

Zero Trust Access モジュール

- Zero Trust Access （1 ページ）
- デスクトップでの Zero Trust Access の起動と実行 （2 ページ）
- Zero Trust Access モジュールタイルの更新 （5 ページ）
- Android デバイスでの Zero Trust Access （5 ページ）
- iOS デバイスでの Zero Trust Access （6 ページ）
- リソースアクセスの開始 （6 ページ）
- デスクトップでの登録解除方法 （6 ページ）
- デスクトップでのアンインストール方法 （6 ページ）
- デスクトップでの Zero Trust Access の設定 （6 ページ）
- ユーザーアクションを必要としない証明書登録の使用 （7 ページ）
- ZTA Linux でのセキュアブートとカーネルロックダウン （8 ページ）
- デスクトップ Zero Trust Access モジュールの操作の詳細 （8 ページ）
- デスクトップでの Zero Trust Access モジュールのトラブルシューティング （9 ページ）
- Android 用 Zero Trust Access アプリのトラブルシューティング （10 ページ）
- iOS 用 Zero Trust Access アプリのトラブルシューティング （10 ページ）

Zero Trust Access

Cisco Secure Client タイルに「Zero Trust Access に登録済み」と表示されている場合、Zero Trust Accessモジュールは有効で実行中です。このアクセスは、ネットワーク上の誰と何を把握し、理解し、制御することを目的としています。ユーザーが誰であるかを明確に把握することで、その人のロールや職務、およびそれらのロールに付与されるネットワーク権限に基づいて、適切なレベルのアクセス権を付与します。AnyConnect VPN を超えて、ネットワーク全体でよりきめ細かい制御と安全なユーザー体験を提供します。VPNはネットワーク制御を通過するすべてのものを信頼しますが、Zero Trust Access のアプローチでは、証明されるまでアクセス権を持つユーザーやデバイスを信頼しません。自動的に信頼されることはなく、検証が済むと、限定的なアクセス権のみが付与され、再検証されます。ネットワークを超えてゼロトラストモデルを拡張し、インターネットからアプリケーションを隠すことで攻撃対象領域を削減します。

現在、Zero Trust Accessモジュールは Cisco Secure Access サービスのみをサポートしています。詳細については、Secure Access のマニュアルを参照してください。マニュアルでは、ゼロトラ

スト接続を許可するためのプライベートリソースの設定、それらの接続を使用してリソースにアクセスできるユーザーを決定するアクセスルールの設定、トラフィックステアリングなどについて説明しています。

デスクトップでの Zero Trust Access の起動と実行

事前展開を使用してインストールするには、Windows 用の **cisco-secure-client-win-*version*-zta-k9.msi** をダウンロードします。macOS の事前展開の場合は、**cisco-secure-client-macos-*version*-predeploy-k9.dmg**をダウンロードすると、Zero Trust モジュールがオプションコンポーネントの一部になります。Linux の事前展開では、Debian ディストリビューションの場合は **cisco-secure-client-zta-*version*_amd64.deb** を、RPM ディストリビューションの場合は **cisco-secure-client-zta-*version*.x86_64.rpm** をダウンロードします。

Web 展開を使用してインストールするには、Windows の場合は **cisco-secure-client-win-*version*-webdeploy-k9.pkg** を、Linux の場合は **cisco-secure-client-linux64-*version*-webdeploy-k9.pkg** をダウンロードします。ASA 設定のモジュール名は zta です。

Duo Desktop は、Cisco Secure Client とは別のスタンドアロン アプリケーションですが、Zero Trust Access モジュールインストーラ（Windows および macOS 用）にもパッケージ化され、自動的にインストールされます。ただし、macOS では、macOS 11 以降で MDM を介して Zero Trust Access を展開する場合、Duo Desktop には追加のセットアップ要件があります。これらの追加の Duo セットアップ要件については、「Guide to Duo Device Health App certificate deployment for macOS 11+ users」を参照してください。その他の Duo の詳細については、Duo Desktop のマニュアルを参照してください。Linux では、Zero Trust Access モジュールが機能するために Duo Desktop をインストールする必要はなく、利用可能なパッケージにも含まれていません。

