用するすべてのユーザーが会議を主催したり会議に参加したりできます。

ステップ 6 (オプション) [Authentication Token] で、[Delete] をクリックして Webex 認証を削除します。

ThousandEyes の統合の構成

外部 ThousandEyes API エージェントと通信するように Cisco DNA Center を構成して、認証トークンを使用して ThousandEyes の統合を有効にできます。統合後、Cisco DNA Center はアプリケーションヘルス ダッシュボードに ThousandEyes エージェントのテストデータを提供します。

始める前に

Cisco Catalyst 9300 および 9400 シリーズスイッチをサポートするアプリケーションホスティングを介して ThousandEyes エージェントを展開したことを確認します。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [External Services] > [ThousandEyes Integration] の順に選択します。

ステップ 2 [Insert new token here] フィールドに、認証トークンを入力します。

(注) OAuth ベアラートークンを受け取るには、[ThousandEyes] ページに移動します。
<https://app.thousandeyes.com/>

ステップ 3 [Save] をクリックします。

デバッグログの設定

サービスの問題のトラブルシューティングに役立てるために、Cisco DNA Center サービスのログレベルを変更できます。

ログレベルによって、ログファイルでキャプチャされるデータ量が異なります。各ログレベルは累積的です。つまり、各レベルには、指定されたレベル以上のレベルで生成されたデータがあれば、すべて含まれます。たとえば、ログレベルを [Info] に設定すると、[Warn] および [Error] ログもキャプチャされます。より多くのデータをキャプチャして、問題のトラブルシューティングに役立つようにログレベルを調整することをお勧めします。たとえば、ログレベルを調整することで、より多くのデータをキャプチャし、根本原因分析または RCA サポートファイルで確認できるようになります。

サービスのデフォルトのログレベルには情報提供 ([Info]) が含まれています。情報提供からのログレベルを、さまざまなログレベル ([Debug] または [Trace]) に変更して、より詳細な情報をキャプチャできます。



注意 開示される可能性がある情報のタイプによっては、[Debug] レベル以上で収集されたログでアクセスを制限する必要があります。



(注) ログファイルが作成されると Cisco DNA Center ホストの一元的な場所に保存されます。この場所から、Cisco DNA Center は、GUI でログを照会して表示できます。ログファイルの合計圧縮サイズは 2 GB です。ログファイルが 2 GB を超える場合、古いログファイルは新しいファイルで上書きされます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、[System]>[Settings]>[System Configuration]>[Debugging Logs] の順に選択します。

[Debugging Logs] ウィンドウには、次のフィールドが表示されます。

- Services
- Logger Name
- Logging Level
- Timeout

ステップ 2 [Services] ドロップダウンリストからサービスを選択し、そのログレベルを調節します。

[Services] ドロップダウンリストには、現在 Cisco DNA Center に設定され、実行しているサービスが表示されます。

ステップ 3 [Logger Name] を入力します。

これは、ロギングフレームワークにメッセージを出力するソフトウェアコンポーネントを制御するために追加された高度な機能です。この機能を使用する際は、十分注意してください。この機能を誤用すると、テクニカルサポートのために必要な情報が失われる可能性があります。ログメッセージは、ここで指定されたロガー (パッケージ) に対してのみ書き込まれます。デフォルトでは、ロガー名には *com.cisco* で始まるパッケージが含まれています。追加のパッケージ名はカンマ区切り値として入力できます。明示的に指示されていない限り、デフォルト値は削除しないでください。*を使用すると、すべてのパッケージがログに記録されます。

ステップ 4 [Logging Level] ドロップダウンリストで、サービスの新しいログレベルを選択します。

Cisco DNA Center では次のログレベルがサポートされています (詳細は以下、降順)。

- [Trace] : トレースメッセージ

- [Debug] : デバッグメッセージ
- [Info] : 正常だが重要な状態メッセージ
- [Warn] : 警告状態メッセージ
- [Error] : エラー状態メッセージ

ステップ 5 [Timeout] フィールドで、ログレベルの期間を選択します。

ログレベルの期間を15分単位で設定します（～無制限）。期間を無制限に指定する場合、トラブルシューティング作業が完了するたびに、デフォルトのログレベルをリセットする必要があります。

ステップ 6 選択内容を確認し、[Apply] をクリックします

（選択内容をキャンセルするには [Cancel] をクリックします）。

ネットワークの再同期間隔の設定

[System] > [Settings] > [Network Resync Interval] の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールの概要](#)を参照してください。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 メニューアイコン（☰）をクリックして、[System] > [Settings] > [Device Settings] > [Network Resync Interval] の順に選択します。

ステップ 2 [Resync Interval] フィールドに、新しい時間値（分）を入力します。

ステップ 3 （オプション）すべてのデバイスに対して設定された既存のポーリング間隔をオーバーライドする場合は、[Override for all devices] チェックボックスをオンにします。

ステップ 4 [Save] をクリックします。

監査ログの表示

監査ログは、Cisco DNA Centerで実行されているさまざまなアプリケーションに関する情報を取得します。さらに、監査ログは、デバイス Public Key Infrastructure (PKI) 通知についての情報も取得します。これらの監査ログの情報は、アプリケーションまたはデバイス PKI 証明書に関連する問題（ある場合）のトラブルシューティングを支援するために使用できます。

監査ログは、発生したシステムイベント、発生した場所、開始したユーザーを記録するシステムでもあります。監査ログを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。

ステップ 1 メニューアイコン (☰) をクリックして、**[Activities] > [Audit Logs]** の順に選択します。

[監査ログ (Audit Logs)] ウィンドウで、ネットワーク内の現在のポリシーに関するログを表示できます。これらのポリシーは、Cisco DNA Center にインストールされているアプリケーションによってネットワークデバイスに適用されます。

ステップ 2 タイムラインスライダをクリックして、ウィンドウに表示するデータの時間範囲を次のとおり指定します。

- [Time Range] 領域で、[Last 2 Weeks]、[Last 7 Days]、[Last 24 Hours]、または [Last 3 Hours] の時間範囲を選択します。
- カスタム範囲を指定するには、[日付 (By date)] をクリックし、開始日時と終了日時を指定します。
- [Apply] をクリックします。

ステップ 3 対応する子監査ログを表示するには、監査ログの横にある矢印をクリックします。

各監査ログは、いくつかの子監査ログの親になることができます。矢印をクリックすると、一連の追加の子監査ログを表示できます。

(注) 監査ログは、Cisco DNA Center によって実行されたタスクに関するデータをキャプチャしません。子監査ログは、Cisco DNA Center によって実行されたタスクのサブタスクです。

ステップ 4 (任意) 左側のペインに表示された監査ログのリストで特定の監査ログメッセージをクリックします。右側のペインで **[イベント ID (Event ID)] > [イベント ID をクリップボードにコピー (Copy Event ID to Clipboard)]** をクリックします。コピーされた ID を API で使用すると、イベント ID に基づく監査ログメッセージを取得できます。

監査ログの右側のペインに各ポリシーの **[説明 (Description)]**、**[ユーザー (User)]**、**[インターフェイス (Interface)]**、**[宛先 (Destination)]** が表示されます。

(注) 監査ログには、ペイロード情報を含む POST、DELETE、PUT などのノースバウンド操作の詳細と、デバイスにプッシュされた設定などのサウスバウンド操作の詳細が表示されます。Cisco DevNet の API の詳細については、『[CISCO DNA Center PlatformIntent APIs](#)』を参照してください。

- ステップ 5** (任意) [Filter] をクリックして、[User ID]、[Log ID]、または [Description] でログをフィルタリングします。
- ステップ 6** [Subscribe] をクリックして監査ログイベントを登録します。
syslog サーバーのリストが表示されます。
- ステップ 7** 登録する syslog サーバーのチェックボックスをオンにし、[Save] をクリックします。
(注) 監査ログイベントの登録を解除するには、syslog サーバーのチェックボックスをオフにして [Save] をクリックします。
- ステップ 8** 右側のペインで、[Search] フィールドを使用して、ログメッセージ内の特定のテキストを検索します。
- ステップ 9** メニューアイコン (☰) をクリックして、[Activities] > [Scheduled Tasks] で、OS の更新やデバイスの交換などの予定、進行中、完了および失敗の管理タスクを確認します。
- ステップ 10** メニューアイコン (☰) をクリックして、[Activities] > [Work Items] タブで、進行中、完了、および失敗の作業項目を確認します。

