

Cisco Secure Firewall Device Manager の新機能（リリース別）

最終更新：2025 年 4 月 8 日

各リリースの新機能

このドキュメントでは、各リリースの新機能と廃止された機能について説明します。



- (注) パッチの大部分は、リリースノートに記載されている緊急のバグ修正に限定されています。パッチに機能や動作の変更が含まれている場合は、「親」リリースの項で説明されています。

アップグレードの影響

アップグレードと展開により、システムでトラフィックが処理されるか、他の操作をしなくても異なる動作が発生する場合、機能がアップグレードに影響を与えます。これは特に、新しい脅威検出およびアプリケーション識別機能で一般的です。望ましくない結果を避けるために、アップグレードの前または後にアクションを実行する必要がある場合、機能がアップグレードに影響を与える可能性もあります。たとえば、設定を変更する必要がある場合などです。新しい機能を利用するために、アップグレード後に新しい設定を有効にするか、ポリシーを展開するする必要がありますが、これはアップグレードの影響とみなされません。

以下の機能の説明には、必要に応じてアップグレードの影響が含まれています。

Snort 3

Snort 3 は、Threat Defense をバージョン 6.7 (Device Manager 搭載) で起動するためのデフォルトの検査エンジンです。

Management Center 展開用の Snort 3 機能は、新しい Device Manager 機能としてリストされていない場合でも、Device Manager にも適用されます。ただし、Management Center は Device Manager よりも多くの設定可能なオプションを提供する場合がありますことに注意してください。Snort のバージョン別の機能拡張については、[Cisco Secure Firewall Management Center の新機能（リリース別）](#)を参照してください。



- 重要** まだ Snort 2 検査エンジンを使用している場合は、検出とパフォーマンスを向上させるために、今すぐ Snort 3 に切り替えてください。Snort 2 は将来のリリースで廃止され、最終的に Threat Defense のアップグレードを妨げるものになります。

侵入ルールとキーワード

アップグレードにより、新規および更新された侵入ルールおよびプリプロセッサルール、既存のルールの変更後のステータス、デフォルト侵入ポリシーの変更後の設定をインポートして自動的に有効化が可能です。現在のバージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU/LSPを更新しても、そのルールはインポートされません。アップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

新しいキーワードの詳細については、Snort リリースノート：<https://www.snort.org/downloads> を参照してください。

FlexConfig

アップグレードにより、以前は FlexConfig が必要だった機能について、Web インターフェイスまたはスマート CLI のサポートが追加されることがあります。アップグレードでは FlexConfig は変換されません。アップグレード後、Web インターフェイスまたは Smart CLI で新しくサポートされた機能を設定します。新しい設定を確認したら、廃止された FlexConfig を削除できます。

以下の機能の説明には、必要に応じて、廃止された FlexConfig に関する情報が含まれています。廃止された FlexConfig の完全なリストについては、[コンフィギュレーションガイド](#)を参照してください。



注意 廃止されたコマンドを使用して新しく FlexConfig オブジェクトを割り当てたり作成したりすることはできませんが、ほとんどの場合、既存の FlexConfigs は引き続き動作し、展開も可能です。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

REST API

REST API の新機能については、[Cisco Secure Firewall Threat Defense REST API ガイド](#) を参照してください。

言語設定

英語以外の言語で Web インターフェイスを使用している場合は、メンテナンスリリースやパッチで導入される機能が、次のメジャーリリースまで翻訳されない可能性があります。

推奨リリース：バージョン 7.4.2

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを最新パッチを含む推奨リリース以上にアップグレードすることをお勧めします。シスコサポートおよびダウンロードサイトでは、推奨リリースに金色の星が付いています。バージョン 7.2.6 以降または 7.4.1 以降では、新しい推奨リリースが使用可能になると **Management Center** から通知され、製品のアップグレードページに推奨リリースが表示されます。

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「[Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報](#)」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

バージョン 7.6.0 のデバイスマネージャ機能

表 1:バージョン 7.6.0 のデバイスマネージャ機能

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 1200	<p>Cisco Secure Firewall 1200 が導入されました。これには、次のモデルが含まれます。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 1210CX (1000BASE-T ポート X 8) • Cisco Secure Firewall 1210CP (1000BASE-T ポート X 8)。ポート 1/5 ~ 1/8 は、Power on Ethernet (PoE) をサポートします。 • Cisco Secure Firewall 1220CX (1000BASE-T ポート X 8、SFP+ ポート X 2)。 <p>Cisco Secure Firewall CSF-1210CE、CSF-1210CP、および CSF-1220CX Hardware Installation Guideを参照してください。</p>
Firepower 1000 および Cisco Secure Firewall 3100 の前面パネル USB-A ポートを無効にします。	<p>Firepower 1000 および Cisco Secure Firewall 3100 の前面パネル USB-A ポートを無効にできるようになりました。デフォルトでは、ポートは有効になっています。</p> <p>新規/変更された CLI コマンド：system support usb show、system support usb port disable、system support usb port enable</p> <p>Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。</p>

機能	説明
AWS 展開の IMDSv2 サポート。	<p>AWS 向けの Threat Defense は、IMDSv1 よりもセキュリティが向上したインスタンス メタデータ サービス バージョン 2 (IMDSv2) をサポートするようになりました。AWS でインスタンス メタデータ サービスを有効にすると、デフォルトは IMDSv2 Optional モードのままですが、IMDSv2 Required を選択することをお勧めします。また、アップグレードされたインスタンスに切り替えることをお勧めします。</p> <p>Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。</p>
サポート終了 : Firepower 2110、2120、2130、2140。	Firepower 2110、2120、2130、または 2140 ではバージョン 7.6 以降は実行できません。
ファイアウォールと IPS の機能	
オブジェクトグループの検索パフォーマンスの強化。	<p>オブジェクトグループの検索が高速になり、使用するリソースが少なくなりました。</p> <p>新しい CLI コマンド : clear asp table network-object、show asp table network-group</p> <p>変更された CLI コメント (拡張出力) : debug acl logs、packet-tracer、show access-list、show object-group</p> <p>Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。</p>
管理およびトラブルシューティングの機能	
URL フィルタ処理のインターネットアクセス要件を更新しました。	<p>アップグレードの影響。 システムは新しいリソースに接続します。</p> <p>システムは、URL フィルタリングデータのために *.talos.cisco.com にアクセスする必要があります。regsvc.sco.cisco.com または est.sco.cisco.com へのアクセスは不要になりました。</p>
Firewall Device Manager のカナダフランス語の翻訳。	<p>Firewall Device Manager には、英語、中国語、日本語、および韓国語に加えて、カナダフランス語バージョンが含まれています。ブラウザの言語としてカナダフランス語を選択する必要があります。他のタイプのフランス語を選択しても、フランス語バージョンは表示されません。</p> <p>参照 : Viewing Pages in Languages Other Than English [英語]</p>
パフォーマンス機能	

機能	説明
Cisco Secure Firewall 3100 のハードウェア DTLS 1.2 暗号化アクセラレーション。	<p>Cisco Secure Firewall 3100 は、DTLS 1.2 暗号化アクセラレーションと出力最適化をサポートするようになりました。これにより、DTLS 暗号および復号トラフィックのスループットが向上します。これは、新しいデバイスとアップグレードされたデバイスで自動的に有効になります。無効にするには、FlexConfig を使用します。</p> <p>新規/変更された FlexConfig コマンド：flow-offload-dtls、flow-offload-dtls egress-optimization、show flow-offload-dtls</p> <p>参照：Advanced Configuration [英語]</p>

バージョン 7.4.x の Device Manager 機能



- (注) バージョン 7.4 の機能に対する Device Manager のサポートは、バージョン 7.4.1 から始まります。これは、Device Manager をサポートするプラットフォームではバージョン 7.4.0 を使用できないためです。

表 2: バージョン 7.4.x の Device Manager 機能

機能	説明
プラットフォーム機能	
VMware vSphere/VMware ESXi 8.0 向けの Threat Defense Virtual	<p>VMware vSphere/VMware ESXi 8.0 で、VMware 用の Threat Defense Virtual を展開できるようになりました。</p> <p>必要最低限の Threat Defense：バージョン 7.4.2</p> <p>Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。</p>
Firepower 1010E のサポートが再開されています。	<p>バージョン 7.2.3 で導入され、バージョン 7.3 で一時的に廃止された Firepower 1010E のサポートが再開されています。</p> <p>参照：「Cabling for the Firepower 1010」</p>
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	<p>Cisco Secure Firewall 3130 および 3140 向けに次のネットワークモジュールが導入されました。</p> <ul style="list-style-type: none"> 2 ポート 100G QSFP+ ネットワークモジュール (FPR3K-XNM-2X100G) <p>参照：Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド</p>
VPN 機能	

機能	説明
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPsec フローのオフロード。	<p>アップグレードの影響。条件を満たす接続のオフロードが開始されます。</p> <p>Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。この機能はアップグレードにより自動的に有効になります。</p> <p>FlexConfig と flow-offload-ipsec コマンドを使用して構成を変更できます。</p>
インターフェイス機能	
マージされた管理インターフェイスと診断インターフェイス。	<p>アップグレードの影響。アップグレード後にインターフェイスをマージします。</p> <p>7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。</p> <p>7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。</p> <p>マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [Devices] > [Interfaces] > [Management] インターフェイス • (インターフェイスに移動) [System Settings] > [Management Interface] • [Devices] > [Interfaces] > [Merge Interface action needed] > [Management Interface Merge] <p>新規/変更されたコマンド：show management-interface convergence</p>

機能	説明
Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開します。	<p>Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開できるようになりました。Azure の展開には引き続き少なくとも 2 つのデータインターフェイスが必要ですが、GCP では診断インターフェイスをデータインターフェイスに置き換える必要があります、新しい最小は 3 つです（以前は、Threat Defense Virtual の展開には、1 つの管理インターフェイス、1 つの診断インターフェイス、および少なくとも 2 つのデータインターフェイスが必要でした）。</p> <p>制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。</p> <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>
Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 に対するインラインセット。	Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 デバイスでインラインセットを設定できます。[インターフェイス (Interface)] ページに [インラインセット (inline sets)] タブを追加しました。
ライセンス機能	
ライセンス名の変更およびキャリアライセンスのサポート。	<p>ライセンス名が次のように変更されました。</p> <ul style="list-style-type: none"> • Threat は IPS に変更 • Malware は Malware Defense に変更 • Base は Essentials に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 <p>さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。これらの機能を設定するには、FlexConfig を使用します。</p> <p>参照：「Licensing the System」</p>
管理およびトラブルシューティングの機能	
デフォルトの NTP サーバーが更新されました。	<p>アップグレードの影響。 システムは新しいリソースに接続します。</p> <p>デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。別の NTP サーバーを使用するには、[デバイス (Device)] を選択し、[システム設定 (System Settings)] パネルで [タイムサービス (Time Services)] をクリックします。</p>

機能	説明
HTTPS 管理ユーザーアクセス用の SAML サーバー。	<p>HTTPS 管理アクセスに外部認証を提供するように SAML サーバーを設定できます。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーを使用する場合は、ログインに共通アクセスカード (CAC) を使用できます。</p> <p>SAML アイデンティティ ソース オブジェクトの設定を更新し、該当オブジェクトを受け入れるように[システム設定 (System Settings)] > [管理アクセス (Management Access)] ページを更新しました。</p>
Threat Defense 高可用性ペアの設定の不一致を検出します。	<p>CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。</p> <p>新規/変更された CLI コマンド : show failover config-sync error、show failover config-sync stats</p> <p>参照 : Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
Cisco Secure Firewall 3100 でドロップされたパケットをキャプチャします。	<p>MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100 は、これらのドロップされたパケットをキャプチャできるようになりました。</p> <p>新規/変更された CLI コマンド : capture コマンドの [drop {disable mac-filter}]。</p> <p>参照 : Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
FXOS アップグレードに含まれるファームウェアのアップグレード。	<p>シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。</p> <p>Firepower 4100/9300 の場合、バージョン 2.14.1 以降への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。</p> <p>ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。</p> <p>参照 : Cisco Firepower 4100/9300 FXOS ファームウェア アップグレードガイド</p>

機能	説明
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	<p>Firepower 1000/2100 または Firepower 4100/9300 のデータプレーンプロセスがクラッシュすると、デバイスを再起動する代わりにプロセスがリロードされます。データプレーンをリロードすると、Snort を含む他のプロセスも再起動します。ブートアップ中にデータプレーンがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードループが回避されます。</p> <p>この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。</p> <p>新規/変更された ASA CLI コマンド : data-plane quick-reload、show data-plane quick-reload status</p> <p>新規/変更された Threat Defense CLI コマンド : show data-plane quick-reload status</p> <p>サポートされているプラットフォーム : Firepower 1000/2100、Firepower 4100/9300</p> <p>参照 : Cisco Secure Firewall Threat Defense コマンドリファレンス および Cisco Secure Firewall ASA シリーズ コマンドリファレンス</p>

バージョン 7.3.x の Device Manager 機能

表 3: バージョン 7.3.x の Device Manager 機能

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3105。	<p>Cisco Secure Firewall 3105 を導入しました。</p> <p>必要最低限の Threat Defense : バージョン 7.3.1</p>
Cisco Secure Firewall 4100 のネットワークモジュール。	<p>Firewall 4100 向けに次のネットワークモジュールが導入されました。</p> <ul style="list-style-type: none"> 2 ポート 100G ネットワークモジュール (FPR4K-NM-2X100G) <p>サポートされているプラットフォーム : Firepower 4112、4115、4125、4145</p>
ISA 3000 システム LED によるシャットダウンのサポート。	<p>この機能のサポートが再開されました。ISA 3000 をシャットダウンすると、システム LED が消灯します。その後、少なくとも 10 秒間待ってからデバイスの電源を切ってください。この機能はバージョン 7.0.5 で導入されましたが、バージョン 7.1 ~ 7.2 で一時的に廃止になりました。</p>

機能	説明
OCI 用の Threat Defense Virtual の新しいコンピューティングシェイプ。	<p>OCI 用の Threat Defense Virtual では、次のコンピューティングシェイプのサポートが追加されています。</p> <ul style="list-style-type: none"> • インテル VM.DenseIO2.8 • インテル VM.StandardB1.4 • インテル VM.StandardB1.8 • インテル VM.Standard1.4 • インテル VM.Standard1.8 • インテル VM.Standard3.Flex • インテル VM.Optimized3.Flex • AMD VM.Standard.E4.Flex <p>VM.Standard2.4 および VM.Standard2.8 コンピューティングシェイプは、2022 年 2 月に注文可能期間が終了したことに注意してください。バージョン 7.3 以降を展開する場合は、別のコンピューティングシェイプをお勧めします。</p> <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>
サポート終了：Firepower 4110、4120、4140、4150。	Firepower 4110、4120、4140、または 4150 ではバージョン 7.3 以降は実行できません。
サポート終了：Firepower 9300：SM-24、SM-36、SM-44 モジュール。	SM-24、SM-36、または SM-44 モジュールを搭載した Firepower 9300 ではバージョン 7.3 以降は実行できません。
Firepower 1010E はバージョン 7.3 をサポートしていません。	<p>バージョン 7.2.3 で導入された Firepower 1010E は、バージョン 7.3 をサポートしていません。サポートは、バージョン 7.4 で再開されています。</p> <p>バージョン 7.2.x の Firepower 1010E をバージョン 7.3 にアップグレードすることはできません。また、そこで再イメージ化しないでください。バージョン 7.3 を実行している Firepower 1010E デバイスがある場合は、サポートされているリリースに再イメージ化します。</p>
ファイアウォールと IPS の機能	

機能	説明
SSL 復号ポリシーでの TLS 1.3 のサポート、および復号できない接続の設定可能な動作。	<p>アップグレードの影響。</p> <p>TLS 1.3 トラフィックの SSL 復号ルールを設定できます。TLS 1.3 のサポートは、Snort 3 を使用する場合にのみ利用できます。復号できない接続のデフォルト以外の動作も設定できます。Snort 3 を使用している場合、アップグレード時に、すべての SSL/TLS バージョンが選択されているルールに対して TLS 1.3 が自動的に選択されます。それ以外の場合、TLS 1.3 は選択されません。Snort 2 から Snort 3 に切り替えると、同じ動作が発生します。</p> <p>[ルールの追加/編集 (Add/Edit Rule)] ダイアログボックスの [詳細 (Advanced)] タブにオプションとして TLS 1.3 を追加しました。また、SSL 復号ポリシー設定を再設計して、TLS 1.3 復号を有効にし、復号できない接続アクションを設定する機能を含めました。</p> <p>参照：「Advanced Criteria for SSL Decryption Rules」 および 「Configure Advanced and Undecryptable Traffic Settings」</p>
洗練された URL フィルタリングルックアップ。	<p>URL フィルタリングルックアップの実行方法を明示的に設定できるようになりました。ローカル URL データベースのみを使用するか、ローカルデータベースとクラウドルックアップの両方を使用するか、クラウドルックアップのみを使用するかを選択できます。URL フィルタリングシステム設定オプションを拡張しました。</p> <p>参照：「Configuring URL Filtering Preferences」</p>
インターフェイス機能	
仮想アプライアンスの IPv6 サポート。	<p>Threat Defense Virtual は、次の環境で IPv6 をサポートするようになりました。</p> <ul style="list-style-type: none"> • AWS • Azure • KVM • VMware <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>
DHCPv6 クライアント。	<p>DHCPv6 から IPv6 アドレスを取得できるようになりました。</p> <p>新規/変更画面：[デバイス (Device)] > [インターフェイス (Interfaces)] > [インターフェイスの編集 (Edit Interface)] > [詳細設定 (Advanced)]</p> <p>参照：「Configure Advanced Interface Options」</p>
管理およびトラブルシューティングの機能	

