

---

# Ericom Blaze ドキュメント

---

Ver. 9.5

株式会社アシスト 仮想化事業推進室

**アシスト**

# 目次

第 1 章	改訂履歴	2
第 2 章	システム要件	3
2.1	Ericom Blaze . . . . .	3
第 3 章	製品のリリースノート	6
3.1	Ericom Blaze リリースノート . . . . .	6
第 4 章	管理者ガイド	11
4.1	Ericom Blaze 管理者ガイド . . . . .	11
4.2	Secure Gateway 管理者ガイド . . . . .	66
4.3	AccessToGo 管理者ガイド . . . . .	118
第 5 章	APPENDIX	183
5.1	Ericom Secure Gateway の CSR 作成 . . . . .	183
5.2	Blaze Client/AccessNow 利用時のエラー . . . . .	191
5.3	サポートポリシー . . . . .	194
5.4	サポート / お問い合わせ先 . . . . .	196
第 6 章	法律に基づく告知および免責事項	202

**注意:**

現時点では、Ericom 社でも 9.5 のマニュアルは未公開ため、管理者ガイドについては 9.1 の情報を掲載しております。

## 第 1 章

### 改訂履歴

改定日	版数	改訂内容
2021/9/3	1.1 版	<ul style="list-style-type: none"><li>Windows 10 SAC 21H1 をサポート開始に伴い、「<i>Ericom Blaze</i> リリースノート (ページ 6)」の「新機能および修正点」を更新しました。</li></ul>
2021/3/12	初版	

## 第 2 章

# システム要件

## 2.1 Ericom Blaze

### 2.1.1 サーバ要件

Ericom Access Server	<p>OS</p> <ul style="list-style-type: none"> <li>• Windows 7<sup>*1</sup>、8.1、10<sup>*4</sup></li> <li>• Windows Server 2008<sup>*2</sup>、2008R2<sup>*2</sup>、2012R2、2016、2019<sup>*4</sup></li> </ul>
----------------------	--

\*1 以下の条件で Windows 7 ESU へのサポート

1. お客様が Microsoft 社と Windows 7 ESU の契約を有しており、提供されている ESU の最新版を適用していること
2. サポート期間は 1 年※

※ Microsoft 社自体が Windows 7 ESU を 1 年更新としているため次年度以降サポートするかは 1 年が経過する前に、お客様のニーズを確認して改めて判断 (2 年目 (2021 年 1 月-2022 年 1 月まで) についてもサポート)

\*4 Windows Server 2016 以降と Windows 10 の長期サービスチャネルと半期チャネルのサポート対応については、パートナー Web もしくは AWSC の資料検索より対象資料をダウンロードいただき、ご一読ください。

\*2 Windows Server 2008 R2 ESU へのサポートについて

Windows Server 2008 R2 ESU は以下の条件でサポートとなります。

お客様が Microsoft 社と Windows Server 2008 R2 ESU の契約を有しており、提供されている ESU の最新版を適用していること。サポート期間は 1 年 ※

※ Microsoft 社自体が Windows Server 2008 R2 ESU を 1 年更新としているため次年度以降サポートするかは 1 年が経過する前に、お客様のニーズを確認して改めて判断 (2 年目 (2021 年 1 月-2022 年 1 月まで) についてもサポート)。但し、**Windows Server 2008** は製品の導入前提に必要な **.Net Framework** のバージョンが未対応のため、**2020 年 1 月 14 日**以降はサポート対象外 となります。

Ericom Secure Gateway*3	<p>OS</p> <ul style="list-style-type: none"> <li>Windows Server 2008*5、2008R2*5、2012R2、2016、2019*4</li> </ul> <p>参考スペック) 複数のセッションを中継する場合</p> <p>CPU 4 Core 以上 メモリ 8 GB 以上 HDD 80 GB 以上</p>
-------------------------	--

## 2.1.2 クライアント要件

### Windows でタッチインターフェースを有するデバイス

タッチインターフェースの機能を有するデバイスにおいてソフトウェアキーボードでの入力はサポートされません。



警告:

ただし、デバイスに元々付属の物理的なキーボード、または、USB 等で接続した物理キーボードを利用する場合において、タッチ機能を OS 上で無効化して利用いただくことで物理キーボードでの入力はサポート可能です。

タッチ機能を無効化せずとも問題なく利用できる端末もございますが、製品動作サポートの観点ではタッチ機能の無効化状態での利用を動作サポート可とさせていただきます。

## Blaze クライアントの場合

\*3 簡易的な SSL ゲートウェイとしてご利用いただけます。Windows のみの対応。

\*5 Windows Server 2008 R2 ESU へのサポートについて

Windows Server 2008 R2 ESU は以下の条件でサポートとなります。

お客様が Microsoft 社と Windows Server 2008 R2 ESU の契約を有しており、提供されている ESU の最新版を適用していること。サポート期間は 1 年 ※

※ Microsoft 社自身が Windows Server 2008 R2 ESU を 1 年更新としているため次年度以降サポートするかは 1 年が経過する前に、お客様のニーズを確認して改めて判断 (2 年目 (2021 年 1 月-2022 年 1 月まで) についてもサポート)。但し、**Windows Server 2008** は製品の導入前提に必要な **.Net Framework** のバージョンが未対応のため、**2020 年 1 月 14 日**以降はサポート対象外 となります。

Microsoft Windows	<p>OS</p> <ul style="list-style-type: none"> <li>Windows 7*9、8.1、10*6</li> <li>Windows Embedded Standard 7*8</li> <li>Windows Server 2008R2*10、2012R2、2016、2019*6</li> </ul>
Apple macOS	未サポート
Linux	Linux Ubuntu 16.04 LTS、18.04 LTS*7

## モバイルクライアント (AccessToGo) の場合

Apple iOS*11	<p>OS</p> <ul style="list-style-type: none"> <li>iOS 11.x、12.x*13、13.x、14.x*14</li> </ul>
iPadOS	<p>iPadOS</p> <ul style="list-style-type: none"> <li>13.x、14.x*14</li> </ul>
Google Android*12	<p>OS</p> <ul style="list-style-type: none"> <li>Android 6.x、7.x、8.x、9.0*13</li> </ul>

\*9 以下の条件で Windows 7 ESU へのサポート

- お客様が Microsoft 社と Windows 7 ESU の契約を有しており、提供されている ESU の最新版を適用していること
- サポート期間は 1 年※

※ Microsoft 社自体が Windows 7 ESU を 1 年更新としているため次年度以降サポートするかは 1 年が経過する前に、お客様のニーズを確認して改めて判断 (2 年目 (2021 年 1 月-2022 年 1 月まで) についてもサポート)

\*6 Windows Server 2016 以降と Windows 10 の長期サービスチャネルと半期チャネルのサポート対応については、パートナー Web もしくは AWSC の資料検索より対象資料をダウンロードいただき、ご一読ください。

\*8 Windows10 IoT は未サポートです。

\*10 Windows Server 2008 R2 ESU へのサポートについて

Windows Server 2008 R2 ESU は以下の条件でサポートとなります。

お客様が Microsoft 社と Windows Server 2008 R2 ESU の契約を有しており、提供されている ESU の最新版を適用していること。サポート期間は 1 年 ※

※ Microsoft 社自体が Windows Server 2008 R2 ESU を 1 年更新としているため次年度以降サポートするかは 1 年が経過する前に、お客様のニーズを確認して改めて判断 (2 年目 (2021 年 1 月-2022 年 1 月まで) についてもサポート)

\*7 Ericom Blaze Client for Linux 9.0 は未リリースのため、ご利用時は ver.8.5 のクライアントをご利用ください。

\*11 Bluetooth キーボードは英語配列のみサポート

\*13 iOS11.x と 12.x、および Android7.x は モバイルクライアント (AccessToGo, Ericom Blaze Client, Ericom WebConnect Mobile Client, Ericom Connect Mobile Client) 8.1.2 以上でのみサポート。Android 8.x および 9.0 はモバイルクライアント (AccessToGo, Ericom Blaze Client, Ericom WebConnect Mobile Client, Ericom Connect Mobile Client) 9.2 以上でのみサポート

\*14 iOS13.x と iPadOS13.x および iOS14.x と iPadOS14.x はモバイルクライアント (AccessToGo, Ericom Blaze Client, Ericom WebConnect Mobile Client, Ericom Connect Mobile Client) 9.2.1 以上でのみサポート

\*12 Bluetooth キーボードは非サポート

## 第3章

# 製品のリリースノート

## 3.1 Ericom Blaze リリースノート

### 3.1.1 パッケージング

■ Ericom Blaze に含まれているコンポーネントのバージョン

(パッケージ番号 : b\_9500001)

コンポーネント	モジュール名
Ericom Access Server 本体インストーラ (32bit)	EricomAccessServer.msi
Ericom Access Server 本体インストーラ (64bit)	EricomAccessServer64.msi
Ericom Blaze クライアント (Windows 用 32bit)	EricomBlazeClient.msi
Ericom Blaze クライアント (Windows 用 64bit)	EricomBlazeClient64.msi
Ericom Secure Gateway インストーラ	EricomSecureGateway.exe
HP ユニバーサルプリンタドライバ (UPD) 64bit	upd-ps-x64-7.0.0.24832.exe
HP ユニバーサルプリンタドライバ (UPD) 32bit	upd-ps-x32-7.0.0.24832.exe
Lexmark ユニバーサルプリンタドライバ (UPD)	Lexmark_Universal_v2_UD1_Installation_Package_02212020.exe

### 3.1.2 新機能および修正点

#### Blaze Client 9.5.0.58607

【リリース日 : 2021/9/3】



## 新機能

- Blaze Client 9.5 で Windows 10 SAC 21H1 をサポート開始しました。

【リリース日：2021/3/12】

AccessNow 9.5 とバージョン番号を揃えるため、Blaze 9.5 としてリリースしています。

## ■ Ericom Access Server 9.5.0.58804

【リリース日：2021/9/3】

## 新機能

- Access Server 9.5 で Windows 10 SAC 21H1 をサポート開始しました。

【リリース日：2021/3/12】

AccessNow 9.5 とバージョン番号を揃えるため、Blaze 9.5 としてリリースしています。

## ■ 3.1.3 制限事項および既知の不具合

### ■ Blaze クライアント

#### 入力関係

- [英数] キーが効きません。
- Ubuntu において [ひらかな/ローマ字/カタカナ] キーと [英数] キーが有効になりません。
- Windows 10 で [Ctrl]+[Alt]+[End] のコンビネーションキーが効きません。

#### リダイレクト・印刷関係

- プリンタリダイレクトを利用する場合、クライアントは 7.6.1 以降のバージョンを使用してください。

- プリンタリダイレクトを [汎用] で利用する場合、クライアント PC に Acrobat Reader DC を導入してください。また、事前に Adobe Reader DC を 1 度起動し、ライセンス規約に「同意する」ボタンを押下しておく必要があります。
- EricomRDP では、DynamicDrives が機能しません。この問題は、現在 Ericom 社へエスカレーション中です。
- Blaze 接続において、HP 汎用ドライバを利用しており印刷が遅い場合は、Lexmark のご利用をご検討ください。  
※ Lexmark は、Ericom 製品バージョン 8.5 以降で利用可能です。

#### アプリケーションウィンドウ関係

- フルスクリーンモードの間、セッションが終了すると、最小化機能と最大化機能が機能しなくなることがあります。  
→ アプリケーションを再起動して、ウィンドウサイズを調整します。
- Blaze セッションが最小化されると、復元できないことがあります。 → アプリケーションを終了し、再起動してセッションに再接続します。
- シームレスなアプリケーションウィンドウをドラッグするとスムーズに機能しないことがあります。ウィンドウのドラッグ操作が完了するまで黒色の空白領域が表示されます。
- Ericom Connect 8.0 でサポートを開始した EricomRDP は Ericom Blaze の単体利用ではサポートされておられません。
- Windows Server 2008 R2 上で AccessPad(Blaze クライアント) を利用した場合、Alt + Tab でウィンドウを切り替えたあと、公開アプリケーションへの最初の文字が欠落する問題があります。
- Blaze Client for Linux ではフルスクリーンで起動したセッションをリサイズした場合、再びフルスクリーンに戻すことができません。一度セッションを切断し、再接続してください。
- マルチディスプレイ利用時は、全てのディスプレイの拡大・縮小の倍率は同一でご利用ください。(Windows10 の場合、「テキスト、アプリ、その他の項目のサイズを変更する」の設定を複数のディスプレイで同じ設定でご利用ください。) 倍率が異なる場合、正しく公開アプリケーションの表示がされない場合があります。
- 以下 3 つ全ての条件で利用しているケースでは、公開アプリケーションが起動できない場合があります。
  - 接続元端末側でマルチモニタを使用している
  - Microsoft シームレスモードを使用している
  - 接続先 RDS サーバが Windows Server 2019 である

回避策として、Blaze Client ログイン画面の [Programs] にある「Hide Taskbar when remote program is in Full Screen/Maximize mode」にチェックを入れて接続してください。

- Blaze 接続でリモートの全画面プリントスクリーンを取得する場合は、「Ctrl+PrtSC」とする必要があります。

## その他

- Blaze クライアントとして Windows 10 IoT は問題があるためサポートされません。
- 端末のコンピュータ名が日本語（ダブルバイト）になっている場合、AccessPad 等による接続時に下記エラーが発生する  
Unable to connect to sca.sumple.com Ericom Secure Gateway error (4) WebSocket negotiation with host failed.
- アプリケーションを閉じても接続先サーバ上から当該ユーザのセッションが切断で残る場合は、Windows 側のタイムアウトのポリシーなどを利用し、切断セッションのログオフをご確認ください。

## ■ Mobile Client(AccessToGo)

### 入力関係

- ソフトウェアキーボードの [undo] と [redo] がボタン効かない場合があります。
- iOS で Bluetooth キーボードを利用する場合、英語配列のみがサポートされます。
- Android においては Bluetooth キーボードの利用はサポートされていません。
- iOS で Bluetooth キーボード利用時に「Alt+Tab」のコンビネーションキーでリモートのアプリケーションの切り替えをすると、最後に起動した 2 つのアプリケーションしか切り替えることができません。
- iPhone にて VGA 出力コネクタを接続後に、モバイルクライアントを利用開始すると画面の一部しか表示されません。  
→ 回避策として、モバイルクライアントを起動後に VGA 出力コネクタを iPhone に接続してください。
- リモートの Windows8.1 もしくは Windows10 の IME で自動変換候補が表示されている時に、表示されている候補を選択して確定すると確定文字の後ろに入力した文字が追加されます。
- iOS10 以降と iPadOS において、Bluetooth キーボードや Smart Keyboard を利用した場合に、iOS 側の変換候補が表示  
→ モバイルクライアント利用時の文字入力には、iOS の IME を利用せず、リモートの Windows 側 IME を利用してください。
- Bluetooth キーボードや Smart Keyboard を利用している場合、「英数」「かな」入力の切り替えはキーボード上のキーではなく、「Control + Space」等のショートカットキーをご利用ください。JIS 配列のキーボードの「英数」「かな」キーでは正しく切り替えができません。
- バックスラッシュが利用可能なシステムでは、円記号ではなくバックスラッシュをご利用ください。円記号は利用できない場合があります。

#### リダイレクト・印刷関係

- iOS や Android ではローカルドライブのリダイレクトはできません。

#### アプリケーションウィンドウ関係

- iOS や Android ではアプリ公開の設定時は EXE ファイルの指定のみが可能です。(バッチファイル、URL、ドキュメントは使用できません。)

#### AccessServer との互換性

- AccessToGo および Ericom Blaze Mobile Client 7.6.1 と Access Server 3.2 を組合わせて利用する場合に、Access Server が異常終了する場合があります。その場合は、Access Server 3.4 以上にバージョンアップしてご利用ください。
- AccessToGo 9.2.0 から Access Server 7.3 以下のバージョンに接続するとアプリを起動するとセッションの切断と再接続

→ 以下いずれかの回避策で対応をお願いします。

- アプリプロパティを変更し Blaze 利用を Off にする
- Access Server のバージョンを 7.3 以上にバージョンアップする

#### その他

- Android/iOS とともに、端末のサイズが 5.5 インチ未満の場合とメモリが 320MB の場合、以下のメッセージが出力されます  
「警告：デバイスの RAM が 320MB 未満ではアプリケーション予期せず終了したり遅くなる場合があります」

## Access Server

- Access Server 8.5 以上ではバージョン毎にライセンスキーの申請が必要となります。新規導入の場合だけでなく、バージョンアップ時にもライセンスキーの再請求が必要となります。
- Access Server 8.5 以上ではセントラル・サーバの機能は利用できません。

## 第 4 章

# 管理者ガイド



注意:

現時点では、Ericom 社でも 9.5 のマニュアルは未公開ため、管理者ガイドについては 9.1 の情報を掲載しております。

## 4.1 Ericom Blaze 管理者ガイド

### 4.1.1 Ericom Blaze 管理者ガイド

#### 概要

Ericom Blaze は、衛星通信、ブロードバンド、支社などの大部分のワイド・エリア・ネットワーク (WAN) 上で、強化されたりモート・コンピューティング体験をエンドユーザに提供します。Microsoft リモート・デスクトップ・プロトコル (RDP) のアクセラレートと圧縮を行うことにより、これが実現されています。それにより、高いフレーム・レート、向上した応答時間、よりスムーズな画面の更新が提供されます。Ericom Blaze は、以下の動作を実行します:

- RDP 通信を分析し、ビットマップなどのグラフィック要素を識別し圧縮します。最適なユーザ・エクスペリエンスを提供するために、品質と圧縮の比率を設定可能です。
- タスクバーやスタート・メニューなどの主要なグラフィック要素を識別し、全体の品質設定に関わらず、高い品質でそれらを圧縮します。これにより、視覚的に品質低下のないリモート・コンピューティング体験が提供されます。
- 高パフォーマンスの一括圧縮方式を使用し、RDP 通信全体を圧縮します。
- ネットワーク使用の最適化とデータ・パケットの転送を高速化のために、パケット・シェーピングを実行します。
- 画面がブロックの連続ではなく、1 つのユニットとして表示されるよう、インテリジェントにフレームをレンダリングします。

Ericom Blaze は、RDP に対応しているすべての x86 または x64 ベースのホスト・システムで動作します。例えば、Windows ターミナル・サーバ、リモートの物理システム、VDI ベースのデスクトップなどです。Ericom Blaze は以下のコンポーネントで構成されています:

- **Ericom Access Server:** このコンポーネントは、RDP の圧縮とアクセラレーションのために RDP サーバ/ホストにインストールします。以下のプラットフォームがサポートされています:
  - Windows Server 2008 32 ビットおよび x64
  - Windows Server 2008 R2
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows 7 SP1、8.1、および 10 (x64 および 32-bit)
- **Ericom Blaze クライアント:** このクライアント・コンポーネントは、アクセラレートされた RDP を使用して Access Server に接続します。また、任意の標準 RDP ホストに接続することができます。以下のプラットフォームがサポートされています:
  - Windows 7、Windows 8.1、Windows 10 LTSB、Windows Server 2008、2008 R2、2012 R2、および 2016 LTSB (32 ビットおよび x64)
  - Windows 10 SAC 1709、1803
  - Linux Ubuntu: 16.04 [XFCE、Unity、LXDE: openbox、GNOME: classic] および 18.04 [XFCE、LXDE: openbox、GNOME: shell] (AccessServer8.\*には対応していません)
  - Apple Mac OS 10.11、10.12、10.13 (Intel ベース) (AccessServer8.\*には対応していません)
- **Ericom Blaze モバイル・クライアント:** このクライアント・コンポーネントは、アクセラレートされた Blaze を使用して Access Server に接続します。また、任意の標準 RDP ホストに接続することができます。詳細とサポートされるオペレーティング・システムのバージョンについては、AccessToGo のマニュアルを参照ください。

## 5 分で使用を開始する

Ericom Blaze は、豊富な機能を備えた、使いやすいアプリケーションです。このマニュアルでは、ユーザの環境に最適なアプリケーション設定を支援するために、使用可能なすべての機能を網羅しています。基本的なインストールは約 5 分間で完了し、Blaze クライアント (AccessToGo を起動しているモバイル・デバイスを含む) を起動している任意のデバイスから、Windows RDP ホスト (サーバやワークステーション) にアクセスできるようになります。

1. Ericom の Web サイトから、EricomAccessServer.msi をダウンロードします。
2. MSI インストーラを実行し、すべてのダイアログ・ボックスで Next をクリックし、最後に Finish をクリックします。
3. Blaze を使用するために、Windows ファイアウォールを設定 (または無効化) します。Access Server インストール時に Windows ファイアウォールは自動で設定されます。

4. Ericom の Web サイトから、EricomBlazeClient.msi をダウンロードします
  - (a) モバイル・デバイスから接続している場合、AccessToGo アプリをデバイスにダウンロードします。
5. Blaze Client(または AccessToGo) に Access Server のパラメータを入力し、接続 ボタンを押して接続を開始します。

## 4.1.2 Ericom Access Server

Ericom Access Server では AccessNow HTML5 アクセスと Blaze RDP 圧縮やアクセラレーションの機能が提供されています。試用期間中はすべての機能が利用可能となり、試用期間終了後はアクティベーション・キーを使用してロック解除することで各機能が利用可能になります。ホストには、Windows ターミナル・サーバや Windows ワークステーションなどの RDP アクセスが有効となっている Windows システムを使用できます。Access Server はカスタマイズ可能なポートを使用しており、ポート番号のデフォルトは 3399 となります。AccessNow が使用するポート 8080 も有効にされていますので Blaze Client からポート 8080 で接続する場合は接続先コンピュータ名のフィールドにポート 8080 を明示的に指定してください。(例: 192.168.1.100:8080)



注意:

Ericom Access Server 3.x は、Blaze のバージョン 2.x 以前のバージョンには下位互換性がありません。  
以前のバージョンの Blaze を使用している場合、バージョンが一致するように、すべての  
→Blaze クライアントと  
サーバ・コンポーネントをアップグレードしてください。