Syslog サーバーへの監査ログのエクスポート

セキュリティに関する推奨事項：より安全で簡単なログモニタリングのために、監査ログを Cisco DNA Center からネットワーク内のリモート Syslog サーバーにエクスポートすることを強く推奨します。

syslog サーバーを複数登録することで、監査ログを Cisco DNA Center から複数の syslog サーバーにエクスポートできます。

始める前に

[System] > [Settings] > [External Services] > [Destinations] > [Syslog] 領域で syslog サーバーを設定する必要があります。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[Activities] > [Audit Logs] の順に選択します。
- ステップ 2** [Subscribe] をクリックします。
- ステップ 3** 登録する syslog サーバーを選択し、[Save] をクリックします。
- ステップ 4** 登録を解除するには、syslog サーバーの選択を解除し、[Save] をクリックします。
-

タスクを表示

タスクには、Cisco DNA Center で実行中のタスク、完了したタスク、および失敗したタスクに関する情報が表示されます。

ステップ1 メニューアイコン (☰) をクリックして、[Activities] > [Tasks]の順に選択します。

左側のペインの [SUMMARY] 領域には、次のリストが表示されます。

- [Status] : [Upcoming]、[In Progress]、[Success]、および [Failed] タスクを一覧表示します。
- [Last Updated] : 過去 [3 Hours]、[24 Hours]、または [7 Days] に更新されたタスクを一覧表示します。
- [Categories] : 複数のカテゴリに基づいてタスクを一覧表示します。一度に複数のカテゴリを選択できます。
- [Recurring] : 定期的なタスクを一覧表示します。

ステップ2 タスクリンクをクリックして、[Starts]、[Status]、[Last updated]、および今後のタスク、進行中のタスク、完了したタスク、失敗したタスクに関する追加情報を示すスライドインペインを開きます。

ステップ3 失敗したタスクのスライドインペインで、[Download Error Report] リンクをクリックして、それぞれのタスクのエラーレポートをダウンロードします。

tar ファイルが作成され、ローカルマシンに保存されます。

(注) サポートケースを作成する際に、含めることができるその他の詳細に加えて、ダウンロードしたエラーレポートを添付できます。

高可用性のアクティブ化

Cisco DNA Center クラスタで高可用性 (HA) をアクティブにするには、次の手順を実行します。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [System Configuration] > [High Availability]の順に選択します。

ステップ2 [Activate High Availability] をクリックします。

HA の詳細については、『[Cisco DNA Center High Availability Guide](#)』を参照してください。

統合設定の設定

ファイアウォールなどのルールが、Cisco DNA Center と Cisco DNA Center プラットフォームと通信する必要があるサードパーティ製アプリケーションの間には存在する場合は、[Integration Settings] を設定する必要があります。Cisco DNA Center の IP アドレスが、インターネットや外

部ネットワークに接続する別の IP アドレスに内部的にマッピングされる場合には、このような事例が発生します。



重要 Cisco DNA Center のバックアップおよび復元後、[Integration Settings] ページにアクセスし、（必要に応じて）次の手順を使用して [Callback URL Host Name] または [IP Address] を更新する必要があります。

始める前に

Cisco DNA Center プラットフォーム をインストールしておきます。

- ステップ 1** メニューアイコン（☰）をクリックして、[System] > [設定] > [Integration Settings] の順に選択します。
- ステップ 2** サードパーティ製アプリケーションが Cisco DNA Center プラットフォームと通信するときに接続する必要がある [Callback URL Host Name] または [IP Address] を入力します。
- （注） [Callback URL Host Name] または [IP Address] は、Cisco DNA Center に内部的にマッピングされている外部向けホスト名または IP アドレスです。3 ノードクラスタセットアップの VIP アドレスを設定します。
- ステップ 3** [Apply] をクリックします。

ログインメッセージの設定

Cisco DNA Center にログインしたすべてのユーザーに表示されるメッセージを設定できます。

始める前に

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

- ステップ 1** メニューアイコン（☰）をクリックして、[System] > [Settings] > [System Configuration] > [Login Message] の順に選択します。
- ステップ 2** [Login Message] テキストボックスにメッセージのテキストを入力します。
- ステップ 3** [保存 (Save)] をクリックします。

このメッセージは、Cisco DNA Center ログインページの [Log In] ボタンの下に表示されます。後でこのメッセージを削除する場合は、次の手順を実行します。

1. [Login Message Settings] ページに戻ります。

2. [Clear] をクリックし、[Save] をクリックします。

プロキシの設定

Cisco DNA Center と管理しているネットワークデバイスとの間の仲介として設定されているプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。



- (注) Cisco DNA Center は、Windows New Technology LAN Manager (NTLM) 認証を使用するプロキシサーバーをサポートしていません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、[System]>[Settings]>[System Configuration]の順に選択します。

ステップ 2 [System Configuration] ドロップダウンリストから、[Proxy]>[Outgoing Proxy]を選択します。

ステップ 3 プロキシサーバーの URL アドレスを入力します。

ステップ 4 プロキシサーバーのポート番号を入力します。

- (注)
- HTTP の場合、ポート番号は通常 80 です。
 - ポート番号の範囲は 0 ~ 65535 です。

ステップ 5 (オプション) プロキシサーバーが認証を必要とする場合、[Update] をクリックして、プロキシサーバーにアクセスするためのユーザー名とパスワードを入力します。

ステップ 6 [Validate Settings] チェックボックスをオンにし、適用時に Cisco DNA Center でプロキシ構成時の設定が検証されるようにします。

ステップ 7 選択内容を確認し、[Save] をクリックします。

選択内容をキャンセルするには、[Reset] をクリックします。既存のプロキシ設定を削除するには、[Delete] をクリックします。

プロキシを設定した後、[Proxy] ウィンドウに設定を表示できます。

セキュリティに関する推奨事項

Cisco DNA Centerは、それ自体とモニターおよび管理対象のホスト/ネットワークデバイス用の多数のセキュリティ機能を提供します。セキュリティ機能は、明確に理解して、正しく設定する必要があります。次のセキュリティに関する推奨事項に従うことを強く推奨します。

- Cisco DNA Center は、プライベート内部ネットワーク内、およびインターネットなどの信頼できないネットワークに対して Cisco DNA Center を開いていないファイアウォールの背後に導入してください。
- 管理ネットワークとエンタープライズネットワークが個別にある場合は、Cisco DNA Center の管理インターフェイスとエンタープライズインターフェイスをそれぞれ管理ネットワークとエンタープライズネットワークに接続してください。これにより、Cisco DNA Center の管理に使用されるサービスと、ネットワークデバイスとの通信および管理に使用されるサービスとの間で確実にネットワーク分離が行われます。
- 3 ノードクラスタセットアップで Cisco DNA Center を展開する場合は、クラスタインターフェイスが分離されたネットワークに接続されていることを確認してください。
- パッチのアナウンス後できる限り早急に、セキュリティパッチを含む重要なアップグレードで Cisco DNA Center をアップグレードしてください。詳細については、『[Cisco DNA Center Upgrade Guide](#)』を参照してください。
- HTTPS プロキシサーバーを使用する Cisco DNA Center によってアクセスされるリモート URL を制限してください。Cisco DNA Center は、インターネット経由でアクセスして、ソフトウェアアップデート、ライセンス、デバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザーフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。ただし、HTTPS プロキシサーバーを介して安全な接続を提供します。
- 既知の IP アドレスおよび範囲のみを許可し、未使用のポートへのネットワーク接続をブロックすることにより、ファイアウォールを使用した Cisco DNA Center への入力および出力管理とエンタープライズ ネットワーク接続を制限してください。
- Cisco DNA Center の自己署名サーバー証明書を、内部認証局 (CA) によって署名された証明書に置き換えてください。
- 使用しているネットワーク環境で可能な場合は、SFTP 互換モードを無効にします。このモードでは、レガシー ネットワーク デバイスが古い暗号スイートを使用して Cisco DNA Center に接続できます。
- ブラウザベースのアプライアンス設定ウィザードを無効にします。このウィザードには、自己署名証明書が付属しています。
- 最小 TLS バージョンをアップグレードします。Cisco DNA Center では、TLSv1.1 および TLSv1.2 がデフォルトで有効になっています。使用しているネットワーク環境で可能な場合は、最小 TLS バージョンを 1.2 に設定することを推奨します。詳細については、[最小](#)