機能	説明
CA バンドルの自動更新。	<p>アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカルCAバンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しいCA証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLIを使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド：configure cert-update auto-update、configure cert-update run-now、configure cert-update test、show cert-update</p> <p>バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。</p> <p>参照：Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
認証局による信頼できる証明書のチェックをスキップ。	<p>信頼できるCA証明書としてローカルCA証明書をインストールする必要がある場合は、チェックをスキップできます。</p> <p>信頼できるCA証明書をアップロードするときの[CA証明書チェックのスキップ (Skip CA Certificate Check)]オプションが追加されました。</p>

機能	説明
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。	

機能	説明
	<p>再イメージ化の影響。</p> <p>バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。</p> <ul style="list-style-type: none"> • バージョン 7.1 ～ 7.2 インストールパッケージ : <code>isco-ftd-fp3k.version.SPA</code> • バージョン 7.1 ～ 7.2 アップグレードパッケージ : <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> • バージョン 7.3 以降の統合パッケージ : <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> <p>Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。</p> <p>Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。</p> <ul style="list-style-type: none"> • Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当する アップグレードガイド を参照してください。 • Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100」、次に「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。 『Cisco FXOS トラブルシューティング ガイド (Firepower Threat Defense

機能	説明
	<p>を実行している Firepower 1000/2100 および Cisco Secure Firewall 1200/3100/4200 向け)』の「Reimage the System with a New Software Version」を参照してください。</p>
Threat Defense REST API バージョン 6.4 (v6)。	<p>ソフトウェアバージョン 7.3 用の脅威に対する防御 REST API はバージョン 6.4 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.4 の URL バージョンパス要素は、他のすべてのバージョン 6.x (v6) と同じであることに注意してください。</p> <p>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン (☰) をクリックし、[API Explorer] を選択します。</p> <p>参照：Cisco Secure Firewall Threat Defense REST API ガイド</p>

バージョン 7.2.x の Device Manager 機能

表 4:バージョン 7.2.x の Device Manager 機能

機能	説明
プラットフォーム機能	
Firepower 1010E。	<p>Power over Ethernet (PoE) をサポートしていない Firepower 1010E を導入しました。</p> <p>必要最低限の Threat Defense : 7.2.3</p> <p>参照：「Cabling for the Firepower 1010」</p>
GCP 向け Threat Defense Virtual。	<p>デバイスネージャを使用して、GCP 対応 Threat Defense Virtual を構成できるようになりました。</p> <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>

機能	説明
Megaport 対応 Threat Defense Virtual。	<p>デバイスマネージャを使用して、Megapor (Megaport Virtual Edge) 対応 Threat Defense Virtual を構成できるようになりました。高可用性はサポートされていません。</p> <p>必要最低限の Threat Defense : 7.2.8</p> <p>その他のバージョンの制限：最初からバージョン 7.3.x または 7.4.x を新規展開できない場合があります。代わりに、バージョン 7.2.8 ~ 7.2.x を展開した後にアップグレードします。</p> <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>
Cisco Secure Firewall 3100 のネットワークモジュール。	<p>Cisco Secure Firewall 3100 向けに次のネットワークモジュールが導入されました。</p> <ul style="list-style-type: none"> • 6 ポート 1G SFP ネットワークモジュール、SX (マルチモード) (FPR-X-NM-6X1SX-F) • 6 ポート 10G SFP ネットワークモジュール、SR (マルチモード) (FPR-X-NM-6X10SR-F) • 6 ポート 10G SFP ネットワークモジュール、LR (シングルモード) (FPR-X-NM-6X10LR-F) • 6 ポート 25G SFP ネットワークモジュール、SR (マルチモード) (FPR-X-NM-X25SR-F) • 6 ポート 25G ネットワークモジュール、LR (シングルモード) (FPR-X-NM-6X25LR-F) • 8 ポート 1G 銅ケーブル ネットワークモジュール、RJ45 (銅ケーブル) (FPR-X-NM-8X1G-F) <p>必要最低限の Threat Defense : 7.2.1</p>
KVM の仮想 Threat Defense を備えた Intel イーサネット ネットワーク アダプタ E810-CQDA2 ドライバ。	<p>KVM の仮想 Threat Defense で Intel イーサネット ネットワーク アダプタ E810-CQDA2 ドライバをサポートするようになりました。</p> <p>必要最低限の Threat Defense : 7.2.1</p> <p>参照：「Deploy the Threat Defense Virtual on KVM」</p>
ISA 3000 によるシャットダウンのサポート。	<p>ISA 3000 のシャットダウンのサポートが再開されました。この機能はバージョン 7.0.2 で導入されましたが、バージョン 7.1 で一時的に廃止になりました。</p>
ファイアウォールと IPS の機能	

機能	説明
オブジェクトグループ検索は、アクセス制御のためにデフォルトで有効になっています。	<p>CLI 構成コマンド object-group-search access-control は現在、デフォルトで有効になっています。FlexConfig を使用してコマンドを設定している場合は、その機能がまだ必要かどうかを評価する必要があります。この機能を無効にする必要がある場合は、FlexConfig を使用して no object-group-search access-control コマンドを実装します。</p> <p>参照： Cisco Secure Firewall ASA シリーズ コマンド リファレンス</p>
ルールヒットカウントは再起動後も継続します。	<p>デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。 show rule hits コマンドを使用して、HA ペアまたはクラスタ全体の累積カウントを表示したり、ノードごとのカウントを表示したりできます。</p> <p>次の脅威に対する防御 CLI コマンドを変更しました： show rule hits。</p> <p>参照：「Examining Rule Hit Counts」</p>
VPN 機能	
IPsec フローがオフロードされます。	<p>Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされません。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。</p> <p>FlexConfig と flow-offload-ipsec コマンドを使用して構成を変更できます。</p> <p>参照：「IPSec Flow Offload」</p>
インターフェイス機能	
Cisco Secure Firewall 3130 および 3140 のブレイクアウトポートのサポート。	<p>Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレイクアウトポートを構成できるようになりました。</p> <p>新しい/変更された画面：[デバイス (Devices)] > [インターフェイス (Interfaces)]</p> <p>参照：「Manage the Network Module for the Secure Firewall 3100」</p>

機能	説明
インターフェイスでの Cisco TrustSec の有効化または無効化。	<p>名前付きか名前なしにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。</p> <p>インターフェイス構成ダイアログボックスに [Propagate Security Group Tag] 属性を追加し、さまざまなインターフェイス API に ctsEnabled 属性を追加しました。</p> <p>参照：「Configure Advanced Options」</p>
ライセンス機能	
ISA 3000 の永久ライセンス予約のサポート。	<p>ISA 3000 は、承認されたお客様向けのユニバーサル永久ライセンスの予約をサポートするようになりました。</p> <p>参照：「Applying Permanent Licenses in Air-Gapped Networks」</p>
管理およびトラブルシューティングの機能	
完全な展開を強制する機能。	<p>変更を展開すると、システムは通常、最後の正常な展開以降に加えられた変更のみを展開します。ただし、問題が発生した場合は、デバイスの構成を完全に更新するフル展開を強制するように選択できます。展開ダイアログボックスに [Apply Full Deployment] オプションを追加しました。</p> <p>参照：「Deploying Your Changes」</p>
CA バンドルの自動更新。	<p>アップグレードの影響。 システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLI を使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド： <code>configure cert-update auto-update</code>、<code>configure cert-update run-now</code>、<code>configure cert-update test</code>、<code>show cert-update</code></p> <p>バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。</p> <p>参照： Cisco Secure Firewall Threat Defense コマンドリファレンス</p>

機能	説明
Threat Defense REST API バージョン 6.3 (v6)。	<p>ソフトウェアバージョン 7.2 用の脅威に対する防御 REST API はバージョン 6.3 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.3 の URL バージョンパス要素は、6.0、6.1 および 6.2 と同じ v6 である点に注意してください。</p> <p>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン (☰) をクリックし、[API Explorer] を選択します。</p> <p>参照：Cisco Secure Firewall Threat Defense REST API ガイド</p>

FDM バージョン 7.1.x の機能

表 5: FDM バージョン 7.1.x の機能

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3100。	<p>Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。</p> <p>ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ (SED) です。SSD が 2 つある場合、ソフトウェア RAID を形成します。</p> <p>バージョン 7.1 の Device Manager には、これらのデバイスのオンラインヘルプが含まれていないことに注意してください。Cisco.com に掲載されているドキュメントを参照してください。</p> <p>新しい/変更された画面：[Devices] > [Interfaces]</p> <p>新しい/変更された脅威に対する防御 コマンド：<code>configure network speed</code>、<code>configure raid</code>、<code>show raid</code>、<code>show ssd</code></p>

機能	説明
AWS 用 FTDv のインスタンス。	<p>AWS 用 FTDv により、次のインスタンスのサポートが追加されています。</p> <ul style="list-style-type: none"> • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5n.xlarge、c5n.2xlarge、c5n.4xlarge • i3en.xlarge、i3en.2xlarge、i3en.3xlarge • inf1.xlarge、inf1.2xlarge • m5.xlarge、m5.2xlarge、m5.4xlarge • m5a.xlarge、m5a.2xlarge、m5a.4xlarge • m5ad.xlarge、m5ad.2xlarge、m5ad.4xlarge • m5d.xlarge、m5d.2xlarge、m5d.4xlarge • m5dn.xlarge、m5dn.2xlarge、m5dn.4xlarge • m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.xlarge、m5zn.2xlarge、m5zn.3xlarge • r5.xlarge、r5.2xlarge、r5.4xlarge • r5a.xlarge、r5a.2xlarge、r5a.4xlarge • r5ad.xlarge、r5ad.2xlarge、r5ad.4xlarge • r5b.xlarge、r5b.2xlarge、r5b.4xlarge • r5d.xlarge、r5d.2xlarge、r5d.4xlarge • r5dn.xlarge、r5dn.2xlarge、r5dn.4xlarge • r5n.xlarge、r5n.2xlarge、r5n.4xlarge • z1d.xlarge、z1d.2xlarge、z1d.3xlarge
Azure 用 FTDv のインスタンス。	<p>Azure 用 FTDv により、次のインスタンスのサポートが追加されています。</p> <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

機能	説明
ASA 5508-X および 5516-X のサポートは終了します。サポートされる最後のリリースは脅威に対する防御 7.0 です。	ASA 5508-X または 5516-X に脅威に対する防御脅威に対する防御 7.1 はインストールできません。これらのモデルで最後にサポートされるリリースは脅威に対する防御 7.0 です。
ファイアウォールと IPS の機能	
Snort 3 のネットワーク分析ポリシー (NAP) 設定。	<p>Snort 3 の実行時に、Device Manager を使用してネットワーク分析ポリシー (NAP) を設定できます。ネットワーク分析ポリシーはトラフィック前処理検査を制御します。インスペクタは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックがさらに検査されるように準備します。すべてのトラフィックに使用する NAP を選択し、ネットワークのトラフィックに最適な設定をカスタマイズできます。Snort 2 の実行中は NAP を設定できません。</p> <p>[ポリシー (Policies)] > [侵入 (Intrusion)] の設定ダイアログボックスにネットワーク分析ポリシーが追加されました。これには、直接の変更が可能な組み込み JSON エディタと、上書きをアップロードしたり、作成したものをダウンロードしたりするためのその他の機能があります。 ></p>
変換後の宛先としての完全修飾ドメイン名 (FQDN) オブジェクトの手動 NAT サポート。	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
改善されたアクティブ認証アイデンティティルール。	<p>ID ポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスの IP アドレスではなく、完全修飾ドメイン名 (FQDN) にユーザーの認証をリダイレクトできます。FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名 (SAN) に指定できます。</p> <p>ID ポリシー設定に [ホスト名にリダイレクト (Redirect to Host Name)] オプションが追加されました。</p>
VPN 機能	

機能	説明
サイト間 VPN のバックアップリモートピア	<p>リモートバックアップピアを含めるようにサイト間 VPN 接続を設定できます。プライマリリモートピアが使用できない場合、システムはバックアップピアの 1 つを使用して VPN 接続を再確立しようとします。バックアップピアごとに個別の事前共有キーまたは証明書を設定できます。バックアップピアは、ポリシーベースの接続でのみサポートされ、ルートベース（仮想トンネルインターフェイス）の接続では使用できません。</p> <p>バックアップピア設定を含むように、サイト間 VPN ウィザードを更新しました。</p>
リモートアクセス VPN（MSCHAPv2）のパスワード管理。	<p>リモートアクセス VPN のパスワード管理を有効にできます。これにより、AnyConnect はユーザーに期限切れのパスワードの変更を求めることができます。パスワード管理がない場合、ユーザーは AAA サーバーを使用して期限切れのパスワードを直接変更する必要があります。AnyConnect はユーザーにパスワードの変更を要求しません。LDAP サーバーの場合は、パスワードの有効期限が近づいていることをユーザーに通知する警告期間を設定することもできます。</p> <p>リモートアクセス VPN 接続プロファイルの認証設定に [パスワード管理を有効にする（Enable Password Management）] オプションが追加されました。</p>
AnyConnect VPN SAML 外部ブラウザ。	<p>リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。</p> <p>リモートアクセス VPN 接続プロファイルウィザードが更新され、SAML ログインエクスペリエンスを設定できるようになりました。</p>

管理およびトラブルシューティングの機能

機能	説明
システムインターフェイスの完全修飾ドメイン名 (FQDN) から IP アドレスへのマッピングを更新するためのダイナミック ドメイン ネーム システム (DDNS) のサポート。	<p>アップグレードの影響。アップグレード後に、FlexConfig をやり直します。</p> <p>ダイナミックアップデートを DNS サーバーに送信するように、システムのインターフェイスに DDNS を設定できます。これにより、インターフェイスに定義された FQDN が正しいアドレスに解決され、ユーザーが IP アドレスではなくホスト名を使用して簡単にシステムにアクセスできるようになります。これは、DHCP を使用してアドレスを取得するインターフェイスに特に役立ちますが、静的にアドレス指定されたインターフェイスにも役立ちます。</p> <p>アップグレード後に FlexConfig を使用して DDNS を設定した場合は、変更を再度展開する前に、Device Manager または脅威に対する防御 API を使用して設定をやり直し、FlexConfig ポリシーから DDNS FlexConfig オブジェクトを削除する必要があります。</p> <p>Device Manager を使用して DDNS を設定し、Management Center 管理に切り替えると、DDNS 構成が保持され、Management Center が DNS 名を使用してシステムを検索できるようになります。</p> <p>Device Manager で、[System Settings] > [DDNS Service] ページが追加されました。脅威に対する防御 API で、DDNSService および DDNSInterfaceSettings リソースが追加されました。</p>
デバイス CLI で、 dig コマンドが nslookup コマンドに置き換わります。	<p>デバイス CLI で完全修飾ドメイン名 (FQDN) の IP アドレスを検索するには、dig コマンドを使用します。nslookup コマンドは削除されます。</p>
Device Manager を使用した DHCP リレー構成。	<p>Device Manager を使用して DHCP リレーを構成できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。</p> <p>[システム設定 (System Settings)] > [DHCP] > [DHCP リレー (DHCP Relay)] ページを追加し、DHCP サーバーを新しい DHCP 見出しの下に移動しました。 > ></p>
Device Manager の自己署名証明書のキータイプとサイズ。	<p>Device Manager で新しい自己署名内部および内部 CA 証明書を生成するときに、キータイプとサイズを指定できます。キータイプには、RSA、ECDSA、および EDDSA があります。許可されるサイズはキータイプによって異なります。推奨される最小長よりも小さいキーサイズの証明書をアップロードすると、警告が表示されるようになりました。また、可能な場合は置き換える必要がある脆弱な証明書を見つけるために役立つ、事前定義された脆弱キー検索フィルタもあります。</p>