Access Server は、RDP ホストまたはプロキシとして動作する専用のシステム(「ジャンプ」サーバとも呼ばれます)にインストール可能です。Access Server を RDP ホストに直接インストールすることをお勧めします。ファイル転送などの一部の機能は、Access Server が RDP ホスト自体にインストールされている場合においてのみ利用可能となります。Access Server は比較的軽快に動作するため、RDP ホストのパフォーマンスや拡張性への影響は最小限にとどまります。

### Ericom Access Server 要件

- Windows オペレーティング・システム (7/2008 以降)
- ホスト OS にて受信用 RDP 接続が有効である (例: ターミナル・サーバ)
- ハードディスク上の 80MB の空き容量
- MMX および SSE2 対応 CPU
- Access Server による 3399) ポートまた AccessServer(32/64).exe のトラフィックが可能に設定されたファイアウォール

Access Server はアクセラレーションまたは HTML5 アクセスが必要とされる各サーバ/ホストにインストールする必要があります。すべてのユーザのセッションをアクセラレーションするために、1つのターミナル・サーバのインストールが必要です。各ワークステーションやデスクトップ(物理または仮想)にインストールが必要です。Microsoft の Sysprep または Symantec の Ghost を使用してデプロイされるイメージの一部として、Access Server を含むことが可能です。

すべてのネットワーク・インターフェースに対するバインド・サービス

仮想ネットワーク環境において、1つの仮想 NIC のみを使用するのではなく、すべての仮想ネットワークのインターフェースを使用するために、Access Server をバインドすることをお勧めします。対象とするエンド



ユーザが、Access Server で使用するネットワークのインターフェースに常時アクセス可能であることを確認してください。

#### ホストのファイアウォール設定

エンドユーザのデバイスから Ericom Access Server へのトラフィック通信を許可していることを確認してください。ファイアウォールの設定が必要となる場合があります。(Access Server をインストールすると自動で受信規則が登録されます)

Windows オペレーティング・システムでは、Windows ファイアウォールが Access Server ポート (デフォルトは 3399) を許可するよう設定されていることを確認してください。



注意:

接続の問題を解決するには、一時的に Windows ファイアウォールを無効にします。ファイアウォールを無効にした場合のみで接続が可能となる場合、Access Server が使用するポートをブロックする規則が存在している可能性があります。

Ericom が使用するポートを許可する規則を追加するには、以下の手順を実行します (手順は Windows 7/2008 をベースにしています):

- コントロール・パネルに進み、Windows ファイアウォール に進みます。詳細設定 を選択し、受信の規則 を選択します。新しい規則 をクリックします。

- ポート を選択し、次へ をクリックします。指定のポート 3399 を入力します:

- 次へ をクリックし、接続を許可する を選択します

- 次へ をクリックし、規則を適用するネットワークを選択します (すべて選択)
- 次へ をクリックし、規則に名称 (Ericom) を設定した後、完了 をクリックします

### ポート転送の設定

Blaze が有効となっているホストへポート転送するためにファイアウォールを設定する際には、Access Server ポート (デフォルト: 3399) へ転送されていることを確認してください。3389(デフォルトの RDP ポート) には転送しないでください。カスタム・ポートが使用されている場合、Communication ページで設定されているポート値に転送するようファイアウォールを設定します。

### NLA サポート

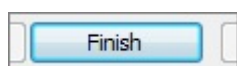
Blaze クライアントでは、以下の 3 つの条件の下で NLA がサポートされています:

- アクセラレーション が有効化されている
- ユーザ名とパスワードが適切なフィールドに入力されている
- 「常に資格情報を求める」のチェックボックスがオフになっている

非アクセラレーション・モードの Blaze クライアントでは、NLA はサポートされていません。

### Ericom Access Server のインストール

- EricomAccessNowServer.msi を実行し、インストール・ウィザードの指示に従います。
- License Agreement を確認し、同意します。
- Install をクリックします。(必要に応じて、セキュリティ権限を上げるリクエストを許可します) 最後のスクリーンにて Finish をクリックし、インストールを完了します。



- Access Server ポートが利用可能であり、ホスト・システムにアクセスが可能なことを確認します。Access Server は自動的に必要な規則を Windows の ファイアウォールに追加しますが、ネットワーク上でのファイアウォール設定の追加が必要になる場合があります。



- インストールの後、Access Server はサービスとしてシステム上で実行されます。



- このサービスはシステム起動時に自動的に実行されるよう設定されています。
- サービスが停止しているか、またはデフォルトの 3399 ポートを認識できない場合には、クライアントはホストに接続できません。他のアプリケーションが同じポートを使用していないかを確認します。

Access Server は、Microsoft System Center のようなアプリケーション管理ツールを使用した、自動的なサイレント・インストールも可能です。

- サイレント・インストールを実施するには、次を実行します: `msiexec /I "EricomAccessServer.msi" /q`
- EricomAccessServer.msi は .msi ファイルへの有効なパスを表しています。
- Windows 7、8、Windows Server 2008 と 2012 では、このコマンドはより権限の高い管理者の資格情報が必要とされる場合があります。
- ヘルプ・ダイアログを表示するには、パラメータを指定せずに MSIEEXEC を実行します。



注意:

Access Server は、ホスト名に英文字以外の文字が含まれるシステムにはインストールできません。

## Ericom Access Server の使用

Access Server の設定を変更するには: スタート | すべてのプログラム | Ericom Software | Access Server Configuration に進みます。スタート・メニューのないシステムでは、以下のコマンドラインを使用して GUI を開始することができます。

<ドライブ> :`Program Files (x86)Ericom SoftwareEricom Access ServerServerConfiguration.hta`



注意:

Access Server は、AccessNow と Blaze 製品の両方で使用されます。

## Access Server の設定

Server Configuration コンソールは一連のタブを提供し、管理者がサーバ・サービスへの様々な設定を行うことが可能です。 Configuration コンソールは Microsoft Internet Explorer 7 またはそれ以上のバージョンを持つシステム上に限り動作します。(このコンソールは IE6 がインストールされているシステムでは起動できません)



### Tips:

ターミナル・サーバに Access Server をインストールする際、エンドユーザによる予期しない変更を避けるために、エンドユーザ向けには Server Configuration アプリケーションを非表示にすることをお勧めします。

## General

このページは Access Server のサービスの再起動および停止の機能を提供します。一部の設定変更では、サービスの再起動が必要です。またこのページでは、システム上でアクティブな Ericom セッションの数が表示されます。



### 注意:

Access Server のサービスが再起動される際、サーバ上のすべての AccessNow と Blaze のセッションの接続が解除されます。

Access Server service state:	Running
Access Server status:	Active
Number of sessions:	0
Started at	09/23/13 08:40:00
<input type="button" value="Start Server"/>	
<input type="button" value="Stop Server"/>	

## Licensing Information

このページでは、AccessNow と Blaze のライセンス情報が表示されます。 Connected to licensing server の項目には、現在使用されているライセンス・サーバが表示されます。



注意:

本番環境の VDI やターミナル・サーバ環境では、ライセンス・サーバは強固なシステム上で一元管理される必要があります。詳細については、セントラル・サーバの設定のセクションを参照してください。

デフォルトでは、Access Server は DNS lookup を使用して Licensing Server を特定します。使用される DNS エントリは、`ericom-license-server.<ドメイン名>` または `_ericom-license-server._tcp.<ドメイン名>` となります。DNS エントリが存在しない場合には、Access Server により同じコンピュータ上で実行されているライセンス・サーバへの接続が試行されます。

他の方法としては、Licensing server address 内の Access Server Configuration で、ライセンス・サーバのアドレスを明示的に指定します。ライセンス・サーバ・アドレスの変更後、General タブを使用して Access Server を再起動します。

有効なライセンスが見つからない場合、Access Server は猶予期間が終了するまで実行が可能となります。猶予期間の終了後、Access Server は、ユーザ・セッションを許可しなくなります。この「猶予期間」は 30 日間の期間内で最大 10 日間有効となります。

#### ライセンス・サーバのポートを変更する

ライセンス・サーバは、デフォルトでポート 8888 を介して通信します。同一システム上の他のアプリケーションがポート 8888 を使用している場合には、ライセンス・サーバのポート値をレジストリで変更することができます。レジストリ・エディタを使用して次に移動します。

HKLM | SOFTWARE | Ericom Software | LicenseServer

下記の文字列値を追加します。

#### Listening Port



上記の例では、ポートが 9999 へと変更されています。値を設定した後、Ericom Licensing Server サービスを再起動します。カスタム・ポートを使用してセントラル・ライセンス・サーバに接続する各 Access Server において、アドレスの後ろにコロンを付けてポート値を指定する必要があります。例:

Use DNS lookup  
 Licensing server address:

## ライセンスのアクティベーション

Licensing の下の Activation をクリックし、シリアル番号とアクティベーション・キーを製品の設定フィールドに入力します。

評価版で使用したインストールのアクティベーションには、目的の Client type を選択し、シリアル番号と key to send to Ericom の内容を記載し supportusa@ericom.com へ送信し、処理を依頼します。その後、アクティベーション・キーが返信されます。そのアクティベーション・キーを入力した後、Activate License ボタンをクリックします。ライセンスを有効にするために Access Server を再起動する必要はありません。

評価期間を延長するには、Ericom の営業担当者に key to send to Ericom の内容を送信し、処理を依頼します。依頼が承認された後、標準的な 30 日間の延長のキーが提供されます。

General	Licensing	Performance	Communication	Acceleration	Security	Logging	Advanced
Information		Activation					
<b>Client type:</b>		<div style="border: 1px solid black; padding: 2px;">         AccessNow          AccessNow_VMwareView          Blaze       </div>					
<b>License Description:</b>							
License Status:	Valid						
License Type:	Concurrent Users						
Counting Mode:	Permanent						
Expiration Date:	Never Expires						
Number of Licenses:	10						
Used Licenses:	0						
<p>If you have received a serial number from Ericom, please enter it into the field below before clicking the "Email to Ericom" button.</p>							
Serial Number:	<input type="text"/>						
Key to send to Ericom:	<input type="text" value="CJ68ZM-797THY"/>	<input type="button" value="Email Key To Ericom"/>					
Key received from Ericom:	<input type="text"/>						
<p>Copy the key received from Ericom Software into the form and click the "Activate License" button to activate the software license.</p>							

## Performance

このページには現在のサーバのパフォーマンス統計が表示されます。

General	Licensing	Performance	Communication	Acceleration	Security	Logging	Advanced
<b>Server to Client communication</b>							
Number of sessions:	0						
Average compression ratio:	69 %						
Total data received from host:	5 MB						
Total data sent to client:	1 MB						
<p>Real-time cumulative performance information for all sessions since Blaze Server was started. Counters are reset when the Blaze Server service is restarted. Display is automatically updated approximately once every 10 seconds.</p>							

## Communication

このページは、Access Server のリスニング・ポートと RDP を実行しているホストのアドレスを変更する機能を提供します。

デフォルト (8080) 以外のリスニング・ポートを使用している場合、ポート番号を Access Server のアドレスまたは Blaze クライアントの Computer フィールドで明示的に指定する必要があります。(例: rdpdemo.ericom.com:22)

AccessNow Web クライアント:

Ericom AccessNow Server:	rdpdemo.ericom.com:22
--------------------------	-----------------------

Blaze クライアント:

Computer:	rdpdemo.ericom.com:22
-----------	-----------------------

接続先のシステムが Access Server を実行していない場合、RDP ホストのアドレスが使用されます。この場合では、Access Server はエンドユーザと接続先ホスト・システム間でゲートウェイのプロキシとして動作します。このタイプの設定により AccessNow と Blaze のパフォーマンスに悪影響が生じる場合があるため、お勧めしません。

両方の設定の変更には、サービスの再起動が必要です。(General タブから)

General	Licensing	Performance	Communication	Acceleration	Security	Logging	Advanced
<p>Access Server port number: <input type="text" value="8080"/> <input type="button" value="Restore Default (8080)"/></p> <p>Changing this setting will take effect only after the Access Server service is restarted.</p> <p>Specifies the TCP/IP port on which the Access Server service listens for incoming connections. Do not use a port number which is already in use by some other service or application on the computer. If you do, Access Server service will not start.</p> <p><b>Important:</b> Access Server Clients automatically connect to port 8080 when using accelerated RDP. If a different port value is selected, that value must be explicitly specified in the Clients' host address field.</p> <hr/> <p>RDP host address: <input type="text" value="localhost"/></p> <p>Changing this setting will take effect only after the Access Server service is restarted.</p>							

複数のネットワーク・カードを備えたマシンにて Access Server を実行している場合は、RDP ホストのアドレスを localhost から、システムに RDP アクセス可能なネットワーク・カードの IP アドレスまたは DNS アドレスへ変更します。

## Acceleration

このページはアクセラレーション/品質レベルを強制的に適用し、動的圧縮を無効にする機能を提供します。Override client acceleration / quality settings チェックボックスがオンの場合、すべてのセッションで既存の設定が適用され、クライアントの設定は無視されます。この設定をオン、またはオフとする場合、変更を適用するためにサービスを再起動する必要があります。設定が有効にされている場合、アクセラレーション・

レベルの変更にはサービスの再起動は必要ではありませんが、新たな設定を使用するにはアクティブ・ユーザーの再接続が必要です。

Dynamic Compression はスクリーンの小さなグラフィカル・オブジェクト (ツールバーのアイコン、スタート・メニューのアイコン等) を識別し、Blaze の Quality 設定が Low の場合には High のクオリティを使用し、Blaze の Quality 設定が Low より高くなっている場合には Best のクオリティを使用してオブジェクトを圧縮します。その他のグラフィカル・オブジェクトは選択された品質で圧縮されます。これにより、リモート・デスクトップのセッションでの高画質な画面表示を提供します。デフォルトでは、この機能は有効にされています。無効するには、「Use dynamic compression」ボックスをオフとします。

General	Licensing	Performance	Communication	Acceleration	Security	Logging	Advanced
<input type="checkbox"/> <u>O</u> verride client acceleration / quality settings Acceleration / Quality: <span>Very Fast / Good Quality (recommended) ▼</span> Enable in order to ignore the performance / image quality settings requested by the Ericom Access Server Clients. Instead, use the specified performance / image quality settings for all incoming accelerated connections.							
<input checked="" type="checkbox"/> <u>U</u> se dynamic compression Dynamic compression improves perceived display quality by utilizing lower compression settings for specific screen elements. Small but important screen elements, such as window titlebars and the Start Menu, use a higher quality setting, which is computed dynamically from the general image quality setting. Dynamic compression utilizes High quality when image quality is set to Low; and Best quality when the image quality setting is higher than Low.							
Changing this setting may take effect only after the Access Server service is restarted.							

## Security

このページでは Access Server のセキュリティ設定を構成します。



General	Licensing	Performance	Communication	Acceleration	Security	Logging	Advanced
---------	-----------	-------------	---------------	--------------	----------	---------	----------

### Ericom Access Server supports strong SSL encryption

Encrypt Access Server communication:

By default Ericom Access Server uses the same security settings as Microsoft RDP - if RDP is encrypted then Access Server will be encrypted. If RDP is not encrypted then Access Server will not be encrypted either. Set to **Always** for Ericom Access Server to always encrypt regardless of the RDP settings.

**Data transmitted from the clients to the server, including user credentials, is always encrypted regardless of Access Server and RDP security settings.**

For best performance and lowest load on the server set the RDP Security Level to Low (for 2003/XP also set the Security Layer to RDP Security Layer). This setting can be changed using the RDS (TS) Session Host Configuration or using Local Computer / Group Policies. After performing this change, modify setting above to **Always** if encryption is required.

### SSL Certificate

**Friendly Name:**

**SAN:** DNS Name= [REDACTED]

**Thumbprint:** [REDACTED]

**Issued By:** [REDACTED] **Issued To:** [REDACTED]

**Valid From:** 2013/09/11 08:47:16 **Valid To:** 2014/09/11 08:47:16

### Change Certificate

To change the above certificate, enter a new certificate's thumbprint below (eg. [REDACTED]).

Certificate Thumbprint:

Note: this change will only take effect after you click apply AND restart Access Server.

Ericom Access は統合された 128-bit SSL 暗号化を提供します。パフォーマンスを向上するには、ホストの RDP Security Encryption レベルを低に設定し、Encrypt Blaze communication を Always に変更します。この設定により、RDP 暗号化の代わりに Ericom SSL 暗号化が使用されます。詳細については、このドキュメントの「Ericom Optimization」の章を参照してください。

カスタムまたは信頼された証明書を使用するには、証明書の拇印を Thumbprint のフィールドに入力し、Apply ボタンをクリックします。上の画像で例示されている黒いボックスのように、GUI に証明書のプロパティが表示されます。変更点を適用するためにサービスを再起動します。



注意:

信頼された証明書をインストールする際、Access Server の DNS アドレスが証明書の名前と一致する必要があります。ワイルドカード証明書を使用する場合、ドメインが一致する必要があります。例えば、証明書が \\*.acme.com 用である場合は、サーバ名は acme.com で終わる必要があります。

## Logging

このページでは、特定のログ機能を有効化/無効化する機能が提供されます。Ericom 社のサポートは、診断を目的としてデバッグのログを要求することがあります。デバッグのログはここで有効にすることができます。

**Advanced (管理者用)**

このページは、システムのレジストリに保存されている高度な Ericom Access Server 設定へのアクセスを提供します。

Export Setting – Access Server のレジストリ・キー をユーザのホーム・フォルダ (例: マイ ドキュメント) にエクスポートします。

Import Settings – 以前保存した AccessNow Server のレジストリ設定をインポートします。

Advanced Configuration – regedit.exe を実行、Access Server のレジストリ・キーを開きます。デフォルトでは、デフォルトから変更された設定のみレジストリに保存されます。



## Keep Alive 設定

Blaze の設定	説明	用途	デフォルト
session keepalive seconds:i:	クライアントが RDP ホストに Keep Alive メッセージを送信する間隔 (秒)。	ファイアウォールによってアイドル・セッションがドロップするのを防ぎます。設定すると、RDP セッションがアイドル状態となりません。AccessPad、Blaze および AccessToGo で使用されます。	0
tcp keepalive time ms:i:	TCP ソケットがアイドル状態となっている時間。この時間にキープ・アライブ・メッセージの送信を開始します。	ソケットの切断が Blaze によって素早く認識されます。AccessPad、Blaze および AccessToGo で使用されます。	10000
tcp keepalive interval ms:i:	TCP キープ・アライブ・メッセージの間隔。それらの 5 つが失敗した場合、ソケットは切断されます。	ソケットの切断が Blaze によって素早く認識されます。AccessPad、Blaze および AccessToGo で使用されます。	1000
session heartbeat seconds:i:	クライアントがハートビートを送信する間隔 (秒)。	AccessServer は、ハートビートを使用してクライアントの切断を認識し、サード・パーティのアイドル設定をオフセットします。ロードバランサおよび Secure Gateway とともに動作します。AccessPad、Blaze、AccessNow および AccessToGo で使用されます。(AccessServer 7.3 以降が必要です)	3
session heartbeat probes:i:	クライアントが切断状態であるとサーバーが判断する、欠落したハートビート数。	AccessServer は、接続を切断状態と分類するために、この設定を使用します。AccessPad、Blaze、AccessNow および Ac-	5

## ■ 拡張されたセッション・スクリプト

この製品は、RDP ホストにおける Windows のビルトインのスクリプト機能を拡張します。このメカニズムにより、セッションの開始時や終了時、接続時や切断時に特定のコマンドを実行する機能のレイヤーが追加されます。

### 起動後のログイン・スクリプト (`_login`)

適切な拡張子を使用して、`_login` という名前のファイルを作成します。例えば、「`_login.vbs`」という名前のスクリプト・ファイルや、「`_login.exe`」という名前の実行可能ファイルなどです。作成したファイルを、Access Server インストール・フォルダ内に `script` という名前のフォルダ内に保存します。このフォルダが見つからない場合には、フォルダを作成します。このスクリプトは、TS/RDS セッションがスタートアップフォルダを処理した後、新しいセッションの開始時に実行されます。

### 起動前のログイン・スクリプト (`__login`)

「`_login`」と同様、「`__login`」はセッションの開始時に実行されますが、こちらは TD/RDS がスタートアップフォルダを処理する前に実行されます。

### セッション接続時のスクリプト (`_connect`)

適切な拡張子を使用して `_connect` という名前のファイルを作成し、Access Server インストール・フォルダ内の `script` という名前のフォルダに保存します。このフォルダが見つからない場合には、フォルダを作成します。このスクリプトは既存の TS/RDS セッションへの接続時に実行されます。

### セッション切断時のスクリプト (`_disconnect`)

適切な拡張子を使用して `_disconnect` という名前のファイルを作成し、Access Server インストール・フォルダ内の `script` という名前のフォルダに保存します。このフォルダが見つからない場合には、フォルダを作成します。このスクリプトは、TS/RDS セッションからの切断時に実行されます。

### 新しいファイルを作成する VB スクリプトのサンプル

```
Set objFileToWrite = CreateObject("Scripting.FileSystemObject").OpenTextFile("newfile.txt",2,true)
objFileToWrite.WriteLine("hello world")
objFileToWrite.Close
```

### 4.1.3 ライセンスの概要

#### 評価 (デモ) 期間

各 Access Server のインストールには、同一のデバイスにインストールするライセンス・サーバが含まれています。デフォルトでは、ライセンス・サーバには 30 日間の検証期間が含まれています。この期間中、ライセンス・サーバは最大 50 の同時ユーザ接続を許可します。評価期間は、Ericom 営業担当に連絡し延長することが可能です。

#### ライセンス・モード



注意:

バージョン 8.5 以降で (評価用ライセンスではなく) 正規のライセンスを利用する場合は、ライセンス・モードに関しては弊社サポートセンターまでお問い合わせください。