[TLS バージョンの変更と RC4-SHA の有効化 \(安全でない\) \(82 ページ\)](#) を参照してください。

最小 TLS バージョンの変更と RC4-SHA の有効化 (安全でない)

セキュリティに関する推奨事項 : Cisco DNA Center の受信用の TLS 接続については、最小 TLS バージョンを TLSv1.2 にアップグレードすることを推奨します。

外部ネットワークからのノースバウンド REST API 要求 (ノースバウンド REST API ベースのアプリケーション、ブラウザ、および HTTPS を使用して Cisco DNA Center に接続しているネットワークデバイスなど) は、Transport Layer Security (TLS) プロトコルを使用して保護されます。

デフォルトでは、Cisco DNA Center は TLSv1.1 と TLSv1.2 をサポートしますが、SSL/TLS 接続の RC4 暗号はサポートしません。RC4 暗号には既知の弱点があるため、ネットワークデバイスでサポートされている場合は、最小 TLS バージョンを TLSv1.2 にアップグレードすることを推奨します。

Cisco DNA Center 制御下のネットワークデバイスが既存の最小 TLS バージョン (TLSv1.1) または暗号をサポートできない場合、Cisco DNA Center には最小 TLS バージョンをダウングレードし、RC4-SHA を有効にする設定オプションが用意されています。ただし、セキュリティ上の理由から、Cisco DNA Center TLS のバージョンをダウングレードしたり RC4-SHA 暗号を有効にしたりすることは推奨されません。

Cisco DNA Center で TLS のバージョンの変更や RC4-SHA の有効化が必要な場合は、アプライアンスにログインし、CLI を使用して行います。



(注) CLI コマンドは、リリースごとに変更される可能性があります。次の CLI の例では、すべての Cisco DNA Center リリースに適用されない可能性のあるコマンド構文を使用しています。

始める前に

この手順を実行するためには、maglev SSH アクセス権限が必要です。



重要 このセキュリティ機能は、Cisco DNA Center にポート 443 を適用します。この手順の実行により、Cisco DNA Center インフラストラクチャへのポートのトラフィックが数秒間無効になることがあります。したがって、TLS の設定は頻繁に行わないようにし、オフピーク時間またはメンテナンス期間中にのみ行う必要があります。

ステップ 1 SSH クライアントを使用して、設定ウィザードで指定した IP アドレスで Cisco DNA Center アプライアンスにログインします。

SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスは、アプライアンスを外部ネットワークに接続します。

ステップ 2 要求された場合は、SSH アクセス用にユーザー名とパスワードを入力します。

ステップ 3 次のコマンドを入力して、クラスタで現在有効になっている TLS バージョンを確認します。

例

```
Input
$ magctl service tls_version --tls-min-version show
Output
TLS minimum version is 1.1
```

ステップ 4 クラスタの TLS バージョンを変更する場合は、次のコマンドを入力します。たとえば、Cisco DNA Center 制御下のネットワークデバイスが既存の TLS バージョンをサポートできない場合は、現在の TLS バージョンを下位バージョンに変更する必要があることがあります。

例：TLS バージョン 1.1 から 1.0 への変更

```
Input
$ magctl service tls_version --tls-min-version 1.0
Output
Enabling TLSv1.0 is recommended only for legacy devices
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.0 for api-gateway
deployment.extensions/kong patched
```

例：TLS バージョン 1.1 から 1.2 への変更 (RC4-SHA を有効にしていない場合のみ可能)

```
Input
$ magctl service tls_version --tls-min-version 1.2
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.extensions/kong patched
```

(注) RC4-SHA 暗号が有効になっている場合、TLS バージョン 1.2 を最小バージョンとして設定することはサポートされていません。

ステップ 5 クラスタで RC4-SHA を有効にするには、次のコマンドを入力します (セキュアでないため、必要な場合だけにしてください)。

TLS バージョン 1.2 が最小バージョンである場合、RC4-SHA 暗号を有効にすることはサポートされていません。

例：TLS バージョン 1.2 が有効になっていない

```
Input
$ magctl service ciphers --ciphers-rc4=enable kong
Output
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

ステップ 6 プロンプトで次のコマンドを入力して、TLS および RC4-SHA が設定されていることを確認します。

例

```
Input
$ magctl service display kong
```

```
Output
containers:
- env:
  - name: TLS_V1
    value: "1.1"
  - name: RC4_CIPHERS
    value: "true"
```

RC4 および TLS の最小バージョンが設定されている場合は、**magctl service display kong** コマンドの `env:` にリストされます。これらの値が設定されていない場合は、`env:` に表示されません。

ステップ7 以前に有効にした RC4-SHA 暗号を無効にする場合は、クラスタで次のコマンドを入力します。

```
Input
$ magctl service ciphers --ciphers-rc4=disable kong
Output
WARNING: Disabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

ステップ8 Cisco DNA Center アプライアンスからログアウトします。

プロキシ証明書の設定

ネットワーク構成によっては、プロキシゲートウェイは、Cisco DNA Center と管理するリモートネットワーク（さまざまなネットワークデバイスを含む）の間に存在する可能性があります。80 や 443 などの一般的なポートは DMZ のゲートウェイプロキシを通過します。このため、Cisco DNA Center 用に設定されたネットワークデバイスからの SSL セッションは、プロキシゲートウェイで終了することになります。したがって、これらのリモートネットワーク内にあるネットワークデバイスは、プロキシゲートウェイ経由でのみ Cisco DNA Center と通信できます。ネットワークデバイスが Cisco DNA Center または、（存在する場合は）プロキシゲートウェイと安全で信頼できる接続を確立するため、ネットワークデバイスは、関連する CA ルート証明書で、または特定の状況ではサーバー独自の証明書を使って、適切にプロビジョニングされた PKI トラストストアを保有する必要があります。

PnP 検出/サービスによってデバイスのオンボード中にそのようなプロキシが配置されている場合は、ネットワークデバイスが安全に Cisco DNA Center を信頼および認証できるように、プロキシと Cisco DNA Center サーバー証明書を同一にすることを推奨します。

プロキシゲートウェイが Cisco DNA Center と管理対象のリモートネットワークの間に存在するネットワークトポロジでは、次の手順を実行してプロキシゲートウェイ証明書を Cisco DNA Center にインポートします。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。
- Cisco DNA Center とそのサービスに到達するプロキシゲートウェイの IP アドレスを使用する必要があります。

- プロキシゲートウェイで現在使用されている証明書ファイルを持っている必要があります。証明書ファイルの内容は、次のいずれかで構成されている必要があります。
 - PEM または DER 形式のプロキシゲートウェイの証明書、および自己署名された証明書。
 - PEM または DER 形式のプロキシゲートウェイの証明書、および有効な既知の CA によって発行された証明書。
 - PEM または DER 形式のプロキシゲートウェイの証明書とそのチェーン。

デバイスとプロキシゲートウェイで使用される証明書は、次の手順に従って、Cisco DNA Center にインポートする必要があります。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[System]>[Settings]>[System Configuration]の順に選択します。
- ステップ 2** [System Configuration] ドロップダウンリストから、[Proxy]>[Incoming Proxy] を選択します。
- ステップ 3** [Proxy Certificate] ウィンドウで、(存在する場合は) 現在のプロキシゲートウェイ証明書のデータを表示します。
- (注) [Expiration Date and Time] は、グリニッジ標準時 (GMT) 値で表示されます。証明書有効期限の 2 ヶ月前に、Cisco DNA Center の GUI にシステム通知が表示されます。
- ステップ 4** プロキシゲートウェイ証明書を追加するには、自己署名証明書または CA 証明書を [Drag and Drop Here] 領域にドラッグアンドドロップします。
- (注) PEM または DER ファイル (公開キー暗号化標準のファイル形式) だけが、この領域を使用して Cisco DNA Center にインポートできます。さらに、この手順には秘密キーは必要ではなく、Cisco DNA Center にアップロードもされません。
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** [Proxy Certificate] ウィンドウを更新し、更新されたプロキシゲートウェイ証明書のデータを表示します。[Proxy Certificate] ウィンドウに表示された情報は、新しい証明書名、発行者、および証明機関を反映するように変更する必要があります。
- ステップ 7** プロキシゲートウェイ証明書の機能を有効にするには、[Enable] ボタンをクリックします。
- [Enable] ボタンをクリックすると、プロキシゲートウェイからの要求時にコントローラがインポートされたプロキシゲートウェイ証明書を返します。[Enabled] ボタンをクリックしない場合、コントローラは独自の自己署名証明書またはインポートされた CA 証明書をプロキシゲートウェイに返します。
- プロキシゲートウェイ証明書の機能が使用されている場合、[Enable] ボタンはグレー表示されます。
-