機能	説明
信頼できる CA 証明書の使用検証の制限。	<p>信頼できる CA 証明書を使用して特定のタイプの接続を検証できるかどうかを指定できます。SSL サーバー（ダイナミック DNS で使用）、SSL クライアント（リモートアクセス VPN で使用）、IPsec クライアント（サイト間 VPN で使用）、または LDAPS などの Snort 検査エンジンによって管理されていないその他の機能の検証を許可または阻止できます。これらのオプションの主な目的は、特定の証明書に対して検証できるため、VPN 接続が確立されないようにすることです。</p> <p>信頼できる CA 証明書のプロパティとして [検証の使用 (Validation Usage)] が追加されました。</p>
Device Manager での管理者パスワードの生成。	Device Manager での初期システム設定時、または Device Manager で管理者パスワードを変更するときに、ボタンをクリックしてランダムな 16 文字のパスワードを生成できるようになりました。
起動時間と tmatch コンパイルステータス。	<p>show version コマンドには、システムの起動（ブート）にかかった時間に関する情報が含まれるようになりました。設定が大きいくほど、システムの起動に時間がかかることに注意してください。</p> <p>新しい show asp rule-engine コマンドは、tmatch コンパイルのステータスを表示します。Tmatch コンパイルは、アクセスグループ、NAT テーブル、およびその他のいくつかの項目として使用されるアクセスリストに使用されます。これは、非常に大きな ACL と NAT テーブルがある場合には、CPU リソースを消費し、進行中のパフォーマンスに影響を与える可能性がある内部プロセスです。コンパイル時間は、アクセスリスト、NAT テーブルなどのサイズによって異なります。</p>
show access-list element-count 出力の拡張。	<p>show access-list element-count コマンドの出力が拡張されました。オブジェクトグループ検索を有効にして使用すると、出力には要素数のオブジェクトグループの数に関する詳細が含まれます。</p> <p>さらに、show tech-support 出力には show access-list element-count と show asp rule-engine からの出力が含まれます。</p>
Device Manager を使用して Management Center による管理のために脅威に対する防御を設定。	<p>Device Manager を使用して初期設定を実行すると、管理および Management Center アクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。脅威に対する防御 CLI を使用すると、管理と Management Center のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。</p> <p>Management Center に切り替えると、Device Manager を使用して脅威に対する防御を管理できなくなります。</p> <p>新規/変更された画面：[システム設定 (System Settings)]、[管理センター (Management Center)] ></p>

機能	説明
CA バンドルの自動更新。	<p>アップグレードの影響。 システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLI を使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド： <code>configure cert-update auto-update</code>、<code>configure cert-update run-now</code>、<code>configure cert-update test</code>、<code>show cert-update</code></p> <p>バージョンの制限： この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。</p> <p>参照：Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
FTD REST API バージョン 6.2 (v6)。	<p>ソフトウェアバージョン 7.1 用の脅威に対する防御 REST API はバージョン 6.2 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.2 の URL バージョンパス要素は、6.0/1 と同じ v6 である点に注意してください。</p> <p>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン (⋮) をクリックし、[API Explorer] を選択します。</p>

FDM バージョン 7.0.x の機能

表 6: FDM バージョン 7.0.x の機能

機能	説明
プラットフォーム機能	
HyperFlex および Nutanix 向け FTDv。	Cisco HyperFlex および Nutanix Enterprise Cloud に FTDv が導入されました。
VMware vSphere/VMware ESXi 7.0 向け FTDv。	VMware vSphere/VMware ESXi 7.0 に FTDv を展開できるようになりました。バージョン 7.0 でも VMware 6.0 のサポートは終了します。FTD をアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。

機能	説明
AWS における Threat Defense Virtual の新しいデフォルトパスワード	AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義 ([Advanced Details] > [User Data]) していなければ、Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。
ISA 3000 によるシャットダウンのサポート。	バージョン 7.0.2 以降では、ISA 3000 をシャットダウンできるようになりました。以前は、デバイスを再起動することしかできませんでした。 バージョン 7.0.5 以降では、ISA 3000 をシャットダウンすると、システム LED が消灯します。その後、少なくとも 10 秒間待つてからデバイスの電源を切ってください。 バージョンの制限：バージョン 7.1 では、この機能のサポートが一時的に廃止されます。サポートは、バージョン 7.2 で再開されています。
ファイアウォールと IPS の機能	
システム定義の NAT ルールの新しいセクション 0。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、 show nat detail コマンド出力に表示されます。
Snort 3 のカスタム侵入ルール。	オフラインツールを使用して、Snort 3 で使用するカスタム侵入ルールを作成し、侵入ポリシーにアップロードできます。独自のカスタムルールグループにカスタムルールを編成して、必要に応じて簡単に更新できます。Device Manager で直接ルールを作成することもできますが、ルールの形式はアップロードされたルールと同じです。Device Manager には、ルール作成のガイドンスはありません。新しい侵入ルールの基礎として、システム定義のルールを含む既存のルールを複製できます。 侵入ポリシーの編集時に、 [Policies] > [Intrusion] ページにカスタムグループとルールのサポートが追加されました。
Device Manager 管理対象システムの Snort 3 の新機能	Device Manager 管理対象システムで Snort 3 を検索エンジンとして使用する場合、次の追加機能を設定できるようになりました。 <ul style="list-style-type: none"> • 時間ベースのアクセス制御ルール (Threat Defense API のみ)。 • 複数の仮想ルータ。 • SSL 復号ポリシーを使用した TLS 1.1 以下の接続の復号。 • SSL 復号ポリシーを使用したプロトコル FTPS、SMTPS、IMAPS、POP3S の復号。

機能	説明
URL カテゴリとレピュテーションに基づく DNS 要求のフィルタリング。	<p>URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用できます。ルックアップ要求の完全修飾ドメイン名 (FQDN) にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザーは DNS 解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーションフィルタリングを適用するには、このオプションを使用します。この機能を使用するには、URL フィルタリングライセンスが必要です。</p> <p>アクセスコントロールポリシーの設定に [Reputation Enforcement on DNS Traffic] オプションが追加されました。</p>
Snort 2 を搭載したメモリが少ないデバイス用の小規模 VDB。	<p>アップグレードの影響。メモリが少ないデバイスのアプリケーション ID が影響を受けます。</p> <p>Snort 2 を搭載したバージョン 7.0.6 以降のデバイスの場合、VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB (別称: VDB lite) がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。</p> <p>メモリが少ないデバイス: ASA-5508-X、ASA-5516-X</p> <p>バージョンの制限: 小規模 VDB は、すべてのバージョンでサポートされているわけではありません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードする場合、Snort 2 を実行しているメモリの少ないデバイスに VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。</p>
VPN 機能	
リモートアクセス VPN の Device Manager SSL 暗号設定	<p>Device Manager でリモートアクセス VPN 接続に使用する TLS バージョンと暗号化の暗号を定義できます。以前は、脅威に対する防御 API を使用して SSL を設定する必要がありました。</p> <p>次のページが追加されました: [Objects] > [SSL Ciphers]、[Device] > [System Settings] > [SSL Settings]。</p>
Diffie-Hellman グループ 31 のサポート。	IKEv2 プロポーザルおよびポリシーで Diffie-Hellman (DH) グループ 31 を使用できるようになりました。
デバイス上の仮想トンネルインターフェイスの最大数は 1024 です。	作成できる仮想トンネルインターフェイス (VTI) の最大数は 1024 です。以前のバージョンでは、送信元インターフェイスあたりの最大数は 100 でした。

機能	説明
サイト間 VPN セキュリティアソシエーションの IPsec ライフタイム設定。	<p>セキュリティアソシエーションが再ネゴシエートされるまでに維持する期間のデフォルト設定を変更できます。</p> <p>サイト間 VPN ウィザードに [Lifetime Duration] オプションと [Lifetime Size] オプションが追加されました。</p>
ルーティング機能	
ISA 3000 の仮想ルータサポート。	ISA 3000 デバイスには最大 10 の仮想ルータを設定できます。
等コストマルチパス (ECMP) ルーティング。	<p>複数のインターフェイスを含むように ECMP トラフィックゾーンを設定できます。これにより、ゾーン内の任意のインターフェイスで、既存の接続のトラフィックが脅威に対する防御デバイスに出入りできるようになります。この機能により、脅威に対する防御デバイス上での等コストマルチパス (ECMP) のルーティングや、脅威に対する防御デバイスへのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。</p> <p>ECMP トラフィックゾーンはルーティングにのみ使用されます。これらはセキュリティゾーンとは異なります。</p> <p>[ルーティング (Routing)] ページに [ECMP トラフィックゾーン (ECMP Traffic Zones)] タブが追加されました。脅威に対する防御 API に ECMPZones リソースが追加されました。</p>
インターフェイス機能	
新しいデフォルトの内部 IP アドレス。	192.168.1.0/24 のアドレスが DHCP を使用して外部インターフェイスに割り当てられている場合、IP アドレスの競合を避けるために、内部インターフェイスのデフォルト IP アドレスが 192.168.1.1 から 192.168.95.1 に変更されています。
デフォルトの外部 IP アドレスで IPv6 自動設定が有効になりました。管理用の新しいデフォルト IPv6 DNS サーバー。	外部インターフェイスのデフォルト設定には、IPv4 DHCP クライアントに加えて、IPv6 自動設定が含まれています。デフォルトの管理 DNS サーバーには、IPv6 サーバー：2620:119:35::35 も含まれるようになりました。
ISA 3000 の EtherChannel サポート。	<p>Device Manager を使用して ISA 3000 で EtherChannel を設定できるようになりました。</p> <p>新しい/変更された画面：[デバイス (Devices)] > [インターフェイス (Interfaces)] > [EtherChannel]</p>
ライセンス機能	

機能	説明
Threat Defense Virtual のパフォーマンス階層型ライセンス。	Threat Defense Virtual は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマートライセンスをサポートするようになりました。使用可能なパフォーマンスライセンスのいずれかで Threat Defense Virtual のライセンスを取得すると、2つのことが発生します。まず、デバイスのスループットを指定されたレベルに制限するレートリミッタがインストールされます。次に、VPN セッションの数は、ライセンスで指定されたレベルに制限されます。
管理およびトラブルシューティングの機能	
脅威に対する防御 API を使用した DHCP リレー設定。	<p>アップグレードの影響。アップグレード後の展開ができない場合があります。</p> <p>脅威に対する防御 API を使用して DHCP リレーを設定できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。</p> <p>以前のリリースで FlexConfig を使用して DHCP リレーを設定した場合は (<code>dhcprelay</code> コマンド)、アップグレード後に API を使用して設定を再実行し、FlexConfig オブジェクトを削除する必要があります。</p> <p>脅威に対する防御 API に次のモデルを追加しました：<code>dhcprelayservices</code></p>
ブートストラップ処理の高速化と Device Manager への早期ログイン	Device Manager 管理対象システムを最初にブートストラップするプロセスが改善され、より高速になりました。したがって、デバイスを起動してから Device Manager にログインするまで待機する必要はありません。また、ブートストラップの進行中にログインできるようになりました。ブートストラップが完了していない場合は、プロセスのステータス情報が表示されるため、デバイスで何が発生しているかがわかります。
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	<p>ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。</p> <p>次のコマンドが変更されました：<code>clear local-host</code>（廃止）、<code>show local-host</code></p>

機能	説明
Device Manager 管理対象デバイスのアップグレード準備状況チェック。	<p>アップロードした脅威に対する防御アップグレードパッケージをインストールする前に、アップグレード準備状況チェックを実行できます。準備状況チェックでは、システムに対してアップグレードが有効であり、システムがパッケージのインストールに必要な他の要件を満たしていることを確認します。アップグレードの準備状況チェックを実行すると、インストールの失敗を回避できます。</p> <p>[Device]>[Updates]ページの[System Upgrade]セクションに、アップグレードの準備状況チェックを実行するリンクが追加されました。</p>
CA バンドルの自動更新。	<p>アップグレードの影響。 システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカルCAバンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しいCA証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA証明書を更新するにはソフトウェアをアップグレードする必要がありますがありました。CLIを使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド : <code>configure cert-update auto-update</code>、<code>configure cert-update run-now</code>、<code>configure cert-update test</code>、<code>show cert-update</code></p> <p>バージョンの制限 : この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。</p> <p>参照 : Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
FTD REST API バージョン 6.1 (v6)。	<p>ソフトウェアバージョン 7.0 の脅威に対する防御 REST API はバージョン 6.1 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.1 の URL バージョンパス要素は、6.0 : v6 と同じであることに注意してください。</p> <p>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン (⋮) をクリックし、[API Explorer] を選択します。</p>

FDM バージョン 6.7.x の機能

表 7: FDM バージョン 6.7.x の機能

機能	説明
プラットフォーム機能	
ASA 5525-X、5545-X、5555-X でのサポートが終了します。最後にサポートされていたリリースは脅威に対する防御 6.6 です。	脅威に対する防御 6.7 を ASA 5525-X、5545-X、5555-X にインストールすることはできません。これらのモデルで最後にサポートされていたリリースは脅威に対する防御 6.6 です。
ファイアウォールと IPS の機能	
アクセス制御ルールの照合のための TLS サーバーアイデンティティ検出。	<p>TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するため、[TLS サーバーアイデンティティ検出 (TLS Server Identity Discovery)] を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。</p> <p>[アクセス制御の設定 (Access Control Settings)] (⚙️) ボタンとダイアログボックスが [ポリシー (Policy)] > [アクセス制御 (Access Control)] ページに追加されました。</p>
外部の信頼できる CA 証明書のグループ。	<p>SSL 復号ポリシーで使用される信頼できる CA 証明書のリストをカスタマイズできるようになりました。デフォルトでは、ポリシーはすべてのシステム定義の信頼できる CA 証明書を使用しますが、カスタムグループを作成して証明書を追加したり、デフォルトグループを独自のより制限されたグループに置き換えることができます。</p> <p>[オブジェクト (Objects)] > [証明書 (Certificates)] ページに証明書グループが追加され、SSL 復号ポリシー設定を変更して証明書グループを選択できるようになりました。</p>

機能	説明
<p>パッシブ ID ルールの Active Directory レルムシーケンス。</p>	<p>Active Directory (AD) サーバーとそのドメインの番号付きリストであるレルムシーケンスを作成し、パッシブ認証 ID ルールで使用できます。レルムシーケンスは、複数の AD ドメインをサポートしている状態で、ユーザーベースのアクセス制御を実行するときに役立ちます。各 AD ドメインの個別のルールを記述する代わりに、すべてのドメインを対象とする単一のルールを作成できます。シーケンス内の AD レルムの順序は、ID の競合が発生した場合に、その競合を解決するために使用されます。</p> <p>[オブジェクト (Objects)]>[アイデンティティソース (Identity Sources)] ページに AD レルム シーケンス オブジェクトが追加され、そのオブジェクトをパッシブ認証アイデンティティルールのレルムとして選択できるようになりました。脅威に対する防御 API に RealmSequence リソースが追加されました。また IdentityRule リソースには、アクションとしてパッシブ認証を使用するルールのレルムとしてレルム シーケンス オブジェクトを選択する機能が追加されました。</p>
<p>TrustSec セキュリティグループタグ (SGT) グループオブジェクトの FDM サポートと、アクセス制御ルールでのそれらの使用</p>	<p>脅威に対する防御 6.5 では、SGT グループオブジェクトを設定し、それらをアクセス制御ルールの一致基準として使用するためのサポートが 脅威に対する防御 API に追加されました。さらに、ISE によってパブリッシュされた SXP トピックをリッスンするように ISE アイデンティティ オブジェクトを変更できます。これらの機能を FDM で直接設定できるようになりました。</p> <p>新しいオブジェクトである SGT グループが追加され、それらを選択および表示できるようにアクセス制御ポリシーが更新されました。また、サブスクライブするトピックの明示的な選択を含むように ISE オブジェクトを変更しました。</p>
<p>Snort 3.0 のサポート。</p>	<p>新しいシステムでは、Snort 3.0 がデフォルトの検査エンジンです。古いリリースから 6.7 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、Snort 3.0 に切り替えることができます。このリリースでは、Snort 3.0 は、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1 以下の接続の復号をサポートしていません。これらの機能が不要な場合にのみ Snort 3.0 を有効にしてください。Snort 2.0 と Snort 3.0 の間を自由に切り替えることができるため、必要に応じて、変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。</p> <p>[デバイス (Device)]>[更新 (Updates)] ページの [侵入ルール (Intrusion Rules)] グループに Snort のバージョンを切り替える機能が追加されました。脅威に対する防御 API では、IntrusionPolicy リソースアクション/toggleinspectionengine が追加されました。</p> <p>さらに、Snort 3 ルールパッケージの更新で追加、削除、または変更された侵入ルールを示す新しい監査イベント、ルール更新イベントがあります。</p>