Ericom のライセンス・サーバのサービスは Ericom AccessNow と Blaze のライセンスを管理します。Ericom Blaze クライアントや AccessNow を使用したすべての接続に Ericom のライセンスが必要です。1 つのライセンス・サーバで複数の Access Server のライセンスを管理することが可能です。ライセンスには 2 つのモードがあります。

**同時ユーザ:** 同一のライセンス・サーバを使用するすべての Access Server へ同時に接続しているアクティブ・ユーザ数により、Ericom のライセンスがカウントされます。このライセンス・モードでは以下の点が考慮されます:

- 同一ユーザが 1 つのクライアント・デバイスで開く Ericom のセッション数に対し、ライセンスの限度は適用されません。ユーザが 1 つのデバイスで開くセッション数に関わりなく、ライセンスが 1 つだけ使用されます。
- 同一ユーザが複数のデバイスから複数の Blaze セッションを同時に使用する場合、デバイスの数と同じ数のライセンスが使用されます。
- 複数のユーザが同じデバイスを使用する場合 (例: Mac のファスト・ユーザ・スイッチの利用)、アクティブな Blaze セッションを使用するユーザと同じ数のライセンスが必要です。

**指定ユーザ:** 同一ライセンス・サーバを使用するいずれかの Access Server に接続したことのある登録名の総数により、Ericom のライセンスがカウントされます。このライセンス・モードでは以下の点が考慮されます:

- ライセンスは、ユーザが初回に使用した任意の名前に割り当てられます。
- ユーザ名が 14 日間で一度も Blaze クライアントの実行に使用されなかった場合、ライセンスは自動的にリリースされます。その名前に割り当てられたライセンスは、14 日間の期間が経過する前にリリースすることはできません。
- Access Server を RDP ホストにインストールする必要があります。(PtTSAgent もこの方法を必要とするため) Access Server がゲートウェイとして使用されている場合、同時ユーザのライセンスのみが利用可能となります。

## 4.1.4 Ericom Blaze Client for Windows

Ericom Blaze クライアントは、Ericom Access Server を実行中で Blaze が有効化された Access Server に接続します。



注意:

Ericom Access Server 3.x は、Blaze のバージョン 2.x 以前のバージョンには下位互換性がありません。

以前のバージョンの Blaze を使用している場合、バージョンが一致するように、すべての

→Blaze クライアントと

サーバ・コンポーネントをアップグレードしてください。

## Ericom Blaze クライアントの要件

Ericom Blaze クライアントは、ユーザのデバイスにインストールされます。

- サポートされているプラットフォームの一覧については、セクション 1 の「概要」を参照ください。
- ハードディスク上の 30 MB の空き容量
- MMX 対応の CPU

## Ericom Blaze クライアントをインストールする

- Blaze インストーラにより、以前のインストールが上書きされる場合があります。
- Ericom Blaze Client.msi を実行します。
- License Agreement を確認し、同意します。Next をクリックします。

I Do Not Agree

I Agree

- Next をクリックし、Blaze クライアントを使用するために .rdp ファイルを関連付けます。システムに .blaze 拡張子が自動的に追加されます。関連付けられているファイルをダブル・クリックすると、ファイルの設定を使用して Blaze クライアントが起動します。

### File Associations

Select the file types you want to be associated with Blaze

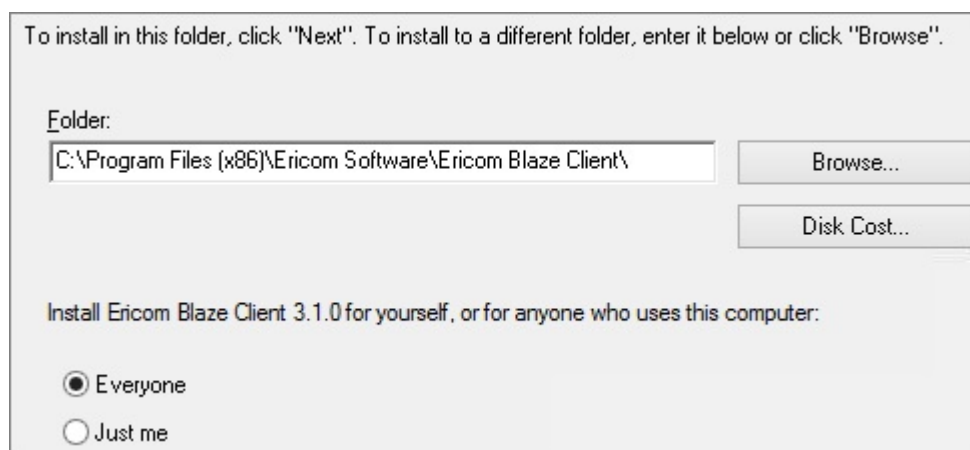
RDP Remote Desktop Connection



### Tips:

.rdp ファイルを使用して Blaze セッションを RDP クライアント (MSTSC.exe) に自動接続するには、まず最初に Blaze クライアントを使用して .rpd ファイルを保存する必要があります。Blaze クライアントを使用して保存する前に .rdp ファイルを起動した場合、Blaze クライアントユーザ・インターフェースが開きます。Blaze クライアントを使用して .rdp ファイルを保存するとすべての設定が保持され、今後は起動時に自動接続するようになります。

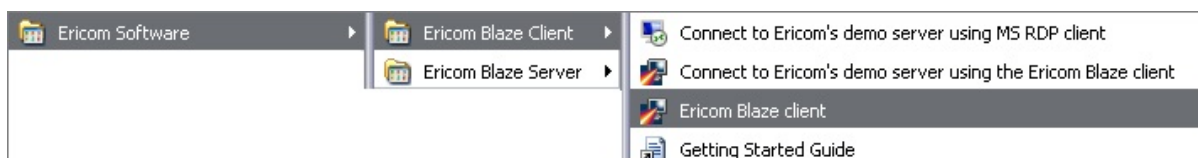
- インストール場所を選択し、Ericom Blaze を利用できるユーザを指定します。



- Next をクリックしてインストールを開始し、完了するのを待ちます (セキュリティ昇格を受け入れるよう要求される場合があります)。
- 終了のプロンプトが表示されたら Close をクリックすると、Blaze クライアントが使用できるようになります。

## Ericom Blaze Client for Windows を使用する

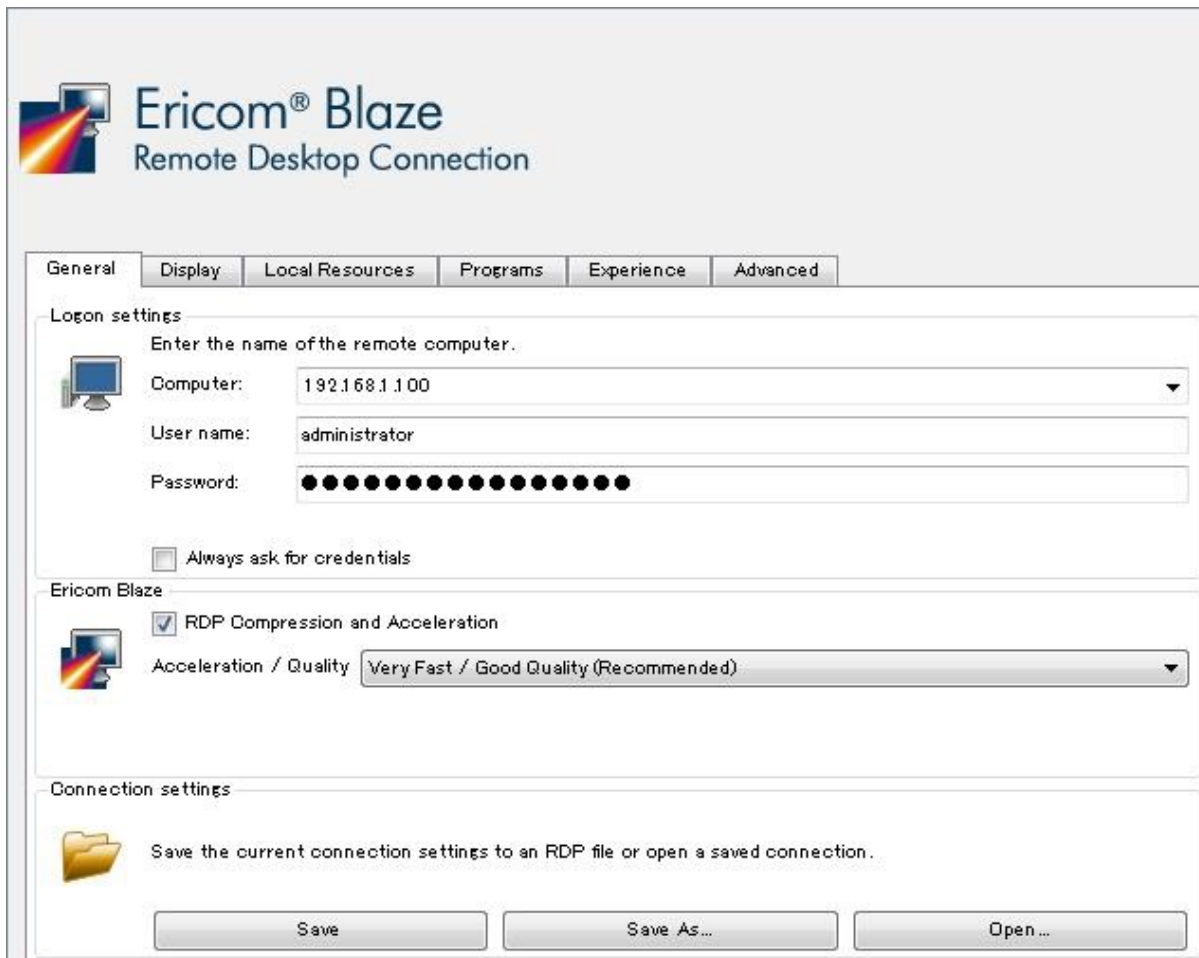
インストールが完了すると、スタート・メニューまたはデスクトップアイコンから Ericom Blaze クライアントを起動できます。



.blaze 拡張子を持つ構成ファイルをダブル・クリックすることでも、Ericom Blaze クライアントを起動可能です。この方法では、構成ファイルで指定された設定を使用し Blaze クライアントがすぐに接続します。構成のユーザ・インターフェースは表示されません。.blaze ファイルは、「blaxe.exe」実行可能ファイルのパラメータとしても使用できます。



## 「General (全般)」タブの設定



The screenshot shows the 'Ericom® Blaze Remote Desktop Connection' dialog box with the 'General' tab selected. The 'Logon settings' section includes a 'Computer' dropdown menu with '192.168.1.100' selected, a 'User name' text box with 'administrator', and a 'Password' text box with masked characters. There is an unchecked checkbox for 'Always ask for credentials'. The 'Ericom Blaze' section has a checked checkbox for 'RDP Compression and Acceleration' and a dropdown menu for 'Acceleration / Quality' set to 'Very Fast / Good Quality (Recommended)'. The 'Connection settings' section has a folder icon and a text box for saving settings, with 'Save', 'Save As...', and 'Open...' buttons below.

Computer(コンピュータ) Ericom Access Server を実行しているホストまたは任意の標準 RDP ホストのアドレスを入力します (ホスト名または IP アドレス)。デフォルトでは、ポート番号が指定されていない場合はポート 3399 が Blaze のアクセス対象となる接続に使用され、ポート 3389 が通常の RDP に使用されます。

別のポート番号を指定するには、「:<ポート番号>」をアドレスの末尾に追加します。ポート 23 を使用する例: rdpdemo.ericom.com:23

User name(ユーザ名) / Password(パスワード) (オプション項目) - 宛先ホストにログインするための資格情報を入力します。ホストのログイン・ダイアログを回避するために、両方を入力します。

RDP Compression and Acceleration(RDP 圧縮とアクセラレーション) - 圧縮とアクセラレーションを無効にするには、このボックスをオフにします。無効にした場合、RDP が使用されます。

Ericom Blaze Acceleration(アクセラレーション) / Quality(画質) 設定



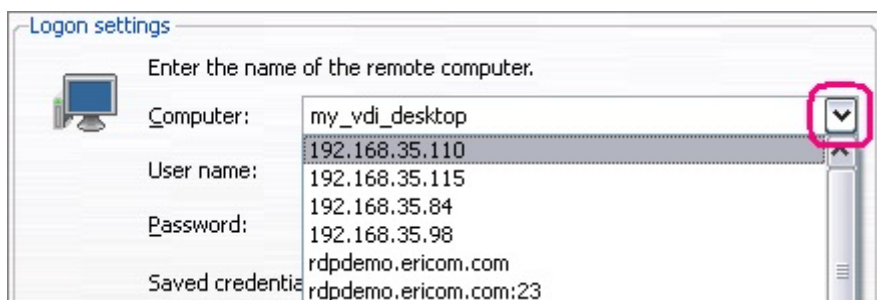
- ロスレス – ロスレス圧縮
- **Moderate(低速) / Highest(最高画質)** - ほぼ完璧な品質 (最小限の非可逆圧縮) ほぼ正確な画像レンダリングが必要な場合に適しています。
- **Good(中低速) / Very High(高画質)** - 画像品質のロスを最小限に抑えます。
- **Fast(中速) / High(中画質)** - 若干品質が低下し、「中低速」よりも若干高速化します。
- **Very Fast(高速) / Good(中低画質)**- バランスの取れた品質とパフォーマンスを提供し、ほとんどのケースに最適です。
- **Fastest(最高速) / Fair(低画質)** - 品質は低下しますが、パフォーマンスを向上します。帯域幅が限られている場合に適し、特にグラフィックを多用するアプリケーションを使用する場合に有効です。

#### 接続設定:

- **Save(保存)** - 読み込みした元のファイルに現在の設定を保存します。設定をファイルから読み込んでいない場合、「Save As」(下記を参照)と同じ動作をします。
- **Save As…(名前を付けて保存)…** - 新しい「.blaze」ファイルに設定を保存します。「.rdp」拡張子のファイルへの保存も可能です。
- **Open…(開く)…** - 既存の「.blaze」ファイルから設定を読み込みます。「.rdp」拡張子のファイルから設定を読み込むことも可能です。

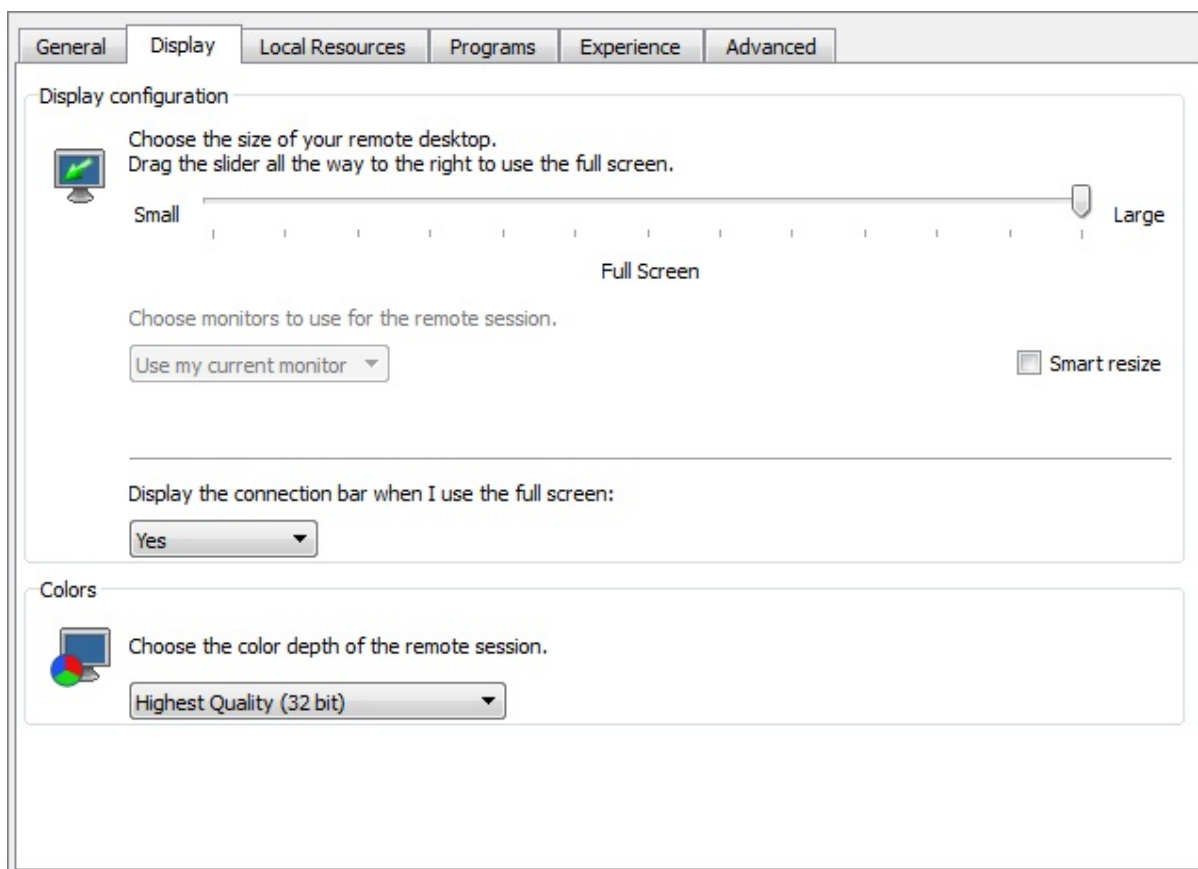
#### 以前の設定にアクセスする

- 過去のすべての有効なセッションの設定は、再利用のために自動的に保存されます。
- 以前の設定を使用するには、Computer 名の右側のドロップダウン矢印アイコンをクリックします。セッションは、使用順に表示され、最近使用したセッションが上部に表示されます。表示例:



Ericom Blaze セッションを開始するためのすべてのパラメータを設定後、Connect ボタンをクリックします。

## 「Display (表示)」タブの設定



表示設定 - Ericom Blaze セッションの画面サイズを指定します。フルスクリーン・セッションでは、ローカルの画面全体が使用されます。

**Choose monitors to use for the remote session**(リモート・セッションに使用するモニタを選択してください)

- 「Use my current monitor(現在の自分のモニタを使用する)」 - 現在のモニタ (Blaze ダイアログが表示されるもの) のみを Blaze セッションで開きます。
- 「Use all my monitors(自分のすべてのモニタを使用する)」 - すべてのモニタを Blaze セッションで開きます。

Windows 7、8、Windows Server 2008 R2 または Windows Server 2012 に接続する場合、RDP Multimon 機能が使用されます。この機能により、ローカル・モニタに正確にマッチする仮想モニタがリモート・セッション内に作成されます。

それ以前のバージョンの Windows に接続する場合、マルチモニタ・スパンニング機能が使用されます。この機能により、すべてのローカル・モニタをカバーする単一のリモート・モニタが作成されます。これは「MSTSC.exe」の「/span」フラグと同様です。使用されているモニタ数に関係なく、デスクトップの最大解像度は 4096x2048 となります。このモードでは、モニタ内に適切に表示されるよう、Ericom Blaze により自動的にウィンドウのサイズと大きさが調整されます。例えば、アプリケーション・ウィンドウを最大化した場合、プライマリ・モニタのみがカバーされます。

- 「Span all my monitors(すべてのモニタを結合する)」 - Blaze セッションによりすべてのモニタが開かれます。

マルチモニタ・スパニング機能により、すべてのローカル・モニタをカバーする単一のリモート・モニタが作成されます。この機能はすべてのオペレーティング・システム向けに実装されています。

- 「Use Monitor X(モニタ X を使用)」 - 「X」として識別されたモニタが Blaze セッションで開かれます (X はモニタの数値識別子を表します)。

## スマート・リサイズ

スマート・リサイズ機能により、ウィンドウ・サイズが変更されたときに、自動的にセッションの画面表示の比率を自動的に調整されます。元の縦横比が維持されます。スクロールバーは表示されません。

## Display the connection bar when I use the full screen(フルスクリーンの使用時に接続バーを表示する)

Blaze のフルスクリーン・モードには以下の 3 つのモードがあります:

- 「Yes(はい)」 - 接続バーが利用可能な状態で、自動非表示モードで開始されます (デフォルト) で 「ピン留め」モードへの変更が可能です。
- 「Yes(はい) (Pinned(ピン留め))」 - 接続バーが利用可能な状態で、固定モードで開始されます。固定を解除し、自動非表示モードへ変更することが可能です。
- 「No(いいえ)」 - 接続バーは利用できません。この設定は、キオスク端末やシンクライアント環境に役立ちます。

**Colors(カラー)** - Ericom Blaze の色深度を指定します。ホスト・プラットフォームにより提供される最高品質の色設定を使用するには、それが 32 ビット・カラーかそれ以下かに関わらず、32 ビット・カラーを指定します (例えば、Windows 2003 では 24 bit が使用されます)。

**Display the connection bar** - フルスクリーン・モードで RDP ウィンドウの上部に表示される Ericom Blaze RDP バーを非表示にするには、このボックスをオフにします。



## 「Local Resources (ローカルリソース)」タブの設定

**RemoteAudio(リモートオーディオ)** - Ericom Blaze セッションのオーディオ設定を指定します。



注意:

帯域幅の限られた接続や高レイテンシの接続では、オーディオ品質が低下する場合があります。

**Keyboard(キーボード)** - Windows キーの組み合わせの設定を指定します。

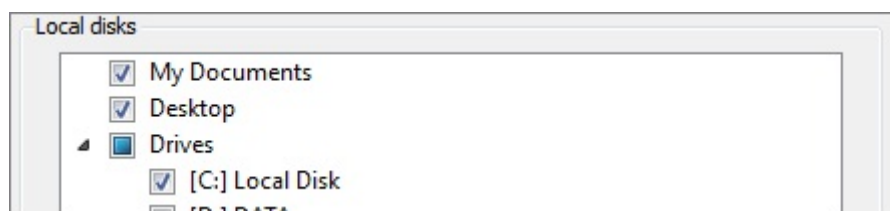
**Local devices and resources(ローカルのデバイスとリソース)** 「Clipboard/クリップボード」 - テキストとイメージのクリップボード・リダイレクトを有効にします。ファイルのコピー & ペーストはサポートさ