SSL インターセプトプロキシ証明書のアップロード

Cisco DNA Center とソフトウェアアップデートのダウンロード元である Cisco Cloud との間に設定されたプロキシサーバーで SSL 復号が有効になっている場合、正式な認証局から発行された証明書を使用してプロキシが構成されていることを確認してください。プライベート証明書を使用している場合は、次の手順を実行します。



(注) セキュリティを強化するため、ルートシェルへのアクセスは Cisco DNA Center で無効になっています。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。ただし、このセクションのコマンドを使用するには、ルートシェルに一時的にアクセスする必要があります。[制限付きシェルの一時的な無効化 \(100 ページ\)](#) を参照してください。

ステップ 1 プロキシサーバーの証明書 (.pem 形式) を Cisco DNA Center サーバーの /home/maglev ディレクトリに転送します。

ステップ 2 maglev ユーザーとして Cisco DNA Center サーバーに SSH で接続し、次のコマンドを入力します。<proxy.pem> は、プロキシサーバーの TLS/SSL 証明書ファイルです。

```
$ sudo /usr/local/bin/update_cacerts.sh -v -a /home/maglev/<proxy.pem>
```

このコマンドは、次のような出力を返します。

```
Reading CA cert from file /tmp/sdn.pem
Adding certificate import_1E:94:6D:2C:81:22:BB:B2:2E:24:BD:72:57:AE:35:AD:EC:5E:71:44.crt
Updating /etc/ca-certificates.conf
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Deleting tempfiles /tmp/file0PpQxV /tmp/filePtmQ8U /tmp/filercR3cV
```

ステップ 3 コマンド出力で、「1 added」の行を探し、追加された数がゼロでないことを確認します。チェーン内の証明書に基づき、この数は 1 または 1 を超える場合があります。

ステップ 4 次のコマンドを入力して、docker およびカタログサーバーを再起動します。

```
sudo systemctl restart docker
magctl service restart -d catalogserver
```

ステップ 5 Cisco DNA Center GUI からクラウド接続を確認します。

証明書および秘密キーのサポート

Cisco DNA Center は、セッション (HTTPS) の認証に使用される PKI 証明書管理機能をサポートしています。これらのセッションでは、CA と呼ばれる一般に認められた信頼されたエージェントを使用します。Cisco DNA Center は、PKI 証明書管理機能を使用して、内部 CA から X.509 証明書をインポートして保存し、管理します。インポートされた証明書は Cisco DNA Center の

アイデンティティ証明書になり、Cisco DNA Center は認証のためにこの証明書をクライアントに提示します。クライアントは、ノースバウンドAPIアプリケーションとネットワークデバイスです。

Cisco DNA Center GUI を使用して次のファイルを（PEM または PKCS ファイル形式で）インポートできます。

- X.509 証明書
- 秘密キー（Private key）



- (注) 秘密キーについては、Cisco DNA Center で RSA キーのインポートをサポートしています。DSA、DH、ECDH、および ECDSA キータイプはサポートされていないため、インポートしないでください。また、独自のキー管理システムで秘密キーを保護する必要があります。秘密キーのモジュラスサイズは最小でも 2048 ビット必要です。

インポートする前に、内部 CA で発行された有効な X.509 証明書と秘密キーを取得する必要があります。証明書は所有する秘密キーに対応している必要があります。インポートすると、X.509 証明書と秘密キーに基づくセキュリティ機能が自動的にアクティブ化されます。Cisco DNA Center は証明書を、要求するデバイスまたはアプリケーションに提示します。ノースバウンドAPIアプリケーションとネットワークデバイスでは、これらのログイン情報を使用して Cisco DNA Center との信頼関係を確立できます。



- (注) 自己署名証明書を使用したり、Cisco DNA Center にインポートしたりすることは推奨されません。内部 CA から有効な X.509 証明書をインポートすることをお勧めします。さらに、PnP 機能を正常に動作させるには、自己署名証明書（デフォルトで Cisco DNA Center にインストールされている）を、内部 CA によって署名された証明書で置き換える必要があります。

Cisco DNA Center は一度に 1 つのインポート済み X.509 証明書および秘密キーだけをサポートします。2 つ目の証明書および秘密キーをインポートすると、最初の（既存の）インポート済み証明書および秘密キーの値が上書きされます。

証明書チェーンのサポート

Cisco DNA Center では、GUI を介して証明書と秘密キーをインポートできます。Cisco DNA Center にインポートされる証明書（署名された証明書）につながる証明書チェーンに含まれる下位証明書がある場合は、それらの下位証明書とそれらの下位 CA のルート証明書と一緒に、インポートされる単一のファイルに追加する必要があります。これらの証明書を追加する場合は、認定の実際のチェーンと同じ順序で追加する必要があります。

次の証明書は、単一の PEM ファイルと一緒に貼り付ける必要があります。証明書のサブジェクト名と発行元を調べて、正しい証明書がインポートされ、正しい順序が維持されていることを確認してください。また、チェーンに含まれるすべての証明書と一緒に貼り付けられていることを確認してください。

- [Signed Cisco DNA Center certificate] : 件名フィールドに CN=<FQDN of Cisco DNA Center> が含まれていて、発行元が発行機関の CN を持っている。



(注) 内部認証局 (CA) による署名入りの証明書をインストールする場合は、Cisco DNA Center へのアクセスに使用するすべての DNS 名 (Cisco DNA Center の FQDN を含む) が証明書の **alt_names** セクションで指定されていることを確認してください。詳細については、『[Cisco DNA Center Security Best Practices Guide](#)』の「Generate a Certificate Request Using Open SSL」を参照してください。

- [Issuing (subordinate) CA certificate that issues the Cisco DNA Center certificate] : 件名フィールドに Cisco DNA Center の証明書を発行する (下位) CA の CN が含まれていて、発行元がルート CA の CN である。
- [Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate] : 件名フィールドがルート CA で、発行元が件名フィールドと同じ値である。それらが同じ値でない場合は、その次の発行元を追加していきます。

Cisco DNA Center サーバー証明書の更新

Cisco DNA Center は、X.509 証明書と秘密キーの Cisco DNA Center へのインポートとストレージをサポートします。インポートをすると、証明書と秘密キーを使用して、Cisco DNA Center、ノースバウンド API アプリケーション、およびネットワーク デバイスの間に安全で信頼できる環境を作成することができます。

GUI の [Certificates] ウィンドウを使用して、証明書と秘密キーをインポートできます。

始める前に

内部 CA から発行された有効な X.509 証明書を取得する必要があります。証明書は所有する秘密キーに対応している必要があります。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [System Certificates] の順に選択します。

ステップ 2 [System] タブで、現在の証明書データを確認します。

このウィンドウを最初に表示したときに現在の証明書として表示されるのは、Cisco DNA Center の自己署名証明書のデータです。自己署名証明書の有効期限は、数年先に設定されています。

(注) 有効期限の日時は、グリニッジ標準時 (GMT) 値で表示されます。証明書有効期限の 2 ヶ月前に、Cisco DNA Center の GUI にシステム通知が表示されます。

[System] タブには次のフィールドが表示されます。

- [Current Certificate Name] : 現在の証明書の名前。

- [Issuer] : 証明書に署名し、証明書を発行したエンティティの名前。
- [Authority] : 自己署名または CA の名前。
- [Expires] : 証明書の有効期限。

ステップ 3 [System Certificate] ウィンドウで、[Replace Certificate] をクリックします。

Cisco DNA Center 2.3.2 以降では、初めて CSR を生成する場合に、[Generate New CSR] リンクが表示されます。それ以外の場合は、[Download existing CSR] リンクが表示されます。既存の CSR をダウンロードしてプロバイダーに送信し、証明書を生成できます。既存の CSR を使用しない場合は、[Delete existing CSR] をクリックし、次の [Confirmation] ウィンドウで [Accept] をクリックします。[Generate New CSR] リンクが表示されます。