機能	説明
Snort 3 のカスタム侵入ポリシー。	<p>Snort 3 を検査エンジンとして使用している場合は、カスタム侵入ポリシーを作成できます。これに対し、Snort 2 を使用する場合にのみ、事前定義されたポリシーを使用できます。カスタム侵入ポリシーを使用すると、ルールのグループを追加または削除し、グループレベルでセキュリティレベルを変更して、グループ内のルールのデフォルトアクション（無効化、アラート、またはドロップ）を効率的に変更できます。Snort 3 の侵入ポリシーを使用すると、Cisco Talos 提供の基本ポリシーを編集することなく、IPS/IDS システムの動作をより詳細に制御できます。</p> <p>侵入ポリシーを一覧表示するように [ポリシー (Policies)] > [侵入 (Intrusion)] ページが変更されました。新しいポリシーを作成したり、既存のポリシーを表示または編集（グループの追加/削除、セキュリティレベルの割り当て、ルールのアクションの変更など）することができます。複数のルールを選択し、それらのアクションを変更することもできます。さらに、アクセス制御ルールでカスタム侵入ポリシーを選択できます。</p>
侵入イベント用の複数の syslog サーバー。	<p>侵入ポリシー用に複数の syslog サーバーを設定できます。侵入イベントは各 syslog サーバーに送信されます。</p> <p>侵入ポリシー設定ダイアログボックスに、複数の syslog サーバーオブジェクトを選択する機能が追加されました。</p>
URL レピュテーション照合にレピュテーションが不明なサイトを含めることが可能です。	<p>URL カテゴリのトラフィック一致基準を設定し、レピュテーション範囲を選択する場合に、レピュテーションが不明な URL をレピュテーション照合に含めることができます。</p> <p>アクセス制御ルールと SSL 復号ルールの URL レピュテーション基準に [レピュテーションが不明なサイトを含める (Include Sites with Unknown Reputation)] チェックボックスが追加されました。</p>
VPN 機能	
仮想トンネルインターフェイス (VTI) とルートベースのサイト間 VPN。	<p>VPN 接続プロファイルのローカルインターフェイスとして仮想トンネルインターフェイスを使用して、ルートベースのサイト間 VPN を作成できるようになりました。ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウドサービスプロバイダーや大企業の VPN 管理が簡素化されます。</p> <p>インターフェイスのリストのページに [仮想トンネルインターフェイス (Virtual Tunnel Interfaces)] タブが追加され、VTI をローカルインターフェイスとして使用できるように、サイト間 VPN ウィザードが更新されました。</p>

機能	説明
<p>Threat Defense リモートアクセス VPN 接続を行うための Hostscan およびダイナミックアクセスポリシー (DAP) の API サポート。</p>	<p>Hostscan パッケージとダイナミックアクセスポリシー (DAP) ルール XML ファイルをアップロードし、XML ファイルを作成するよう DAP ルールを設定することで、接続中のエンドポイントのステータスに関連する属性に基づいてグループポリシーをリモートユーザーに割り当てる方法を制御することができます。Cisco Identity Services Engine (ISE) がいない場合は、これらの機能を使用して認可変更を実行できます。Hostscan のアップロードと DAP の設定は脅威に対する防御 API を使用してのみ行えます。FDM を使用して設定することはできません。Hostscan および DAP の使用方法の詳細については、AnyConnect のマニュアルを参照してください。</p> <p>dapxml、hostscanpackagefiles、hostscanxmlconfigs、ravpns の各脅威に対する防御 API オブジェクトモデルを追加または変更しました。</p>
<p>外部 CA 証明書の証明書失効チェックの有効化。</p>	<p>脅威に対する防御 API を使用して、特定の外部 CA 証明書の証明書失効チェックを有効にすることができます。失効チェックは、リモートアクセス VPN で使用される証明書に特に役立ちます。FDM を使用して証明書の失効チェックを設定することはできません。脅威に対する防御 API を使用する必要があります。</p> <p>ExternalCACertificate リソースに revocationCheck、crlCacheTime、および oscpDisableNonce 属性が追加されました。</p>
<p>安全性の低い Diffie-Hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートがなくなりました。</p>	<p>アップグレードの影響。アップグレード後の展開ができない場合があります。</p> <p>6.6 で廃止されていた以下の機能が削除されました。それらを IKE プロポーザルまたは IPsec ポリシーで引き続き使用している場合は、アップグレード後にそれらを置き換えないと、設定変更を展開できません。VPN が正しく機能するように、サポートされる DH および暗号化アルゴリズムにアップグレードする前に VPN 設定を変更することをお勧めします。</p> <ul style="list-style-type: none"> • Diffie-Hellman グループ : 2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム : DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます (これが唯一のオプションです)。 • ハッシュアルゴリズム : MD5。
<p>リモートアクセス VPN 用のカスタムポート。</p>	<p>リモートアクセス VPN (RA VPN) 接続に使用するポートを設定できます。RA VPN に使用されているインターフェイスで FDM に接続する必要がある場合は、RA VPN 接続のポート番号を変更できます。FDM が使用するポート 443 は、デフォルトの RA VPN ポートでもあります。</p> <p>RA VPN ウィザードのグローバル設定ステップが更新され、ポート設定が追加されました。</p>

機能	説明
リモートアクセス VPN を認証するための SAML サーバーのサポート。	<p>SAML 2.0 サーバーをリモートアクセス VPN の認証ソースとして設定できます。サポートされている SAML サーバーは次のとおりです : Duo。</p> <p>[オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] ページでのアイデンティティソースとして SAML サーバーが追加され、それを使用できるようにリモートアクセス VPN 接続プロファイルが更新されました。</p>
AnyConnect モジュールプロファイルの Threat Defense API サポート	<p>脅威に対する防御 API を使用して、AMP イネーブラ、ISE ポスチャ、Umbrella といった AnyConnect で使用されるモジュールプロファイルをアップロードできます。これらのプロファイルは、AnyConnect プロファイルエディタパッケージからインストールできるオフラインプロファイルエディタを使用して作成する必要があります。</p> <p>AnyConnectClientProfile モデルに anyConnectModuleType 属性が追加されました。最初はモジュールプロファイルを使用する AnyConnect クライアントプロファイルオブジェクトを作成できますが、FDM で作成されたオブジェクトを変更して正しいモジュールタイプを指定するには、依然として API を使用する必要があります。</p>
ルーティング機能	
スマート CLI による EIGRP のサポート。	<p>アップグレードの影響。アップグレード後の展開ができない場合があります。</p> <p>以前のリリースでは、FlexConfig を使用して、[詳細設定 (Advanced Configuration)] ページで EIGRP を設定しました。今回、[ルーティング (Routing)] ページでスマート CLI を直接使用して EIGRP を設定するようになりました。</p> <p>FlexConfig を使用して EIGRP を設定した場合は、リリース 6.7 にアップグレードするときに、FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、スマート CLI オブジェクトで設定を再作成する必要があります。スマート CLI の更新が完了するまでは、参照用に EIGRP FlexConfig オブジェクトを保持できます。設定は自動的に変換されません。</p> <p>[ルーティング (Routing)] ページに EIGRP スマート CLI オブジェクトが追加されました。</p>
インターフェイス機能	

機能	説明
ISA 3000 ハードウェアバイパスの持続性。	<p>永続化オプションを使用して、ISA 3000 インターフェイスペアのハードウェアバイパスを有効にできるようになりました。電源が回復した後、ハードウェアバイパスは手動で無効にするまで有効のままになります。持続性のないハードウェアバイパスを有効にすると、電源が回復した後にハードウェアバイパスが自動的に無効になります。ハードウェアバイパスが無効になっていると、短時間のトラフィック中断が発生する可能性があります。永続化オプションを使用すると、トラフィックの短時間の中断が発生するタイミングを制御できます。</p> <p>新規/変更された画面 : [デバイス (Device)] > [インターフェイス (Interfaces)] > [ハードウェアバイパス (Hardware Bypass)] > [ハードウェアバイパスの設定 (Hardware Bypass Configuration)]</p>
Firepower 4100/9300 における脅威に対する防御動作リンク状態と物理リンク状態の同期。	<p>Firepower 4100/9300 シャーシでは、脅威に対する防御動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。脅威に対する防御アプリケーションインターフェイスの管理状態は考慮されません。脅威に対する防御からの同期がない場合は、たとえば、脅威に対する防御アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、脅威に対する防御のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。</p> <p>(注) この機能は、Radware vDP デコレータを使用する脅威に対する防御ではサポートされません。</p> <p>新規/変更された シャーシマネージャ 画面 : [Logical Devices] > [Enable Link State]</p> <p>新規/変更された FXOS コマンド : set link-state-sync enabled、show interface expand detail</p> <p>サポートされているプラットフォーム : Firepower 4100/9300</p>
Firepower 1100 および 2100 SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	<p>自動ネゴシエーションを無効にするように Firepower 1100 および 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。</p> <p>新規/変更画面 : [Device] > [Interfaces] > [Edit Interface] > [Advanced Options] > [Speed]</p> <p>サポートされるプラットフォーム : Firepower 1100 および 2100</p>

管理およびトラブルシューティングの機能

機能	説明
<p>失敗した脅威に対する防御ソフトウェアのアップグレードをキャンセルし、以前のリリースに戻す機能。</p>	<p>脅威に対する防御のメジャーソフトウェアアップグレードが失敗するか、正常に機能しない場合は、アップグレードインストールの実行時の状態にデバイスを戻すことができます。</p> <p>FDMの[システムのアップグレード (System Upgrade)]パネルにアップグレードを元に戻す機能が追加されました。アップグレード時に、FDM ログイン画面にアップグレードステータスが表示され、アップグレードが失敗した場合にキャンセルしたり元に戻すためのオプションが表示されます。脅威に対する防御 API に CancelUpgrade、RevertUpgrade、RetryUpgrade、および UpgradeRevertInfo リソースが追加されました。</p> <p>脅威に対する防御 CLI に show last-upgrade status、show upgrade status、show upgrade revert-info、upgrade cancel、upgrade revert、upgrade cleanup-revert、および upgrade retry コマンドが追加されました。</p>
<p>データインターフェイス上の FDM/脅威に対する防御 API アクセス用のカスタム HTTPS ポート。</p>	<p>データインターフェイスで FDM または 脅威に対する防御 API アクセスに使用する HTTPS ポートを変更できます。ポートをデフォルトの 443 から変更することにより、管理アクセスと同じデータインターフェイスで設定されているその他の機能 (リモートアクセス VPN など) の競合を回避できます。管理インターフェイスの管理アクセス HTTPS ポートは変更できないことに注意してください。</p> <p>[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] > [データインターフェイス (Data Interfaces)] ページにポートを変更する機能が追加されました。</p>
<p>Firepower 1000 および 2100 シリーズデバイス上の Cisco Defense Orchestrator のロータッチプロビジョニング。</p>	<p>Cisco Defense Orchestrator (CDO) を使用して新しい脅威に対する防御デバイスを管理する予定がある場合、デバイスセットアップウィザードを完了することなく、または FDM にログインすることさえなく、デバイスを追加できるようになりました。</p> <p>新しい Firepower 1000 および 2100 シリーズ デバイスは、最初に Cisco Cloud に登録され、CDO で簡単に要求できます。CDO に入ると、CDO からデバイスをすぐに管理できます。このロータッチプロビジョニングでは、物理デバイスと直接やりとりする必要性が最小限に抑えられ、ネットワークデバイスに関する経験が浅い従業員が勤務するリモートオフィスなどの場所にとって理想的です。</p> <p>Firepower 1000 および 2100 シリーズ デバイスの初期プロビジョニング方法が変更されました。また、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページに自動登録が追加されました。これにより、FDM を使用して以前に管理していたアップグレード済みデバイスおよびその他のデバイスのプロセスを手動で開始できます。</p>

機能	説明
Threat Defense SNMP 設定の API サポート	<p>アップグレードの影響。アップグレード後の展開ができない場合があります。</p> <p>脅威に対する防御 API を使用して FDM または CDO 管理対象 脅威に対する防御 デバイスで SNMP バージョン 2c または 3 を設定できます。</p> <p>API リソースの SNMPAuthentication、SNMPHost、SNMPSecurityConfiguration、SNMPServer、SNMPUser、SNMPUserGroup、SNMPv2cSecurityConfiguration、および SNMPv3SecurityConfiguration が追加されました。</p> <p>(注)</p> <p>FlexConfig を使用して SNMP を設定した場合は、脅威に対する防御 API SNMP リソースを使用して設定をやり直す必要があります。SNMP を設定するためのコマンドは、FlexConfig では使用できなくなりました。FlexConfig ポリシーから SNMPFlexConfig オブジェクトを削除するだけで、変更を展開できます。その後、API を使用して機能を再設定するときに、それらのオブジェクトを参照として使用できます。</p>
システムに保持されるバックアップファイルの最大数が 10 から 3 に減少。	<p>システムでは、10 個ではなく最大 3 個のバックアップファイルがシステムに保持されます。新しいバックアップが作成されると、最も古いバックアップファイルが削除されます。必要な場合にシステムを回復するために必要なバージョンを入手できるように、バックアップファイルは異なるシステムにダウンロードしてください。</p>
Microsoft Internet Explorer のサポートの終了。	<p>Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。</p>
Threat Defense API バージョンの下位互換性	<p>脅威に対する防御 バージョン 6.7 以降、ある機能の API リソースモデルがリリース間で変更されない場合、脅威に対する防御 API は古い API バージョンに基づくコールを受け入れることができます。機能モデルが変更された場合でも、古いモデルを新しいモデルに変換する論理的な方法があれば、古いコールが機能します。たとえば、v4 コールを v5 システムで受け入れることができます。コールのバージョン番号として「latest (最新)」を使用する場合、「古い」コールは、このシナリオでは v5 コールとして解釈されるため、下位互換性を利用するかどうかは、API コールの構築方法によって決まります。</p>
Threat Defense REST API バージョン 6 (v6)。	<p>ソフトウェアバージョン 6.7 用の 脅威に対する防御 REST API はバージョン 6 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。</p> <p>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション (More options)] ボタン (⋮) をクリックし、[API エクスプローラ (API Explorer)] を選択します。</p>

FDM バージョン 6.6.x の機能

表 8: FDM バージョン 6.6.x の機能

機能	説明
プラットフォーム機能	
Amazon Web Services (AWS) クラウド用 Threat Defense Virtual における Device Manager のサポート。	Device Manager を使用して AWS クラウド用 Threat Defense Virtual で脅威に対する防御を設定できます。
Firepower 4112 用 Device Manager。	Firepower 4112 用脅威に対する防御が導入されました。 (注) FXOS 2.8.1 が必要です。
VMware 向け FTDv の e1000 インターフェイス。	アップグレードされないようにします。 バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できません。 詳細については、『 Cisco Secure Firewall Threat Defense Virtual スタートアップガイド 』を参照してください。
ファイアウォールと IPS の機能	
デフォルトでは無効になっている、侵入ルールを有効にする機能。	各システム定義の侵入ポリシーには、デフォルトで無効になっているルールがいくつかあります。以前は、これらのルールのアクションをアラートまたはドロップに変更できませんでした。現在では、デフォルトで無効になっているルールのアクションを変更できるようになりました。 [侵入ポリシー (Intrusion Policy)] ページが変更され、デフォルトで無効になっているルールもすべて表示されるようになりました。また、これらのルールのアクションも編集できます。

機能	説明
<p>侵入ポリシーの侵入検知システム (IDS) モード。</p>	<p>侵入検知システム (IDS) モードで動作するように侵入ポリシーを設定できるようになりました。IDS モードでは、アクティブな侵入ルールは、ルールアクションがドロップであってもアラートのみを発行します。したがって、侵入ポリシーをネットワーク内でアクティブな防御ポリシーにする前に、その侵入ポリシーの動作をモニタリングまたはテストできます。</p> <p>Device Manager では、[Policies] > [Intrusion] ページの各侵入ポリシーに、検査モードの表示が追加されました。また [Edit] リンクが追加され、モードを変更できるようになりました。</p> <p>脅威に対する防御 API では、IntrusionPolicy リソースに <code>inspectionMode</code> 属性が追加されました。</p>
<p>脆弱性データベース (VDB)、地理位置情報データベース、および侵入ルールの更新パッケージを手動でアップロードするためのサポート。</p>	<p>VDB、地理位置情報データベース、および侵入ルールの更新パッケージを手動で取得し、Device Manager を使用してワークステーションから脅威に対する防御デバイスにアップロードできるようになりました。たとえば、Device Manager で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。</p> <p>ワークステーションからファイルを選択してアップロードできるように、[デバイス (Device)] > [更新 (Updates)] ページが更新されました。</p>
<p>脅威に対する防御時間に基づいて制限されているアクセス制御ルールの API サポート。</p>	<p>脅威に対する防御 API を使用して、時間範囲オブジェクトを作成できます。このオブジェクトでは、1 回限りの時間範囲または繰り返しの時間範囲を指定します。オブジェクトはアクセス制御ルールに適用します。時間範囲を使用すると、特定の時間帯または一定期間にわたってトラフィックにアクセス制御ルールを適用して、ネットワークを柔軟に使用できます。Device Manager を使用して時間範囲を作成したり、適用したりはできません。また、アクセス制御ルールに時間範囲が適用されている場合、Device Manager は表示されません。</p> <p>TimeRangeObject、Recurrence、TimeZoneObject、DayLightSavingDateRange、および DayLightSavingDayRecurrence リソースが脅威に対する防御 API に追加されました。時間範囲をアクセス制御ルールに適用するために、timeRangeObjects 属性が accessrules リソースに追加されました。さらに、GlobalTimeZone および TimeZone リソースに変更が加えられました。</p>