れていません。

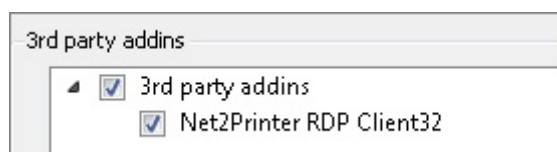
**Local devices and resources(ローカルのデバイスとリソース)「Printers(native drivers)/プリンタ(ネイティブ ドライバ)」** - 標準 RDP 印刷リダイレクトを有効にします。標準 RDP 印刷リダイレクトを有効にするには、ホストとクライアントにプリンタ・ドライバをインストールする必要があります。

**Local devices and resources(ローカルのデバイスとリソース)「Printers(universal drivers)/プリンタ(汎用 ドライバ)」** - ビルトインのユニバーサル・プリンタを有効にします。ユニバーサル・プリンタの詳細については、次のセクションを参照ください。

リモート・ホスト上の ローカル・ディスクのマッピング を指定するには、More devices…(その他のデバイス) をクリックします。マイドキュメント や ローカル・ユーザの デスクトップ などの特別なフォルダをマッピングし、セッションのアクティブ時にプラグインのドライバのマッピングを有効化することが可能です。

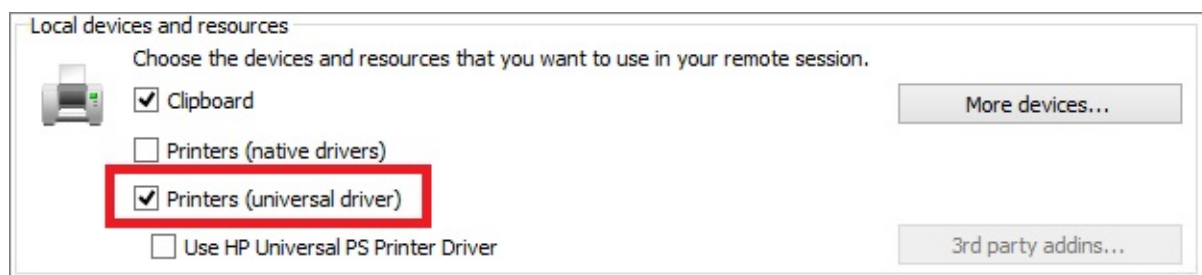


**3rd party addins…(サード・パーティのアドイン)** - サード・パーティ RDP アドインを有効にします (例: 汎用ドライバ印刷のリダイレクト対応)。サード・パーティ・アドインのビット・レベルは、Blaze クライアントのビット・レベルと一致する必要があります。例えば、x64 ベースのサード・パーティ・コンポーネントがインストールされている場合、x64 Blaze クライアントとともに使用する必要があります。ビット・レベルを混在することはできません。混在している場合、サード・パーティのコンポーネントはアドインの一覧に表示されません。



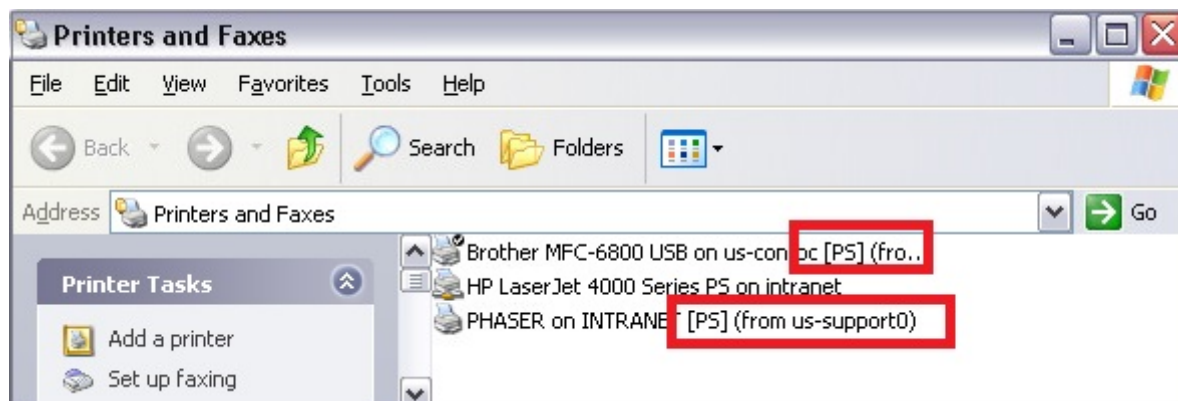
### ビルトインの汎用ドライバ印刷

Ericom Blaze では、汎用ドライバ印刷機能がサポートされています。ビルトインの汎用プリンタは PostScript をベースにしており、リモートで実行された印刷ジョブをローカル・プリンタにリダイレクトします。汎用プリンタの使用を有効にするには、「Printers(universal drivers) / プリンタ (汎用 ドライバ)」オプションをオンにします。



Blaze RDP セッションでは、リモート・デスクトップ上で設定された他のプリンタと並んで、リダイレクト

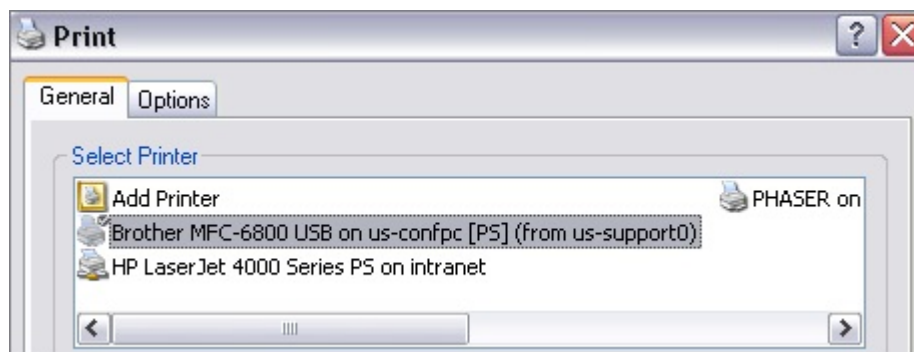
したプリンタが表示されます。リダイレクトしたプリンタは、ラベルのコンピュータ名に「[PS]」という文字が追加されます。



注意:

印刷ジョブには、汎用 HP PostScript ドライバが使用されるため、一部のプリンタ特有の機能は使用できない場合があります (例: 両面印刷)。プリンタ特有の機能をサポートするには、サード・パーティの印刷ソリューションまたは標準 RDP 印刷 (RDP ホストにプリンタ・ドライバを読み込む) の使用を検討してください。

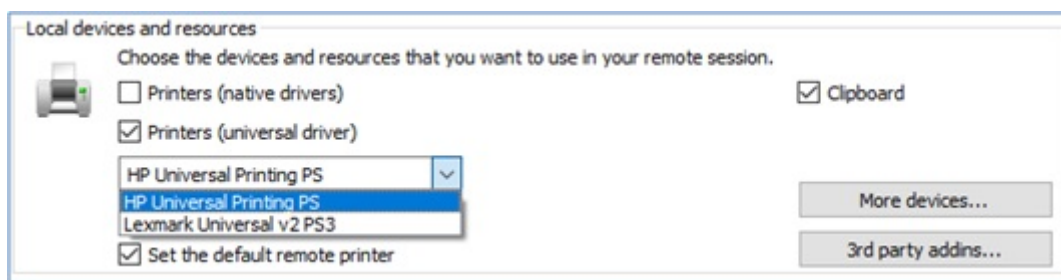
リダイレクトしたプリンタを使用して印刷するには、アプリケーションの印刷ダイアログが表示された際に、目的のプリンタを選択します。



### Windows 8、10、2012R2、および 2016 RDP ホストでの汎用ドライバ印刷

Windows 8、10、2012、2012R2、および 2016 での Blaze ユニバーサル印刷をサポートするためには、HP Universal PS ドライバが必要です。Lexmark<sup>®</sup> および HP<sup>®</sup> の汎用ドライバがサポートされており、Lexmark が推奨されています。インターネット上で、使用中のオペレーティング・システムにドライバをダウンロードしてください。

汎用ドライバをインストール後、Blaze クライアントを起動します。ローカルリソースダイアログボックスに移動し、「プリンタ (汎用ドライバ)」をチェックし、目的のドライバを選択します。このフィールドは、別の汎用ドライバを選択した場合には編集することができます (PostScript ドライバが推奨されています)。



次にユーザがログインした際に Ericom プリンタが表示されます (セッションのプリンタが有効化されている場合)。この時点でプリンタ・ドライバは RDP ホスト・システム上に存在するため、サード・パーティ汎用プリンタ のすべてのインスタンスが Windows の プリンタ メニューから削除される可能性があります。



注意:

最高の正確性とパフォーマンスのために、Lexmark 汎用ドライバを利用することも可能です。Lexmark ドライバが想定通りに機能しない場合は、HP ドライバを試してください。

#### デフォルトのローカル・プリンタのみをリダイレクト

RDP プリンタ・リダイレクトには、リダイレクトされたすべてのプリンタを表示する時間が必要です。リモート・セッションでデフォルトのローカル・プリンタのみが必要な場合、「Redirect only the default local printer(デフォルトのローカル・プリンタのみをリダイレクト)」を選択します (他のすべてのプリンタはリダイレクトされなくなります)。

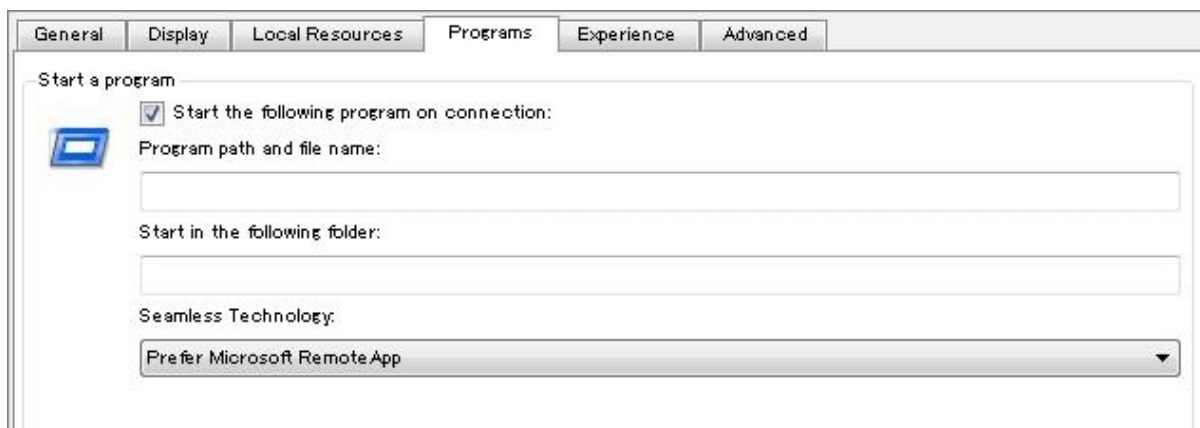
Redirect only the default local printer

#### デフォルトのリモート・プリンタを設定

この設定がオンの場合、デフォルトのローカル・プリンタはデフォルトのリモート・プリンタとなり、リモートのデフォルト設定をすべて上書きします。この設定がオフの場合、すべてのデフォルトのリモート・プリンタはデフォルトのままとなり、デフォルトのローカル・プリンタはプリンタの一覧から使用可能な別のプリンタとなります。

Set the default remote printer

## 「Programs(プログラム)」タブの設定 (シームレス・アプリケーション)



Ericom Blaze シームレス アプリケーションは、ローカル・アプリケーションとしてユーザのデスクトップ上に表示されるリモート・アプリケーションです。リモート・デスクトップは表示されません。これにより、ユーザのローカル・アプリケーションと並べてリモート・アプリケーションを表示することができます。シームレス・アプリケーションは、Blaze クライアントを介したアクセラレーション有り/アクセラレーションなしのモードでサポートされています。アプリケーションが起動されるホスト・システム上に Access Server が必要です。

接続時に次のプログラムを起動する をオンにし、シームレス・アプリケーションとして起動するプログラムのパスと開始するフォルダを指定します。アプリケーションのパスは、リモート システム上のパスを入力してください。ローカル (ユーザ) システム上のアプリケーション・パスを入力しないでください。

2008 R2 または 2012 RDS サーバでは、シームレス・ウィンドウを使用するために、RemoteApps 機能を有効にする必要があります。ただし、Access Server はビルトインの PtTSAgent コンポーネントを使用してリクエストされたアプリケーションを起動するため、アプリケーションを RemoteApp のリストに手動で追加する必要はありません。

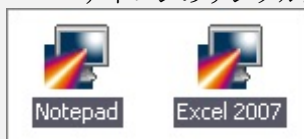
2008(R2 以外) 以前のオペレーティング・システムでは、Ericom シームレスはサポートされていません。これらのオペレーティング・システムには、Microsoft シームレスを使用してください。



### Tips:

Blaze シームレス・アプリケーションを Microsoft RemoteApps の代替として使用できます。Blaze 設定ファイルを使用して、Access Server を実行中のリモート・ホストからシームレス・アプリケーションを起動できます。ユーザのデスクトップ上に Blaze アイコンを配置することで、Blaze が有効なアプリケーションにユーザが簡単にアクセスできます。

アイコンのサンプル:



Ericom Blaze では、2 種類の シームレス・エンジンがサポートされています。Ericom のエンジンと Microsoft のエンジンです。特定のアプリケーションは片方のエンジンでの表示が優れている場合があるため、選択したエンジンが問題を引き起こしている場合、代替設定を使用します。

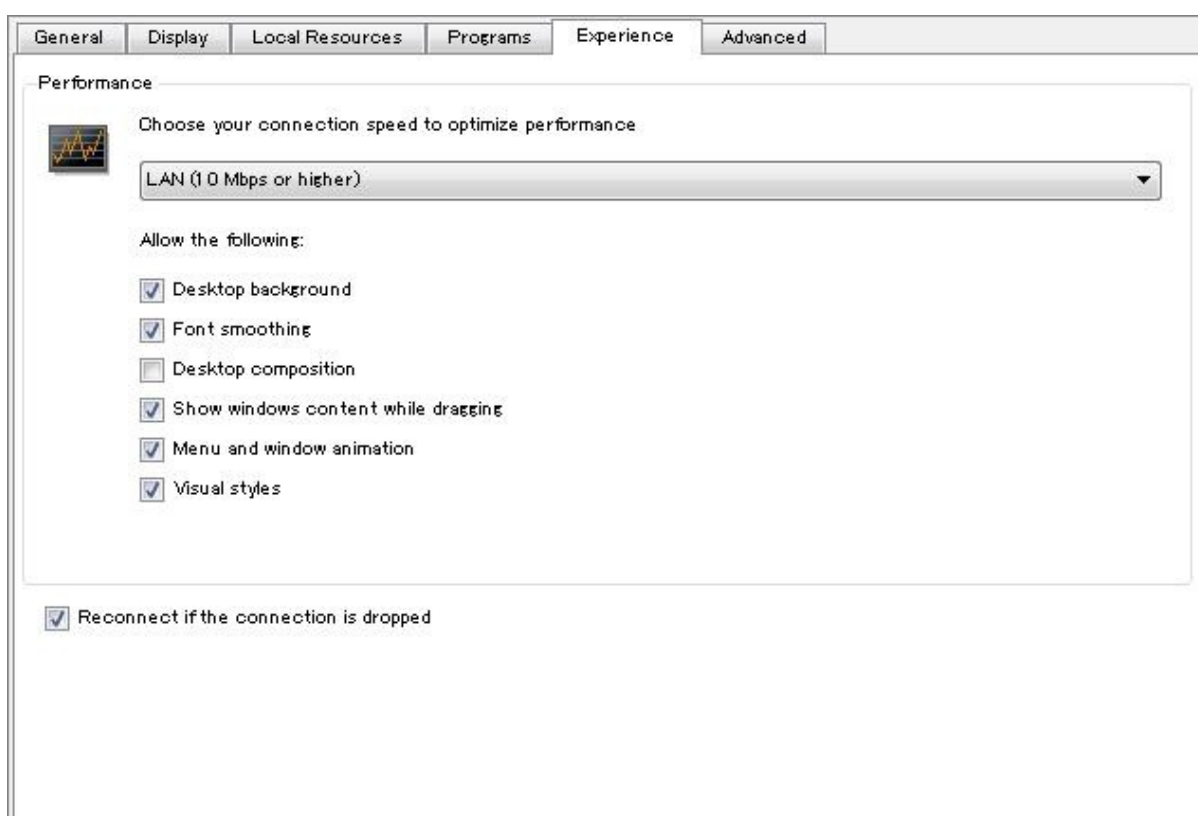




注意:

オペレーティング・システムの制約により Microsoft RemoteApp 機能が使用できない場合、Ericom Blaze には Ericom Seamless が使用されます。

## 「Experience(エクスペリエンス)」タブの設定



最適なパフォーマンスの接続速度を選択する ドロップダウン・ボックスをクリックし、ユーザのネットワーク速度に最適な設定を選択します。セッションの機能は、各チェックボックスをオフにすることで個別に無効にできます。



注意:

Show window content while dragging(ドラッグ時にウィンドウの内容を表示) を選択する場合、RDP ホストでもこの設定を有効にする必要があります。この設定の方法はオペレーティング・システムにより異なるため、設定の手順を見つけるには、「"Show window content"(ドラッグ時にウィンドウの内容を表示)」をインターネット検索してください。

- Reconnect if the connection is dropped(接続が中断された場合に再接続する) - ネットワークの停止により Blaze セッションが中断された場合の自動的な再接続を有効にします。

## 「Advanced(詳細)」タブの設定

### Ericom Secure Gateway

ユーザの接続に Ericom Secure Gateway を使用する場合、Connect using Ericom Secure Gateway (Ericom Secure Gateway を使用して接続) チェックボックスをオンにします。Ericom Secure Gateway サーバのアドレスを入力します。ポートを明示的に指定しない場合、デフォルトの 443 が使用されます。カスタム・ポートを指定するには、以下の記入例のように「:」を入力し、アドレスの後にポート値を入力します。Ericom Secure Gateway のインストールと設定については、「Ericom Secure Gateway 管理者用マニュアル」を参照ください。

Secure Gateway にログインするにはユーザ・アカウントが必要です。このユーザ・アカウントは、手動で入力するか、Blaze クライアントに保存されている資格情報から渡すことができます。

### ゲートウェイとしての Access Server の使用

Access Server は、RDP ホストへのゲートウェイ・プロキシとして動作することができます。これは、RDP ホスト上にサード・パーティのコンポーネントをインストールできない状況で役立ちます。

Access Server ゲートウェイを有効にする際、(エンドユーザ・のマシンからではなく)Access Server から認識可能なコンピュータ・アドレスの値を入力します このアドレスは、ping コマンドや telnet コマンドを介して Access Server システムからアクセス可能である必要があります。

Access Server をゲートウェイとして使用する場合、複数ユーザにとっての単一障害点となります。Access Server を実行するシステムに十分なリソースが割り当てられていることを確認し、冗長化のための 2 台目のサーバの追加を検討してください。



ゲートウェイ・モードでのパフォーマンスの低下を最小限に抑えるため、Access Server と RDP ホストのレイテンシを最小限に保ちます。

**Tips:**

### ローカル・カーソルのオプション

ローカル・カーソルを有効にするには、テキスト・エディタを使用して「.blaze」ファイルを編集し、ファイルの末尾に以下のいずれかを追加します:

#### 1. "null cursor:s:cross"

十字カーソルが表示されます

#### 2. "null cursor:s:arrow"

ローカルの標準矢印カーソルが表示されます

#### 3. "null cursor:s:png"

「blaze.exe」ディレクトリ内の「null\_cursor.png」ファイルが使用されます この画像は、32x32 ピクセルであり、最大 32 ビット・カラーで、アルファ値 (0 = 透明、255 = 完全に不透明) を含むものである必要があります。

#### 4. "null cursor:s:bmp"

「null\_cursor.bmp」と「null\_cursor\_map.bmp」という 2 つのビットマップ・ファイルを使用しますカーソルのビットマップ (B) とマスク (M) のビットは以下のように結合されます:

B=1 かつ M=1 では、黒が指定されます

B=0 かつ M=1 では、白が指定されます

B=0 かつ M=0 では、透明が指定されます

B=1 かつ M=0 では、Windows では XOR 演算された結果が指定され、他のすべてのプラットフォームでは結果が定義されていません。



**注意:**

この設定を .blaze ファイルに手動で設定した後は、新しい設定を上書き保存しないでください。新しい設定の保存操作によりこの設定が上書きされ、手動で再度追加することが必要になります。

---

## Ericom Blaze for Windows の GUI 日本語表示

Ericom Blaze はインストール後にユーザ・インターフェースを日本語に変更することができます。日本語インターフェースにするには Windows のショートカットのプロパティで言語設定のパラメータを追加します。

1. 新規でデスクトップに日本語インターフェースの Blaze 用ショートカットを作成します。デスクトップ上で右クリックし、表示されるコンテキストメニューから新規作成 - ショートカットを選択します。
2. ショートカットの作成ダイアログが表示されます。参照ボタンをクリックして `Blaze.exe` を選択し、ショートカットを作成します。インストール先のデフォルトは下記のパスです。(32 ビット版の Blaze クライアントの場合は Program Files が "Program Files (x86)" になります)