ステップ 4 [Generate New CSR] リンクをクリックします。

ステップ 5 [Certificate Signing Request Generator] ウィンドウで、必須フィールドに入力します。

ステップ 6 [Generate New CSR] をクリックします。

生成された新しい CSR は自動的にダウンロードされます。

[Certificate Signing] ウィンドウには、CSR のプロパティが表示され、次のことができます。

- CSR プロパティをプレーンテキストでコピーします。
- Base64 をコピーして MS CA に貼り付けます。
- Base64 をダウンロードします。

ステップ 7 (任意) ディザスタリカバリに同じ証明書を使用する場合は、[Use system certificate for Disaster Recovery as well] チェックボックスをオンにします。

ステップ 8 Cisco DNA Center にインポートする証明書のファイル形式タイプを選択します。

- [PEM] : プライバシー エンハンスド メール ファイル形式。
- [PKCS] : 公開キー暗号化標準ファイル形式。

(注) [Generate New CSR] オプションを選択して証明書を要求した場合、[PKCS] ファイルタイプは無効になります。

ステップ 9 証明書発行元から p7b で証明書の完全なチェーン (サーバーおよび CA) が提供されていることを確認します。不明な場合は、次の手順を実行し、チェーンを確認して組み立てます。

- a) p7b バンドルを DER 形式でダウンロードし、dnac-chain.p7b として保存します。
- b) dnac-chain.p7b 証明書を Cisco DNA Center クラスタに SSH を介してコピーします。
- c) 次のコマンドを入力します。

```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```

- d) すべての証明書が出力に記載され、発行者と Cisco DNA Center 証明書が含まれていることを確認します。PEM としてアップロードを続行します。証明書がルーズファイルにある場合は、次の手順を実行して、個々のファイルをダウンロードして組み立てます。

ステップ 10 証明書発行元からルーズファイルで証明書とその発行元 CA チェーンが提供された場合は、次の手順を実行します。

- a) PEM (base64) ファイルを収集するか、`openssl` を使用して DER を PEM に変換します。
- b) 証明書とその発行元 CA を連結し、証明書から下位 CA に続いてルート CA までを `dnac-chain.pem` ファイルに出力します。

