Secure Access拡張機能

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

クローム エンタープライズ プレミアム 向け シトリックス セキュア アクセス 拡張機能 4
Secure Access 拡張機能ログ 4
Chrome Enterprise 用 Citrix Secure Access コントロール 5
サポートされているコントロール 6
ポリシー内のユーザーとグループ 7
ユーザーまたはグループの検索 7
同期されたユーザーとグループを使用する 7
キーロギング対策制御 9
前提条件 9
キーロギング対策ポリシーを構成する 9
クリップボードコンテナ制御 11
前提条件 11
クリップボードコンテナ制御を有効にする 12
クリップボード共有スコープを有効にする 12
Webアプリケーションのドメインサフィックス 15
前提条件 15
DNSサフィックスの構成 15
セッション記録の制御 17
アーキテクチャ 17
前提条件 18
システム要件 18
環境をセットアップする 18
セッションレコーディングサイトを構成する 19
Secure Private Accessでセッションレコーディングブラウザポリシーを構成する 19
エンドポイント用のセッション録画エージェントを含むWorkspaceアプリをインストールする 19

© 1997–2026 Citrix Systems, Inc. All rights reserved.

録画されたセッションを再生する 19
ベストプラクティス 20
ブラウザセッションの再認証制御 21
前提条件 21
ブラウザセッションの再認証制御を有効にする 21
SSH制御 23
この統合の利点 23
ユースケース 24
システム要件 24
前提条件 24
SSHアクセス用にSecure Private Accessを構成する 25
SSHポリシーを構成する 25
リモートデスクトップ制御 26
この統合の利点 26
ユースケース 27
システム要件 27
前提条件 27
RDPアクセス用にSecure Private Accessを構成する 28
リモートデスクトップポリシーを構成する 28

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クローム エンタープライズ プレミアム 向け シトリックス セキュア アクセス 拡張機能

Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能は、Chrome ブラウザから直接、内部および外部アプリケーションへの安全なクライアントレスアクセスを可能にします。これは、Citrix Secure Private Access と Chrome Enterprise の機能を組み合わせることで、エンタープライズグレードのセキュリティ、ゼロトラストアクセス、コンテキスト制御、および最新のユーザーエクスペリエンスを提供します。

組織は、この拡張機能を使用して、VPN やネイティブクライアントのインストールを必要とせずに、SaaS アプリケーション、内部 Web アプリ、SSH サーバー、および RDP システムへの安全なアクセスを提供できます。

Secure Access ブラウザ拡張機能は、Secure Private Access を Chrome Enterprise Premium と統合すると自動的にインストールされます。セットアップ手順については、Google Chrome 統合のセットアップ を参照してください。インストール後、Chrome ブラウザの右上隅にあるアイコンから拡張機能にアクセスできます。



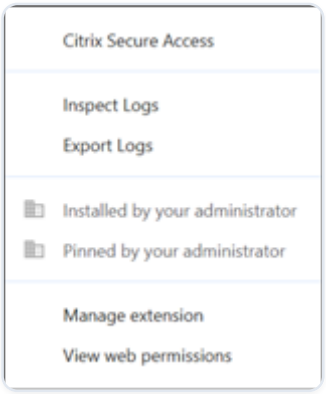
Secure Access 拡張機能ログ

Secure Access ブラウザ拡張機能ログは、監視とトラブルシューティングに不可欠です。エンドユーザーは、問題が発生したときに、ログを確認およびダウンロードして、管理者またはサポートチームと共有できます。

ログを確認またはダウンロードするには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ブラウザ拡張機能アイコンを右クリックします。
   - ログを確認するには、**ログの検査** をクリックします。
   - ログをダウンロードするには、**ログのエクスポート** をクリックします。



Chrome Enterprise 用 Citrix Secure Access コントロール

Citrix Secure Private Access は、Google Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能によって配信および適用されるセキュリティポリシーをサポートしています。詳細については、サポートされているコントロール を参照してください。

これらのポリシーは、Secure Private Access 管理コンソールから構成できます。

1. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
2. ポリシーを選択し、**管理**をクリックします。

   利用可能なコントロール(/en-us/citrix-secure-private-access/media/secure-access-controls.png)
3. ポリシーのルールを追加します。

   アンチキーロギングルール(/en-us/citrix-secure-private-access/media/spa-browser-add-akl-rule.png)
4. ブラウザコントロールをブラウザセッションに適用するための**アクセスモード**条件を追加します。ブラウザポリシーの場合、値は**ブラウザ**です。アクセスモードの詳細については、「アクセスモードベースのポリシー適用」を参照してください。
5. ポリシーを評価する必要がある条件を選択します。

   アンチキーロギングポリシー条件(/en-us/citrix-secure-private-access/media/spa-browser-policy-condition.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- ユーザーまたはグループを選択する際、管理者は、選択したユーザーディレクトリのエントリがGoogle Directoryと同期され、正しく構成されているかを確認できます。Secure Private Accessポリシーは、同期されたユーザーとグループを使用する場合にのみ正しく評価されます。そうでない場合、警告が表示されることがあります。詳細については、「同期されたユーザーとグループを使用する」を参照してください。
- また、ユーザーとグループの詳細については、およびを参照してください。