**"C:\Program Files\Ericom Software\Ericom Blaze Client\Blaze.exe"**

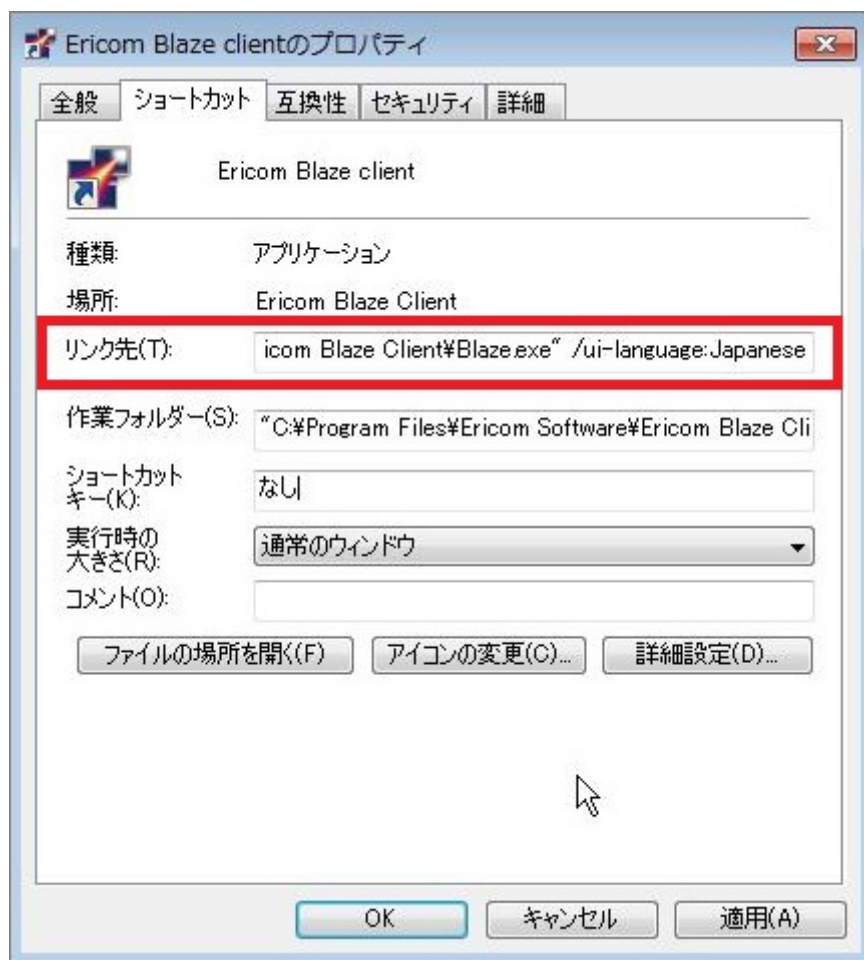
3. 作成されたショートカットアイコンのプロパティを表示します。
4. プロパティの「ショートカット」タブの「リンク先」には 2. で設定したパスが登録されています。そのパスの後ろに以下のパラメータを追加します。

**`/ui-language:Japanese`**

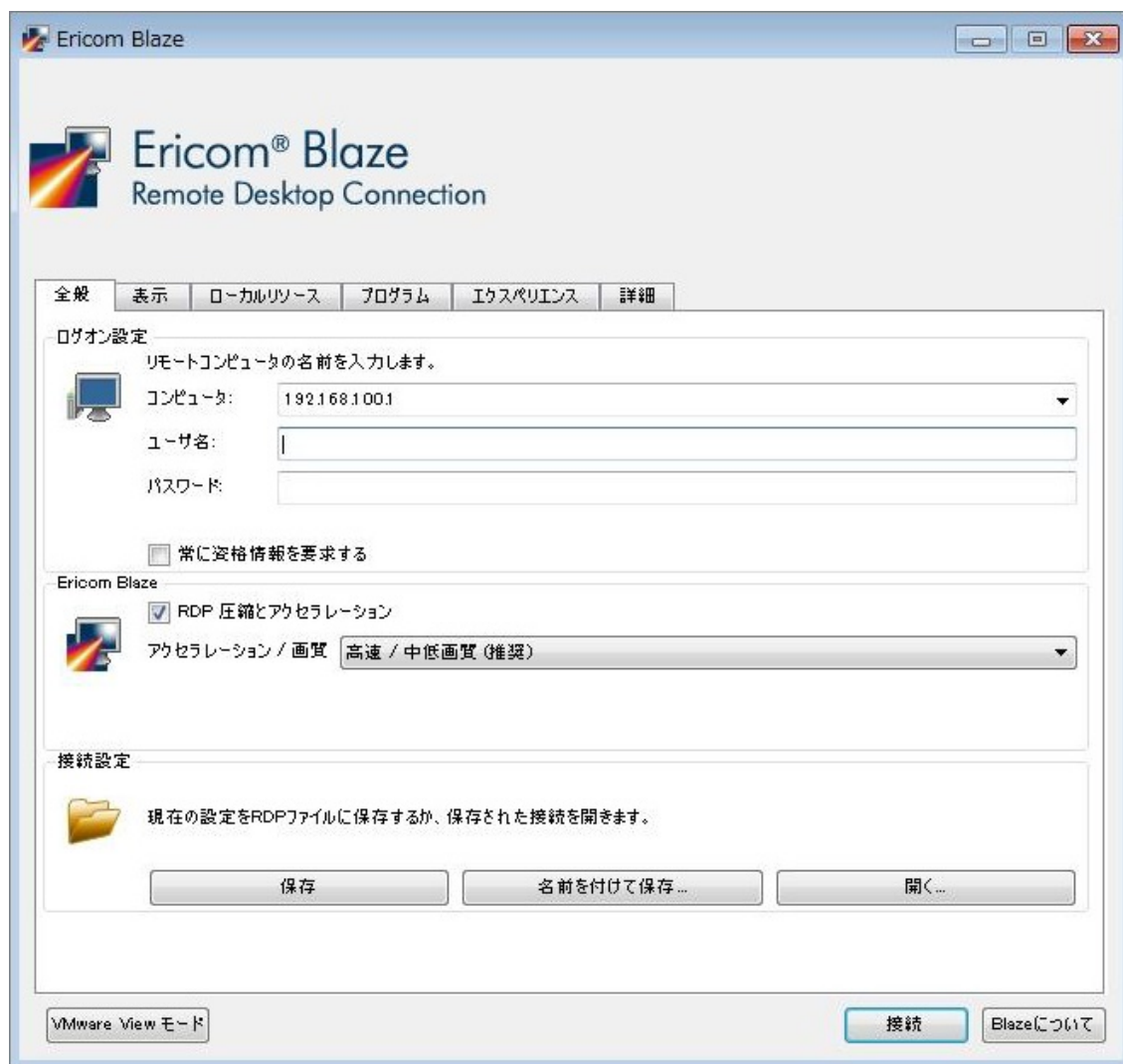
リンク先フィールドは以下の記述になります。

**"C:\Program Files\Ericom Software\Ericom Blaze Client\Blaze.exe"**

**`/ui-language:Japanese`**

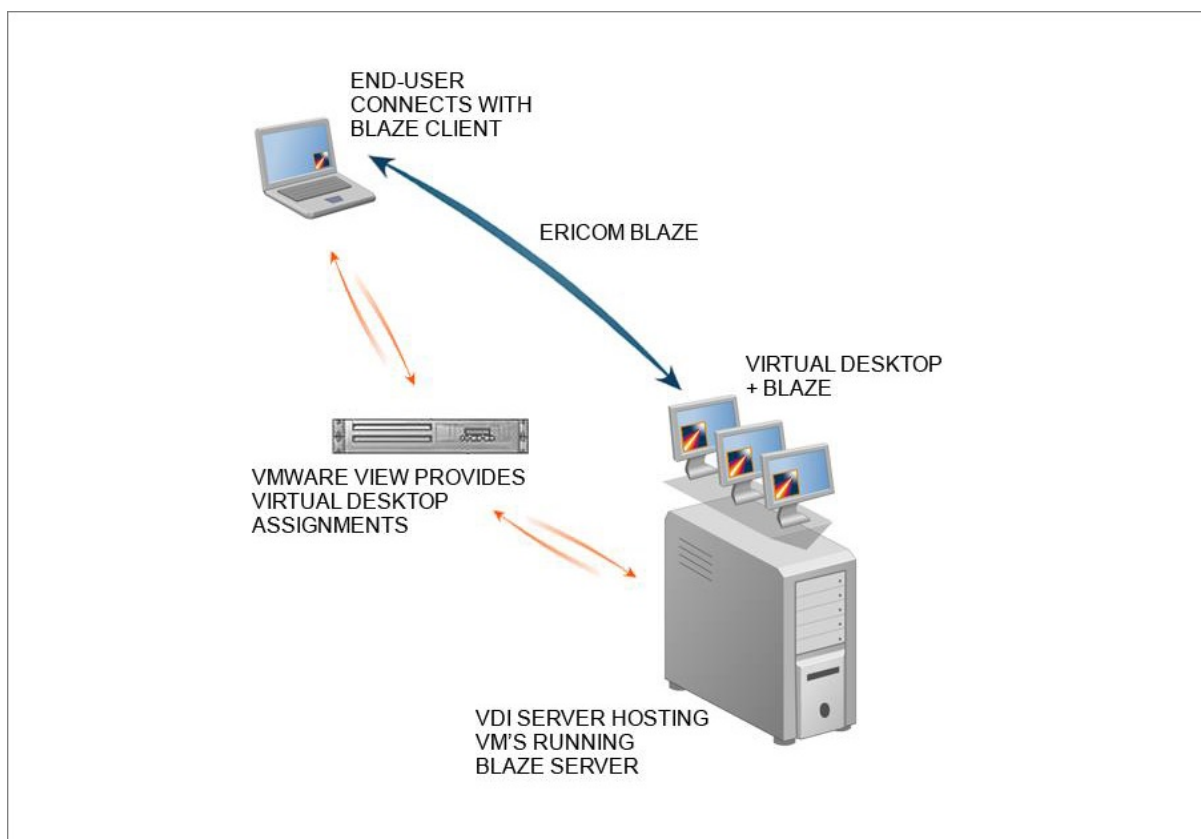


5. パラメータを追加したショートカットをダブルクリックすると日本語ユーザ・インターフェースになった Blaze クライアントが起動します。



## 4.1.5 VMWARE® VIEW クライアント・モード

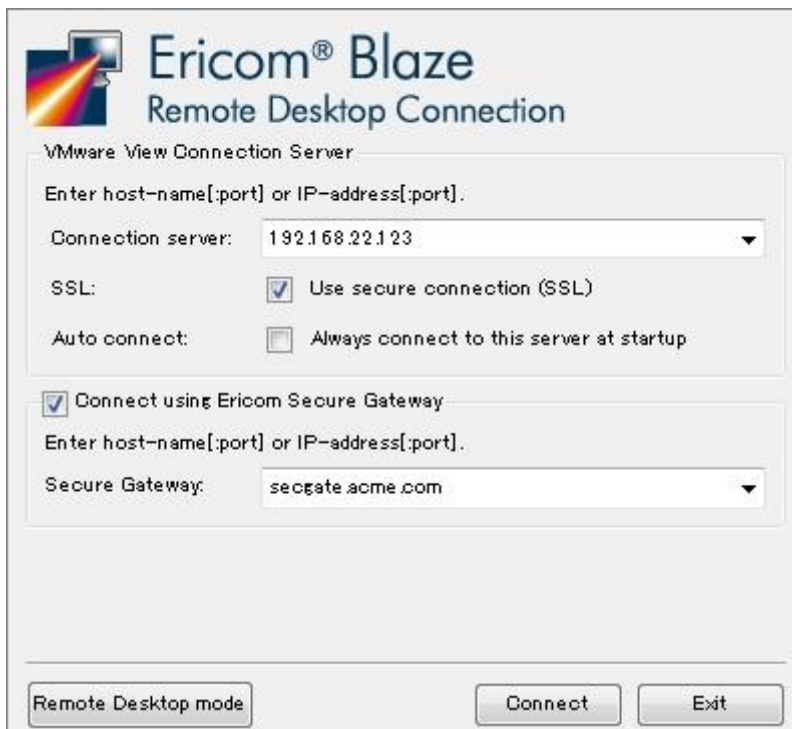
Ericom Blaze クライアントは、VMware View 5.2 および 5.3 の接続ブローカーをサポートしています。Ericom Blaze は、認証のために View ブローカーを使用した後、目的の仮想デスクトップに直接接続します。VMware View アクセス用に Ericom Blaze RDP Acceleration を使用する場合、View クライアントの代わりに Blaze クライアントが使用されます。Blaze クライアントには View クライアントは必要とされず、View クライアントを置き換える必要もありません。



Blaze クライアントで VMware View モード を有効にするには、VMware View mode ボタン をクリックします。

Switch to VMware View mode

Ericom Blaze - VMware View インターフェースが表示されます。



Ericom® Blaze  
Remote Desktop Connection

VMware View Connection Server

Enter host-name[:port] or IP-address[:port].

Connection server: 192.168.22.123

SSL:  Use secure connection (SSL)

Auto connect:  Always connect to this server at startup

Connect using Ericom Secure Gateway

Enter host-name[:port] or IP-address[:port].

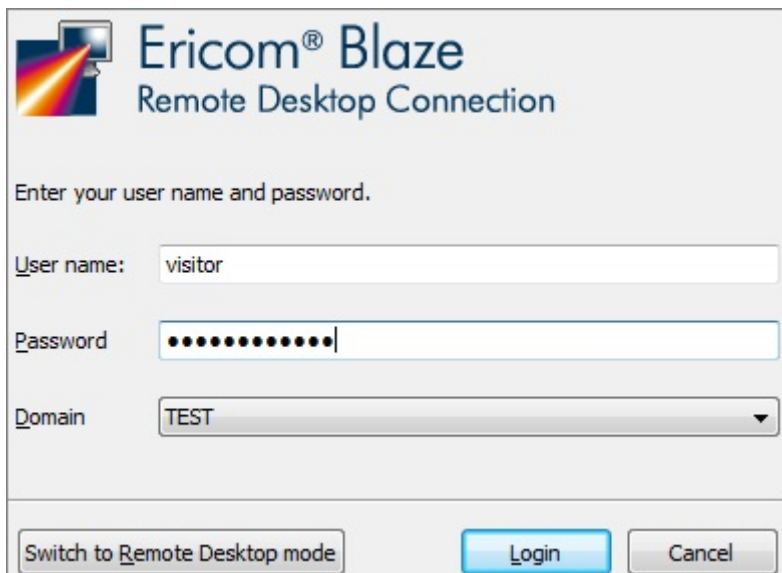
Secure Gateway: secgate.acme.com

Remote Desktop mode    Connect    Exit

VMware View 接続ブローカーで SSL が必要とされている場合は、SSL を有効にします。

Computer の欄に VMware View サーバのアドレスを入力し、接続をクリックします。

ユーザの資格情報を要求する次のダイアログが表示されます。



Ericom® Blaze  
Remote Desktop Connection

Enter your user name and password.

User name: visitor

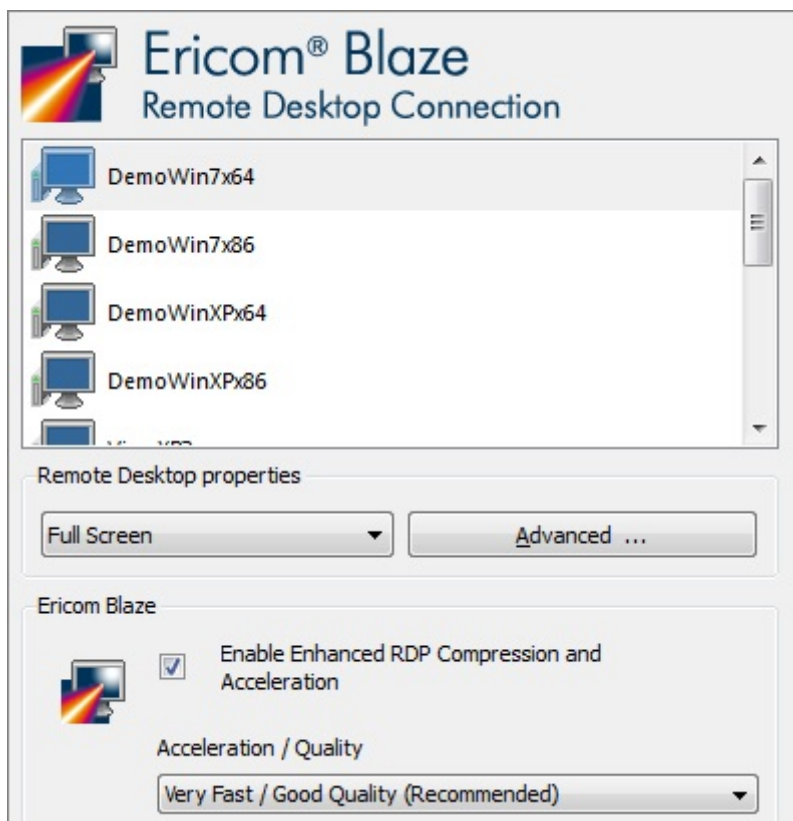
Password: ●●●●●●●●

Domain: TEST

Switch to Remote Desktop mode    Login    Cancel

認証が完了すると、View ブローカーを介してユーザが利用可能なデスクトップの一覧が、Blaze クライアントに表示されます。





任意の Blaze 設定を構成し、選択したデスクトップに接続するために Connect ボタンをクリックします。

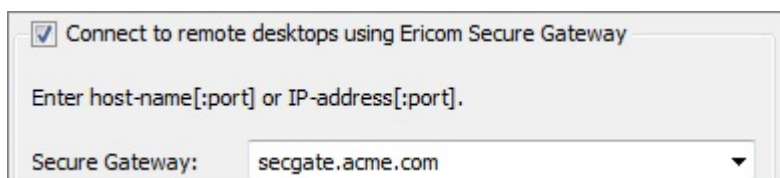


注意:

Blaze クライアントでは、PCoIP がサポートされていません。Ericom Blaze と Blaze プロトコルは、View クライアントと PCoIP プロトコルからは独立して機能します。

## Secure Gateway Access

Ericom Secure Gateway を使用する場合 - Connect using Ericom Secure Gateway チェックボックスをオンにします。Ericom Secure Gateway サーバのアドレスを入力します。ポートを明示的に指定しない場合、デフォルトの 443 が使用されます。ポートを指定するには、以下の記入例のように「:」を入力し、アドレスの後にポート値を入力します。上記の例では、Secure Gateway のアドレスは secgate.acme.com です。ポートの指定がないため、443 が自動的に使用されます。



## 4.1.6 Ericom Blaze Client for Mac

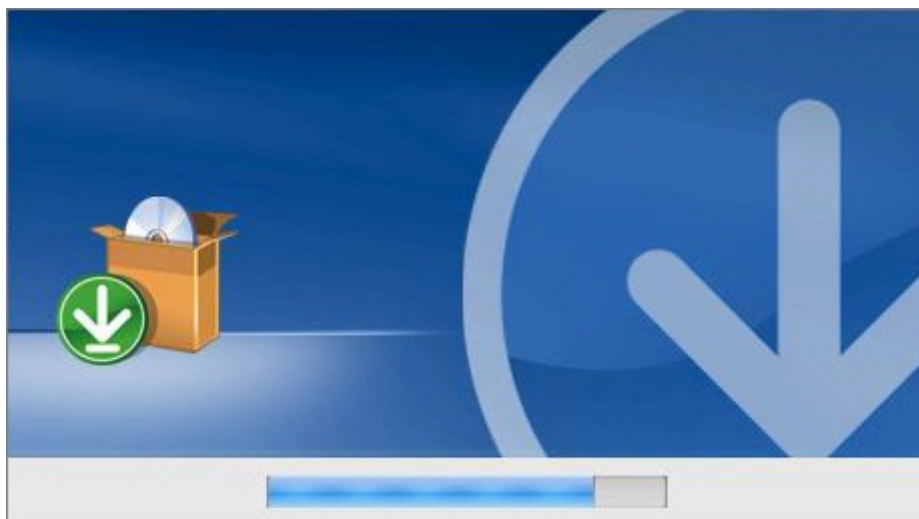
### インストールの前提条件

- Mac OS X 10.8 以降
  - ハードディスク上の 30 MB の空き容量
  - MMX 対応の CPU

注意： **Blaze Client for Mac** はバージョン **3.1** です。 **AccessServer 7.\*** には対応していません。

### Ericom Blaze Client for Mac のインストール

Ericom Blaze Client for Mac を起動するには、インストーラを起動し、インストール・ウィザードの指示に従ってください。



### Ericom Blaze Client for Mac を使用する

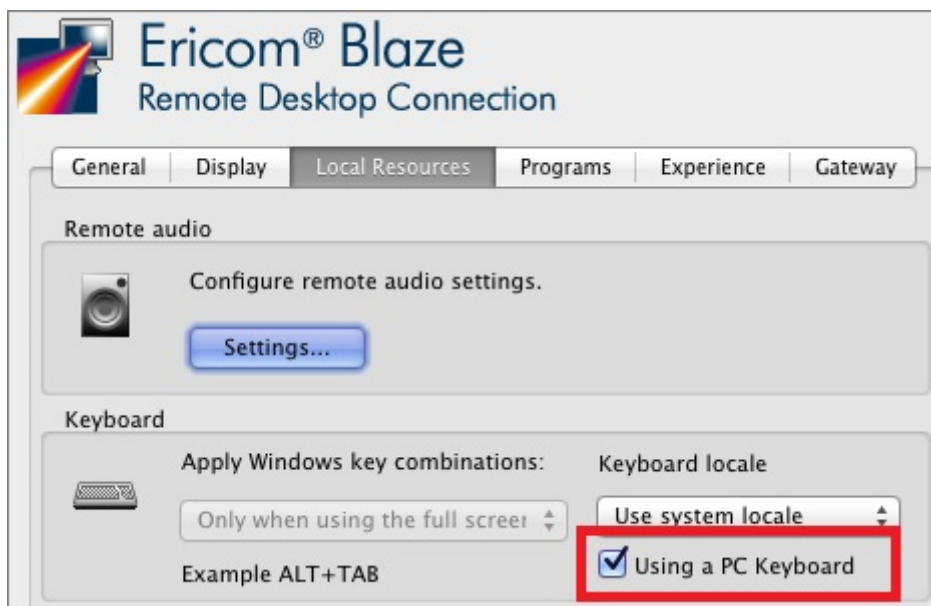
Ericom Blaze クライアントを起動するには、blaze の実行可能ファイルまたはショートカットを実行します。