ソフトウェアがインストールされると、ユーザーは、Zero Trust Access モジュールを使用してサービスにサインインし、クライアント証明書と必要なサービス URL を取得するための登録を求められます。Cisco Secure Access の登録にはユーザー認証部分が含まれ、これらの登録は再起動後も維持されます。登録はグローバル/マシンコンテキストに保存されますが、ローカルユーザーに関連付けられ、ローカルユーザーごとに適用されます。

始める前に

- 新しい macOS の要件により、5.1.x 以降の新規インストールまたは 5.0.x 以前からのアップグレードを実行する場合は、1 回限りの管理者権限が必要です。以降の更新では必要ありません。この制限は、MDM を介して macOS デバイスを管理し、アプリケーションを事前承認することで回避できます。詳細については、「Managed Login Items」を参照してください。ZTA モジュールが機能するには、事前にユーザーの承認が必要です。
- Linux では、バージョン 5.1.17.x 以降の新規インストールを実行したり、新しいバージョンにアップグレードしたりするには、管理者権限が必要です。
- Zero Trust Access モジュールは、Windows 10 および 11（TPM 対応デバイス）、macOS 14、macOS 15、および macOS 26（Secure Enclave）、Ubuntu 24.04/Red Hat 9.0 以降（TPM 対応デバイス）でサポートされています。

- Windows および Linux デバイスは、トラステッド プラットフォーム モジュール バージョン 2.0 を含むシステムで実行されている必要があります。macOS デバイスは、Apple T1 チップを搭載した Touch Bar 付き MacBook Pro コンピューター（016 および 2017）、Apple T2 Security チップを搭載した Intel ベースの Mac コンピューター、Apple シリコン搭載 Mac コンピューターなど、Secure Enclave を含むシステムで実行されている必要があります。
- Zero Trust Access モジュールを使用する場合は、Windows WebView2 をインストールし、アウトオブバンドで展開する必要があります。
- macOS 11 以降で Zero Trust Access を事前展開する場合は、『Additional DUO Desktop requirements on macOS 11 （and later）』を参照して追加の要件を確認してください。
- 適切に機能させるためには、AnyConnect VPN と Zero Trust Access のバージョンが一致している必要があります。AnyConnect VPN は 5.1.1.38、Zero Trust Access は 5.1.1.4867 が必要です。
- 最適なパフォーマンスを得るには、ダイナミックスプリット除外トンネリングを使用して、zpc.sse.cisco.com をターゲットとするトラフィックをトンネルから除外する必要があります。設定手順については、「ダイナミックスプリット除外トンネリングの設定」を参照してください。トンネルを介したそのドメインの解決で最適な地理的位置を持つ IP アドレスが生成されない場合は、名前解決がトンネルの外部でのみ試行されるように、スプリット除外のスプリット DNS も設定する必要があります。スプリット除外トンネリングの設定については、「スプリット DNS」を参照してください。
- Linux デバイスでは、Secure Client をインストールする前に、エンドポイントに GNU Privacy Guard（GPG）キーをインストールする必要があります。GPG は必要なオープンソース暗号化ソフトウェアを提供します。
- Sqlite および Iz4 は、Linux デバイスの標準システムパスから解決されるため、インストーラにはバンドルされていません。これらのライブラリのいずれかが欠落している場合、DEB/RPM パッケージの依存関係と要件が原因でインストールが失敗します。
- Linux デバイスでは、UI は Windows や macOS とは異なり、モジュール情報の表示にはタイルではなくタブが使用されます。

現在の制限事項または制約事項

- macOS では Duo Desktop ログの DART 収集はありません。
- サーバーが最初にトラフィックを送信するトンネリングアプリケーション（例：MySQL）はサポートされません。
- 複数のユーザーがエンドポイントに同時にログインしている場合、Zero Trust Access 機能は無効になります。
- ZTA の Web 展開は、macOS ではサポートされていません。
- すべての TCP 接続または UDP フローは、クライアント アプリケーションで開始する必要があります。