詳細な構成手順については、各コントロールのドキュメントを参照してください。

サポートされているコントロール

Citrixは、Secure Private AccessとChrome Enterprise Premiumの統合で、以下のSecure Accessコントロールをサポートしています。

コントロール	機能
キーロギング対策	エンドポイント上のキーロガーマルウェアがユーザー入力をキャプチャするのを防ぐために、キーストロークを難読化します。
クリップボードコンテナ	ユーザーがブラウザと他のアプリの間でコピー＆ペーストできる内容を制御します。
DNSサフィックス	短い内部URL（「wiki/」など）を完全なアドレスに自動的に補完します。
セッション記録	監査およびコンプライアンスのためにブラウザセッションのアクティビティを記録します。
ブラウザセッションの再認証	設定された時間間隔の後、ブラウザセッションの定期的な再認証を強制します。
SSH接続	ユーザーがターミナルクライアントを必要とせずに、ブラウザタブ内で直接SSH接続を確立できるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コントロール	機能
リモートデスクトップ (RDP)	ユーザーがRDPクライアントを必要とせずに、ブラウザタブ内で直接リモートデスクトップセッションを起動できるようにします。

ポリシー内のユーザーとグループ

以下のセクションでは、ユーザーとグループに関する詳細情報を提供します。

ユーザーまたはグループの検索

選択したユーザーとグループはグリッドに表示されます。グリッドの各行には、異なるドメイン、フォレスト、またはIDプロバイダー (IdP) 間で同じ名前のユーザーまたはグループを明確に区別できるように、以下のID詳細が表示されます。

- **名前** – ユーザーまたはグループの表示名。
- **メール** – IDに関連付けられているメールアドレス。
- **IDPタイプ** – Azure AD、Active Directory、Okta、GoogleなどのIDプロバイダー。
- **OID** – IDのオブジェクトIDまたはセキュリティ識別子。
- **ドメイン** – ユーザーまたはグループが属するドメイン。

グリッドを名前でフィルタリングしたり、個々の行を削除したり、複数のエントリを選択して**選択したものを削除**を使用してまとめて削除したりできます。

同期されたユーザーとグループを使用する

ユーザーまたはグループを選択する際、管理者は、選択したユーザーディレクトリからのエントリがGoogle Directoryと同期され、正しく構成されているかを確認できます。Secure Private Accessポリシーは、同期されたユーザーとグループを使用する場合にのみ正しく評価されます。そうでない場合、以下の警告が表示されることがあります。

- **テナントアカウントの権限が不足しています。**

  修正: Google管理コンソールで、テナントサービスアカウントに**ユーザー > 読み取り**および**グループ > 読み取り**の権限を割り当てます。SPAは、ユーザーまたはグループが存在することを確認するためにこれらの権限を必要とします。

- **ユーザーまたはグループが同期されていません。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修正: 検索または選択されたユーザーまたはグループは、Google Directoryと同期されていません。SPAポリシーで使用する前に、ディレクトリエンティティをGoogle Directoryと同期してください。

- **グループアクセス設定が不十分です。**

  対処法： Google 管理コンソールで、選択したグループのアクセス設定を開き、**メンバーを表示できるユーザー**に少なくとも**グループメンバー**オプションが選択されていることを確認します。

注:

この機能は、Google Chrome の統合が正常に完了した後にのみ利用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

キーロギング対策制御

サイバー犯罪者は、パスワード、クレジットカード番号、機密性の高い企業データなどの機密情報を盗むために、キーロガーなどの悪意のあるソフトウェアを使用します。

Chrome Enterprise Premium (CEP) 用のCitrix Secure Accessブラウザ拡張機能は、データの保護に役立つキーロギング対策をサポートしています。この機能はキーストロークをスクランブル化するため、悪意のあるプログラムが入力された情報をキャプチャしようとしても、判読不能な文字のみが記録され、実際のテキストは安全に作業アプリケーションに配信されます。

サポートされている展開: Citrix Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows 11以降。

注:

ネイティブRDPセッションでは、キーロギング対策はサポートされていません。

前提条件

キーロギング対策を有効にする前に、次の前提条件が満たされていることを確認してください。

- CWAバージョン2603以降がインストールされていること。
- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。

キーロギング対策ポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. > に移動し、 をクリックします。
3. を選択し、 をクリックします。
4. をクリックして、ユーザーがキーロギング対策を有効にするためのルールを追加します。
    a. ルールの名前を入力し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 要件に基づいて、ユーザーやグループなどの条件を選択します。また、**地理的位置**、**ネットワークロケーション**、**デバイスポスチャチェック**などの条件を追加することもできます。

c. **次へ**をクリックします。

5. 「**保存**」をクリックします。

アンチキーロギングポリシー用に構成されたルールの数は、**ブラウザポリシー > アンチキーロギング**タブに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クリップボードコンテナ制御

WebアクセスにChromeを、ネイティブアプリケーションにVDIを使用する展開では、クリップボードコンテナ機能を使用して、ブラウザとVDIセッション間のデータ共有を制御できます。クリップボードデータは、ローカルエンドポイントのクリップボードに書き込まれることなく、Citrixセッション間で直接転送されます。 これにより、セキュリティが向上し、ユーザーは両方の環境で柔軟に作業できるようになります。