Blaze クライアント 2.5 以降では、.blaze 拡張子が Blaze クライアントに関連付けられています。任意の .blaze 設定ファイルをダブル・クリックすると、その設定ファイルを使用して Blaze クライアントが起動します。

主な機能の使用法の説明については、「Blaze Client for the Windows」の章を参照してください。このセクションは、Windows 版と Mac 版の Blaze クライアントの機能の違いをカバーしています。

#### PC キーボードを使用する

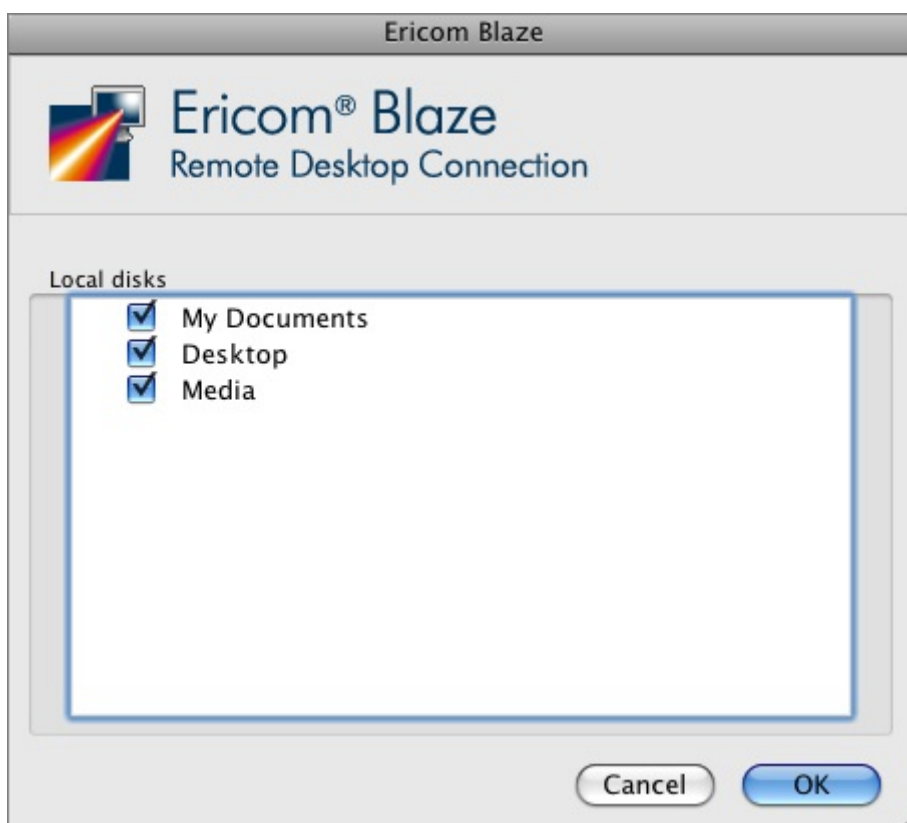
Windows ベースの物理キーボードを使用する場合、Blaze クライアントの Local Resources(ローカルリソース) タブに移動し、Using a PC Keyboard の設定をオンにします。



この設定がオンの場合、Mac から Windows へのキー・マッピングの一部が無効になります。コントロールと Windows キーは、ネイティブと同様に動作します。この設定がオフの場合、デフォルトの Mac キーボード・エミュレーションが使用されます。コントロール (CTRL) キーは Windows キーとして動作し、Command(コマンド) キーは Windows のコントロール (CTRL) キーとして動作します。

#### ドライブ・マッピング

ドライブ・マッピングのオプションを設定するには、ローカルリソースに移動し、More devices…ダイアログに移動します。ドライブ・マッピング・ダイアログでは、以下の 3 つのオプションが提供されます:



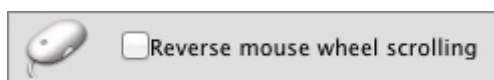
- ホーム・ディレクトリにマップするには、My Documents を選択します
- デスクトップ・ディレクトリをマップするには、Desktop を選択します
- 「/media」ディレクトリをマップするには、メディアを選択します。このディレクトリは、CD-ROM、フロッピー・ディスクや Zip ドライブなどのリムーバブル・メディア上にファイル・システムをマウントするために使用されます。

### プリンタのリダイレクト

Mac クライアント向けのプリンタ・リダイレクトでは、PostScript プリンタのみがサポートされています。さらに、HP PS Universal ドライバを Windows RDP ホストにインストールする必要があります (詳細については、このマニュアルのビルトインの汎用ドライバ印刷 のセクションを参照ください)。

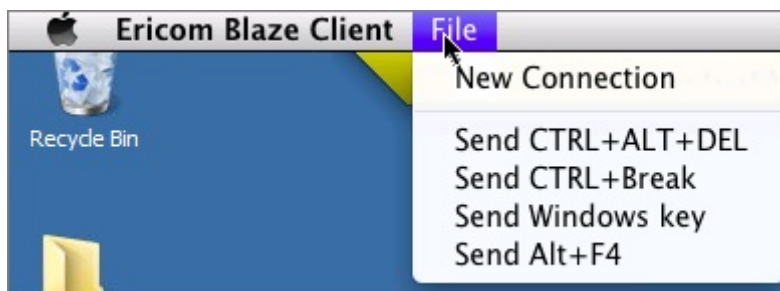
### 逆方向のスクロール・ホイール

一部の Mac 製品では、スクロール・ホイールが逆方向に動作します。現在のスクロール・ホイールの方向を変更するには、ローカルリソース・タブ内の Reverse mouse wheel scrolling を選択します。



### Blaze クライアントのファイル・メニュー

Ericom Blaze Client for Mac では、追加機能を実行するための ファイル・メニューが提供されます。例えば、新しい接続を開く機能や、Windows 関連の様々なキーの組み合わせを送信する機能があります。フルスクリーン・モードでファイル・メニューにアクセスするには、画面左上隅にマウスを移動します。Mac ツールバーと並んで、ファイル・メニューの選択が表示されます



### Blaze タイトル・バーを非表示にする

Blaze Client for Mac 7.6 以降では、以前の黄色い Blaze タイトル・バーが廃止され、オペレーティング・システムのネイティブ・タイトル・バーに変更されました。タイトル・バーを固定する機能は使用できなくなりました。

「すべてのモニタを使用する」モードを使用して Blaze for Mac を接続すると、タイトル・バーで復元ボタンを利用できなくなります。

## 4.1.7 Ericom Blaze Client for Linux

### Ericom Blaze Client for Linux 8.x (64 ビット) をインストールする

インストールの前提条件は以下のとおりです：

- Ubuntu 16.04 / 18.04 LTS
- MMX 対応の CPU
- 以下の依存関係：
  - `sudo apt-get install libqt5x11extras5`
  - `sudo apt-get install libqt5printsupport5`
  - `sudo apt-get install libqt5serialport5`
  - `sudo apt-get install libqt5multimedia5-plugins`

Debian ベースの Linux ディストリビューション用の deb インストーラが提供されています。インストールするには、以下のコマンドを実行します：

```
dpkg -i ericom-blaze-client_x64.deb
```

アプリケーションは次のディレクトリにインストールされます：`/opt/ericom/ericom-blaze-client/` アプリケーションを起動するには、このディレクトリから「`./blaze`」を実行します。

### Ericom Blaze Client for Linux 3.x (32 ビット) をインストールする

インストールの前提条件は以下のとおりです：

- 大部分の最新の Linux ディストリビューション。例えば、Red Hat、Fedora、Suse、Ubuntu など。Linux カーネル 2.6 以上が必要です。
- ハードディスク上の 20 MB の空き容量
- MMX 対応の CPU
- Blaze を使用する前に以下の X11 ライブラリをインストールする必要があります：Xcursor、Xrandr、Xinerama



注意：

Blaze Client for Linux はバージョン 3.2 です。AccessServer 7.\* には対応していません。

### Ericom Blaze Client for Linux をインストールする

Ericom Blaze Client for Linux に、以下の 4 種類のインストーラがあります：

- 「rpm」 - Red Hat、Fedora、Suse など、ほとんどの Linux ディストリビューション用

- 「deb」 - Ubuntu や HPÅ¸ ThinConnect などの、Debian ベースの Linux ディストリビューション用
- ほとんどの Linux 環境に対応したグラフィカル・インストーラ - root や他のユーザが使用可能です。
- すべてのファイルを含む「Blaze.tar.gz」アーカイブ - Linux シンクライアントへのインストールに適しています。

「rpm」を使用してインストールするには、次のコマンドを入力します：

```
rpm -I Ericom-Blaze-Client.rpm
```

「deb」を使用してインストールするには、Ericom-Blaze-Client.deb ファイルをダブル・クリックします。

「deb」バージョンのインストールは、次のコマンドからもインストールできます：

```
dpkg -i Ericom-Blaze-Client.deb
```



注意：

Linux シンクライアントに Blaze の 「deb」 パッケージをインストールする場合、シンクライアント・ベンダー製のソフトウェア・インストール・ツールが必要になることがあります。

グラフィカル・インストーラを使用するには、以下の手順を実行します：

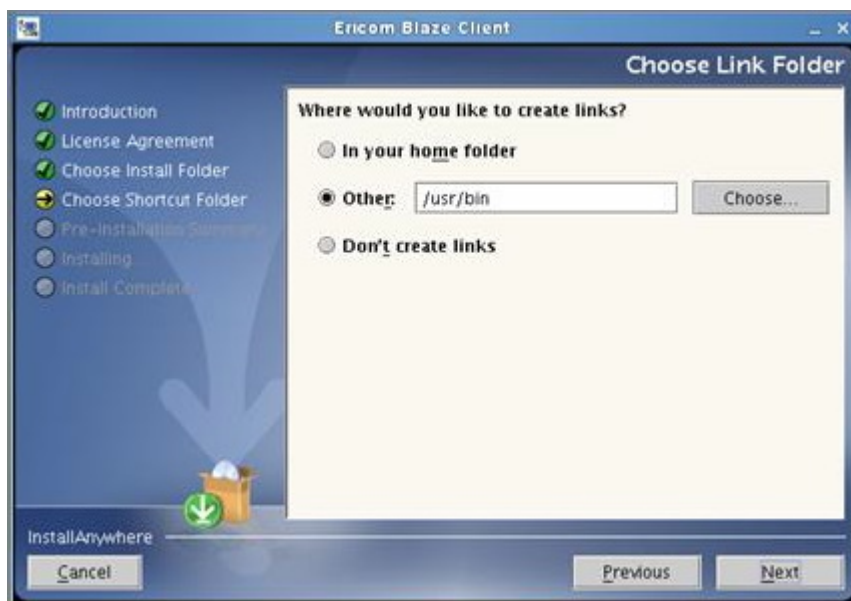
1. 「Ericom-Blaze-Client-For-Linux.zip」を解凍します。
2. zip ファイルから展開された「Ericom-Blaze-Client-For-Linux.sh」を起動します
3. インストール・ウィザードの指示に従います

root でインストーラを実行する場合、デフォルトで次の場所にインストールされます： /Ericom-Blaze-Client

それ以外の場合、インストールを行うユーザのホーム・ディレクトリにインストール・ディレクトリが作成されます。例えば：

```
/home/user/Ericom-Blaze-Client
```

インストール・ディレクトリには、blaze という名前の実行可能ファイルが含まれています。Ericom Blaze クライアントを起動するには、このファイルを実行します。グラフィカル・インストーラでは、実行可能ファイルへのリンク・ファイルを希望するディレクトリ内に作成するオプションが提供されます。デフォルトは、/usr/bin です。



対象のフォルダの書き込み権限が必要です。権限がない場合、エラー・メッセージが表示されます。

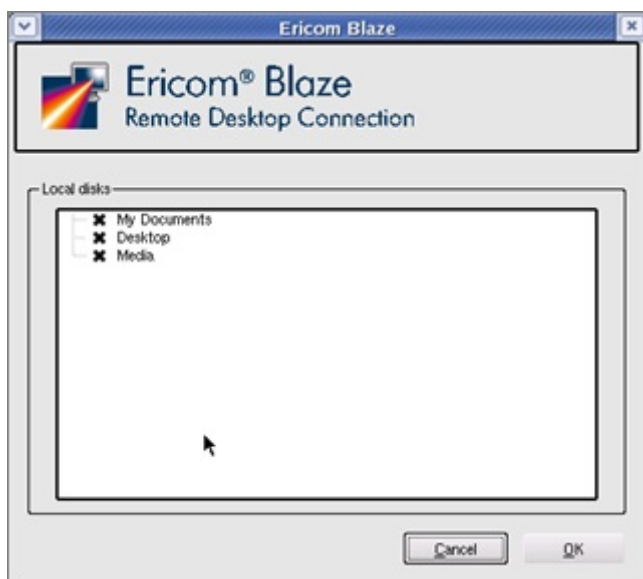
## Ericom Blaze Client for Linux を使用する

Ericom Blaze クライアントを起動するには、blaze の実行可能ファイルまたはリンクを実行します。Windows プラットフォーム上と同様の接続ウィザードが表示されます。詳細については、「*Blaze Client for Windows* (ページ 29)」の章を参照ください。実行可能ファイルは次のディレクトリにあります: /opt/Ericom-Blaze-Client

主な機能の使用法の説明については、「*Blaze Client for the Windows* (ページ 29)」の章を参照してください。このセクションは、Windows 版と Linux 版の Blaze クライアントの機能の違いをカバーしています。

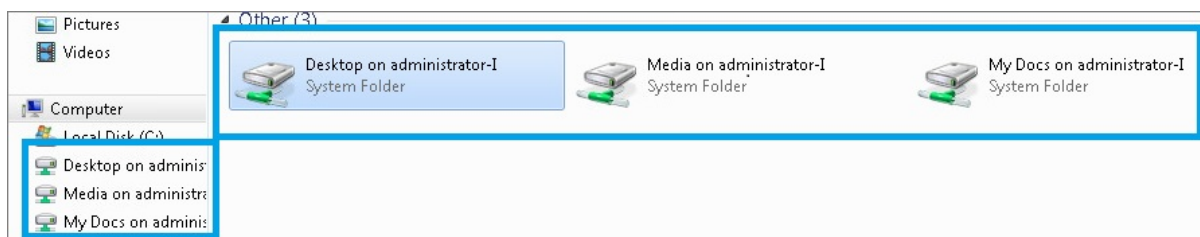
### ドライブ・マッピング

ドライブ・マッピング・ダイアログでは、以下の 3 つのオプションが提供されます:



- ホーム・ディレクトリにマップするには、My Documents を選択します
- デスクトップ・ディレクトリをマップするには、Desktop を選択します
- 「/media」ディレクトリをマップするには、メディアを選択します。このディレクトリは、CD-ROM、フロッピー・ディスクや Zip ドライブなどのリムーバブル・メディア上にファイル・システムをマウントするために使用されます。

Windows セッションに Blaze Linux クライアントが接続されると、コンピュータの一覧にドライブが表示されます。

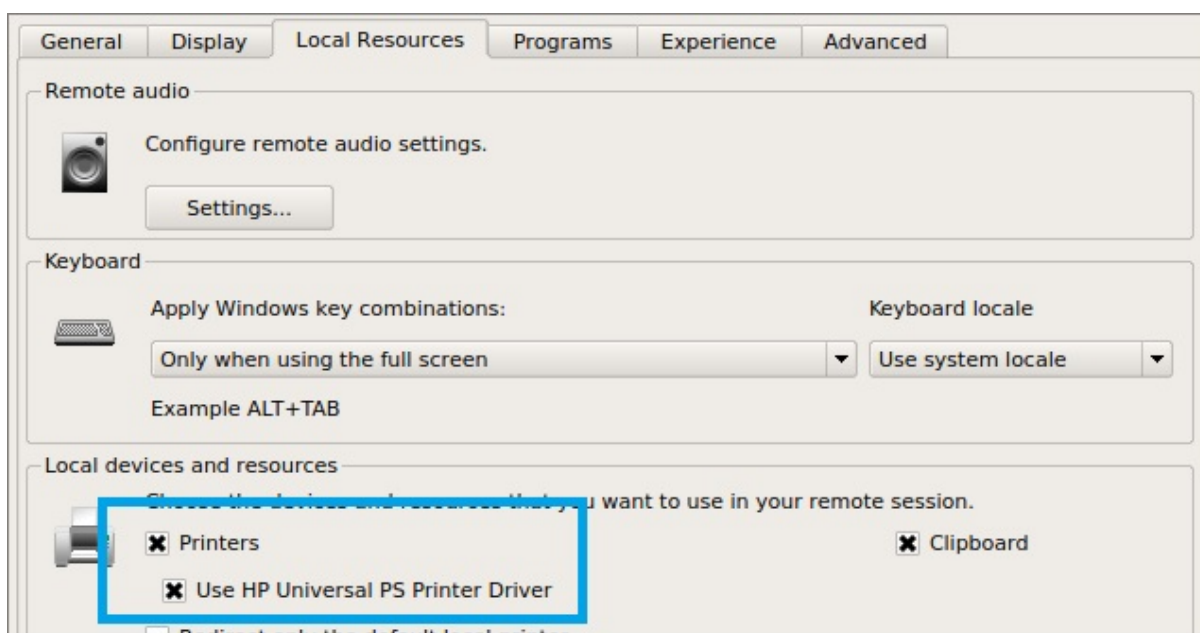


### プリンタのリダイレクト

Linux クライアント向けのプリンタ・リダイレクトでは、PostScript プリンタのみがサポートされています。Windows RDP ホスト上に、以下のプリンタ・ドライバをインストールする必要があります。

- 32 ビット・システム (x86) 上には、Windows PostScript 用の HP Universal Print ドライバをインストールします。
- 64 ビット・システム (x64) 上には、Windows PostScript x64 用の HP Universal Print ドライバをインストールします。

印刷を有効にするには、ローカルリソース・タブをクリックし、「Printers」と「Use HP Universal PS Printer Driver」をオンにします。





## 4.1.8 Ericom をアンインストールする

### Windows

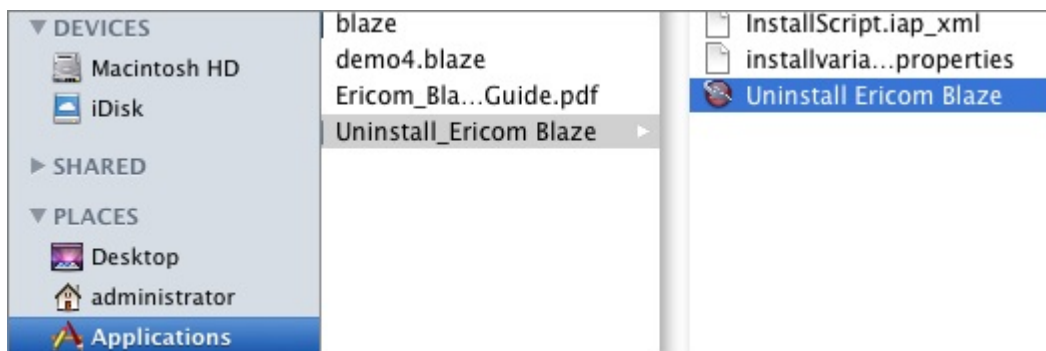
コントロール・パネルの「プログラムの追加と削除」を使用して Ericom Blaze クライアントと Access Server をアンインストールします。



目的のアプリケーションを選択し、アンインストール または 削除 をクリックし、アンインストール・プロセスを開始します。

### Mac

Blaze のアプリケーション・ディレクトリからアンインストールを実行します



### Linux

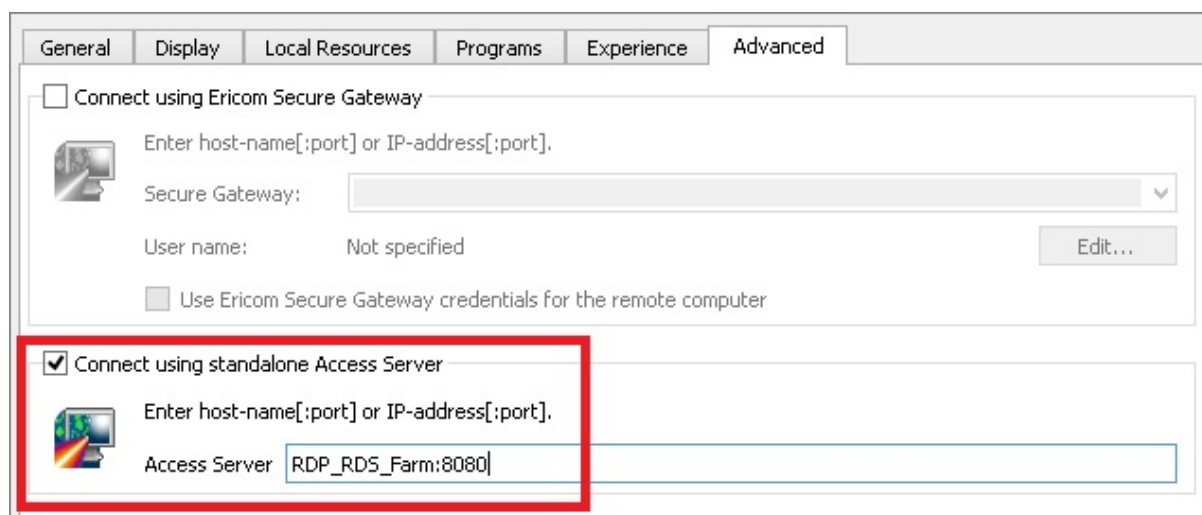
システムのアプリケーション・マネージャ (例: Ubuntu 上の Synaptic) を使用して、Ericom Blaze Client for Linux を削除します。