```
cat certificate.pem subCA.pem rootCA.pem > dnac-chain.pem
```

- c) PEM としてアップロードを続行します。

ステップ 11 [PEM] ファイルの場合、次のタスクを実行します。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、[PEM] ファイルをインポートします。

(注) PEM ファイルには、有効な PEM 形式の拡張子 (.pem) が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、[Private Key] をインポートします。

(注) 秘密キーには、有効な秘密キー形式の拡張子 (.key) が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

- 秘密キーの [Encrypted] 領域から、暗号化オプションを選択します。

- 暗号化を選択した場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 12 [PKCS] ファイルの場合、次のタスクを実行します。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、[PKCS] ファイルをインポートします。

(注) PKCS ファイルには、有効な PKCS 形式の拡張子 (.pfx または .p12) が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- [Password] フィールドで証明書用のパスフレーズを入力します。

(注) PKCS の場合は、インポートした証明書もパスフレーズを必要とします。

- [Private Key] フィールドについては、秘密キーの暗号化オプションを選択します。

- [Private Key] フィールドで、暗号化を選択した場合は、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 13 [Save] をクリックします。

(注) Cisco DNA Center サーバーの SSL 証明書が置き換えられると、自動的にログアウトされるため、再度ログインする必要があります。

ステップ 14 [Certificates] ウィンドウに戻り、更新された証明書データを確認します。
[System] タブに表示される情報が更新され、新しい証明書名、発行者、および認証局が反映されます。

外部 SCEP ブローカーの使用

Cisco DNA Center では、ネットワークデバイスへの証明書の登録とプロビジョニングに Simple Certificate Enrollment Protocol (SCEP) が使用されます。独自の SCEP ブローカと証明書サービスを使用したり、外部の SCEP ブローカを使用したりできます。外部 SCEP ブローカをセットアップするには、以下の手順を実行します。



(注) SCEP の詳細については、「[Simple Certificate Enrollment Protocol Overview](#)」を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [PKI Certificates] の順に選択します。

ステップ 2 [PKI Certificates] ウィンドウで、[Use external SCEP broker] オプションボタンをクリックします。

ステップ 3 外部証明書をアップロードするには、次のいずれかのオプションを使用します。

- ファイルを選択する
- ドラッグアンドドロップしてアップロードする

(注) .pem、.crt、.cer などのファイルタイプのみ使用できます。ファイルサイズは 10 MB を超えることはできません。

ステップ 4 [Upload] をクリックします。

ステップ 5 デフォルトでは、[Manages Device Trustpoint] が有効になっています。つまり、デバイスで sdn-network-infra-iwan トラストポイントが設定されます。Cisco DNA Center 次の手順を実行してください。

- a) デバイスが SCEP 経由で証明書を要求する登録 URL を入力します。
- b) (任意) 証明書で使用される任意のサブジェクトフィールド (国、地域、州、組織、組織単位など) を入力します。共通名 (CN) は、デバイスのプラットフォーム ID とデバイスのシリアル番号を使用して Cisco DNA Center によって自動的に設定されます。
- c) [Revocation Check] フィールドで、ドロップダウンリストをクリックし、適切な失効チェックオプションを選択します。
- d) (任意) [Auto Renew] チェックボックスをオンにして、自動登録の割合を入力します。

[Manages Device Trustpoint] が無効になっている場合、デバイスが有線およびワイヤレスのアシユアランステレメトリを送信するようにするため、デバイスに手動で sdn-network-infra-iwan トラストポイントを設定

し、証明書をインポートする必要があります。Cisco DNA Center「[デバイス証明書トラストポイントの設定](#)」を参照してください。

ステップ 6 [保存 (Save)] をクリックします。

外部 CA 証明書がアップロードされます。

アップロードされた外部証明書を置き換える場合は、[Replace Certificate] をクリックし、必要な詳細を入力します。

内部 PKI 証明書への切り替え

外部証明書をアップロードした後、内部証明書に切り替える場合は、次の手順を実行します。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [PKI Certificates] の順に選択します。

ステップ 2 [PKI Certificates] ウィンドウで、[Use Cisco DNA Center] オプションボタンをクリックします。

ステップ 3 [Switching back to Internal PKI Certificate] アラートで、[Apply] をクリックします。

[Settings have been updated] メッセージが表示されます。詳細については、「[PKI 証明書のロールをルートから下位に変更](#)」を参照してください。

Cisco DNA Center PKI 証明書のエクスポート

Cisco DNA Center では、デバイスを認証するための、AAA（「トリプル A」と発音）サーバーまたは Cisco ISE サーバーなどの外部エンティティを設定するために必要なデバイス証明書をダウンロードできます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [PKI Certificates] の順に選択します。

ステップ 2 [Download CA Certificate] をクリックして、デバイス CA をエクスポートし、信頼できる CA として外部エンティティに追加します。

証明書の管理

デバイス証明書の管理

管理対象デバイスがデバイスを認証および識別するために Cisco DNA Center によって発行された証明書を表示および管理できます。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [Device Certificate] の順に選択します。

[Device Certificate] ウィンドウには、発行された証明書のステータスが個別のステータスタブに表示されません。

- [Expired] ステータスタブ：有効期限が切れた証明書のリストを表示します。
- [Expiring] ステータスタブ：有効期限が近づいている証明書のリストを昇順で表示します。
- [All] ステータスタブ：有効な証明書、期限切れの証明書、および期限切れ間近の証明書のリストを表示します。
- [Revoked] ステータスタブ：取り消された証明書を表示します。

ステップ 2 証明書を検索する場合は、検索フィールドに検索文字列を入力します。

選択したステータスタブの [Issue To] の値に一致する証明書が表示されます。

ステップ 3 有効な証明書を取り消す場合は、次の手順を実行します。

- a) [All] ステータスタブをクリックします。
- b) [Actions] 列で、取り消す証明書に対応する [Revoke] アイコンをクリックします。
- c) 確認ウィンドウで、[OK] をクリックします。

ステップ 4 証明書の詳細をエクスポートする場合は、[Export] をクリックします。

証明書の詳細が CSV 形式でエクスポートされます。

デバイス証明書の有効期間の設定

Cisco DNA Center では、Cisco DNA Center のプライベート（内部）CA で管理および監視しているネットワークデバイスの証明書の有効期間を変更できます。Cisco DNA Center での証明書の有効期間のデフォルト値は 365 日です。Cisco DNA Center GUI を使用して証明書の有効期間を変更すると、それ以降に Cisco DNA Center に対して証明書を要求するネットワークデバイスにその有効期間の値が割り当てられます。



- (注) デバイス証明書のライフタイム値を CA 証明書のライフタイム値より大きくすることはできません。さらに、CA 証明書の残りの有効期間が設定されたデバイスの証明書の有効期間より短い場合、デバイス証明書の有効期間の値は CA 証明書の残りの有効期間と同じになります。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [Device Certificate] の順に選択します。

ステップ 2 デバイス証明書と現在のデバイス証明書の有効期間を確認します。

ステップ3 [Device Certificate] ウィンドウで、[Modify] をクリックします。

ステップ4 [Device Certificate Lifetime] ダイアログボックスに、新しい値を入力します（日数）。

ステップ5 [Save] をクリックします。

PKI 証明書のロールをルートから下位に変更

デバイス PKI CA は Cisco DNA Center のプライベート CA であり、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。デバイス PKI CA のロールをルート CA から下位 CA に変更するには、次の手順を実行します。

Cisco DNA Center のプライベート CA をルート CA から下位 CA に変更するときは、次のことに注意してください。

- Cisco DNA Center が下位 CA の役割を果たすようにする場合、すでにルート CA（たとえば Microsoft CA）があり、Cisco DNA Center を下位 CA として認めているものと見なされます。
- 下位 CA が完全に設定されていない限り、Cisco DNA Center は内部ルート CA としての役割を継続します。
- Cisco DNA Center 用の証明書署名要求ファイルを生成し（次の手順の記述に従う）、手動で外部ルート CA に署名させる必要があります。



(注) Cisco DNA Center は、この期間中は内部ルート CA として実行し続けます。

- 証明書署名要求が外部ルート CA によって署名された後、GUI を使用してこの署名ファイルを Cisco DNA Center にインポートし直す必要があります（次の手順の記述に従う）。

インポート後、Cisco DNA Center は下位 CA として自身を初期化し、下位 CA の既存機能をすべて提供します。

- 内部ルート CA から下位 CA への切り替え前にデバイスの制御可能性が有効になっている場合（デフォルト）、新しいデバイス証明書は自動的に更新されます。
- GUI に表示されている下位 CA 証明書有効期間は、証明書から読み取られたもので、システム時刻を使って計算されたものではありません。したがって今日、証明書を有効期間 1 年でインストールして来年の 7 月に GUI で見ると、証明書の有効期間はそのときでも 1 年間と表示されます。
- 下位 CA 証明書として PEM または DER 形式のみを使用できます。
- 下位 CA は上位の CA と連携しないため、上位レベルの証明書がある場合は、その失効に注意してください。このため、下位 CA からネットワークデバイスに対して、証明書の失効に関する情報が通知されることもありません。下位 CA にはこの情報がないため、すべてのネットワークデバイスは下位 CA を Cisco Discovery Protocol (CDP) 送信元としてのみ使用します。

[PKI Certificate Management] ウィンドウの GUI を使用して、Cisco DNA Center のプライベート（内部）CA のロールをルート CA から 下位 CA に変更できます。

始める前に

ルート CA 証明書のコピーが必要です。

-
- ステップ 1** メニューアイコン（☰）をクリックして、[System] > [Settings] > [PKI Certificate] の順に選択します。
- ステップ 2** [CA Management] タブをクリックします。
- ステップ 3** GUI で既存のルートまたは下位 CA 証明書の設定情報を確認します。
- [Root CA Certificate] : 現在のルート CA 証明書（外部または内部）を表示します。
 - [Root CA Certificate Lifetime] : 現在のルート CA 証明書の最新の有効期間を表示します（日数）。
 - [Current CA Mode] : 現在の CA モードを表示します（ルート CA または下位 CA）。
 - [Sub CA mode] : ルート CA から下位 CA に変更できます。
- ステップ 4** [CA Management] タブで、[Sub CA Mode] チェックボックスをオンにします。
- ステップ 5** [Next] をクリックします。
- ステップ 6** 表示される警告内容を確認します。
- ルート CA から下位 CA に変更するプロセスは元に戻すことができません。
 - ルート CA モードで登録された、または証明書が発行されたネットワーク デバイスがないことを確認する必要があります。ネットワークデバイスを誤ってルート CA モードで登録した場合は、ルート CA から下位 CA に変更する前に、取り消しをする必要があります。
 - 下位 CA の設定プロセスが終了しなければ、ネットワークデバイスをオンラインにできません。
- ステップ 7** [OK] をクリックして続行します。
- [PKI Certificate Management] ウィンドウに、[Import External Root CA Certificate] フィールドが表示されます。
- ステップ 8** [Import External Root CA Certificate] フィールドにルート CA 証明書をドラッグアンドドロップして、[Upload] をクリックします。
- ルート CA 証明書が Cisco DNA Center にアップロードされ、証明書署名要求の生成に使用されます。アップロードプロセスが完了すると、「Certificate Uploaded Successfully」というメッセージが表示されます。
- ステップ 9** [Next] をクリックします。
- Cisco DNA Center で証明書署名要求が生成されて表示されます。
- ステップ 10** Cisco DNA Center で生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。

- [Download] リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。
その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。
- [Copy to the Clipboard] リンクをクリックして、証明書署名要求ファイルの内容をコピーします。
その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。

ステップ 11 証明書署名要求ファイルをルート CA に送信します。

ルート CA から下位 CA ファイルが返されます。このファイルを Cisco DNA Center にインポートし直す必要があります。

ステップ 12 ルート CA から下位 CA ファイルを受信した後、Cisco DNA Center の GUI に再度アクセスし、[PKI Certificate Management] ウィンドウに戻ります。

ステップ 13 [CA Management] タブをクリックします。

ステップ 14 [Change CA mode] ボタンの [Yes] をクリックします。

[Yes] をクリックすると、GUI に証明書署名要求が表示されます。

ステップ 15 [Next] をクリックします。

[PKI Certificate Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。

ステップ 16 [Import Sub CA Certificate] フィールドに下位 CA 証明書をドラッグアンドドロップして、[Apply] をクリックします。

下位 CA 証明書が Cisco DNA Center にアップロードされます。

アップロードが完了すると、GUI の [CA Management] タブに、下位 CA モードが表示されます。

ステップ 17 [CA Management] タブのフィールドを確認します。

- [Sub CA Certificate] : 現在の下位 CA 証明書を表示します。
- [External Root CA Certificate] : ルート CA 証明書を表示します。
- [Sub CA Certificate Lifetime] : 下位 CA 証明書の有効期間を表示します (日数)。
- [Current CA Mode] : SubCA モードを表示します。

ロールオーバー下位 CA 証明書のプロビジョニング

Cisco DNA Center では、既存の下位 CA の有効期間が 70% 以上経過している場合に、ユーザーがロールオーバー下位 CA として下位証明書を適用することができます。

始める前に

- 下位 CA ロールオーバー プロビジョニングを開始するには、PKI 証明書の権限を下位 CA モードに変更しておく必要があります。PKI 証明書のロールをルートから下位に変更 (94 ページ) を参照してください。
- 現在の下位 CA 証明書の有効期限が 70 % 以上経過していることが必要です。この状態になると、Cisco DNA Center の [CA Management] タブの下に [Renew] ボタンが表示されません。
- ロールオーバー下位 CA の署名付き PKI 証明書のコピーが必要です。

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [PKI Certificate] の順に選択します。

ステップ 2 [CA Management] タブをクリックします。

ステップ 3 CA 証明書の設定情報を確認します。

- [Subordinate CA Certificate] : 現在の下位 CA 証明書を表示します。
- [External Root CA Certificate] : ルート CA 証明書を表示します。
- [Subordinate CA Certificate Lifetime] : 現在の下位 CA 証明書の有効期間 (日数) を表示します。
- [Current CA Mode] : SubCA モードを表示します。

ステップ 4 [Renew] をクリックします。

Cisco DNA Center は既存の下位 CA を使用して、ロールオーバー下位 CA の証明書署名要求を生成し、表示します。

ステップ 5 生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。

- [Download] リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。
その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。
- [Copy to the Clipboard] リンクをクリックして、証明書署名要求ファイルの内容をコピーします。
その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。

ステップ 6 証明書署名要求ファイルをルート CA に送信します。

次にルート CA がロールオーバー下位 CA ファイルを返送してくると、それを Cisco DNA Center にインポートし直す必要があります。

下位 CA ロールオーバーの証明書署名要求は、RootCA モードから SubCA モードに切り替えた際にインポートした下位 CA に署名したルート CA と同じルート CA によって署名される必要があります。

- ステップ 7** ルート CA からロールオーバー下位 CA ファイルを受信した後、[PKI Certificate Management] ウィンドウに戻ります。
- ステップ 8** [CA Management] タブをクリックします。
- ステップ 9** 証明書署名要求が表示されている GUI で [Next] をクリックします。
[PKI Certificate Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。
- ステップ 10** 下位ロールオーバー CA 証明書を [Import Sub CA Certificate] フィールドにドラッグアンドドロップし、[Apply] をクリックします。
ロールオーバー下位 CA 証明書が Cisco DNA Center にアップロードされます。
アップロードが終了すると、GUI が変更され、[CA Management] タブの [Renew] ボタンが無効になります。

デバイス証明書トラストポイントの設定

Cisco DNA Center で [Manages Device Trustpoint] が無効になっている場合、デバイスが有線およびワイヤレスのアシユアランステレメトリを Cisco DNA Center に送信するようにするため、デバイスに手動で `sdn-network-infra-iwan` トラストポイントを設定し、証明書をインポートする必要があります。

SCEP を介して外部 CA から登録するには、次の手動設定が必要です。

- ステップ 1** 次のコマンドを入力します。