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows。

前提条件

以下の前提条件が満たされていることを確認してください。

- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。
- Citrix Workspaceアプリ 2603.10以降。
- 2607 LTSR以降を実行しているWindows VDA (クリップボード共有スコープのGAバージョン)。詳細については、「クリップボード共有スコープ」(/us/en/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/ica-policy-settings/cross-session-clipboard-exchange.htm)を参照してください。
- 2507 LTSRを実行しているWindows VDA (クリップボード共有スコープのプレビューバージョン) では、以下を有効にします。
    - **DaaSとのクロス・クリップボード・コンテナ**機能。詳細については、「DaaSとのクロス・クリップボード・コンテナ」(/us/en/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/ica-policy-settings/cross-session-clipboard-exchange.html)を参照してください。この機能は現在、DaaSでプレビューとして利用可能です。
    - **クリップボード共有スコープ**レジストリ。詳細については、「クリップボード共有スコープレジストリを有効にする」(/us/en/citrix-secure-private-access/hybrid/spa-hybrid-cep-spa-integration/browser-extension/spa-cep-clipboard-container.html#enable-clipboard-container-control)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クリップボードコンテナ制御を有効にする

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **クリップボードコンテナ**を選択し、**管理**をクリックします。
4. 「**ルールを追加**」をクリックして、VDAとブラウザ間のクリップボード共有のルールを追加します。

   a. ルールの名前を入力し、「**次へ**」をクリックします。

   b. ユーザーやグループなど、要件に基づいて条件を選択します。**地理的位置**、**ネットワークロケーション**、**デバイス姿勢チェック**などの条件を追加することもできます。

   c. **次へ**をクリックします。

   d. クリップボード共有を許可するURLとSecure Private Accessアプリケーションを定義します。

   e. ポリシーのスコープを選択します。

   - **ブラウザ全体に適用** — このポリシーは、管理対象プロファイル内のすべてのクリップボードアクティビティを管理します。
   - **特定のアプリケーションとURLに適用** — このポリシーは、選択されたアプリケーションと入力されたURL/ドメインパターンに限定されます。
     - **アプリケーションを選択** — アプリケーションピッカーを使用して、特定の公開済みアプリケーションを選択します。
     - **URLまたはドメイン** - 特定のアプリケーションのURLまたはドメインを入力します。

   クリップボードコンテナアクション(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-action.png)

5. 「**保存**」をクリックします。

   クリップボードコンテナポリシー用に構成されたルールの数は、「**ブラウザポリシー > クリップボードコンテナ**」タブに表示されます。

クリップボード共有スコープを有効にする

VDAバージョン2607の場合:

仕組みを参照してください。

VDAバージョン2507の場合:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この**Clipboard Sharing Scope**レジストリを有効にします。

1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\ に移動します。
3. `ClipboardSharingScope` という名前の REG_DWORD 値を作成します。

クリップボードコンテナレジストリ (/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-registry1.png)

`ClipboardSharingScope` ポリシーは、VDA クリップボードデータをどこで共有できるかを制御します。新しい DDC ポリシーが利用可能になるまで、この設定は前述のレジストリキーを使用して構成できます。

サポートされている値	スコープ	説明
0	無制限	クリップボードデータはクライアントシステムのクリップボードにコピーされ、クライアント、VDA、および CEP からアクセスできます。
1	VDA のみ	クリップボードデータは VDA のみにアクセス可能です。クライアントシステムのクリップボードと CEP はクリップボードコンテンツにアクセスできません。
2	CEP のみ	クリップボードデータは CEP のみにアクセス可能です。クライアントシステムのクリップボードと VDA はクリップボードコンテンツにアクセスできません。
3	VDA と CEP	クリップボードデータは VDA と CEP の両方からアクセス可能です。クライアントシステムのクリップボードはクリップボードコンテンツにアクセスできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クリップボードコンテナのレジストリ値(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-registry2.png)

注:

- CEPのみ (2) およびVDAとCEP (3) モードは、CEP拡張機能のクリップボードコンテナ機能と連携するように設計されています。
- クリップボードコンテナポリシーが有効になっている場合、管理者が構成したURLのみがVDIとクリップボードデータを交換することが許可されます。

```
>-  Content copied from the approved web applications can be pasted into the VDI.

>-  Content copied from the VDI can be pasted only into administrator-configured, paste-allowed URLs.

>-  If a user attempts to paste VDI clipboard content into a website that is not included in the policy, the paste operation is blocked and an error message appears.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Webアプリケーションのドメインサフィックス

ユーザーがブラウザに短い内部ホスト名（例: `sw` または `server001`）を入力するシナリオでは、ドメインサフィックス機能は、オペレーティングシステムのDNSサフィックス設定に依存するのではなく、ブラウザ管理のDNSサフィックスポリシーを使用して、DNSサフィックスを自動的に追加し、それらを完全修飾ドメイン名（FQDN）に変換します。

DNSサフィックス機能は、**Windows**と**macOS**の両プラットフォームでサポートされており、一般的なURL入力形式全体に一貫して適用されます。これには以下が含まれます。

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: WindowsおよびmacOS。

前提条件

Citrix Secure AccessとChrome Enterpriseの統合が構成されていることを確認してください。詳細については、Google Chrome Enterprise Premiumとの統合を参照してください。

DNSサフィックスの構成

1. Secure Private Access管理コンソールにログインします。
2. a. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **DNSサフィックス**を選択し、**管理**をクリックします。
4. **ルールの追加**をクリックして、URLに追加するドメインのルールを追加します。

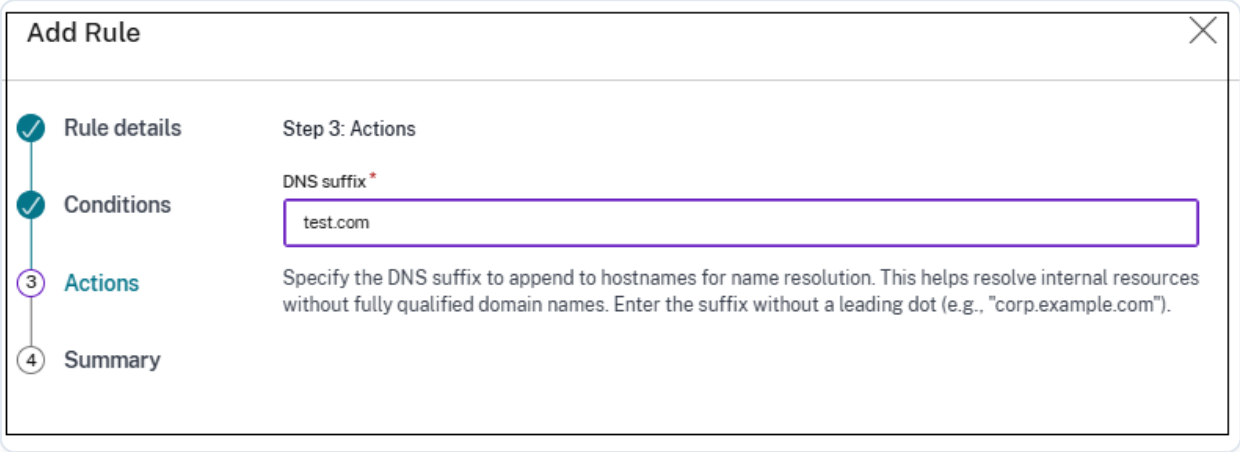
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. ルールの名前を入力し、**次へ**をクリックします。

b. ユーザーやグループなど、要件に基づいて条件を選択します。**地理的位置**、**ネットワークロケーション**、**デバイスポスチャチェック**などの条件を追加することもできます。

c. **次へ**をクリックします。

d. アクセス用に付加するドメインを定義します。



5. 「**保存**」をクリックします。

DNSサフィックスポリシーに設定されたルールの数は、「**ブラウザポリシー > DNSサフィックス**」タブに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッション記録の制御

セッション記録は、取得と再生のためにセッションを記録、カタログ化、アーカイブします。

セッション記録は、次の主要な利点を提供します。

- アプリケーションおよびデスクトップセッションの記録を自動的にトリガーするための柔軟なポリシーを提供します。
- IT担当者がユーザーアクティビティを監視および調査できるようにし、規制遵守とセキュリティ監視のための内部統制をサポートします。
- 問題の特定を迅速化し、解決までの時間を短縮することで、テクニカルサポートを支援します。

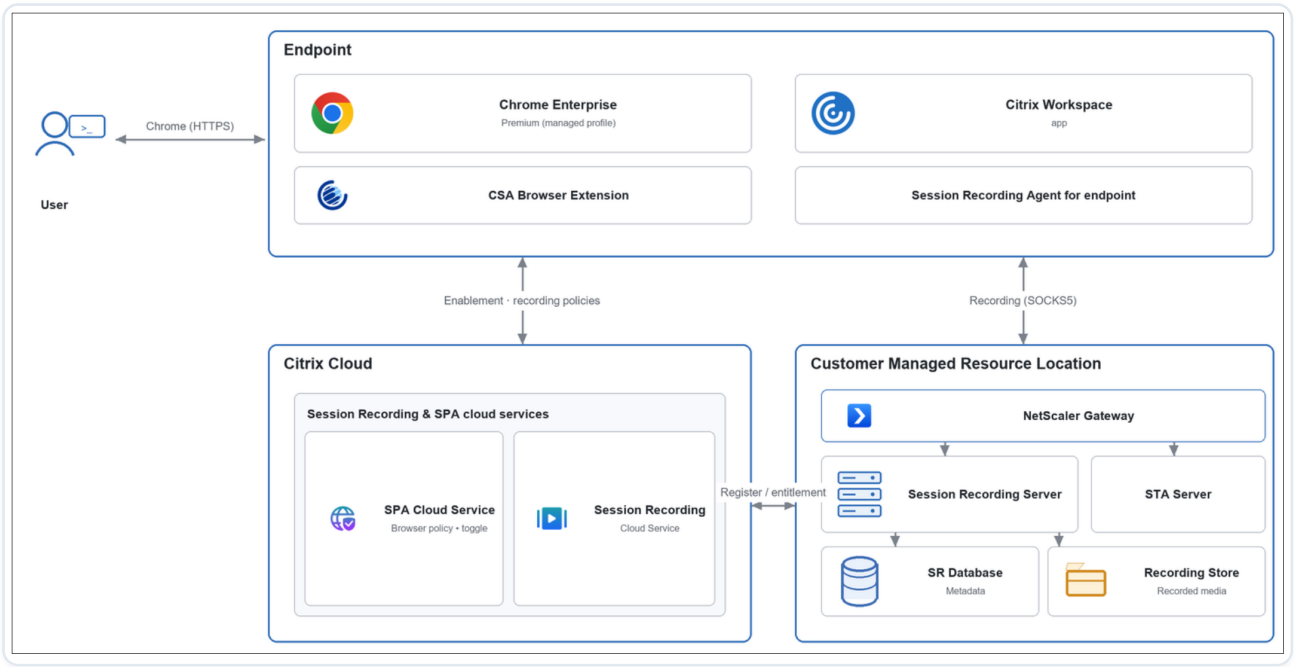
詳細については、Benefitsを参照してください。

アーキテクチャ

セッション記録ソリューションは、次の3つのプレーンにまたがります。

- 管理されたChromeプロファイル、Citrix Secure Access拡張機能、およびエンドポイント用Session Recording Agentを備えたエンドポイント。
- Secure Private AccessおよびSession Recordingクラウドサービスを収容するCitrix Cloudコントロールプレーン。
- NetScaler Gateway、STAサーバー、Session Recordingサーバー、およびそのデータベースと記録ストアを含む、顧客管理のリソースロケーション。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



前提条件