- Linux で RPM または DEB インストーラを使用するように切り替える前に、スクリプトインストーラによってインストールされた Cisco Secure Client（およびすべてのモジュール）をアンインストールする必要があります。アウトオブバンドのスクリプトインストーラを使用して、既存の RPM または DEB のインストールを更新することはできません。
- サーバーで一意のクライアント IP アドレスを必要とするプロトコル（SMBv1 など）はサポートされません。（SMBv3 は想定どおりに機能します）。
- Linux 上の Zero Trust Access は、integrity モードまたは confidentiality モードで設定されたセキュアブートまたは Linux カーネルロックダウンをサポートしていません。また、IPv6 のみは、Ubuntu 24.04 ではサポートされていません。
- ICMP または DNS SRV ディスカバリに依存しないクライアント TCP または UDP アプリケーションは、次の制限付きでサポートされます。

手順

ステップ 1 Zero Trust Access の使用を開始するには、登録が必要です。Cisco Secure Client の [Zero Trust Access] タイルで **[登録（Enroll）]** をクリックします。

ステップ 2 使用する電子メールアドレスを入力します。

ステップ 3 目的の組織が SSO/SAML ログインで自動選択されている場合は、認証用の電子メールアドレスとパスワードを入力します。複数の組織に属している場合は、ドロップダウンメニューから適切な組織を選択します。

[Zero Trust Access] タイル（Linux ではタブ）は、認証プロセスが完了した場合、または登録を続行している場合に表示されます。Zero Trust Access モジュールは、共通の Cisco Secure Client フォルダにインストールされます。

- Windows： C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA
- macOS：/opt/cisco/secureclient/zta
- Linux：/opt/cisco/secureclient/zta

登録時のセキュリティを最大限に高めるために、確立された MFA ベースの認証を活用し、ユーザー認証には生体認証 ID を使用することを強くお勧めします。

次のタスク

DART ログファイルの場所については、デスクトップでの Zero Trust Access モジュールのトラブルシューティング （9 ページ） を参照してください。

これらの手順については、デスクトップでの登録解除方法 （6 ページ） または デスクトップでのアンインストール方法 （6 ページ） を参照してください。

相互運用性の要件と予想されるフローについては、デスクトップ Zero Trust Access モジュールの操作の詳細 （8 ページ） を参照してください。

Zero Trust Access モジュールタイルの更新

[詳細（Advanced）] タブには、以下が含まれるようになりました。

- [設定の同期（Config Sync）] セクション（[設定（Configuration）] ウィンドウから再配置）
- [登録（Enrollment）] セクション（組織とユーザー名に固有の新しい登録フィールドを含む）
- ZTA モジュールに現在適用されているプロファイルを簡単に識別できるプロファイル名と組織名（Windows および macOS）
- 新しく追加された [ZTNAプロキシ設定の一時停止（ZTNA Proxy Config Pause）] セクション

プロキシ設定を一時停止する方法

Secure Access 内では、プロファイルは、アクセスのタイプを考慮してプロファイルごとに処理されます。[セキュアなプライベートアクセス（Secure Private Access）] と [セキュアなインターネットアクセス（Secure Internet Access）] の両方に、[セキュアなプライベートアクセス適用の一時停止（Pause Secure Private Access Enforcement）] のオプションがあります。[Cisco Secure Clientエンドユーザーの一時停止の有効化（Enable Cisco Secure Client end user pause）] をクリックすると、エンドユーザーは、この ZTA プロファイルの設定の適用を、一定期間または無期限に一時停止することを選択できます。

Secure Client の [プロキシ設定の一時停止（Proxy Config Pause）] では、使用可能なプロキシ設定が表示され、それらを一時的に無効にするかどうかを決定できます。[一時停止（Pause）] を押すと、タイマーがポップアップして残り時間をカウントダウンします。その後、一時停止したプロキシ設定が自動的に再度有効になります。一時停止機能を使用すると、[Zero Trust Access モジュール（Zero Trust Access Module）] セクションで、ZTA モジュールタイルの下部にステータス更新（データ信頼ネットワークの一時停止、ユーザーの一時停止、キャプティブポータルの一時停止など）が表示されます。