```
crypto pki trustpoint sdn-network-infra-iwan
  enrollment url http://<SCEP_enrollment_URL_to_external_CA>
  fqdn <device_FQDN>
  subject-name CN=<device_platform_ID>_<device_serial_number>_sdn-network-infra-iwan
  revocation-check <crl, crl none, or none> # to perform revocation check with CRL, CRL fallback
  to no check, or no check
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection matches the fingerprint
  given
```

- ステップ 2** (任意、ただし推奨) 証明書を自動的に更新し、証明書の有効期限を回避します。

```
auto-enroll 80 regenerate
```

- ステップ 3** (任意) 登録 URL に到達可能なインターフェイスを指定します。それ以外の場合、http サービスの送信元インターフェイスがデフォルトで設定されます。

```
source interface <interface>
```

証明書の更新

Cisco DNA Center は、Kubernetes によって生成された証明書や、Kong および資格情報マネージャサービスが使用する証明書など、多数の証明書を使用します。これらの証明書は1年間有効

効です。証明書はクラスタをインストールするとすぐに開始され、期限切れに設定される前に Cisco DNA Center によって 1 年自動的に更新されます。

- 期限切れになる前に証明書を更新することを推奨します。
- 今から 100 日間の間に期限切れになるように設定されている証明書のみを更新できます。この手順では、それ以降に期限切れになる証明書については何も実行されません。
- このスクリプトでは、サードパーティ/認証局 (CA) 署名付き証明書ではなく、自己署名証明書のみを更新します。サードパーティ/CA 署名付き証明書の場合、スクリプトは Kubernetes と資格情報マネージャによって使用される内部証明書を更新します。
- 自己署名証明書の場合、更新プロセスではルート CA が変更されないため、証明書をデバイスにプッシュする必要はありません。
- クラスタという用語は、単一ノードと 3 ノード Cisco DNA Center 設定の両方に適用されます。

ステップ 1 各クラスタノードが正常であり、問題が発生していないことを確認します。

ステップ 2 そのノードで現在使用されている証明書のリストとそれらの有効期限を表示するには、次のコマンドを入力します。

```
sudo maglev-config certs info
```

ステップ 3 次のコマンドを入力して、すぐに期限切れになるように設定されている証明書を更新します。

```
sudo maglev-config certs refresh
```

ステップ 4 他のクラスタノードに対して上記の手順を繰り返します。

ステップ 5 ユーティリティのヘルプを表示するには、次のように入力します。

```
$ sudo maglev-config certs --help
Usage: maglev-config certs [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  info
  refresh
```

トラストプールの設定

Cisco DNA Center には、事前インストールされているシスコ トラストプールバンドル (シスコが信頼する外部ルートバンドル) が含まれています。Cisco DNA Center は、シスコからの更新されたトラストプールバンドルのインポートとストレージもサポートしています。トラストプールバンドルは、Cisco DNA Center およびそのアプリケーションとの信頼関係を確立するために、サポートされるシスコ ネットワーキング デバイスによって使用されます。



- (注) シスコ トラストプールバンドルは、サポートされているシスコデバイスのみをアンバンドルして使用できる、ios.p7b と呼ばれるファイルです。この ios.p7b ファイルには、シスコを含む有効な認証局のルート証明書が含まれています。この Cisco trustpool バンドルは、シスコクラウド (Cisco InfoSec) で使用できます。リンクは <https://www.cisco.com/security/pki/> にあります。

このトラストプールバンドルは、同じ CA を使用してすべてのネットワークデバイスの証明書および Cisco DNA Center の証明書を管理する、安全で便利な方法を提供します。トラストプールバンドルは Cisco DNA Center によって使用され、自身の証明書およびプロキシゲートウェイ証明書 (存在する場合) を検証し、それが有効な CA 署名付き証明書を判断します。さらに、PnP ワークフローの開始時にネットワーク PnP 対応デバイスにアップロードできるように、また、その後の HTTPS ベースの接続で Cisco DNA Center を信頼できるように、トラストプールバンドルを使用できます。

GUI の [Trustpool] ウィンドウを使用して、シスコ トラストプール バンドルをインポートします。

- ステップ 1** メニューアイコン (≡) をクリックして、[System] > [Settings] > [Trust & Privacy] > [Trustpool] の順に選択します。
- ステップ 2** [Trustpool] ウィンドウで、[Update] ボタンをクリックしてトラストプールバンドルの新規ダウンロードおよびインストールを開始します。
- [Update] ボタンは、ios.p7b ファイルの更新バージョンが使用可能で、インターネットアクセスが可能なきにのみアクティブになります。
- Cisco DNA Center に新しいトラストプールバンドルがダウンロードおよびインストールされると、Cisco DNA Center はシスコのデバイスのダウンロードをサポートするよう、このトラストプールバンドルを使用可能にします。
- ステップ 3** 新しい証明書ファイルをインポートする場合は、[Import] をクリックしてローカルシステムから有効な証明書ファイルを選択し、[Import Certificate] ウィンドウで [Import] をクリックします。
- ステップ 4** [Export] をクリックして、証明書の詳細を CSV 形式でエクスポートします。

制限付きシェルの一時的な無効化

セキュリティを強化するために、Cisco DNA Center は制限付きシェルをサポートします。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。

制限付きシェルでは、次のコマンドがサポートされています。

```
$ ?
Help:
  cat          concatenate and print files in restricted mode
  clear       clear the terminal screen
  date       display the current time in the given FORMAT, or set the system
```

```

date
  debug          enable console debug logs
  df             file system information
  dmesg          print or control the kernel ring buffer.
  du            summarize disk usage of the set of FILEs, recursively for
directories.
  free          quick summary of memory usage
  history       enable shell commands history
  htop          interactive process viewer.
  ip           print routing, network devices, interfaces and tunnels.
  last         show a listing of last logged in users.
  ls           restricted file system view chrooted to maglev Home
  lscpu        print information about the CPU architecture.
  magctl       tool to manage a Maglev deployment
  maglev       maglev admin commands
  maglev-config tool to configure a Maglev deployment
  manufacture_check tool to perform manufacturing checks
  netstat      print networking information.
  nslookup     query Internet name servers interactively.
  ntpq         standard NTP query program.
  ping        send ICMP ECHO_REQUEST to network hosts.
  ps          check status of active processes in the system
  rca         root cause analysis collection utilities
  reboot      Reboot the machine
  rm          delete files in restricted mode
  route       print the IP routing table.
  runonce     Execute runonce scripts
  scp         restricted secure copy
  sftp        secure file transfer
  shutdown    Shutdown the machine
  ssh         OpenSSH SSH client.
  tail        Print the last 10 lines of each FILE to standard output
  top         display sorted list of system processes
  traceroute  print the route packets trace to network host.
  uname       print system information.
  uptime      tell how long the system has been running.
  vi          text editor
  w           show who is logged on and what they are doing.

```

ネットワークで CLI ベースのスクリプトまたはトラブルシューティング コマンドを使用している場合は、現在の Cisco DNA Center リリースで制限付きシェルをバイパスするオプションがあります。デフォルトでは、Cisco DNA Center 2.3.3 で制限付きシェルが有効になっています。制限付きシェルを無効にする場合は、次の手順を実行します。

ステップ 1 次の CLI コマンドを入力して、シェルタイプを確認します。