機能	説明
アクセス コントロール ポリシーのオブジェクトグループ検索。	<p>動作中、脅威に対する防御 デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、Device Manager にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。</p> <p>Device Manager では、FlexConfig を使用して object-group-search access-control コマンドを有効にする必要があります。</p>
VPN 機能	
サイト間 VPN のバックアップピア（脅威に対する防御 API のみ）。	<p>脅威に対する防御 API を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。</p> <p>バックアップピアのもう 1 つの主な用途は、プライマリハブやバックアップハブなど、トンネルのもう一方の端に 2 つの異なるデバイスがある場合です。通常、システムはプライマリハブへのトンネルを確立します。VPN 接続が失敗すると、システムはバックアップハブとの接続を自動的に再確立できます。</p> <p>SToSConnectionProfile リソースで outsideInterface に対して複数のインターフェイスを指定できるように、脅威に対する防御 API が更新されました。また、BackupPeer リソースと remoteBackupPeers 属性が SToSConnectionProfile リソースに追加されました。</p> <p>Device Manager を使用してバックアップピアを設定したり、バックアップピアの存在を Device Manager に表示したりはできません。</p>
リモートアクセス VPN での Datagram Transport Layer Security (DTLS) 1.2 のサポート。	<p>リモートアクセス VPN で DTLS 1.2 を使用できるようになりました。これは、脅威に対する防御 API のみを使用して設定できます。Device Manager を使用して設定することはできません。ただし、DTLS 1.2 はデフォルトの SSL 暗号グループの一部になったため、グループポリシーの AnyConnect 属性で Device Manager を使用して DTLS の一般的な使用が可能になりました。DTLS 1.2 は、ASA 5508-X または 5516-X モデルではサポートされていないことに注意してください。</p> <p>DTLSV1_2 を列挙値として受け入れるように sslcipher リソースの protocolVersion 属性が更新されました。</p>

機能	説明
<p>安全性の低い Diffie-hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートを廃止。</p>	<p>次の機能は廃止されており、将来のリリースでは削除されます。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。これらの機能から移行し、実用可能になったらすぐにより強力なオプションを使用してください。</p> <ul style="list-style-type: none"> • Diffie-Hellman グループ : 2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム : DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム : MD5。
<p>ルーティング機能</p>	
<p>仮想ルータと Virtual Routing and Forwarding (VRF) -Lite。</p>	<p>複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。</p> <p>仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP (MBGP) をサポートしていません。</p> <p>[ルーティング (Routing)] ページが変更され、仮想ルータを有効化できるようになりました。有効にすると、[ルーティング (Routing)] ページに仮想ルータのリストが表示されます。仮想ルータごとに個別のスタティックルートとルーティングプロセスを設定できます。</p> <p>また、[vrf name all] キーワードセットを次の CLI コマンドに追加し、必要に応じて出力が仮想ルータ情報を表示するよう変更しました。 clear ospf、clear route、ping、show asp table routing、show bgp、show ipv6 route、show ospf、show route、show snort counters</p> <p>show vrf コマンドが追加されました。</p>
<p>OSPF および BGP の設定を [Routing] ページに移動しました。</p>	<p>以前のリリースでは、スマート CLI を使用して、[詳細設定 (Advanced Configuration)] ページで OSPF と BGP を設定しました。これらのルーティングプロセスは、これまでと同様にスマート CLI を使って設定しますが、そのオブジェクトを [ルーティング (Routing)] ページで直接使用できるようになりました。これにより、仮想ルータごとにプロセスを簡単に設定できます。</p> <p>OSPF および BGP スマート CLI オブジェクトは、[詳細設定 (Advanced Configuration)] ページでは使用できなくなりました。6.6 にアップグレードする前に、これらのオブジェクトを設定した場合は、アップグレード後に [ルーティング (Routing)] ページでそれらのオブジェクトを見つけることができます。</p>

機能	説明
高可用性機能	
<p>高可用性 (HA) ペアのスタンバイ装置にログインする外部認証ユーザーの制限を削除。</p>	<p>以前は、外部認証されたユーザーは HA ペアのスタンバイユニットに直接ログインできませんでした。スタンバイユニットへのログインが可能になる前は、ユーザーは最初にアクティブ装置にログインしてから、設定を展開する必要がありました。</p> <p>この制約は削除されました。外部認証されたユーザーは、有効なユーザー名/パスワードを提供している限り、アクティブ装置にログインしていない場合でも、スタンバイ装置にログインできます。</p>
<p>脅威に対する防御 API の BreakHAStatus リソースによって、インターフェイスがどのように処理されるかが変更。</p>	<p>以前は、 clearIntfs クエリパラメータを含めて、高可用性 (HA) 設定を中断するデバイス上のインターフェイスの動作ステータスを制御できました。</p> <p>バージョン 6.6 以降では、 clearIntfs クエリパラメータの代わりに使用する新しい属性 interfaceOption があります。この属性は、アクティブノードで使用する場合はオプションですが、非アクティブノードで使用する場合は必須です。次の 2 つのオプションのいずれかを選択できます。</p> <ul style="list-style-type: none"> • DISABLE_INTERFACES (デフォルト) : スタンバイデバイス (またはこのデバイス) 上のすべてのデータインターフェイスが無効になります。 • ENABLE_WITH_STANDBY_IP : インターフェイスにスタンバイ IP アドレスを設定すると、スタンバイデバイス (またはこのデバイス) 上のインターフェイスがスタンバイアドレスを使用するよう再設定されます。スタンバイアドレスを持たないインターフェイスはすべて無効になります。 <p>デバイスが正常なアクティブ/スタンバイ状態になっているときにアクティブノードで [HA の中断 (Break HA)] を使用すると、この属性がスタンバイノードのインターフェイスに適用されます。アクティブ/アクティブまたは一時停止などのその他の状態では、この属性が中断を開始するノードに適用されません。</p> <p>clearIntfs クエリパラメータを使用する場合、 clearIntfs=true は interfaceOption=DISABLE_INTERFACES のように動作します。つまり、 clearIntfs=true のアクティブ/スタンバイペアを中断すると、両方のデバイスが無効にはならなくなり、スタンバイデバイスのみが無効になります。</p> <p>Device Manager を使用して HA を中断すると、インターフェイスオプションには常に DISABLE_INTERFACES が設定されます。スタンバイ IP アドレスを使用してインターフェイスを有効にすることはできません。異なる結果が必要な場合は、API エクスプローラから API コールを使用します。</p>

機能	説明
高可用性の問題の直近の失敗理由を [高可用性 (High Availability)] ページに表示。	高可用性 (HA) が何らかの理由で失敗した場合 (アクティブデバイスが使用できなくなり、スタンバイデバイスにフェールオーバーするなど)、直近の失敗の理由がプライマリデバイスとセカンダリデバイスのステータス情報の下に表示されます。この情報には、イベントの UTC 時刻が含まれます。
インターフェイス機能	
PPPoE のサポート。	<p>ルーテッドインターフェイスの PPPoE を設定できるようになりました。PPPoE は、ハイアベイラビリティ ユニットではサポートされません。</p> <p>新規/変更された画面 : [デバイス (Device)] > [インターフェイス (Interfaces)] > [編集 (Edit)] > [IPv4 アドレス (IPv4 Address)] > [タイプ (Type)] > [PPPoE]</p> <p>新規/変更されたコマンド : show vpdn group、show vpdn username、show vpdn session pppoe state</p>
デフォルトでは DHCP クライアントとして機能する管理インターフェイス。	<p>管理インターフェイスは、192.168.45.45 IP アドレスを使用する代わりに、デフォルトでは DHCP から IP アドレスを取得するように設定されています。この変更により、既存のネットワークに脅威に対する防御を簡単に展開できるようになりました。この機能は、Firepower 4100/9300 (論理デバイスを展開するときに IP アドレスを設定する) と Threat Defense Virtual および ISA 3000 (現在も 192.168.45.45 IP アドレスを使用) を除くすべてのプラットフォームに適用されます。管理インターフェイス上の DHCP サーバーも有効にならなくなりました。</p> <p>デフォルト (192.168.1.1) では、デフォルトの内部 IP アドレスに引き続き接続できます。</p>
Device Manager 管理接続の HTTP プロキシサポート。	<p>Device Manager 接続で使用するために、管理インターフェイスの HTTP プロキシを設定できるようになりました。手動およびスケジュールされたデータベースの更新を含むすべての管理接続は、プロキシを通過します。</p> <p>設定するための [システム設定 (System Setting)] > [HTTP プロキシ (HTTP Proxy)] ページが追加されました。さらに、HTTPProxy リソースが脅威に対する防御 API に追加されました。</p>
管理インターフェイスの MTU の設定。	<p>管理インターフェイスの MTU を最大 1500 バイトに設定できるようになりました。デフォルト値は 1500 バイトです。</p> <p>新規/変更されたコマンド : configure network mtu、configure network management-interface mtu-management-channel</p> <p>変更された画面はありません。</p>
ライセンス機能	

機能	説明
スマートライセンスとクラウドサービスの登録は分離され、登録を個別に管理可能	<p>スマートライセンスアカウントではなく、セキュリティアカウントを使用して、クラウドサービスを登録できるようになりました。Cisco Defense Orchestrator を使用してデバイスを管理する場合は、セキュリティアカウントを使用して登録することを推奨します。スマートライセンスから登録解除せずに、クラウドサービスから登録解除することもできます。</p> <p>[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページの動作を変更し、クラウドサービスから登録解除する機能を追加しました。さらに、このページから Web 分析機能が削除されました。この機能は、[システム設定 (System Settings)] > [Web 分析 (Web Analytics)] ページに移動しました。脅威に対する防御 API では、新しい動作を反映するように CloudServices リソースが変更されました。</p>
パーマネントライセンス予約のサポート。	<p>インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのために Cisco Smart Software Manager (CSSM) に直接登録することはできません。この場合は、ユニバーサルパーマネントライセンス予約 (PLR) モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせ、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。ISA 3000 はユニバーサル PLR をサポートしていません。</p> <p>[デバイス (Device)] > [スマートライセンス (Smart License)] ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。脅威に対する防御 API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。</p>
管理およびトラブルシューティングの機能	
ISA 3000 デバイスの高精度時間プロトコル (PTP) 設定用 Device Manager 直接サポート。	<p>Device Manager を使用して、ISA 3000 デバイスで高精度時間プロトコル (PTP) を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。以前のリリースでは、PTP を設定するために FlexConfig を使用する必要がありました。</p> <p>同じ [システム設定 (System Settings)] ページの PTP と NTP をグループ化し、[システム設定 (System Settings)] > [NTP] ページの名前を [タイムサービス (Time Services)] に変更しました。また、PTP リソースが脅威に対する防御 API に追加されました。</p>

機能	説明
Device Manager 管理 Web サーバー証明書の信頼チェーン検証。	<p>Device Manager Web サーバーの非自己署名証明書を設定する場合は、すべての中間証明書とルート証明書を信頼チェーンに含める必要があります。システムはチェーン全体を検証します。</p> <p>[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] ページの [管理Webサーバー (Management Web Server)] タブに、チェーン内の証明書を選択する機能が追加されました。</p>
バックアップファイルの暗号化のサポート。	<p>パスワードを使用して、バックアップファイルを暗号化できるようになりました。暗号化されたバックアップを復元するには、正しいパスワードを指定する必要があります。</p> <p>定期的なジョブ、スケジュール済みジョブ、および手動ジョブのバックアップファイルを暗号化するかどうかを選択し、復元時にパスワードを提供する機能が、[デバイス (Device)] > [バックアップと復元 (Backup and Restore)] ページに追加されました。また、encryptArchive 属性と encryptionKey 属性が BackupImmediate と BackupSchedule リソースに追加され、encryptionKey が脅威に対する防御 API の RestoreImmediate リソースに追加されました。</p>
クラウドサービスで使用するために Cisco Cloud に送信するイベントを選択するサポート。	<p>Cisco Cloud にイベントを送信するようデバイスを設定すると、送信するイベントのタイプ（侵入、ファイル/マルウェア、接続）を選択できるようになりました。接続イベントの場合、すべてのイベントを送信することも、優先順位の高いイベント（侵入、ファイル、またはマルウェアイベントをトリガーする接続に関連するもの、またはセキュリティインテリジェンスブロッキングポリシーと一致するもの）を送信することもできます。</p> <p>[Cisco Cloudへのイベントの送信を有効にする (Send Events to the Cisco Cloud Enable)] ボタンが機能するよう変更されました。この機能は、[システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページにあります。</p>
脅威に対する防御 REST API バージョン 5 (v5)。	<p>ソフトウェアバージョン 6.6 用の脅威に対する防御 REST API のバージョン番号が 5 になりました。API URL の v1/v2/v3/v4 を v5 に置き換える必要があります。または、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示します。</p> <p>v5 の API には、ソフトウェアバージョン 6.6 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン (⋮) をクリックし、[API Explorer] を選択します。</p>

FDM バージョン 6.4.x の機能

表 9: FDM バージョン 6.4.x の機能

機能	説明
Firepower 1000 シリーズ デバイス設定	<p>Device Manager を使用して、Firepower 1000 シリーズ デバイス上の脅威に対する防御を設定できます。</p> <p>Power over Ethernet (PoE) ポートを通常のイーサネットポートとして使用することはできますが、PoEに関連するプロパティを有効にしたり設定することはできないことにご注意ください。</p>
ISA 3000 のハードウェア バイパス	<p>ISA 3000 のハードウェアバイパスは、[デバイス (Device)] > [インターフェイス (Interfaces)] ページで設定できるようになりました。リリース 6.3 では、FlexConfig を使用してハードウェアバイパスを設定する必要がありました。FlexConfig を使用している場合は、[Interfaces] ページで設定をやり直し、FlexConfig からハードウェアバイパスコマンドを削除してください。ただし、TCP シーケンス番号のランダム化の無効化専用の FlexConfig の部分は引き続き推奨されます。</p>
Device Manager CLI コンソールからシステムを再起動およびシャットダウンする機能	<p>Device Manager で CLI コンソールを使用して reboot コマンドと shutdown コマンドを発行できるようになりました。以前は、システムを再起動またはシャットダウンするために、デバイスに対して個別の SSH セッションを開く必要がありました。これらコマンドを使用するには、管理者権限が必要です。</p>
RADIUS を使用した脅威に対する防御 CLI ユーザーの外部認証および認可。	<p>脅威に対する防御 CLI にログインするユーザーを、外部 RADIUS サーバーを使用して認証および認可できます。外部ユーザーに設定 (管理者) または基本 (読み取り専用) のアクセス権を付与できます。</p> <p>[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] ページの [AAA設定 (AAA Configuration)] タブに SSH 設定を追加しました。</p>
ネットワーク範囲オブジェクトとネストされたネットワークグループオブジェクトのサポート	<p>IPv4 アドレスまたは IPv6 アドレスの範囲を指定するネットワークオブジェクトと、その他のネットワークグループ (つまりネストされたグループ) を含むネットワークグループオブジェクトを作成できるようになりました。</p> <p>これらの機能を含むようにネットワークオブジェクトとネットワークグループオブジェクトの [Add/Edit] ダイアログボックスを変更し、そのタイプのアドレス指定がポリシーの文脈の中で合理的か否かを条件として、これらのオブジェクトを使用できるようにさまざまなセキュリティポリシーを変更しました。</p>