## 4.1.9 Blaze とロード・バランサ

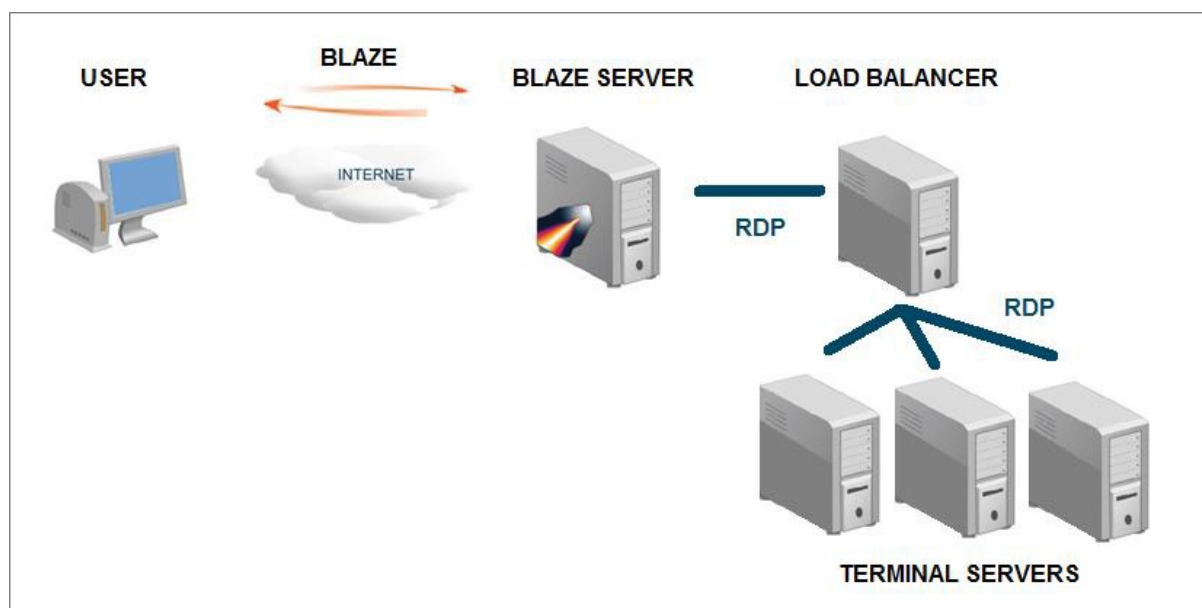
大規模なアプリケーションやデスクトップをホストする展開では、複数の RDP ホスト・サーバが必要になります。高い負荷を処理し、大規模なターミナル・サーバ群へユーザを均等に分散するために、Ericom PowerTermãDc WebConnect 接続ブローカーの使用をお勧めします。ただし、サード・パーティのターミナル・サーバに対応したロード・バランサ (例: Microsoft Windows Server 2008 R2 リモート・デスクトップ・コネクション・ブローカーや 2X Load Balancer) を使用することもできます。

負荷分散された RDP ファームで Blaze を使用するには、専用の強力なサーバに Access Server をインストールします。この場合には、x64 サーバと x64 Access Server の使用を強くお勧めします。Access Server のサーバ側受信ポート (例: 3399) と RDP 送信ポート (例: 3389) を開放します。

Access Server のアドレスに接続するように Ericom Blaze クライアントを設定します。Access Server により、ロード・バランサへの通信が転送されます。良好なパフォーマンスを確保するため、Access Server、ロード・バランサ、RDP ホストを近接させ、レイテンシを最小限にする必要があります。



以下の図は、ロード・バランサと Ericom Blaze の動作の仕組みを示しています。



Ericom Access Server を実行するシステムは、アクティブ・ユーザの総数を処理するために十分なメモリを備えている必要があります。



お願い:

Access Server をゲートウェイとして使用する場合、強力なサーバ (最低 2 コア CPU と 4GB RAM) 上で x64 バージョンを使用することをお勧めします。

## 4.1.10 Blaze クライアントのコマンド・ライン・パラメータ

Blaze.exe [オプション]

/option:<値>

/option:<デフォルト値 | 別の値 | 別の値>

ブール値には、次のいずれかを使用することができます: true、false、yes、no、on、off、1、0

例:

```
Blaze /bpp:32 /f /connection-bar:yes /audio:off /drive:C /drive:desktop /printer:*,3 /clipboard:1 /v:somehost
```

オプション:

**/v:server** [:ポート値] - RDP サーバのホスト名

**/u** : [<ドメイン>] <ユーザ名> または <ユーザ名>[@<ドメイン>]

**/p** : <パスワード>

**/d** : <ドメイン>

**/admin** - 管理者 (またはコンソール) セッション

**/multimon** : <use | span | モニタ番号> - Multimon 機能を使用するか、マルチモニタをスパンして表示するか、特定のモニタを使用します

**/w** : <幅> - リモート デスクトップの幅

**/h** : <高さ> - リモート デスクトップの高さ

**/size** : <幅>x<高さ> - リモート デスクトップの画面サイズ

**/f** - フルスクリーン・モード

**/bpp** : <色深度> セッションの bpp(色深度)

**/shell** : <代替シェル>

---

**/shell-dir** :<代替シェルの作業ディレクトリ>

**/jpeg-quality** :<percentage> 0 = アクセラレーションなし、100 = ロスレス、1-99 = JPEG 品質

**/true-lossless-type** :2 /image-quality:100: 真の可逆圧縮を設定

**/connection-bar** :<yes | no | pinned>接続バーのモード (フルスクリーンのみ)

**/use-esg** :<off | on> Ericom Secure Gateway を使用します

**/esg-creds-mode** :<separate | gw | rdp> - Ericom Secure Gateway の資格情報モード

**/g** :<ゲートウェイ>[:ポート値] - ゲートウェイのホスト名

**/gu** :<[<ドメイン>]<ユーザ名> または <ユーザ名>[<@<ドメイン>]> - ゲートウェイのユーザ名

**/gp** :<パスワード> -ゲートウェイのパスワード

**/gd** :<ドメイン> - ゲートウェイのドメイン

**/access-server** :<サーバ>[:ポート値] - Access Server のホスト名

**/use-scancodes** :<on | off> Unicode をスキャンコードに変換します

**/remote-show-window** :<「+」または「\_」> - デフォルト: 通常, 「+」: 最大化, 「\_」: 最小化

**/xtea-password** :<パスワード> - XTEA パスワード暗号化

**/disable-reconnect** :<off | on> -セッションの再接続を無効化

**/session-name** :<name> 接続名

**/null-cursor-shape** :<default | blank | cross | arrow | bmp | png> null カーソルの形状

**/reverse-mouse-wheel** マウス・ホイールを逆方向にします

**/kbd** :0x<レイアウト ID> または <レイアウト名> - キーボードのレイアウト

---

**/kbd-subtype** :<サブタイプ ID> - キーボードのサブタイプ

**/kbd-fn-key** :<ファンクション・キーのカウンタ> - キーボードのファンクション・キーのカウンタ

**/workarea** : 利用可能なワーク・エリアを使用します

**/monitors** :<\* | 0,1,2...> - 使用するモニタを選択します

**/addins** :<\* | 特定の dll> - 「\*」はすべてのアドインを指定します

**/audio** :<play-on-client | play-on-server | off> - 音声出力モード

**/network** :<none | modem | ow-speed-broadband | satellite | high-speed-broadband | wan | lan> - ネットワーク接続の種類

**/drive** :<\* | C | D.. | dynamic | desktop | docs> - ドライブをリダイレクトします。「\*」はすべて、「C」は「C:」、「dynamic」は後で接続するドライブをリダイレクトします

**/clipboard** :<off | on>-クリップボードをリダイレクトします

**/printer** <\* | 1 | 2 | 3> -1 プリンタをリダイレクトします。1 = ネイティブ、2 = 汎用、3 = 両方

**/uprinter-use-hp** :<off | on> - HP のドライバを使用した汎用ドライバ印刷

**/uprinter-driver** :<ドライバ名> - 汎用印刷ドライバ



**Tips:**

- 「HP」を使用する通常使うプリンタをリダイレクトするには : `"/uprinter-driver:HP Universal Printing PS" "/uprinter-postscript-regex:\b((?i)ps|(?i)postscript)\b" /printer:default,2`
- 「HP」を使用するすべてのプリンタをリダイレクトするには : `"/uprinter-driver:HP Universal Printing PS" "/uprinter-postscript-regex:\b((?i)ps|(?i)postscript)\b" /printer:*,2`

**/fonts** :<off | on> - フォントを滑らかにします (ClearType)

**/aero** :<off | on> - デスクトップ構成

`/window-drag` :<off | on> - 完全なウィンドウのドラッグ

`/menu-anim`s :<off | on> - メニューのアニメーション

`/wallpaper` :<on | off> - 壁紙

`/cache-waiting-list` :<on | off> - キャッシュの待機リストを使用します

`/fast-path` :<on | off> - 高速パス入力/出力

`/x` :[int value] `/y` :[int value] (例: `/x:0 /y:0`) - これは、リモート・セッション・ウィンドウの左上隅の位置を設定します (フルスクリーンではない場合)。8.5 で追加されました

【テクニカル・サポート用途のみ】

`/uprinter-postscript-regex`: `\b((?i)ps|(?i)postscript)\b` - 設定済みの正規表現に基づいて、ps または Po



参考:

- `\b` - 後続の表現または単語に一致することを意味します
- `(?i)` - 大文字と小文字を区別することを意味します
- `|` OR 表現

## ■ プロキシ・モードの設定

バージョン 8.2 以降では、Web プロキシを介して接続するよう Blaze を設定できます。プロキシ設定は、起動したすべての接続に使用されます。

構文:

```
blaze.exe -proxy-mode [proxy_mode] -proxy-server [proxy_server] -proxy-user [proxy_user] -
↔proxy-password [proxy_password]
```

- `proxy_mode` - (数値) 0 - プロキシ・モード: オフ、1 - プロキシ・モード: 自動、2 - プロキシ・モード: 手動。
- `proxy_server` - (文字列) プロキシ・サーバーのホスト名または IP アドレス + コロンとポート番号 (例: `myproxy.com:3138`)。
- `proxy_user` - (文字列、オプション) プロキシへのログインに使用するユーザ名。
- `proxy_password` - (文字列、オプション) 指定したユーザに対応するパスワード。ユーザ名に対してパスワードが必要な場合は、この値は必須です。ユーザ名に対してパスワードが必要であっても、パスワード欄が空白の場合、AccessPad ではプロンプトが表示されません。

## 4.1.11 テクニカル・サポート

現在および以前のバージョンのリリース・ノートは、Ericom の Web サイトのダウンロードページからダウンロードできます。このセクションでは、設定における一般的な問題を解決するための方策を説明します。

### Heartbeat と 7.3 以前のバージョンとの互換性がない

7.3 以前の AccessServer は、バージョン 8.1 で追加されたハートビート機能と互換性がなく、ハートビート・メッセージにより

- session heartbeat seconds:i:0

### アイドル状態の Blaze セッションにより、広い帯域幅が使用される

グラフィックスやアニメーションが豊富なスクリーン・セーバーを無効にしてください。空白の画面またはテキストのスクリーン・セーバーを使用してください。アニメーションを含むスクリーン・セーバーにより、すべてのプロトコルで広い帯域幅が使用されます。

### Blaze は上り帯域を使用しますか？

Ericom Blaze は通信の一部として上り帯域を使用します。ファイル共有プログラムなどの一部のアプリケーションでは、上り帯域が広く使用されます。このようなアプリケーションは上り帯域を制限する必要があります。または、アクティブな Blaze セッションが存在する際は使用しないでください。