Android デバイスでの Zero Trust Access

Zero Trust Access は、Cisco Secure Client とは別にダウンロードした新しいアプリケーションとして、Google Play ストアから入手できます。Samsung Knox 3.10 以降を搭載した Android 14 を実行しているデバイスが必要です。Samsung Knox Service Plugin（KSP）は、Google Play ストアでも入手でき、MDM ベンダー（Ivanti MobileIron など）を Zero Trust Access でのデバイス登録用に設定するときに必要です。初回使用、登録、および障害対応の手順については、『Set up the Zero Trust Access App for Android on Samsung Devices』を参照してください。

iOS デバイスでの Zero Trust Access

Zero Trust Access は、Cisco Secure Client とは別にダウンロードする新しいアプリケーションとして、Apple App Store から入手できます。デバイスで iOS/iPadOS 17.2（またはそれ以降）を実行している必要があります。初回使用、登録、および障害対応の手順については、『Set up the Zero Trust Access App for iOS Devices』を参照してください。

リソースアクセスの開始

登録が完了すると、[Zero Trust Access] タイルにアクティブであることが示されます。その後、アクセスルールに基づいて管理者が使用可能と定義した内部アプリケーションへのアクセスを開始できます。リソースアクセスに関する問題は、[Zero Trust Access モジュール（Zero Trust Access Module）] タイルに表示されます。**[詳細（Details）]** をクリックすると、セキュアなリソースアクセスに影響を与えているものについての詳細を確認できます。

デスクトップでの登録解除方法

Zero Trust Access サービスから登録を解除する場合は、Zero Trust Access モジュールの **[詳細（Advanced）]** タブをクリックし、**[登録解除（Unenroll）]** をクリックします。これによりアカウントの登録が解除され、クライアント証明書が削除され、関連する設定がサービスから削除されます。

デスクトップでのアンインストール方法

macOS では、UI インストーラまたはコマンドラインを使用して、AnyConnect VPN をアンインストールするか、Zero Trust Access モジュールのみをアンインストールします。Windows では、[プログラムの追加/リモート処理（Add/Remote Program）] を使用して AnyConnect VPN をアンインストールするか、Zero Trust Access モジュールのみをアンインストールします。Zero Trust Access をアンインストールしても、Duo Desktop はアンインストールされません。Linux では、オペレーティングシステムのパッケージマネージャを使用して **cisco-secure-client-zta** パッケージを削除し、Zero Trust Access モジュールをアンインストールします。

デスクトップでの Zero Trust Access の設定

登録後、Zero Trust Access モジュールは設定の同期を実行し、適切なフォルダの初期 json 設定を取得します。その後、最新の json ファイルがフォルダにあることを定期的に確認します。チェックの結果によって、Zero Trust Access に設定変更の必要がないかどうか、新しい設定をダウンロードする必要があるかどうかを判断します。必要に応じて、Zero Trust Access モジュールの **[設定（Configuration）]** タブを選択し、**[今すぐ同期（Sync Now）]** をクリックして、SSE

ダッシュボードから最新の json ファイルをプルすることもできます。最後の設定同期の日付が表示されます。

追加の設定はすべて、クラウドの Cisco Secure Access で行います。

ユーザーアクションを必要としない証明書登録の使用

ユーザー証明書を使用した登録では、ユーザーのアクションや認識を必要とせずに、Windows、macOS、または Linux デバイスが Zero Trust Access に登録されます。ユーザーエンドポイントデバイスは、登録および更新時にアイデンティティ証明書を提示します。macOS では、ゼロタッチに使用される証明書はアプリケーションからアクセス可能である必要があります。証明書が MDM によってプッシュされる場合は、MDM 設定ポータルで [すべてのアプリケーションアクセスを許可（Allow all app access）] をクリックして、自動登録中にプロンプトが表示されずに秘密キーにアクセスできるようにします。証明書を手動でインポートする場合、秘密キーにアクセスする際に OS プロンプトを回避するには、次のコマンドラインの手順を実行する必要があります。

各個人ユーザーは、登録できるクライアント証明書を持っている必要があります。現在、同じデバイス上の異なるユーザーに対して異なる選択ファイルは提供されていません。

macOS での手順

1. クライアント証明書をインポートします。

   ```
   security import "PATH_TO_CLIENT_CERT" -k ~/Library/Keychains/login.keychain-db -x -A
   ```