機能	説明
オブジェクトとルールの全文検索オプション	<p>オブジェクトおよびルールでは、全文検索を実行できます。多数の項目を含むポリシーまたはオブジェクトリストを検索することで、ルールまたはオブジェクト内の任意の場所で検索文字列を含むすべての項目を検索できます。</p> <p>ルールを持つすべてのポリシーと [Object] リストのすべてのページに検索ボックスを追加しました。さらに、API でサポートされているオブジェクトの GET コールで filter=fts~search-string オプションを使用して、全文検索に基づいて項目を取得できます。</p>
Device Manager 管理対象 脅威に対する 防御 デバイスでサポートされている API バージョンのリストの取得	<p>GET/api/versions (ApiVersions) メソッドを使用して、デバイスでサポートされる API バージョンのリストを取得できます。API クライアントを使用すると、サポートされるバージョンで有効なコマンドとシンタックスを使用したデバイスへの通信および設定を行うことができます。</p>
アクセス制御ルールのヒットカウント	<p>アクセス制御ルールのヒットカウントを表示できます。ヒットカウントには、接続がルールに一致した頻度が示されます。</p> <p>ヒットカウント情報が含まれるようにアクセスコントロールポリシーを更新しました。脅威に対する防御 API では、HitCounts リソースと、includeHitCounts オプションおよび filter=fetchZeroHitCounts オプションを GET アクセスポリシールールのリソースに追加しました。</p>
ダイナミックアドレス指定と証明書認証のためのサイト間 VPN の強化	<p>ピアの認証に事前共有キーではなく証明書を使用したサイト間 VPN 接続を設定できるようになりました。リモートピアに不明な (ダイナミック) IP アドレスがある接続も設定できます。サイト間 VPN ウィザードと IKEv1 ポリシーオブジェクトにオプションが追加されました。</p>
リモートアクセス VPN での RADIUS サーバーと認可変更のサポート	<p>リモートアクセス VPN (RA VPN) ユーザーの認証、認可、およびアカウントリングに RADIUS サーバーを使用できるようになりました。また、Cisco ISERADIUS サーバーの使用時に認証後にユーザーの認可を変更するために、ダイナミック認証とも呼ばれる Change of Authentication (CoA) を設定できます。</p> <p>RADIUS サーバーとサーバーグループオブジェクトに属性を追加し、RA VPN 接続プロファイル内の RADIUS サーバーグループを選択できるようになりました。</p>
リモートアクセス VPN の複数の接続プロファイルとグループポリシー	<p>複数の接続プロファイルを設定し、そのプロファイルで使用するグループポリシーを作成できます。</p> <p>接続プロファイルおよびグループポリシーが別々のページとなるように [デバイス (Device)] > [リモートアクセス VPN (Remote Access VPN)] ページを変更し、グループポリシーを選択できるように RA VPN 接続ウィザードを更新しました。以前にウィザードで設定した項目の一部は、グループポリシーで設定するようになります。</p>

機能	説明
証明書ベースの2番目の認証ソース、およびリモートアクセスVPNでの二要素認証のサポート	<p>ユーザー認証に証明書を使用したり、接続を確立する前にユーザーを2回認証する必要があるセカンダリ認証ソースを設定することができます。また、2つ目の要素としてRSA トークンまたは Duo パスコードを使用して二要素認証を設定できます。</p> <p>これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。</p>
複数のアドレス範囲を持つIPアドレスプールとリモートアクセスVPN向けのDHCPアドレスプールのサポート。	<p>サブネットを指定する複数のネットワークオブジェクトを選択することで、複数のアドレス範囲を持つアドレスプールを設定できるようになりました。さらに、DHCPサーバーでアドレスプールを設定し、そのサーバーを使用してRA VPN クライアントにアドレスを提供できます。認可にRADIUSを使用する場合は、代わりにRADIUSサーバーでアドレスプールを設定できます。</p> <p>これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。必要に応じて、接続プロファイルではなくグループポリシーでアドレスプールを設定できます。</p>
Active Directory レルムの強化	<p>1つのレルムに最大10の冗長Active Directory (AD) サーバーを含められるようになりました。また、複数のレルムを作成したり、不要になったレルムを削除できます。さらに、レルム内のユーザーのダウンロードの制限は、以前のリリースの2,000から50,000に増えています。</p> <p>複数のレルムとサーバーをサポートするように、[オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] ページを更新しました。レルム内のすべてのユーザーにルールを適用するため、アクセス制御とSSL復号化ルール of ユーザーの基準でレルムを選択することができます。アイデンティティルールとRA VPN接続プロファイルでレルムを選択することもできます。</p>
ISE サーバーの冗長性サポート	<p>パッシング認証向けのIDソースとしてCisco Identity Services Engine (ISE) を設定する際に、ISE ハイアベイラビリティ設定がある場合は、セカンダリISEサーバーを設定できるようになりました。</p> <p>ISE アイデンティティ オブジェクトにセカンダリサーバーの属性が追加されました。</p>
ファイル/マルウェア イベントを外部syslogサーバーに送信	<p>アクセス制御ルールで設定されたファイルポリシーによって生成されるファイル/マルウェアイベントを受信するように、外部syslogサーバーを設定できるようになりました。ファイルイベントはメッセージID430004を使用し、マルウェアイベントは430005を使用します。</p> <p>ファイル/マルウェア syslog サーバーのオプションが [デバイス (Device)] > [システム設定 (System Settings)] > [ログの設定 (Logging Settings)] ページに追加されました。</p>

機能	説明
内部バッファのログおよびカスタムイベントのログフィルタのサポート	<p>内部バッファをシステムロギングの宛先として設定できるようになりました。さらに、イベントログフィルタを作成して、syslog サーバーおよび内部バッファロギングの宛先に対して生成されるメッセージをカスタマイズできます。</p> <p>イベント ログ フィルタ オブジェクトを [オブジェクト (Objects)] ページに追加し、オブジェクトを使用する機能を [デバイス (Device)] > [システム設定 (System Settings)] > [ログの設定 (Logging Settings)] ページに追加しました。内部バッファ オプションも [ログの設定 (Logging Settings)] ページに追加しました。</p>
Device Manager Web サーバーの証明書	<p>Device Manager の設定インターフェイスへの HTTPS 接続に使用される証明書を設定できるようになりました。Web ブラウザがすでに信頼している証明書をアップロードすることで、デフォルトの内部証明書を使用するときに、Untrusted Authority メッセージを回避できます。[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] > [管理 Web サーバー (Management Web Server)] ページが追加されました。</p>
Cisco Threat Response のサポート	<p>Cisco Threat Response のクラウドベースのアプリケーションに侵入イベントを送信するようにシステムを設定できます。Cisco Threat Response は侵入分析に使用できます。</p> <p>Cisco Threat Response を [デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページに追加しました。</p>
VDB、GeoDB、および SRU 更新の手動アップロード。	<p>VDB、地理位置情報データベース、および侵入ルールの更新パッケージを手動で取得し、FDM を使用してワークステーションから FTD デバイスにアップロードできるようになりました。たとえば、FDM で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。</p> <p>ワークステーションからファイルを選択してアップロードできるように、[Device] > [Updates] ページが更新されました。</p> <p>最小 FTD : 6.4.0.10。</p> <p>バージョンの制限 : この機能はバージョン 6.5 では使用できません。バージョン 6.6 でサポートが再開されています。</p>

機能	説明
メモリが少ないデバイス用の小規模 VDB。	<p>VDB363以降では、メモリが少ないデバイスに小規模VDB（別称：<i>VDB lite</i>）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。</p> <p>最小 FTD：6.4.0.17</p> <p>メモリが少ないデバイス：ASA-5508-X、ASA-5515-X、ASA-5516-X、ASA-5525-X、および ASA-5545-X</p> <p>バージョンの制限：小規模 VDB は、すべてのバージョンでサポートされているわけではありません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードする場合、メモリの少ないデバイスに VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。</p>
ユニバーサル永久ライセンス予約 (PLR) モード。	<p>インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのために Cisco Smart Software Manager (CSSM) に直接登録することはできません。この場合は、ユニバーサルパーマネントライセンス予約 (PLR) モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせ、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。</p> <p>[Device]> [Smart License] ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。FTD API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。</p> <p>最小 FTD：6.4.0.10。この機能はバージョン 6.5 で一時的に廃止になりましたが、バージョン 6.6 で戻ります。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.6 以降に直接アップグレードすることをお勧めします。</p>

機能	説明
デフォルトのHTTPSサーバー証明書。	<p>アップグレードの影響。</p> <p>パッチを適用すると、デバイスの現在のデフォルトのHTTPSサーバー証明書が更新される場合があります。証明書は、生成日に応じて、次の期限が設定されています。</p> <ul style="list-style-type: none"> • 6.5.0.5 以降 : 800 日 • 6.5.0 ~ 6.5.0.4 : 3 年 • 6.4.0.9 以降のパッチ : 800 日 • 6.4.0 ~ 6.4.0.8 : 3 年 • 6.3.0 およびすべてのパッチ : 3 年 • 6.2.3 : 20 年
新しい syslog フィールド。	<p>次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。</p> <ul style="list-style-type: none"> • センサー UUID • 最初のパケット時間 • 接続インスタンス ID • 接続数カウンタ <p>これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。</p> <p>最小 FTD : 6.4.0.4</p>
Threat Defense REST API バージョン 3 (v3)	<p>ソフトウェア バージョン 6.4 向けの脅威に対する防御 REST API のバージョン番号が 3 になりました。API URL の v1/v2 は v3 で置き換える必要があります。v3 の API には、ソフトウェアバージョン 6.4 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、ログインした後に、Device Manager の URL の最後を #/api-explorer に変更します。</p>

FDM バージョン 6.3.x の機能

表 10: FDM バージョン 6.3.x の機能

機能	説明 (Description)
高可用性設定。	2つのデバイスをアクティブ/スタンバイ高可用性ペアとして設定できます。ハイアベイラビリティまたはフェールオーバーセットアップは、プライマリデバイスの障害時にセカンダリデバイスで引き継ぐことができるように、2つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。デバイスは、同じモデルで、同じ数と同じタイプのインターフェイスを備えており、同じソフトウェアバージョンを実行している必要があります。ハイアベイラビリティは [デバイス (Device)] ページから設定できます。
パッシブユーザーアイデンティティ取得のサポート。	パッシブ認証を使用するようにアイデンティティポリシーを設定できます。パッシブ認証では、ユーザにユーザ名とパスワードを求めることなくユーザアイデンティティを収集します。システムは、ユーザーが指定したアイデンティティソース (Cisco Identity Services Engine (ISE) /Cisco Identity Services Engine Passive Identity Connector (ISE PIC) を指定可能) からマッピングを取得します。または、リモートアクセスVPNユーザーからログインを取得します。 変更には、[ポリシー (Policies)] > [アイデンティティ (Identity)] でのパッシブ認証ルールをサポートと、または [オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] の ISE 設定が含まれます。
リモートアクセスVPNおよびユーザーアイデンティティに関するローカルユーザーのサポート。	Device Manager で直接ユーザーを作成できるようになりました。その後、これらのローカルユーザーアカウントを使用して、リモートアクセスVPNへの接続を認証できます。ローカルユーザデータベースは、プライマリまたはフォールバック認証ソースとして使用できます。さらに、ローカルユーザー名がダッシュボードに反映され、それらをポリシーでのトラフィック照合に利用できるように、アイデンティティポリシーでパッシブ認証ルールを設定できます。 [オブジェクト (Objects)] > [ユーザー (Users)] ページが追加されました。また、リモートアクセスVPNウィザードが更新され、フォールバックオプションが追加されました。

機能	説明 (Description)
<p>アクセスコントロールポリシーでのVPNトラフィック処理のデフォルト動作の変更 (sysopt connection permit-vpn)。</p>	<p>アクセスコントロールポリシーによるVPNトラフィックの処理方法に対するデフォルト動作が変更されました。6.3以降では、アクセスコントロールポリシーによりすべてのVPNトラフィックが処理されるのがデフォルトです。これにより、URLフィルタリング、侵入防御、およびファイルポリシーを含む高度なインスペクションをVPNトラフィックに適用することができます。VPNトラフィックを許可するアクセス制御ルールを設定する必要があります。または、FlexConfigを使用してsysopt connection permit-vpn コマンド設定することもできます。このコマンドは、VPN終端トラフィックがアクセスコントロールポリシー（および高度なインスペクション）をバイパスするようにシステムに指示します。</p>
<p>FQDNベースのネットワークオブジェクトのサポートと、DNSルックアップに関するデータインターフェイスのサポート。</p>	<p>静的IPアドレスではなく完全修飾ドメイン名 (FQDN) によってホストを指定するネットワークオブジェクト（およびグループ）を作成できるようになりました。システムは、アクセス制御ルールで使用されるFQDNオブジェクトに関して、FQDNからIPアドレスへのマッピングのルックアップを定期的に行います。これらのオブジェクトはアクセス制御ルールのみで使用できます。</p> <p>オブジェクトページにDNSグループオブジェクトが追加されました。また、[システム設定 (System Settings)] > [DNSサーバー (DNS Server)] ページが、データインターフェイスにグループを割り当てられるように変更され、アクセス制御ルールが、FQDNネットワークオブジェクトを選択できるように変更されました。さらに、管理インターフェイスのDNS設定では、DNSサーバーアドレスのセットリストの代わりにDNSグループが使用されるようになりました。</p>
<p>TCP Syslogのサポートと、管理インターフェイスを介して診断Syslogメッセージを送信する機能。</p>	<p>以前のリリースでは、診断Syslogメッセージは（接続および侵入メッセージとは対照的に）常にデータインターフェイスを使用していました。すべてのメッセージが管理インターフェイスを使用するようにSyslogを設定できるようになりました。最終的な送信元IPアドレスは、データインターフェイスを管理インターフェイスのゲートウェイとして使用するかどうかによって異なります。使用する場合は、IPアドレスがデータインターフェイスのものになります。UDPではなくTCPをプロトコルとして使用するようにSyslogを設定することもできます。</p> <p>[オブジェクト (Objects)] > [Syslogサーバー (Syslog Servers)] から Syslogサーバーを追加/編集できるようにダイアログボックスが変更されました。</p>

機能	説明 (Description)
RADIUS を使用した Device Manager ユーザーの外部認証および認可。	<p>Device Manager にログインするユーザーを、外部 RADIUS サーバーを使用して認証および認可できます。外部ユーザーに、管理者アクセス権、読み取り/書き込みアクセス権、または読み取り専用アクセス権を付与できます。Device Manager は5つの同時ログインをサポートでき、6番目のセッションは、最も古いセッションから自動的にログオフされます。必要に応じて、Device Manager のユーザーセッションを強制的に終了させることができます。</p> <p>[オブジェクト (Objects)] > [アイデンティティソース (Identity Sources)] ページに RADIUS サーバーおよび RADIUS サーバークラスオブジェクトが追加され、それらのオブジェクトを設定できるようになりました。[デバイス (Device)] > [システム設定 (System Settings)] > [管理アクセス (Management Access)] に [AAA設定 (AAA Configuration)] タブが追加され、サーバークラスを使用できるようになりました。さらに、[モニタリング (Monitoring)] > [セッション (Sessions)] ページにはアクティブユーザーのリストが表示され、管理ユーザーはセッションを終了させることができます。</p>
保留中の変更のビューと展開の改善。	<p>展開ウィンドウが変更され、展開される保留中の変更がより明確に表示されるようになりました。また、変更を破棄し、変更をクリップボードにコピーして、変更を YAML 形式のファイルでダウンロードするオプションが追加されました。さらに、監査ログで見つけることができるように、展開ジョブに名前を付けることが可能になりました。</p>
監査ログ。	<p>展開、システムタスク、設定の変更、管理ユーザーのログイン/ログアウトなどのイベントを記録する監査ログを表示できます。[デバイス (Device)] > [デバイス管理 (Device Administration)] > [監査ログ (Audit Log)] ページが追加されました。</p>
設定をエクスポートする機能。	<p>記録を保持するためにデバイス設定のコピーをダウンロードできます。ただし、この設定をデバイスにインポートすることはできません。この機能は、バックアップ/復元に代わるものではありません。[デバイス (Device)] > [デバイス管理 (Device Administration)] > [設定のダウンロード (Download Configuration)] ページが追加されました。</p>
未知の URL に関する URL フィルタリングの改善。	<p>アクセス制御ルールでカテゴリベースの URL フィルタリングを実行する場合、ユーザは、カテゴリとレピュテーションが URL データベースに定義されていない URL にアクセスする可能性があります。以前は、Cisco Collective Security Intelligence (CSI) からそれらの URL のカテゴリとレピュテーションのルックアップを実行するオプションを手動で有効にする必要がありました。現在は、このオプションがデフォルトで有効になっています。さらに、ルックアップの結果に関して持続可能時間 (TTL) を設定できるようになりました。これにより、システムは、未知の URL ごとにカテゴリまたはレピュテーションを更新できるようになりました。[デバイス (Device)] > [システム設定 (System Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] ページが更新されました。</p>