- Windows版 Citrix Workspaceアプリ 2603.10以降
- エンドポイント分析 (EPA) バージョン: 26.5.1.7以降

システム要件

- Citrix Secure Private Access（サービスモードまたはハイブリッドモードで展開され、Chrome Enterprise Premium（管理プロファイル付き）と組み合わされたもの）。
- Session Recording CloudサービスとSession Recordingサーバー2511以降。詳細については、はじめにを参照してください。
- 次のコンポーネントを備えたWindows 64ビットまたは32ビットのエンドポイント:
  - Citrix Endpoint Analysis (EPA) プラグイン26.5.1.7以降。
  - Session Recording Endpoint AgentがインストールされているWindows用Citrix Workspaceアプリバージョン2603.10以降

環境をセットアップする

Chrome Enterpriseセッションのエンドポイントレコーディングを有効にして検証するには、次の手順を完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションレコーディングサイトを構成する

エンドポイントレコーディングポリシーの構成に記載されている手順に従ってください。

注:

エンドポイントレコーディングにはNetScaler Gatewayが必要です。Secure Private Accessのどちらの展開タイプでも、STAを介してレコーディングトラフィックをSession Recording Serverにルーティングします。NetScalerがユーザーからアプリケーションへのアクセスを管理しないSecure Private Accessサービスを使用している場合でも、レコーディングトラフィック用のゲートウェイURLを指定する必要があります。

Secure Private Accessでセッションレコーディングブラウザポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **セッションレコーディング**を選択し、**管理**をクリックします。
4. **ルールの追加**をクリックし、ルールの名前を入力して、**次へ**をクリックします。
5. 条件（ユーザーとグループ）を設定します。（オプション）**地理的位置**、**ネットワークロケーション**、**デバイス姿勢チェック**を追加し、**次へ**をクリックします。
6. 「**保存**」をクリックします。ルール数は、**ブラウザポリシー > セッション録画**タブに表示されます。

エンドポイント用のセッション録画エージェントを含むWorkspaceアプリをインストールする

(/ja-jp/citrix-workspace-app-for-windows/install#session-recording-add-on-support)のに記載されている手順に従ってください。

録画されたセッションを再生する

録画はセッション録画コンソールで表示できます。

- ユーザーのChromeワークプロファイルに関連付けられているすべてのウィンドウが録画されます。
- 1つ以上のモニターにまたがる複数のウィンドウが録画されます。
- フォーカスが外れているウィンドウや、他のアプリケーションによって隠されているウィンドウも、全体が録画されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 最小化されたウィンドウや、画面キャプチャ防止が有効になっているウィンドウは、再生中に黒い四角として表示されます。

ベストプラクティス

- **グローバルサイトを1つ維持する**。単一のグローバルエンドポイント録画サイトを使用し、その構成を文書化します。変更すると、他のサイトで構成されているポリシーが意図せず無効になる可能性があります。
- **リージョンを合わせる**。遅延やデータレジデンシーの問題を避けるため、セッション録画クラウドサービスURL、クラウドクライアント、およびバックエンドを同じCitrix Cloudリージョンに保持します。
- **ストレージを計画する**。全画面のWeb/SaaS録画はストレージを大量に消費する可能性があります。サーバー、セッション録画データベース、および録画ストレージを適切にサイジングし、ストレージ消費量を綿密に監視してください。
- **最初にエンタイトルメントとロールを検証する**。Citrix DaaSとCitrix Secure Private Accessのエンタイトルメントの不一致は、展開失敗の最も一般的な原因です。ポリシーを有効にする前に、単一のアクティブな顧客レコードが存在し、必要な管理ロールが割り当てられていることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ブラウザセッションの再認証制御

Citrix Secure Private Access を使用すると、管理者は Chrome Enterprise Premium (CEP) ブラウザセッションのセッションタイムアウトポリシーを適用できます。ユーザーは、ブラウザのアクティビティに関係なく、設定されたセッション期間が経過すると再認証を求められます。これにより、Google Chrome の仕事用プロファイルを通じてアクセスされるアプリケーションのゼロトラストアクセス制御が強化されます。

