Zero Trust Access モジュール

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。

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。

Web 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*-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。macOS で Web 展開するには、**cisco-secure-client-macos-*version*-webdeploy-k9.pkg** をダウンロードします。m

Windows では、Cisco Secure Client と統合されていないスタンドアロンのアプリケーションである Duo Desktop もこのモジュールインストーラにパッケージ化され、自動的にインストールされます。しかし 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 を個別にインストールし、独自の追加セットアップを行う必要があります。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。

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

- Zero Trust Access モジュールは、Windows 10 と 11（TPM 対応デバイス）および macOS 11、12、13、14（TPM 対応デバイス）でサポートされています。
- Windows 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 チップを備えた Touch Bar 搭載の MacBook Pro コンピュータ（016 および 2017）、Apple T2 Security チップを備えた Intel ベースの Mac コンピュータ、Apple シリコンを搭載した Mac コンピュータなど、 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、 macOS 11 以降での Duo Desktop の追加要件 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。

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。
- 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。
  - 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。
  - 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）。

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] タイルは、認証プロセスが完了している場合、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

（注） 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、Zero Trust Access モジュールのトラブルシューティング （6 ページ） を参照してください。

これらの手順については、登録解除方法 （4 ページ） または アンインストール方法 （4 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、Zero Trust Access モジュールの操作の詳細 （5 ページ） 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。

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。

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。

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。

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

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

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。同様に、Network Visibility Module のレポートでは、Zero Trust Access が傍受した個々のネットワークフローはレポートされません。Zero Trust Access が傍受した暗号化されたアプリケーションフローを含む、Zero Trust Access プロキシへのネットワークトラフィックについてのみレポートします。

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 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。

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 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。

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。

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。