2. 正しいパーティションリストを設定します。

   ```
   security set-key-partition-list -S teamid:DE8Y96K9QP -l "PRIVATE_KEY_LABEL" -t private
   ```

次のタスク

エンドポイントからクライアント証明書を選択する場合は、次の詳細を考慮してください。

- UPN（プリンシパル名）または RFC822 名を含めます。両方が存在する場合、UPN は RFC822 よりも優先されます。
- UPN または RFC822 の値は、SSE にインポートされるユーザーアイデンティティにマッピングする必要があります。
- MDM-ID は、ポスチャの相関に使用できるオプションの値です。次に、MDM ID シンタックスの例を示します。
  - Intune：*URL=ID:Microsoft Endpoint Manager:GUID:{{DeviceID}}*

（注） デバイス ID の最大長は 100 文字です。

  - JAMF：*cert ID:JAMF:GUID:$MANAGEMENTID*

- Ivanti/MobileIron：*ID:Mobileiron:GUID:${deviceGUID}*

Linux での手順

1. クライアント証明書をインポートします（.pem 形式）。

```
sudo cp "PATH_TO_CLIENT_CERT" ~/.cisco/certificates/client/
```

2. クライアントキーをインポートします（.key 形式）。

```
sudo cp "PATH_TO_CLIENT_KEY" ~/.cisco/certificates/client/private/
```

証明書内の MDM-ID に関する ISE ドキュメントについては、「Integrate MDM and UEM Servers with Cisco ISE - Integrate Microsoft Endpoint Manager Intune [Cisco Identity Services Engine]」または「Integrate MDM and UEM Servers with Cisco ISE - Integrate Ivanti (previously MobileIron) UEM [Cisco Identity Services Engine]」を参照してください。自動登録および設定に関する詳細は、Secure Access のヘルプに記載されています。

ZTA Linux でのセキュアブートとカーネルロックダウン

セキュアブートとカーネルロックダウンは、Linux オペレーティングシステム構成の一部である独立したテクノロジーです。セキュアブートはハードウェアで実装され、ブートローダーが侵害されていないこと、およびブート時にカーネルが変更されないことを保証するために使用されます。カーネルロックダウンは、ランタイム時のカーネルの変更やカーネルからのデータの抽出を防ぐ Linux カーネルの機能です。これらの機能は独立していますが、通常、セキュアブートを有効にすると、*integrity* モードでカーネルロックダウンも有効になります。

カーネルロックダウンモードには 3 種類あり、それぞれ *none*、*integrity*、および *confidentiality* です。最初の 2 つのモードのみがサポートされています。*confidentiality* は制限が非常に多いため、サポートされる予定はありません。ほとんどの Linux ディストリビューションでのデフォルトモードでは、セキュアブートが無効のときは *none*、有効のときは *integrity* になります。セキュアブート自体は Linux ZTA に影響しません。セキュアブートが有効なモードと無効なモードの両方がサポートされています。

デスクトップ Zero Trust Access モジュールの操作の詳細

除外するドメイン

VPN と Cisco Umbrella SWG との適切な相互運用性を実現するには、VPN トンネリングおよび SWG プロキシングから次のドメイン（および基盤となるサブドメイン/ホスト）を除外する必要があります。

- ztna.sse.cisco.com（登録）
- acme.sse.cisco.com（証明書）
- devices.api.umbrella.com（設定の同期）

- zpc.sse.cisco.com（プロキシング）
- sseposture-routing-commercial.k8s.5c10.org（ポスチャ）
- sseposture-routing-commercial.posture.duosecurity.com（ポスチャ）

設定ファイルが保存されるパス

設定ファイルはグローバルディレクトリに保存されますが、ローカルユーザー単位で追跡されます。ローカル登録ファイルは、次の場所に保存されます。

Windows：C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments

macOS：/opt/cisco/secureclient/zta/enrollments

Linux：/opt/cisco/secureclient/zta/enrollments

キャッシュされた設定ファイルは、次の場所にあります。

Windows：C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs

macOS：/opt/cisco/secureclient/zta/enrollments/cached_configs

Linux：/opt/cisco/secureclient/zta/enrollments/cached_configs

他の Secure Client モジュールとの相互運用性

Zero Trust Access が傍受したトラフィックは、Cisco Umbrella プロキシングや VPN トンネリングには使用できません。傍受される最初のトラフィックは、Zero Trust Access、Cisco Umbrella DNS/SWG、VPN の順になります。