機能	説明 (Description)
デフォルトで、セキュリティインテリジェンス ロギングが有効になりました。	セキュリティ インテリジェンス ポリシーは 6.2.3 で導入され、ロギングはデフォルトで無効になっていました。6.3.0 以降、ロギングはデフォルトで有効になります。6.2.3 からアップグレードした場合、ロギング設定は有効または無効なまま保持されます。ポリシー適用の結果を表示したい場合は、ロギングを有効にします。
パッシブ モード インターフェイス。	<p>インターフェイスはパッシブ モードで設定できます。パッシブに機能する場合、インターフェイスは (ハードウェア デバイスの) スイッチそのものまたは (Threat Defense Virtual の) プロミスキャス VLAN に設定されたモニタリングセッションで送信元ポートからのトラフィックを単にモニターします。</p> <p>パッシブ モードを使用すると、アクティブなファイアウォールとして展開した場合の Threat Defense Virtual デバイスの動作を評価できます。また、IDS (侵入検知システム) サービスが必要な実稼働ネットワーク (脅威について知る必要があるが、デバイスに脅威をアクティブに防止させない) でパッシブ インターフェイスを使用できます。物理インターフェイスの編集時やセキュリティゾーンの作成時にパッシブ モードを選択できます。</p>
OSPF に関する Smart CLI の機能拡張と、BGP のサポート。	Smart CLI の OSPF 設定機能が拡張されました。これには、標準/拡張 ACL、ルートマップ、AS パス オブジェクト、IPv4/IPv6 プレフィックスリスト、ポリシー リスト、および標準/拡張コミュニティ リストに関する新しい Smart CLI オブジェクトタイプが含まれます。また、Smart CLI を使用して BGP ルーティングを設定できるようになりました。これらの機能は、[デバイス (Device)] > [詳細設定 (Advanced Configuration)] ページから使用できます。

機能	説明 (Description)
廃止された FlexConfig コマンド。	<p>次の FlexConfig コマンドが廃止されました。</p> <ul style="list-style-type: none"> • access-list : スマート CLI 拡張アクセスリストまたは標準アクセスリストオブジェクトを使用して、extended および standard アクセスリストを作成できるようになりました。その後、それらは、サービス ポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド (match access-list など) で使用できます。 • as-path : スマート CLI AS パスオブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、自律システムパスフィルタを設定できるようになりました。 • community-list : スマート CLI 拡張コミュニティ リスト オブジェクトまたは標準コミュニティ リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、コミュニティ リスト フィルタを設定できるようになりました。 • dns-group : [オブジェクト (Objects)] > [DNS グループ (DNS Groups)] を使用して DNS グループを設定し、[デバイス (Device)] > [システム設定 (System Settings)] > [DNS サーバー (DNS Server)] を使用してグループ割り当てができるようになりました。 • policy-list : スマート CLI ポリシー リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定できるようになりました。 • prefix-list : スマート CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、IPv4 用のプレフィックス リスト フィルタリングを設定できるようになりました。 • route-map : スマート CLI ルートマップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルートマップを設定できるようになりました。 • router bgp : BGP にスマート CLI テンプレートを使用できるようになりました。
ISA 3000 デバイスに関する機能拡張。	<p>ISA 3000 のアラーム、ハードウェア バイパス、および SD カードによるバックアップ/復元の各機能を設定できるようになりました。アラームとハードウェア バイパスの設定には FlexConfig を使用します。SD カードについては、Device Manager のバックアップおよび復元ページが更新されました。</p>
脅威に対する防御 6.3 以降での ASA 5506-X、5506W-X、5506H-X、および 5512-X のサポートの削除。	<p>脅威に対する防御の 6.3 以降のリリースを ASA 5506-X、5506W-X、5506H-X、および 5512-X にインストールすることはできません。これらのプラットフォームに関してサポートされる脅威に対する防御の最後のリリースは 6.2.3 です。</p>

機能	説明 (Description)
VMware vSphere/VMware ESXi 5.5 のサポートの削除。	バージョン 6.3 では、VMware vSphere/VMware ESXi 6.0 での FTDv のサポートが廃止されています。FTD をアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。
製品の使用情報をシスコに提供するための Web 分析。	<p>ページのヒットに基づいて製品の使用情報を匿名でシスコに提供する Web 分析を有効にできます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブ データは送信されません。Web 分析はデフォルトで有効になっています。</p> <p>[デバイス (Device)] > [システム設定 (System Settings)] > [クラウドサービス (Cloud Services)] ページに Web 分析が追加されました。</p>
脆弱性データベース (VDB) の更新のインストールにより Snort が再起動しなくなりました。	VDB の更新のインストール時に Snort が自動的に再起動されなくなりました。ただし、Snort は、引き続き、次の設定展開時に再起動します。
Snort が再起動されない侵入ルール (SRU) データベースの更新の展開。	侵入ルール (SRU) の更新をインストールした後は、新しいルールを有効にするために設定を展開する必要があります。SRU の更新の展開時に Snort が再起動されなくなりました。
EMS 拡張機能のサポート。	<p>アップグレードの影響。</p> <p>バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが一時的に中止されます。つまり、[復号-再署名 (Decrypt-Resign)] と [復号-既知のキー (Decrypt-Known Key)] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能を一時的にサポート (よりセキュアな通信が可能) しなくなります。EMS 拡張機能は、RFC 7627 によって定義されています。</p> <p>サポートはバージョン 6.3.0.1 で戻ります。</p>
脅威に対する防御 REST API バージョン 2 (v2) 。	ソフトウェア バージョン 6.3 用の脅威に対する防御 REST API のバージョン番号が 2 になりました。API の URL の v1 を v2 に置き換える必要があります。v2 の API には、ソフトウェア バージョン 6.3 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、ログインした後に、Device Manager の URL の最後を ##api-explorer に変更します。

バージョン 6.2.3 の FDM 機能

表 11:バージョン 6.2.3 の FDM 機能

機能	説明
SSL/TLS の復号.	<p>接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URL およびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。[ポリシー (Policies)] > [SSL復号 (SSL Decryption)] ページおよび [モニタリング (Monitoring)] > [SSL復号 (SSL Decryption)] ダッシュボードが追加されました。</p> <p>注目 アクティブな認証を実装するアイデンティティポリシーは、SSL 復号ルールを自動的に生成します。SSL 復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。</p>
セキュリティインテリジェンスブロック。	<p>新しい [ポリシー (Policies)] > [セキュリティ インテリジェンス (Security Intelligence)] ページから設定できるセキュリティインテリジェンスポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセスコントロールポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。</p> <p>また、[ポリシー (Policies)] ダッシュボードの名前を [アクセスおよびSIルール (Access And SI Rules)] に変更し、セキュリティ インテリジェンス同等のルールがアクセスルールとともにダッシュボードに含まれるようになりました。</p>
侵入ルールの調整。	<p>アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント (警告) をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション (ドロップまたは警告に設定) のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、[ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。</p>

機能	説明
侵入ポリシーに基づく自動ネットワーク分析ポリシー (NAP) の割り当て。	以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワーク オブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック (それ以外は同じ送信元/送信先のセキュリティゾーンおよびネットワーク オブジェクトと一致する) に割り当てる場合、完全に一致する NAP および侵入ポリシーは取得されないことに注意してください。カスタム ネットワーク分析ポリシーは作成できません。
脅威、攻撃、およびターゲットのダッシュボード用のドリル ダウン レポート。	脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。 これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポート データが失われます。
[Webアプリケーション (Web Applications)] ダッシュボード。	新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。
新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え	新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。
新しいマルウェア ダッシュボード。	新しいマルウェア ダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイルタイプの情報を参照できます。この情報を表示するには、アクセスルールにファイル ポリシーを設定する必要があります。
自己署名入りの内部証明書、および内部 CA 証明書。	自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成したり、アップロードできるようになりました。これらの機能を、[オブジェクト (Objects)] > [証明書 (Certificates)] ページで設定します。
インターフェイスのプロパティを編集するときに、DHCP サーバの設定を編集する機能。	インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバーの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレス プールを簡単に再定義できます。

機能	説明
製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信。	<p>Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカルサポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなときに、接続を有効にできます。接続はいつでも無効にできます。</p> <p>Cisco Success Network はクラウドサービスです。[デバイス (Device)] > [システム設定 (System Settings)] > [クラウド管理 (Cloud Management)] ページの名前が [クラウドサービス (Cloud Services)] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。</p>
カーネルベースの仮想マシン (KVM) のハイパーバイザデバイス用 Threat Defense Virtual の設定。	<p>Device Manager を使用して、KVM 用の Threat Defense Virtual デバイス上の脅威に対する防御を設定できます。以前は、VMware のみがサポートされていました。</p> <p>(注) Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Device Manager に切り替えることはできません。</p>
VMware ESXi 6.5 のサポート。	VMware vSphere/VMware ESXi 6.5 に FTDv を展開できるようになりました。
ISA 3000 (Cisco 3000 シリーズ産業用セキュリティアプライアンス) デバイスの設定。	Device Manager を使用して ISA 3000 デバイス上の脅威に対する防御を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。
ルール データベースまたは VDB の更新でのオプションの展開。	<p>侵入ルールデータベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。</p> <p>(注) VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。</p>

機能	説明
<p>展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下。</p>	<p>展開を開始する前に、Device Manager により、設定の更新で Snort の再起動が必要かどうかを示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうかはわかるようになったため、混乱が少ないときに展開できます。</p> <p>さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。</p> <ul style="list-style-type: none"> • ユーザーが SSL 復号ポリシーを有効または無効にする • 更新されたルール データベースまたは VDB がダウンロードされた • ユーザーが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した
<p>Device Manager の CLI コンソール。</p>	<p>Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソールセッションを模倣していますが、コマンドのサブセットのみ（show、ping、traceroute、および packet-tracer）を許可します。トラブルシューティングとデバイスのモニターリングに CLI コンソールを使用します。</p>
<p>管理アドレスへのアクセスのブロックをサポートします。</p>	<p>プロトコルが管理 IP アドレスにアクセスできないようにするため、すべての管理アクセス リストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアント IP アドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3 へのアップグレードでは、以前からのプロトコル（HTTPS または SSH）用の空の管理アクセス リストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。</p> <p>また、SSH または HTTPS アクセスを無効にする場合を含み、Device Manager は CLI から管理アクセスリストに加えた変更を認識します。</p> <p>少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。</p>

機能	説明
EMS 拡張機能のサポート。	<p>[復号 - 再署名 (Decrypt-Resign)] と [復号 - 既知のキー (Decrypt-Known Key)] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になりました。EMS 拡張機能は、RFC 7627 によって定義されています。</p> <p>(注) バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよびダウンロード サイトから削除されました。バージョン 6.2.3.9 にアップグレードすると、EMS 拡張機能のサポートも有効になります。バージョン 6.3.0 では EMS 拡張機能のサポートが中止されています。サポートはバージョン 6.3.0.1 で再導入されています。</p> <p>最小 FTD : バージョン 6.2.3.8</p>
FTD の TLS v1.3 ダウングレード CLI コマンド。	<p>新しい CLI コマンドを使用すると、TLS v1.3 接続を TLS v1.2 にダウングレードするタイミングを指定できます。</p> <p>多くのブラウザでは、デフォルトで TLS v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。</p> <p>詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス で system support コマンドを参照してください。これらのコマンドは、Cisco TAC に問い合わせってから使用することをお勧めします。</p> <p>最小 FTD : バージョン 6.2.3.7</p>

機能	説明
デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig。	<p>Smart CLI と FlexConfig により、まだ Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Threat Defense は、いくつかの機能を実装するために ASA 設定コマンドを使用します。ASA 設定コマンドの知識があり、専門家ユーザーの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。</p> <ul style="list-style-type: none"> • Smart CLI : (推奨される方法です。) Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。 • FlexConfig : FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。 <p>注意 Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。</p>
Threat Defense REST API、および API エクスプローラ。	<p>REST API を使用して、Device Manager を介してローカルで管理している脅威に対する防御 デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアント プログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Device Manager にログインし、URL のパスを <code>#/api-explorer</code> (<code>https://ftd.example.com/#/api-explorer</code> など) に変更します。</p>

バージョン 6.2.2 の FDM の機能

表 12:バージョン 6.2.2 の FDM の機能

機能	説明
ASA 5500-X シリーズ デバイスのリモート アクセス VPN の設定	ASA 5500-X シリーズ デバイスでは、AnyConnect クライアント用にリモート アクセス SSL VPN を設定できます。[Device] > [Remote Access VPN] グループから RA VPN を設定します。[Device] > [Smart License] グループから RA VPN ライセンスを設定します。
Threat Defense Virtual for VMware デバイス設定。	Device Manager を使用して、VMware デバイス対応の Threat Defense Virtual 上で脅威に対する防御を設定できます。その他の仮想プラットフォームは Device Manager ではサポートされません。 (注) Device Manager のサポートを得るには、新しい 6.2.2 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Device Manager に切り替えることはできません。

バージョン 6.2.1 の FDM 機能



(注) このリリースは Firepower 2100 シリーズのみに適用されます。

表 13:バージョン 6.2.1 の FDM 機能

機能	説明
リモート アクセス VPN の設定	AnyConnect クライアントのリモート アクセス SSL VPN を設定できます。[Device] > [Remote Access VPN] グループから RA VPN を設定します。[Device] > [Smart License] グループから RA VPN ライセンスを設定します。
Firepower 2100 シリーズ デバイス設定	Device Manager を使用して、Firepower 2100 シリーズ デバイス上の脅威に対する防御を設定できます。

バージョン 6.2.0 の FDM 機能

表 14: バージョン 6.2.0 の FDM 機能

機能	説明
Cisco Defense Orchestrator (CDO) のクラウド管理。	Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。 [Device] > [System Settings] > [Cloud Management] を選択します。Cisco Defense Orchestrator の詳細については、 http://www.cisco.com/go/cdo を参照してください。
アクセスルールのドラッグアンドドロップ。	ルールテーブルで、アクセスルールをドラッグアンドドロップして移動できます。
脅威に対する防御ソフトウェアを Device Manager からアップグレードします。	Device Manager からソフトウェアアップグレードをインストールできます。 [Device] > [Updates] を選択します。

機能	説明
デフォルトの設定変更。	<p>新しいデバイスまたは再イメージ化されたデバイスでは、デフォルト設定に次の重要な変更が含まれます。</p> <ul style="list-style-type: none"> • (ASA 5506-X、5506W-X、5506H-X) 最初のデータ インターフェイスと ASA 5506W-X の Wi-Fi インターフェイスを除き、これらのデバイス モデルのその他すべてのデータ インターフェイスは、「内部」ブリッジグループに構造化され、有効化されます。DHCPサーバーは内部のブリッジグループにあります。ブリッジド インターフェイスにエンドポイントまたはスイッチを接続することができ、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。 • 内部インターフェイス IP アドレスは 192.168.1.1 です。DHCP サーバーは、アドレスプールの 192.168.1.5 ~ 192.168.1.254 のインターフェイスで定義されます。 • HTTPS アクセスは内部インターフェイス上で有効になるため、デフォルトアドレスの 192.168.1.1 で内部インターフェイスを介して Device Manager を開くことができます。ASA 5506-X モデルでは、内部ブリッジグループメンバー インターフェイス経由でこれを実行できます。 • 管理ポートは、192.168.45.0/24 ネットワークの DHCP サーバーをホストします。ワークステーションを管理ポートに直接接続して、IP アドレスを取得し、Device Manager を開いてデバイスを設定できます。 • OpenDNS のパブリック DNS サーバーは、現在、管理インターフェイスのデフォルト DNS サーバーです。以前は、デフォルト DNS サーバーはありませんでした。デバイスの設定時に、別の DNS サーバーを設定できます。 • 管理 IP アドレスのデフォルト ゲートウェイでは、データ インターフェイスを使用してインターネットにルーティングします。したがって、Management 物理インターフェイスをネットワークに配線する必要はありません。

機能	説明
管理インターフェイスおよびアクセスの変更。	<p>管理アドレス機能および Device Manager へのアクセス方法に対するいくつかの変更：</p> <ul style="list-style-type: none"> • HTTPS (Device Manager 用) および SSH (CLI 用) 接続に対するデータインターフェイスを開くことができます。デバイスを管理するために、別の管理ネットワークを必要としたり、管理/診断物理ポートを内部ネットワークに接続したりする必要はありません。[Device]>[System Settings]>[Management Access List] を選択します。 • システムは、外部インターフェイスのゲートウェイ経由でシステムデータベースのアップデートを取得できます。管理インターフェイスまたはネットワークからインターネットへの明示的なルートは必要ありません。デフォルトでは、データインターフェイスを介して内部ルートを使用します。ただし、別の管理ネットワークを使用する場合、特定のゲートウェイを設定できます。[Device]>[System Settings]>[Management Interface] を選択します。 • Device Manager を使用して、DHCP を介して IP アドレスを取得するように管理インターフェイスを設定できます。[Device]>[System Settings]>[Management Interface] を選択します。 • スタティックアドレスを設定する場合、管理アドレスで DHCP サーバーを設定できます。[Device]>[System Settings]>[Management Interface] を選択します。
さまざまなユーザーインターフェイスの変更。	<p>次に、Device Manager ユーザーインターフェイスの注目すべき変更を示します。</p> <ul style="list-style-type: none"> • [デバイス (Device)] メインメニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード (Device Dashboard)] ではなく [デバイスサマリー (Device Summary)] と呼ばれます。 • デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。 • [Device]>[System Settings]>[Cloud Preferences] は、[Device]>[System Settings]>[URL Filtering Preferences] と呼ばれます。 • [System Settings]>[DHCP Server] ページは2つのタブで構成され、グローバルパラメータとは異なる DHCP サーバーテーブルが表示されます。
サイト間 VPN 接続。	<p>事前共有キーを使用して、サイト間のバーチャルプライベートネットワーク (VPN) 接続を設定できます。IKEv1 および IKEv2 接続を設定できます。</p>