セッションの有効期限が切れると、ユーザーはエンタープライズ資格情報と多要素認証 (MFA) を使用して再認証する必要があります。再認証が成功すると、最後にアクティブだったページが復元され、セッションタイマーが再開されます。

サポートされている展開: Secure Private Access サービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows、macOS、Linux、ChromeOS。

前提条件

次の前提条件が満たされていることを確認してください。

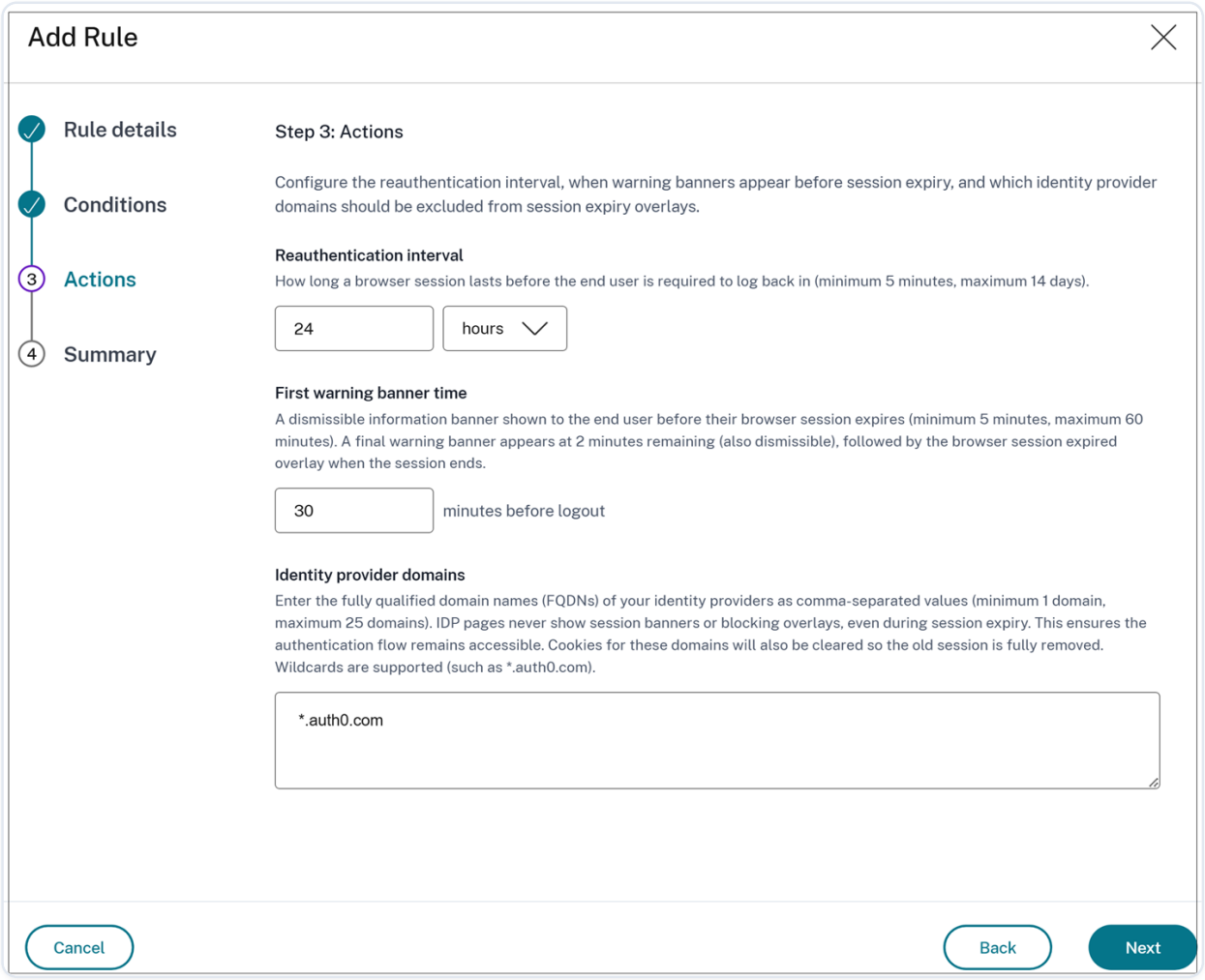
- Citrix Secure Access と Chrome Enterprise Premium (CEP) の統合が完了していること。

ブラウザセッションの再認証制御を有効にする

1. Secure Private Access 管理コンソールにログインします。
2. **>** に移動し、 をクリックします。
3. を選択し、 をクリックします。
4. をクリックして、ブラウザセッションの再認証を有効にするルールを追加します。
    a. ルールの名前を入力し、 をクリックします。
    b. ユーザーやグループなど、要件に基づいて条件を選択します。、、 などの条件を追加することもできます。
    c. **次へ**をクリックします。
    d. 次を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **再認証間隔**: ユーザーが再認証を求められるまでのブラウザセッションの期間。間隔は5分から14日の間で設定でき、分、時間、または日で構成できます。
- **最初の警告バナー表示時間**: ブラウザセッションの有効期限が切れる前にユーザーに表示される、閉じることができる警告バナー。有効期限が切れる5分から60分前までの間で値を設定できます。残り2分になると2番目の警告バナーが表示され、セッション終了時にはセッション期限切れのオーバーレイが表示されます。
- **IDプロバイダーのドメイン**: コンマ区切りの値として指定するIDプロバイダーの完全修飾ドメイン名 (FQDN)。1〜25個のドメインを指定できます。認証フローが中断されないように、IdPページではセッションバナーとブロックオーバーレイは表示されません。古いセッションが完全に削除されるように、セッションの有効期限が切れるとこれらのドメインのCookieがクリアされます。ワイルドカードがサポートされています (例: *.auth0.com)。



5. **次へ**をクリックし、次に**保存**をクリックします。

クリップボードコンテナポリシーに設定されているルールの数が、**ブラウザポリシー > ブラウザセッションの再認証**タブに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSH制御

Citrix Secure Private AccessはChrome Enterprise Premiumと統合されており、ブラウザ内で直接セキュアなSSHセッションを可能にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが効率化されます。

組織はSSHベースのシステムのセキュアなリモート管理を必要としています。スタンドアロンのSSHクライアントを使用する従来の方法では、エンドポイントを管理されていない環境にさらすことでリスクが生じ、堅牢なデータ損失防止（DLP）の実施が不足しているため、コンプライアンスが困難になります。

SSHセッションは、スタンドアロンのSSHクライアントではなくChromeブラウザ内で起動されるようになり、ローカルインストールへの依存が減り、コンプライアンスが向上します。

注:

- この機能は、ハイブリッドおよびクラウド展開向けのChrome Enterprise Premium統合Secure Private Accessセットアップに適用されます。詳細については、以下のトピックを参照してください。
- Secure Private AccessおよびChrome Enterprise Premiumポリシーを構成するには、管理者権限が必要です。
- FreeBSDサーバーへの接続はサポートされていません。

この統合の利点

この統合は、以下の主要な利点を提供します。

- **セキュリティの強化:** 管理されていないSSHクライアントへの依存を排除し、セキュリティリスクへの露出を低減します。
- **アクセスの簡素化:** ブラウザネイティブのアクセスを提供し、追加のソフトウェアインストールの必要性を排除します。
- **コンプライアンス:** 企業DLPポリシーをブラウザ内で直接適用し、規制要件の遵守を支援します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **運用効率:** エンドポイント管理とクライアント展開に関連するITオーバーヘッドを削減します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **医療キオスク:** ネイティブクライアントをインストールすることなく、デバイスのトラブルシューティングのためにセキュアなSSHアクセスを可能にします。