```
$ magctl ssh shell display
```

このコマンドは、シェルに応じて、次の出力のいずれかを返します。

```
$ magctl ssh shell display
Active shell for current user: bash
```

```
$ magctl ssh shell display
Active shell for current user: magshell
```

_shell コマンドは、magshell を使用している場合にのみ機能します。

ステップ 2 上記のコマンド出力で magshell を使用していることが確認され、制限付きシェルを無効にする場合は、次の CLI コマンドとパスワードを入力します。

```

$ _shell -c 'sudo magctl ssh shell bash'
Password:
Warning! Activity within this shell can jeopardize the functioning of the system!
[sudo] password for maglev:
Successfully enabled bash for user, will be effective from next login.

```

ステップ3 変更を有効にするには、CLIセッションを終了してから、CLIセッションに再度ログインします。

ステップ4 (オプション) 制限付きシェルを再度有効にするには、次のCLIコマンドとパスワードを入力します。

```

$ sudo magctl ssh shell magshell
[sudo] password for maglev:
Successfully enabled magshell for user, will be effective from next login.

```

ステップ5 変更を有効にするには、CLIセッションを終了してから、CLIセッションに再度ログインします。

製品使用状況テレメトリの収集について

Cisco DNA Center ではデフォルトでテレメトリデータが収集されますが、一部のデータ収集をオプトアウトできます。データ収集は、製品機能の開発を支援し、運用上の問題に対処して、より優れた価値と投資回収率 (ROI) を実現することを目的としています。シスコが収集するデータの種類は、Cisco.com ID、システム、機能の使用状況、ネットワークデバイスインベントリ、およびソフトウェア利用資格です。収集されるデータの詳しいリストについては、「[Cisco DNA Center のデータシート](#)」を参照してください。一部のデータ収集をオプトアウトするには、シスコのアカウント担当者および Cisco Technical Assistance Center (TAC) にお問い合わせください。

メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Terms and Conditions] > [Telemetry Collection]** の順に選択します。[Telemetry Collection] ウィンドウから、ライセンス契約、プライバシーポリシー、プライバシーデータシートを確認できます。

vManage プロパティの設定

Cisco DNA Center は、統合 vManage 設定を使用してシスコの vEdge 展開をサポートします。vEdge トポロジをプロビジョニングする前に、[Settings] ページで vManage の詳細を保存できます。

ステップ1 メニューアイコン (☰) をクリックして、**[System] > [Settings] > [External Services] > [vManage]** の順に選択します。

ステップ2 vManage プロパティを設定します。

- [Host Name/IP Address] : vManage の IP アドレス。
- [Username] : vManage にログインするために使用される名前。
- [Password] : vManage にログインするために使用されるパスワード。

- [Port Number] : vManage にログインするために使用されるポート。
- [vBond Host Name/IP Address] : vBond の IP アドレス。vManage を使用して NFV を管理する場合に必要です。
- [Organization Name] : 組織の名前。vManage を使用して NFV を管理する場合に必要です。

ステップ3 vManage 証明書をアップロードするには、[Select a file from your computer] をクリックします。

ステップ4 [Save] をクリックします。

アカウントのロックアウト

アカウント ロックアウト ポリシーを設定して、ユーザーによるログインの試行、アカウントのロックアウト期間、ログインの再試行回数を管理できます。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [Account Lockout] の順に選択します。

ステップ2 [Enforce Account Lockout] トグルボタンをクリックして、チェックマークが表示された状態にします。

ステップ3 [Enforce Account Lockout] の次のパラメータの値を入力します。

- Maximum Login Retries
- Lockout Effective Periods (minutes)
- Reset Login Retries after (minutes)

(注) [Info] にカーソルを合わせると、各パラメータの詳細が表示されます。

ステップ4 ドロップダウンリストから [Idle Session Timeout] の値を選択します。

ステップ5 [保存 (Save)] をクリックします。

セッションをアイドル状態のままにすると、セッションタイムアウトの5分前に [Session Timeout] ダイアログボックスが表示されます。セッションを続行する場合は、[Stay signed in] をクリックします。[Sign out] をクリックすると、すぐにセッションを終了できます。

パスワードの有効期限切れ

パスワード有効期限ポリシーを設定して、パスワードの有効期間、パスワードが期限切れになる前にユーザーに通知される日数、および猶予期間を管理できます。

ステップ 1 メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Trust & Privacy] > [Password Expiry]** の順に選択します。

ステップ 2 **[Enforce Password Expiry]** トグルボタンをクリックして、チェックマークが表示された状態にします。

ステップ 3 次の **[Enforce Password Expiry]** パラメータの値を入力します。

- パスワード期限 (日)
- パスワードの期限の警告 (日)
- 猶予期間 (日)

(注) **[Info]** にマウスカーソルを置くと、各パラメータの詳細が表示されます。

ステップ 4 **[Save]** をクリックして、パスワード有効期限設定を保存します。

IP アクセス制御

IP アクセス制御を使用すると、ホストまたはネットワークの IP アドレスに基づいて Cisco DNA Center へのアクセスを制御できます。Cisco DNA Center では、IP アクセス制御に次のオプションがあります。

- すべての IP アドレスに Cisco DNA Center へのアクセスを許可します。デフォルトでは、すべての IP アドレスが Cisco DNA Center にアクセスできます。
- 選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可します。

IP アクセス制御の構成

IP アクセス制御を構成し、選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可するには、次の手順を実行します。

1. [IP アクセス制御の有効化 \(104 ページ\)](#)。
2. [IP アクセスリストへの IP アドレスの追加 \(105 ページ\)](#)。
3. (任意) [IP アクセスリストからの IP アドレスの削除 \(106 ページ\)](#)。

IP アクセス制御の有効化

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
- ステップ 2** [リストされている IP アドレスのみに接続を許可する (Allow only listed IP addresses to connect)] オプションボタンをクリックします。
- ステップ 3** [Add IP List] をクリックします。
- ステップ 4** [Add IP] スライドインペインの [IP Address] フィールドに、IPv4 アドレスを入力します。
- (注) IP アドレスを IP アクセスリストに追加しないと、Cisco DNA Center にアクセスできなくなる可能性があります。
- ステップ 5** [Subnet Mask] フィールドにサブネット マスクを入力します。
- サブネットマスクの有効範囲は 0 ~ 32 です。
- ステップ 6** [Save] をクリックします。
-

IP アクセスリストへの IP アドレスの追加

IP アクセスリストに IP アドレスを追加するには、次の手順を実行します。

始める前に

IP アクセス制御が有効になっていることを確認してください。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
- ステップ 2** [Add] をクリックします。
- ステップ 3** [Add IP] スライドインペインの [IP Address] フィールドに、ホストまたはネットワークの IPv4 アドレスを入力します。
- ステップ 4** [Subnet Mask] フィールドにサブネット マスクを入力します。
- サブネットマスクの有効範囲は 0 ~ 32 です。

IP アクセスリストからの IP アドレスの削除

Settings / Trust & Privacy

IP Access Control

Cisco DNA Center is accessible from all IP addresses by default.

Allow all IP addresses to connect
 Allow only listed IP addresses to connect

IP Address	Subnet Mask
209.165.200.230	32

1 Records

Add IP

IP Address*
209.165.210.0

Subnet Mask*
27

Valid range: 0-32

Cancel Save

ステップ5 [Save] をクリックします。

IP アクセスリストからの IP アドレスの削除

次のセクションでは、IP アクセスリストから IP アドレスを削除して Cisco DNA Center へのアクセスを無効にする方法について説明します。

始める前に

IP アクセスコントロールを有効にして、IP アドレスを IP アクセスリストに追加したことを確認します。

ステップ1 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。

ステップ2 [Action] 列で、対応する IP アドレスの [Action] アイコンをクリックします。

ステップ3 [Delete] をクリックします。

IP アクセス制御の無効化

次のセクションでは、IP アクセス制御を無効にして、すべての IP アドレスに Cisco DNA Center へのアクセスを許可する方法について説明します。

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
- ステップ 2** [Allow all IP addresses to connect] オプションボタンをクリックします。
-

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。