機能	説明
統合ルーティングおよびブリッジングのサポート	<p>統合ルーティングおよびブリッジングによって、ブリッジグループとルーテッドインターフェイスの間でルーティングする機能が提供されます。ブリッジグループは、脅威に対する防御デバイスがルーティングではなくブリッジするインターフェイスのグループです。脅威に対する防御デバイスは、脅威に対する防御デバイスがファイアウォールとして継続的に機能する本当のブリッジではありません。インターフェイス間のアクセスコントロールは管理され、すべての通常のファイアウォールチェックが実行されます。</p> <p>この機能によって、ブリッジグループを設定したり、ブリッジグループ間およびブリッジグループとルーテッドインターフェイスの間でルーティングするようにブリッジグループを設定したりできます。ブリッジグループは、ブリッジ仮想インターフェイス (BVI) を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。脅威に対する防御デバイスにブリッジグループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。BVI は、名前付きインターフェイスにすることができ、メンバー インターフェイスとは別にいくつかの機能 (DHCP サーバーなど) に参加できます。ここで、ブリッジグループ メンバー インターフェイスで他の機能 (NAT、アクセスコントロール ルールなど) を設定します。</p> <p>[Device] > [Interfaces] を選択して、ブリッジグループを設定します。</p>

FDM バージョン 6.1.x の機能

表 15: FDM バージョン 6.1.x の機能

機能	説明
サポートされるデバイス。	<p>Firepower Device Manager を使用して、次のデバイスタイプを管理できます。</p> <ul style="list-style-type: none"> • ASA 5506-X、5506H-X、5506W-X、5508-X、5516-X • ASA 5512-X、5515-X、5525-X、5545-X、5555-X
サポートされるファイアウォールモード。	<p>ルーテッドモードで動作するデバイスのみを設定できます。トランスペアレントモードはサポートされていません。</p>
サポートされるインターフェイスタイプおよびモード。	<p>ルーテッドインターフェイスのみを設定できます。インライン、インラインタップ、またはパッシブインターフェイスは設定できません。</p> <p>また、物理インターフェイスとサブインターフェイスのみを設定できます。EtherChannel や冗長インターフェイスは設定できません。また、PPPoE を設定することもできません。</p>

機能	説明
セキュリティポリシー。	<p>次のタイプのセキュリティポリシーを設定できます。</p> <ul style="list-style-type: none"> • アクセスコントロール：デバイスを通してできる接続を決定します。次のタイプのアクセス制御を実行できます。 <ul style="list-style-type: none"> • セキュリティゾーン、IP アドレス、地理位置情報、プロトコル、およびポートのフィルタリング。 • ユーザー名とユーザーグループのフィルタリング。 • アプリケーションフィルタリング。 • URL カテゴリ、レピュテーション、および個別の URL のフィルタリング。 • 侵入ポリシー、脅威対策。 • ファイルポリシー、マルウェア対策。 • ID ポリシー：IP アドレスに関連付けられているユーザーを判断します。このシステムはアクティブ認証のみをサポートし、パッシブ認証はサポートしていません。 • ネットワークアドレス変換：内部アドレスと外部アドレスを変換します。PAT プールを除き、ほとんどの NAT 機能がサポートされています。
ルーティング。	<p>スタティックルートを設定できます。ダイナミックルーティングプロトコルはサポートされていません。</p>
システムモニタリングと syslog。	<p>Firepower Device Manager には、最近の接続イベントを表示できるイベントビューアが含まれています。長期分析用にイベントを収集するために、外部 syslog サーバーを設定することもできます。</p> <p>また、システムおよびシステムを通過するトラフィックに関する統計情報を提供する多数のダッシュボードもあります。</p>
管理インターフェイスの設定。	<p>Firepower Device Manager から管理アドレスとインターフェイスを設定できます。CLI を使用する必要はありません。CLI または Firepower Device Manager にアクセスできる IP アドレスを制限するために、システムホスト名、管理 IP アドレスとゲートウェイ、DNS サーバー、NTP サーバー、およびアクセスルールを設定できます。</p>

機能	説明
更新のスケジュール。	<p>システムデータベースの更新頻度を制御できます。</p> <ul style="list-style-type: none"> • [デバイス (Device)] メインメニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード (Device Dashboard)] ではなく [デバイスサマリー (Device Summary)] と呼ばれます。 • デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。 • [Device] > [System Settings] > [Cloud Preferences] は、 [Device] > [System Settings] > [URL Filtering Preferences] と呼ばれます。 • [System Settings] > [DHCP Server] ページは2つのタブで構成され、グローバルパラメータとは異なる DHCP サーバーテーブルが表示されます。
バックアップと復元。	Firepower Device Manager からシステムをバックアップおよび復元できます。
トラブルシューティング ファイル。	シスコテクニカルサポートと連携する際に、Firepower Device Manager からトラブルシューティング ファイルを生成できます。

リリース日

表 16: バージョン 7.6 の日付

バージョン	ビルド	日付	プラットフォーム : アップグレード	プラットフォーム : 再イメージ化
7.6.0	113	2024 年 9 月 16 日	すべて	すべて
	41	2024 年 6 月 27 日	—	利用できなくなりました。

表 17: バージョン 7.4 日付

バージョン	ビルド	日付	プラットフォーム
7.4.2.1	30	2024 年 10 月 09 日	すべて
7.4.2	172	2024 年 7 月 31 日	すべて

バージョン	ビルド	日付	プラットフォーム
7.4.1.1	12	2024年4月15日	すべて
7.4.1	172	2023年12月13日	すべて
7.4.0	81	2023年9月7日	Management center Cisco Secure Firewall 4200 シリーズ

表 18: バージョン 7.3 日付

バージョン	ビルド	日付	プラットフォーム
7.3.1.2	79	2024年5月9日	すべて
7.3.1.1	83	2023年8月24日	すべて
7.3.1	19	2023年3月14日	すべて (All)
7.3.0	69	2022年11月29日	すべて (All)

表 19: バージョン 7.2 のリリース日

バージョン	ビルド	日付	プラットフォーム
7.2.9	44	2024年10月22日	すべて
7.2.8.1	17	2024年8月26日	すべて
7.2.8	25	2024年6月24日	すべて
7.2.7	500	2024-04-29	すべて
7.2.6	168	2024年4月22日	利用できなくなりました。
	167	2024年3月19日	利用できなくなりました。

バージョン	ビルド	日付	プラットフォーム
7.2.5.2	4	2024年5月6日	すべて
7.2.5.1	29	2023年11月14日	すべて
7.2.5	208	2023-07-27	すべて (All)
7.2.4.1	43	2023-07-27	すべて (All)
7.2.4	169	2023-05-10	Management center
	165	2023-05-03	デバイス
7.2.3.1	13	2023-04-18	Management center
7.2.3	77	2023年2月27日	すべて (All)
7.2.2	54	2022年11月29日	すべて (All)
7.2.1	40	2022年10月03日	すべて (All)
7.2.0.1	12	2022年8月10日	すべて
7.2.0	82	2022-06-06	すべて

表 20:バージョン 7.1のリリース日

バージョン	ビルド	日付	プラットフォーム
7.1.0.3	108	2023年3月15日	すべて (All)
7.1.0.2	36	2022年8月3日	FMC/FMCv Secure Firewall 3100 シリーズ
7.1.0.1	28	2022年02月24日	FMC/FMCv Secure Firewall 3100 シリーズを除くすべてのデバイス
7.1.0	90	2021年12月1日	すべて (All)

表 21:バージョン 7.0のリリース日

バージョン	ビルド	日付	プラットフォーム
7.0.6.3	50	2024年9月10日	すべて
7.0.6.2	65	2024年4月15日	すべて
7.0.6.1	36	2023年11月13日	すべて
7.0.6	236	2023-07-18	すべて (All)
7.0.5.1	5	2023-04-26	NGIPsv セキュリティ認定コンプライアンスが有効になっているデバイスの場合 (CC/UCAPLモード)。バージョン 7.0.5 FMC で使用します。
7.0.5	72	2022年11月17日	すべて (All)
7.0.4	55	2022年8月10日	すべて
7.0.3	37	2022-06-30	すべて
7.0.2.1	10	2022-06-27	すべて
7.0.2	88	2022年5月5日	すべて (All)
7.0.1.1	11	2022年02月17日	すべて (All)
7.0.1	84	2021-10-07	すべて (All)
7.0.0.1	15	2021年7月15日	すべて
7.0.0	94	2021年5月26日	すべて

表 22:バージョン 6.7のリリース日

バージョン	ビルド	日付	プラットフォーム
6.7.0.3	105	2022年02月17日	すべて (All)

バージョン	ビルド	日付	プラットフォーム
6.7.0.2	24	2021年5月11日	すべて (All)
6.7.0.1	13	2021年3月24日	すべて
6.7.0	65	2020年11月2日	すべて

表 23:バージョン 6.6のリリース日

バージョン	ビルド	日付	プラットフォーム
6.6.7.2	11	2024年4月24日	すべて
6.6.7.1	54	2023年1月26日	すべて (All)
6.6.7	223	2022年7月14日	すべて (All)
6.6.5.2	14	2022年03月24日	すべて
6.6.5.1	15	2021年12月6日	すべて (All)
6.6.5	81	2021年8月3日	すべて (All)
6.6.4	64	2021年4月29日	Firepower 1000 シリーズ
	59	2021年4月26日	FMC/FMCv Firepower 1000 シリーズを除くすべてのデバイス
6.6.3	80	2021年3月11日	すべて
6.6.1	91	2020年9月20日	すべて
	90	2020年9月8日	—

バージョン	ビルド	日付	プラットフォーム
6.6.0.1	7	2020年7月22日	すべて
6.6.0	90	2020年5月8日	Firepower 4112
		2020年4月6日	FMC/FMCv Firepower 4112 を除くすべてのデバイス

表 24: バージョン 6.5 のリリース日

バージョン	ビルド	日付	プラットフォーム : アップグレード	プラットフォーム : 再イメージ化
6.5.0.5	95	2021年2月9日	すべて	—
6.5.0.4	57	2020年3月2日	すべて	—
6.5.0.3	30	2020年2月3日	利用できなくなりました。	—
6.5.0.2	57	2019年12月19日	すべて	—
6.5.0.1	35	2019年11月20日	利用できなくなりました。	—
6.5.0	123	2020年2月3日	FMC/FMCv	FMC/FMCv
	120	2019年10月8日	—	—
	115	2019年9月26日	すべてのデバイス	すべてのデバイス

表 25: バージョン 6.4 のリリース日

バージョン	ビルド	日付	プラットフォーム
6.4.0.18	24	2024年4月24日	すべて
6.4.0.17	26	2023年9月28日	すべて (All)

バージョン	ビルド	日付	プラットフォーム
6.4.0.16	50	2022年11月21日	すべて
6.4.0.15	26	2022-05-31	すべて (All)
6.4.0.14	67	2022年02月18日	すべて
6.4.0.13	57	2021年12月2日	すべて
6.4.0.12	112	2021年5月12日	すべて (All)
6.4.0.11	11	2021年1月11日	すべて (All)
6.4.0.10	95	2020年10月21日	すべて
6.4.0.9	62	2020年5月26日	すべて
6.4.0.8	28	2020年1月29日	すべて
6.4.0.7	53	2019年12月19日	すべて
6.4.0.6	36	2019年10月16日	利用できなくなりました。
6.4.0.5	23	2019年9月18日	すべて
6.4.0.4	34	2019年8月21日	すべて
6.4.0.3	29	2019年7月17日	すべて

バージョン	ビルド	日付	プラットフォーム
6.4.0.2	35	2019年7月3日	FMC/FMCv FTD/FTDv (FirePOWER 1000 シリーズ以外)
	34	2019年6月27日	—
		2019年6月26日	Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv
6.4.0.1	17	2019年6月27日	FMC 1600、2600、4600
		2019年6月20日	Firepower 4115、4125、4145 SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300
		2019年5月15日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 シリーズ NGIPSv

バージョン	ビルド	日付	プラットフォーム
6.4.0	113	2020年3月3日	FMC/FMCv
	102	2019年6月20日	Firepower 4115、4125、4145 SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300
		2019年6月13日	Firepower 1010、1120、1140
		2019年4月24日	Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 シリーズ NGIPSv

表 26:バージョン 6.3 のリリース日

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.3.0.5	35	2019年11月18日	Firepower 7000/8000 シリーズ NGIPSv	—
	34	2019年11月18日	FMC/FMCv すべての FTD デバイス ASA FirePOWER	—
6.3.0.4	44	2019年8月14日	すべて	—

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.3.0.3	77	2019年6月27日	FMC 1600、2600、4600	—
		2019年5月1日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス	—
6.3.0.2	67	2019年6月27日	FMC 1600、2600、4600	—
		2019年3月20日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス	—
6.3.0.1	85	2019年6月27日	FMC 1600、2600、4600	—
		2019年2月18日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス	—
6.3.0	85	2019年1月22日	Firepower 4100/9300	Firepower 4100/9300
	84	2018年12月18日	FMC/FMCv ASA FirePOWER	—
	83	2019年6月27日	—	FMC 1600、2600、4600
		2018年12月3日	Firepower 4100/9300 を除くすべての FTD デバイス Firepower 7000/8000 NGIPSv	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv Firepower 4100/9300 を除くすべてのデバイス

表 27:バージョン 6.2.3 の日付

バージョン	ビルド	日付	プラットフォーム : アップグレード	プラットフォーム : 再イメージ化
6.2.3.18	50	2022 年 02 月 16 日	すべて	—
6.2.3.17	30	2021 年 6 月 21 日	すべて	—
6.2.3.16	59	2020 年 7 月 13 日	すべて	—
6.2.3.15	39	2020 年 2 月 5 日	FTD/FTDv	—
	38	2019 年 9 月 18 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	2019 年 7 月 3 日	すべて	—
	36	2019 年 6 月 12 日	すべて	—
6.2.3.13	53	2019 年 5 月 16 日	すべて	—
6.2.3.12	80	2019 年 4 月 17 日	すべて	—
6.2.3.11	55	2019 年 3 月 17 日	すべて	—
	53	2019 年 3 月 13 日	—	—
6.2.3.10	59	2019 年 2 月 7 日	すべて	—
6.2.3.9	54	2019 年 1 月 10 日	すべて	—
6.2.3.8	51	2019 年 1 月 2 日	利用できなくなりました。	—

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.2.3.7	51	2018年11月15日	すべて	—
6.2.3.6	37	2018年10月10日	すべて	—
6.2.3.5	53	2018年11月6日	FTD/FTDv	—
	52	2018年9月12日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	54	2018年8月13日	すべて	—
6.2.3.3	76	2018年7月11日	すべて	—
6.2.3.2	46	2018年6月27日	すべて	—
	54	2018年6月6日	—	—
6.2.3.1	47	2018年6月28日	すべて	—
	45	2018年6月21日	—	—
	43	2018年5月2日	—	—

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.2.3	113	2020年6月1日	FMC/FMCv	FMC/FMCv
	111	2019年11月25日	—	FTDv: AWS, Azure
	110	2019年6月14日	—	—
	99	2018年9月7日	—	—
	96	2018年7月26日	—	—
	92	2018年7月5日	—	—
	88	2018年6月11日	—	—
	85	2018年4月9日	—	—
	84	2018年4月9日	Firepower 7000/8000 シリーズ NGIPSv	—
	83	2018年4月2日	FTD/FTDv ASA FirePOWER	FTD：物理プラットフォーム FTDv：VMware、FVM Firepower 7000/8000 ASA FirePOWER NGIPSv
79	2018年3月29日	—	—	

表 28:バージョン 6.2.2 の日付

バージョン	ビルド	日付	プラットフォーム
6.2.2.5	57	2018年11月27日	すべて

バージョン	ビルド	日付	プラットフォーム
6.2.2.4	43	2018年9月21日	FTD/FTDv
	34	2018年7月9日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018年6月15日	—
6.2.2.3	69	2018年6月19日	すべて
	66	2018年4月24日	—
6.2.2.2	109	2018年2月28日	すべて
6.2.2.1	80	2017年12月5日	Firepower 2100 シリーズ
	78	2017年11月20日	—
	73	2017年11月6日	FMC/FMCv Firepower 2100 シリーズを除くすべてのデバイス
6.2.2	81	2017年9月5日	すべて

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 –2024 Cisco Systems, Inc. All rights reserved.

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。