- **IT管理:** 管理者は、DLPポリシーが適用された管理対象のChromeブラウザからLinuxサーバーに安全にアクセスできます。
- **請負業者アクセス:** 組織のセキュリティ体制を損なうことなく、サードパーティベンダーに一時的なSSHアクセスを提供します。

システム要件

お使いの環境が以下の要件を満たしていることを確認してください。

- Chrome Enterprise Premium の最新バージョン。
- Citrix Secure Private Access が統合用に構成されていること。
- SSHトラフィックを許可するアクセスポリシーは、Secure Private Access 管理コンソールで作成する必要があります。

前提条件

SSHアプリケーションへのセキュアなアクセスを有効にするために、以下の前提条件が満たされていることを確認してください。

- Citrix Secure Private Access が Google Chrome Enterprise Premium と統合されていること。詳細については、「Google Chrome Enterprise Premium との統合」を参照してください。
- エンドユーザーが、Citrix Secure Access ブラウザ拡張機能を備えた最新の Google Chrome ブラウザをインストールしていること。
- 展開固有の前提条件については、以下のトピックを参照してください。
  - クラウド展開 - Citrix Secure Private Access の使用を開始する
  - ハイブリッド展開 – システム要件と前提条件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSHアクセス用にSecure Private Accessを構成する

1. Citrix Cloud にログインし、**Secure Private Access** をクリックします。
2. 管理コンソールで、**Applications > App Configuration** をクリックし、**Add an app** をクリックします。
3. セキュア プライベート アクセス内で、SSHアプリをTCP/UDPアプリとして構成します。
   - アプリは、サーバーの正確なIPアドレス、範囲、FQDN、またはホスト名を持つことができます。
   - SSHは、デフォルトポートおよび非デフォルトポートでサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDPアプリの作成に関する詳細については、次のトピックを参照してください。

- クラウド展開 - TCP/UDPアプリのサポート
- ハイブリッド展開 – TCP/UDPアプリのサポート

SSHポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **SSH**を選択し、**管理**をクリックします。
4. **ルールの追加**をクリックして、ユーザーがSSHを有効にするためのルールを追加します。
5. ルールの名前を入力し、**次へ**をクリックします。
6. ユーザーやグループなど、要件に基づいて条件を選択します。 1. **地理的位置、ネットワークロケーション**、および**デバイスポスチャチェック**などの条件を追加することもできます。
7. **次へ**をクリックします。
8. 「**保存**」をクリックします。

アンチキーロギングポリシー用に構成されたルールの数は、**ブラウザポリシー > SSH**タブに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リモートデスクトップ制御

Citrix Secure Private Accessは、Chrome Enterprise Premiumと統合されており、ブラウザ内で直接安全なRDPセッションを可能にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが効率化されます。

従来のリモートデスクトップアクセスは、多くの場合、ネイティブRDPクライアントに依存しており、これらは通常、ブラウザベースのDLP適用機能がありません。この欠点により、特に管理されていない環境ではセキュリティリスクが増大する可能性があり、コンプライアンスが困難になります。組織は、これらの懸念に対処する、安全で、準拠しており、簡素化されたリモートアクセスソリューションを必要としています。

この統合により、管理者はクリップボード制御やスクリーンショット防止などのエンタープライズグレードのDLP制御を適用できます。

注:

- この機能は、ハイブリッドおよびクラウド展開向けのChrome Enterprise Premiumと統合されたSecure Private Accessのセットアップに適用されます。詳細については、以下のトピックを参照してください。