証明書の詳細

証明書は有効期間が 5 週間で発行され、更新は有効期限の 2 週間前に開始されます。更新時に、新しいキーが生成されます。自動更新が実行されない場合、ユーザは再登録プロセスに従う必要があります。キーは、Windows および Linux では TPM、macOS ではシステムキーチェーンを使用して、プラットフォームのシステム証明書ストアで生成されます。登録解除またはアンインストール時には、証明書/キーは削除されます。

デスクトップでの Zero Trust Access モジュールのトラブルシューティング

Zero Trust Access で発生したエラーは、[Zero Trust Access] タイルまたは Secure Client UI の [メッセージ履歴（Message History）] タブに表示されます。

次のいずれかが発生する可能性があります。

- 本人確認の要求
- 有効にしてオンにする必要があるファイアウォール

- アクセスを拒否する権限エラー
- 障害または新しい場所への移動が原因で到達できないアプリケーション

DART は、Cisco Secure Client のインストールと接続の問題をトラブルシュートするためのデータを収集します。Diagnostics and Reporting Tool（DART）をインストールし、管理者として実行する必要があります。クライアントに必要なすべてのログは、デフォルトで DARTBundle.zip に格納され、ローカルデスクトップに保存されます。また、バンドルに含めるファイルと、カスタムバンドルの作成でそのファイルを保存する場所を指定することもできます。デフォルトでは、データ収集は米国地域の形式（MM/DD/YY）に基づいています。

（注） DART は、Duo Desktop ログを収集するように拡張されました。Windows では、Duo は PowerShell スクリプトを使用してログを収集します。PowerShell スクリプトの実行はデフォルトでブロックされるため、DART は管理者権限で起動された場合にのみ Duo ログを収集できます。最初の 5.1 リリースでは、DART は macOS または Linux で Duo Desktop ログを収集しません。収集は Windows用に行われます。

DART は、Cisco Secure Client が Windows デバイスで実行されている場合に起動します。macOS デバイスの場合、[アプリケーション（Applications）] > [Cisco] > [Cisco DART] を選択します。それから歯車アイコンをクリックし、**[診断（Diagnostics）]** をクリックします。Linux デバイスでは、DART はアプリケーションランチャーを使用して起動します。

ロギングを強化し、トラブルシューティングを目的とする可視性を高めるために、logconfig.json ファイルを使用して Zero Trust Access のトレースロギングを有効化できます。

Android 用 Zero Trust Access アプリのトラブルシューティング

Android デバイスでは、ログは [ZTA] > [設定（Settings）] に送信されます。[ログを送信（Send Logs）] をクリックして、トラブルシューティングのために Zero Trust Access のアクティビティログを IT ヘルプデスクに電子メールで送信します。また、アプリケーション内で詳細ロギングを有効にして、登録ウィンドウで Zero Trust Access の証明書情報とその他の統計情報を表示することもできます。その他の情報については、「Samsung デバイスでの Zero Trust Access App for Android アプリケーションのセットアップ」を参照してください。

iOS 用 Zero Trust Access アプリのトラブルシューティング

登録済み iOS デバイスをトラブルシュートする場合は、最初に Zero Trust Access のリレー設定が追加されたことを確認する必要があります。[設定（Settings）] > [VPNおよびリレー（VPN&Relays）] に移動すると、追加されたリレー設定を表示できます。[アプリケーションごとのリレー（Per-App Relays）] で、Zero Trust アプリケーションを探し、**情報（i）** アイコン

をクリックして Zero Trust のリレー設定を表示します。ログを表示して送信することもできます。詳細については、「Zero Trust Access App for iOS Devices のセットアップ」を参照してください。

（注） ユーザーが電話設定でリレーを削除した場合、Zero Trust Access のホームビューには、そのリレーを再度追加するよう求めるテキストが表示されます。リレーが再度追加されない限り、登録設定にアクセスして設定の同期または登録解除を実行できません。

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。