- Secure Private AccessおよびChrome Enterprise Premiumポリシーを構成するには、管理者権限が必要です。

サポートされていない機能:

以下の機能はサポートされていません。

- クリップボード共有
- オーディオ/Webカメラ/スマートカード/USBリダイレクト
- 2要素認証および生体認証

この統合の利点

この統合は、以下の主要な利点を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **セキュリティ:** きめ細かなDLPポリシーを適用することで、リモートセッション中のデータ漏洩を防ぎます。
- **コンプライアンス:** 堅牢なセキュリティ制御を通じて、機密性の高い環境向けの規制要件を満たすのに役立ちます。
- **使いやすさ:** 個別のRDPクライアントをインストールする必要がなくなり、ユーザーアクセスと展開が簡素化されます。
- **柔軟性:** 管理対象のChromeブラウザからのセキュアなRDPアクセスをサポートし、一貫性のあるセキュアなエクスペリエンスを提供します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **企業請負業者:** 内部セキュリティを損なうことなく、サードパーティベンダーにセキュアなリモートデスクトップアクセスを提供します。
- **医療従事者:** 医療現場のキオスクまたは共有ワークステーションからWindowsシステムへのセキュアなアクセスを可能にします。
- **ITサポート:** 追加のソフトウェアインストールを必要とせずに、IT担当者がリモートデスクトップのトラブルシューティングを行うことを可能にします。

システム要件

環境が次の要件を満たしていることを確認してください。

- Chrome Enterprise Premiumの最新バージョン。
- Citrix Secure Private Accessが統合用に構成されていること。
- RDPトラフィックを許可するアクセスポリシーは、Secure Private Access管理コンソールで作成する必要があります。

前提条件

RDPアプリケーションへのセキュアなアクセスを有効にするために、次の前提条件が満たされていることを確認してください。

- Citrix Secure Private AccessがGoogle Chrome Enterprise Premium統合で構成されていること。詳細については、「Google Chrome Enterprise Premiumとの統合」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- エンドユーザーが、Citrix Secure Accessブラウザ拡張機能とともに最新のGoogle Chromeブラウザをインストールしていること。
- 展開固有の前提条件については、次のトピックを参照してください。
  - クラウド展開 - Citrix Secure Private Accessの概要
  - ハイブリッド展開 – システム要件と前提条件

RDPアクセス用にSecure Private Accessを構成する

1. Citrix Cloudにログインし、**Secure Private Access**をクリックします。
2. 管理コンソールで、**アプリケーション > アプリ構成**をクリックし、次に**アプリの追加**をクリックします。
3. Configure the RDP app as a TCP/UDP app within Secure Private Access.
   - アプリは、サーバーの正確なIPアドレス、範囲、FQDN、またはホスト名を持つことができます。
   - RDPは、デフォルトポートおよび非デフォルトポートでサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDPアプリの作成に関する詳細については、次のトピックを参照してください。

- クラウド展開 - TCP/UDPアプリのサポート
- ハイブリッド展開 – TCP/UDPアプリのサポート

リモートデスクトップポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、次に**ブラウザポリシーの作成**をクリックします。
3. **リモートデスクトップ**を選択し、次に**管理**をクリックします。
4. リモートデスクトップを有効にするためのルールをユーザーに追加するには、「**ルールを追加**」をクリックします。
5. ルールの名前を入力し、「**次へ**」をクリックします。
6. ユーザーまたはグループなど、要件に基づいて条件を選択します。1. **地理的位置、ネットワークロケーション、デバイスポスチャチェック**などの条件を追加することもできます。
7. **次へ**をクリックします。
8. 「**保存**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アンチキーロギングポリシーに設定されているルールの数は、「**ブラウザポリシー > リモートデスクトップ**」タブに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.