### RDP ポートをカスタム値に変更する

「レジストリ エディタ」(regedit.exe) を使用して、以下の設定を変更します:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-  
Tcp\PortNumber
```

任意のポート値を入力します。この設定は、自動的に Access Server に認識されます。

### 「Ericom Access Server に接続できません」というエラーが表示される

Ericom Access Server が実行されていないか、アクセスできない状態です。

- ping を使用して、サーバ (例: テスト・サーバ) がアクセス可能な状態であることを確認してください。
- ホスト/サーバのファイアウォールで Ericom Blaze のトラフィック (デフォルトでは 3399) が許可されているか確認してください。
- サーバのタスク・マネージャを使用して、AccessServer が実行中であることを確認してください (AccessServer はサービスとして実行されるため、タスク・マネージャですべてのユーザのプロセスが表示されるよう設定する必要があります)。



## ■ RDP アクセラレーションを有効化した Blaze クライアントを起動すると、スプラッシュ・スクリーンが表示された後に何も起きない

Blaze クライアントを Access Server に 接続できていますが、RDP ホストには接続できていません (RDP ホスト上で Access Server を実行中だとしても)。ホストへの RDP アクセスが無効化されているか、RDP アクセスが特定のネットワーク・アダプタに限定されている可能性があります。

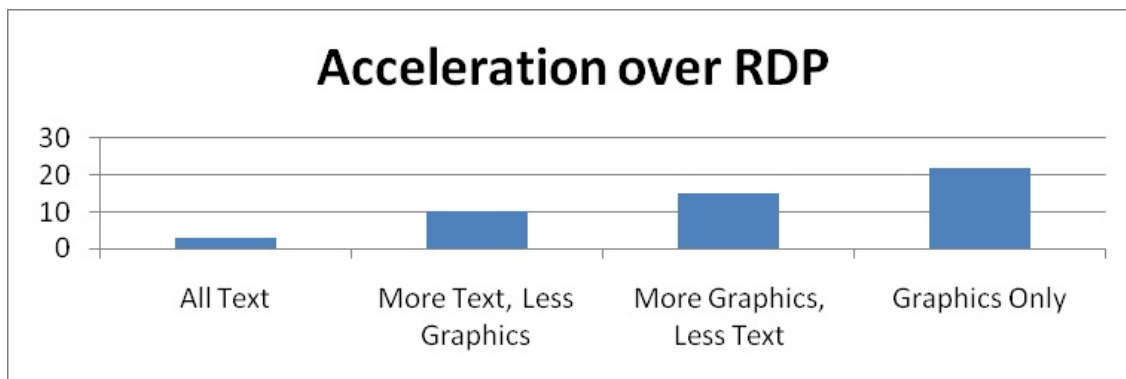
ターミナル・サーバへの RDP アクセスが特定のネットワーク・アダプタに限定されているかを確認するには、管理ツールから「ターミナル・サービス設定」を開きます。表示されるダイアログで、「RDP-Tcp」をダブル・クリックし、「ネットワーク・アダプタ」タブを選択します。ネットワーク・アダプタのドロップダウンが「このプロトコルで構成されたすべてのネットワーク・アダプタ」に設定されていることを確認してください。



## ■ Blaze を使用することで、どの程度のアクセラレーションを期待できますか？

これは、各環境のネットワークのタイプと表示内容により異なります。Blaze は、RDP セッションを最大 20 倍アクセラレートします。ホットスポットなど、高レイテンシ、低帯域幅の制限を持つネットワークで使用した場合に、最も効果を発揮します。ネットワークの制約がない LAN 経由で接続する場合、顕著な改善は見られない可能性があります。

セッションの大部分がテキスト (例: メールの編集) で構成されている場合や、単色画像 (例: 白黒画像) で構成されている場合は、グラフィックの豊富なアプリケーション (例: サテライト・モードの Google マップ) の場合と比較して、アクセラレーションは減少します。

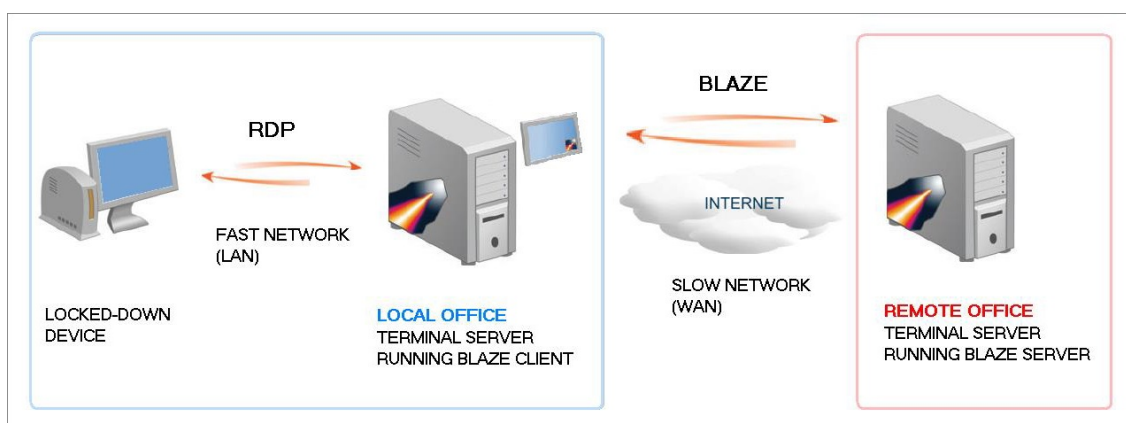


## ■ WYSE ThinOS デバイスでの使用方法

Wyse ThinOS デバイス向けに Blaze アクセスを提供するには、Access Server をゲートウェイとして使用するのが最善の方法です。 これを実装するには、以下の手順を実行します:

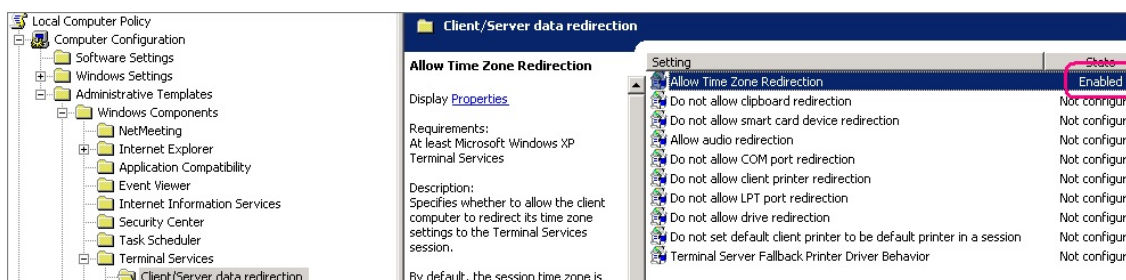
Wyse ターミナルを実行する新しい (ローカル) ターミナル・サーバをセットアップします。 ローカル・ターミナル・サーバに Blaze をインストールします。

(高速 LAN 接続を使用して) RDP ローカル・ターミナル・サーバと Wyse ターミナルを接続し、(低速ネットワーク接続を経由して) リモート・システムに接続するために、Blaze クライアントを実行します。



## ■ タイムゾーンのリダイレクトが動作しない

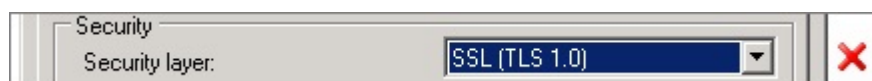
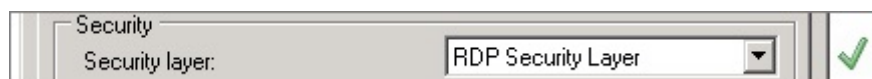
RDP ホスト上のタイムゾーンの同期を有効にしてください。 これは、以下のようにグループ・ポリシー・エディタを使用して設定できます。



## ■ イベント・ビューアー に以下のような TermDD エラーが表示される

エラー: *The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client.*

Access Server には、RDP ホスト上で有効にするためのネイティブ RDP へのアクセスが必要です。このため、RDP Security Layer を SSL へ変更しないでください。RDP Security Layer の設定は変更せず、ビルトインの AccessNow SSL 暗号化または Secure Gateway を使用して SSL 暗号化を追加します。



## 4.2 Secure Gateway 管理者ガイド

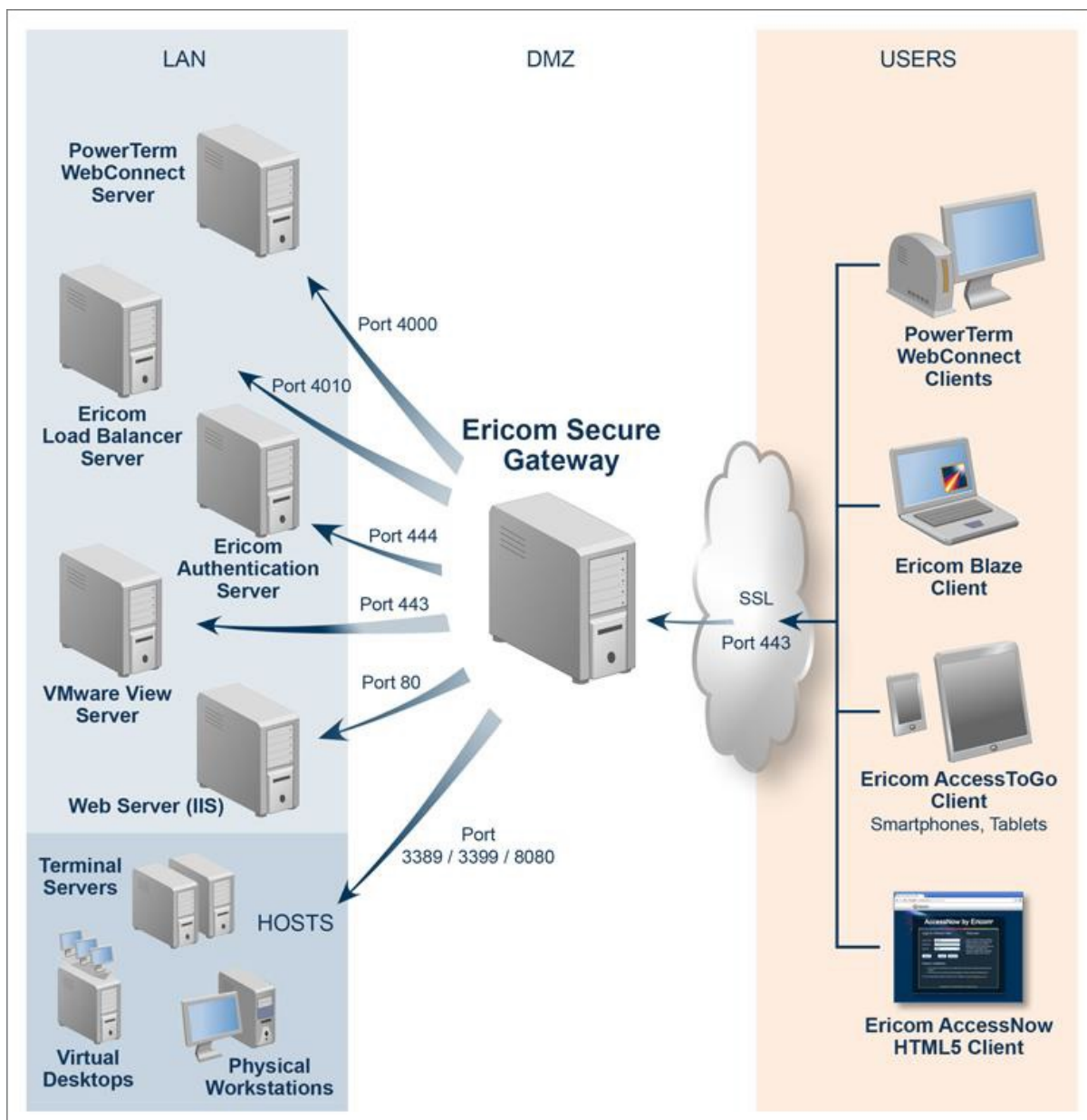
### 4.2.1 概要

Ericom Secure Gateway は、RDP ホスト (仮想デスクトップ、ターミナル・サーバなど) をはじめとする内部ネットワーク・リソースへのセキュアなリモート・アクセスを、エンド・ユーザに提供します。Secure Gateway には、以下の利点があります:

- セキュリティで保護された、単一ポートでの内部リソースへのアクセスが可能
- Ericom クライアント用の VPN の購入、インストール、設定、管理が不要
- その他のリソースを内部ファイアウォールの後方に配置したまま、Ericom Secure Gateway を DMZ にインストール可能
- Ericom Secure Gateway に一度だけ証明書のインストールが必要となり、アクセスする必要があるすべてのホストへの証明書のインストールは不要
- TLS 1.2 準拠
- Ericom Blaze 2.x 以降に対応
- Ericom PowerTerm WebConnect 5.8.0 以降に対応
- Ericom AccessNow™ HTML5 クライアントに対応
- Ericom AccessToGo™ 1.4 以降に対応

### アーキテクチャ

Ericom Secure Gateway は、リモート環境のエンド・ユーザとデータセンターのアプリケーションやデスクトップ間のゲートウェイとして機能します。インターネットと LAN の間のトラフィックをルーティングする DMZ にインストールすることも可能です。VMware View 用に Ericom Blaze を使用する場合 VMware View Security Server の代わりとして Ericom Secure Gateway が使用されます。以下の図は、Secure Gateway により 1 つのポートのみを介したセキュアなリモート・アクセスが可能となる仕組みを示しています。Web トラフィック、コネクション・ブローカー通信、セッション・プロトコルに関連するすべての通信は、SSL ベースの Secure Gateway 接続を通してトンネル接続されます。



注意:

負荷分散機能は有効化されていません。ESG を介した負荷分散ターミナル・サーバの詳細については、Ericom の営業担当者までお問い合わせください。

## 4.2.2 インストール

### 前提条件

Windows 2008R2 以降で Ericom Secure Gateway を実行する必要があります。

- 2008R2 では、TLS 1.0 のサポートが必須です。
- 2016、2019 では TLS 1.1 および 1.2 がサポートされています。

.NET Framework 4.6.2 のフル・インストールが必要です - Microsoft の Web サイトからダウンロードできます。

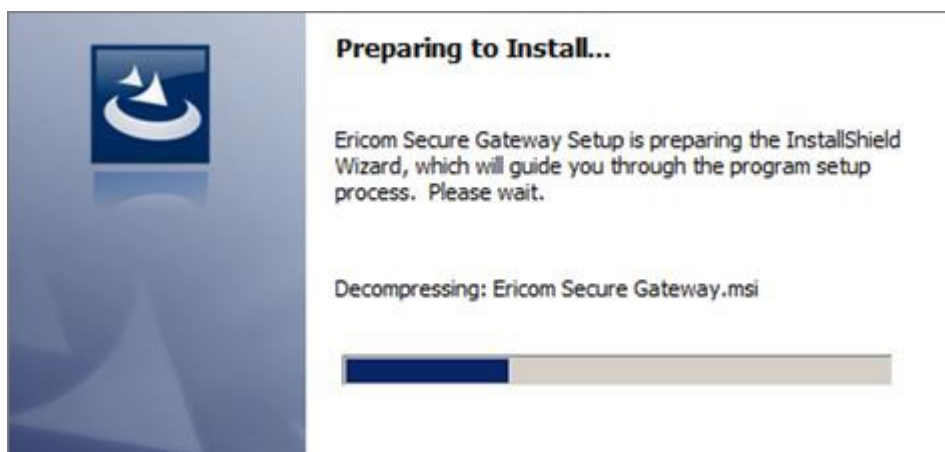
Ericom Secure Gateway により、デフォルトでポート 443 が使用されます。このポートは IIS でも使用される一般的なポートのため、ポートの競合に注意してください。ネットワーク上で以下のポートを設定する必要があります：

- インターネットと Secure Gateway サーバ間に、ポート 443 が必要です。この値は調整可能です。
- RDP アクセス用: Secure Gateway サーバと RDP ホスト間に、ポート 3389 が必要です。この値は調整可能です。
- Ericom Blaze 用: Secure Gateway サーバと Ericom Blaze サーバを実行する RDP ホスト間に、ポート 3399 が必要です。
- Ericom AccessNow 用: Secure Gateway と AccessNow サーバ間に、ポート 8080 が必要です。この値は調整可能です。
- PowerTerm WebConnect 用: Secure Gateway と PowerTermWebConnect サーバ間に、ポート 4000 が必要です。この値は調整可能です。使用するプロトコル (RDP、Blaze、AccessNow) により、上記のポートの 1 つまたは複数が必要になります。
- VMware View 用: Secure Gateway と VMware View ブローカー間に、ポート 443 が必要です。

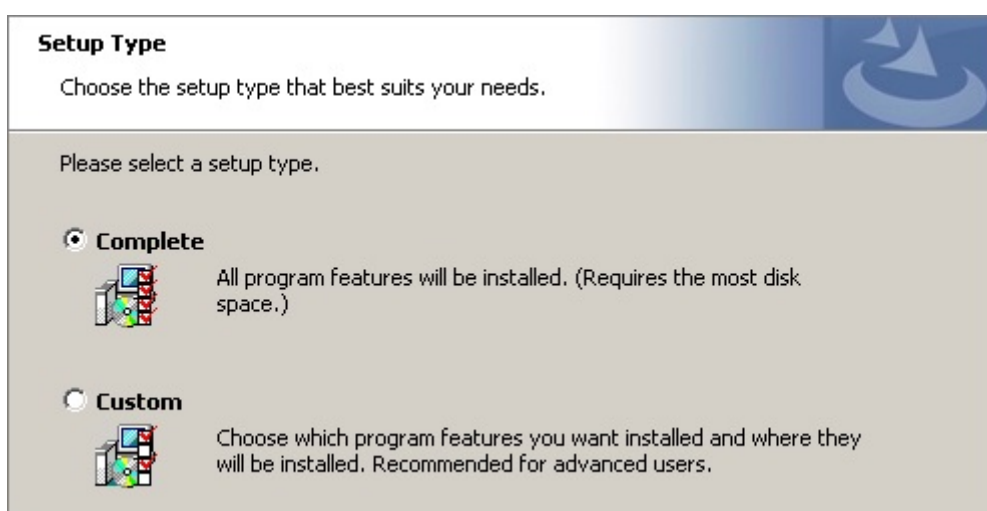
エンド・ユーザと RDP ホスト間のセッション通信には、ホスト上で RDP アクセスを有効化する必要があります。RDP ホストのローカル・ファイアウォールで RDP ポート (3389) が開放されていることを確認してください。Secure Gateway は HTTP プロキシを備えており、デフォルトでポート 80 をリッスンします。これは、インストール後に無効にできます。

### Secure Gateway のインストール

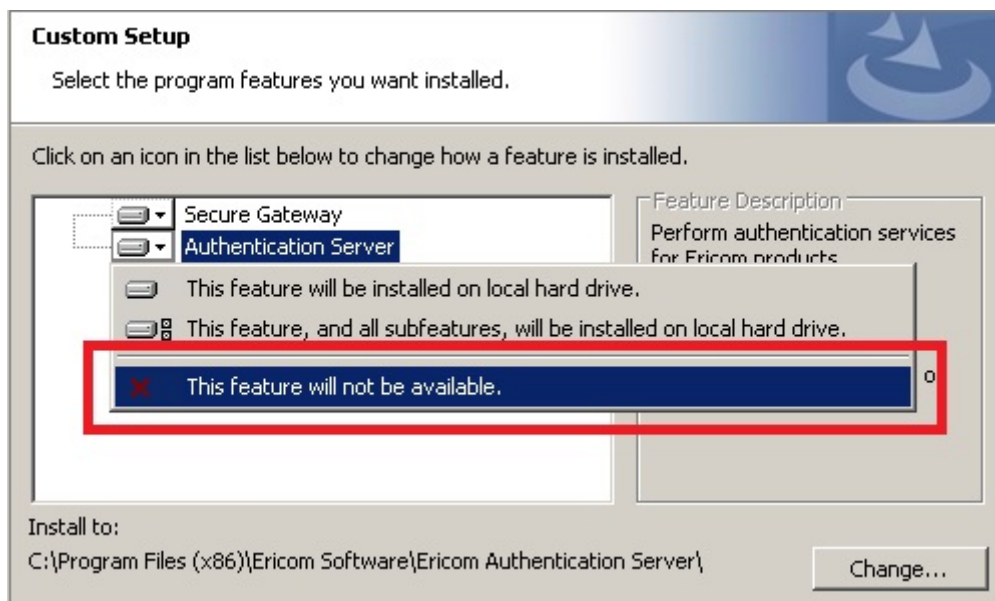
Secure Gateway をインストールするには、Windows 7 SP1、8、2008R2 SP1、2012R2、または 2016 を実行中のサーバでインストーラ (Ericom Secure Gateway Server.msi) を起動します。一部のシステムでは、インストールの実行に承認が必要となる場合があります。Next をクリックし、License Agreement(使用許諾契約) に同意し、Install をクリックしてインストールを実行します。



Setup Type の選択画面が表示された場合、以下のいずれかを選択します:

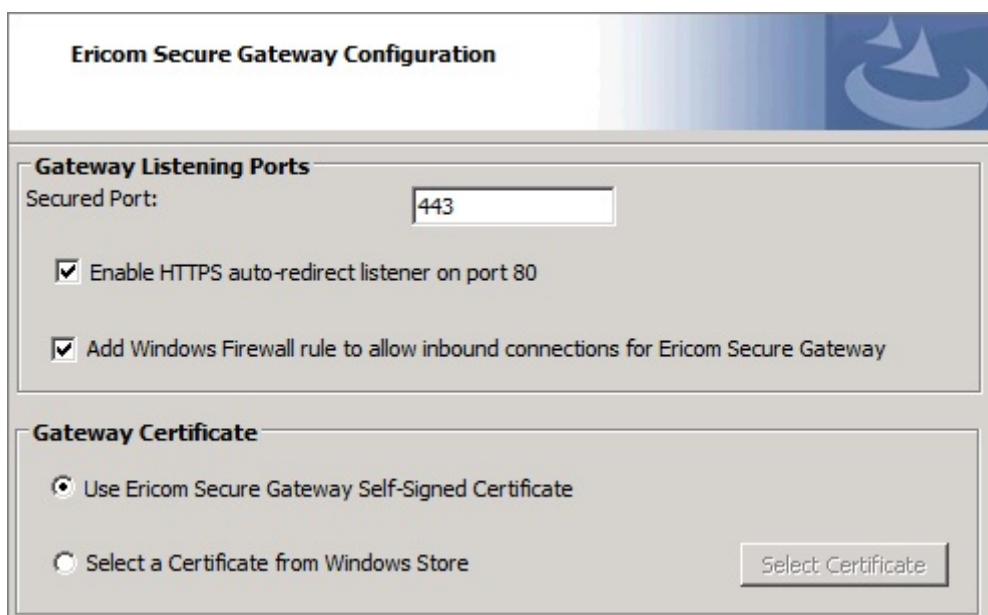


- Complete - Ericom AccessNow や Blaze スタンドアロン (AccessNow for Citrix と AccessNow for Quest vWorkspace を含む) とともに Secure Gateway を使用する場合は、この設定を選択します。上記のスタンドアロン製品群のいずれかと併用して PowerTerm WebConnect や VMware View を使用する場合は、この設定を使用します。
- Custom - Ericom Secure Gateway または 認証サーバのみをインストールするには、このオプションを選択します。PowerTerm WebConnect または VMwareView のみを使用する場合は、認証を処理するブローカーとして認証サーバをインストールする必要はありません。



## Secure Gateway の設定

プロンプトが表示されたら、Secure Gateway でリッスンする必要のあるポートを入力します。デフォルトでは、ポートは 443 となります。Secure Gateway は、HTTPS を使用して特定のポートを介して動作するビルトインの Web サーバを備えています。Enable HTTPS auto-redirect on port 80 の設定をオンにすることで、Secure Gateway により HTTP Web リクエストが自動的に HTTPS にリダイレクトされます。







注意:

同一サーバで IIS を実行している場合、ポートの競合がないことを確認してください。IIS のポートを 80 と 443 以外の値に変更するか、Secure Gateway のポートを 443 以外に変更し、インストール後に HTTP 自動リダイレクト機能を無効にしてください。HTTP または HTTPS いずれかのポートで競合が発生した場合、以下の警告が表示されます:



マシンにインストール済みの信頼された証明書を使用するには、Select Certificate をクリックし、Secure Gateway で使用する証明書を選択します。信頼された証明書は、インストール後に設定することも可能です。

## ■ 認証サーバの設定

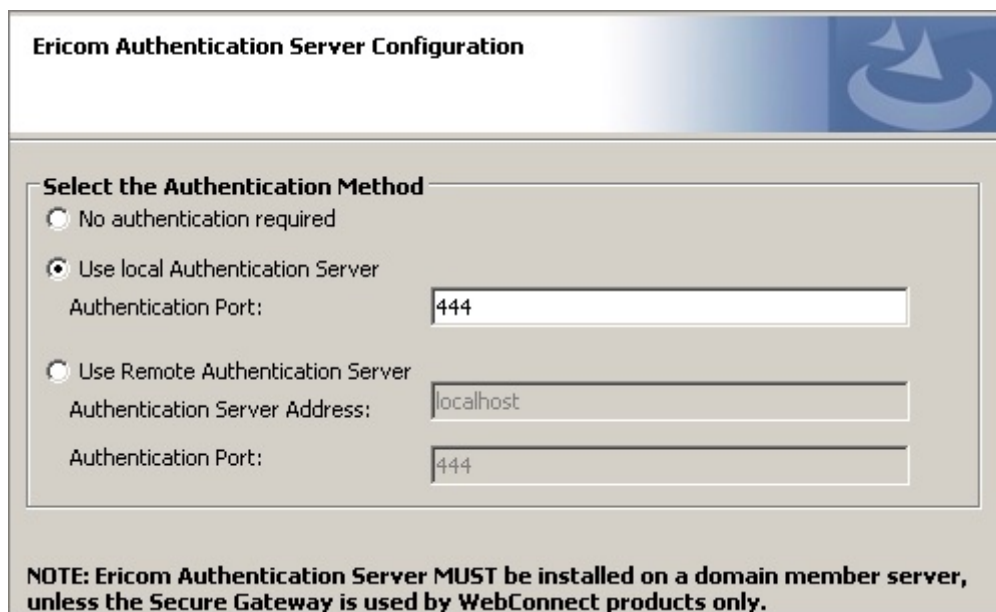
次のダイアログ Authentication Server Configuration では、使用する認証サーバを指定します



注意:

認証サーバは、認証するドメインのメンバーとする必要があります。セキュリティ上のベスト・プラクティスとして、一部のネットワーク上では、DMZ ではなく LAN 上に認証サーバをインストールする必要があります。

- このサーバを新しい認証サーバとして動作させるには、local を選択します。
- 既に使用している認証サーバが存在する場合、Remote Authentication Server を選択し、アドレスとポートを指定します。
- PowerTerm WebConnect または VMware View を使用し、スタンドアロン・クライアント・アクセスが必要ない場合、No authentication required を選択します。



**Ericom Authentication Server Configuration**

**Select the Authentication Method**

No authentication required

Use local Authentication Server  
 Authentication Port:

Use Remote Authentication Server  
 Authentication Server Address:   
 Authentication Port:

**NOTE: Ericom Authentication Server MUST be installed on a domain member server, unless the Secure Gateway is used by WebConnect products only.**



注意:

認証サーバはデフォルトでポート 444 をリッスンするため、このポートが ネットワークと  
 ↔Windows  
 ファイアウォール上で有効化されていることを確認してください。

## ■ コネクション・ブローカーの設定

コネクション・ブローカー・ダイアログを使用して、対応するコネクション・ブローカー (PowerTerm WebConnect または VMware View) とともに動作するように ESG を設定することができます。設定するブローカーを選択します。ブローカーを使用しない場合、No connection broker in use を選択します。PowerTerm WebConnect と VMware View の両方を使用する場合、インストール後に設定を行う必要があります。



**Connection Broker Selection**

PowerTerm WebConnect

VMware View

コネクション・ブローカーを使用中の場合、Only allow connections from a connection broker を有効にすることを強くお勧めします。スタンドアロン・クライアントからのすべての接続は拒否され、Secure Gateway を使用して接続が試行されます。

Only allow connections from a connection broker. Deny connections from standalone clients

## PowerTerm WebConnect の設定

PowerTerm WebConnect サーバ情報が表示されたら、PowerTerm WebConnect と、その Web ページをホストしている Web サーバのアドレスを入力します。そのアドレスは Ericom Secure Gateway サーバからアクセス可能である必要があります (ping.exe telnet.exe を使用して接続を確認します)。

**WebConnect Server**

Address:  Port:

Reminder: Configure PowerTerm WebConnect Server Configuration with the address and port of this Secure Gateway

---

**Ericom Web Server Proxy Configuration**

Ericom Secure Gateway can act as an HTTP Proxy to Ericom Web Server Components

Address:  Port:   HTTP  HTTPS

## VMware View の設定

VMware View サーバ情報が表示されたら、ブローカー・サーバのアドレスを入力します。そのアドレスは Ericom Secure Gateway サーバからアクセス可能である必要があります (ping.exe telnet.exe を使用して接続を確認します)。

**VMware View Server Configuration**

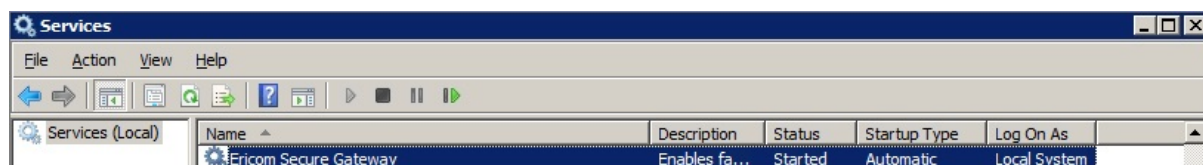
---

VMware View Server

Address:  Port:   SSL

## インストールを完了する

設定データを入力した後、Next をクリックしてインストールを続行します。インストールの最後で Finish をクリックします。Ericom Secure Gateway はサービスとして実行され、Windows サービス・マネージャから停止や再起動できます。



このサービスはシステム起動時に自動的に実行されるよう設定されています。サービスが停止された場合または設定したポートのリッスンができない場合、クライアントはゲートウェイを介してホストに接続できなくなります。設定したポートがサービスによりリッスンできない場合、Windows アプリケーション・イベント・ログにエラー・メッセージが出力されます。すべての設定は、Web ベースの管理コンソールを使用して変更するか、EricomSecureGateway.exe.Config ファイルを編集して変更できます。



注意:

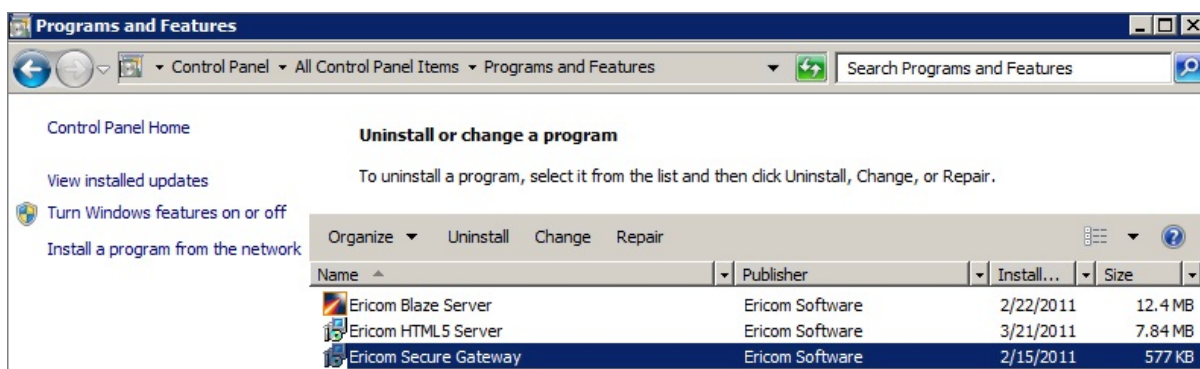
主に PowerTerm WebConnect または VMware View 用に ESG を使用する場合、Web ベースのコンソールに移動し、

Web Server タブの デフォルト フォルダ に目的の製品を設定します。



## Ericom Secure Gateway をアンインストールする

Ericom Secure Gateway のアンインストールには、コントロールパネルの「プログラムの追加と削除」または「プログラムと機能」を使用します。Ericom Secure Gateway を選択し、アンインストール をクリックします。

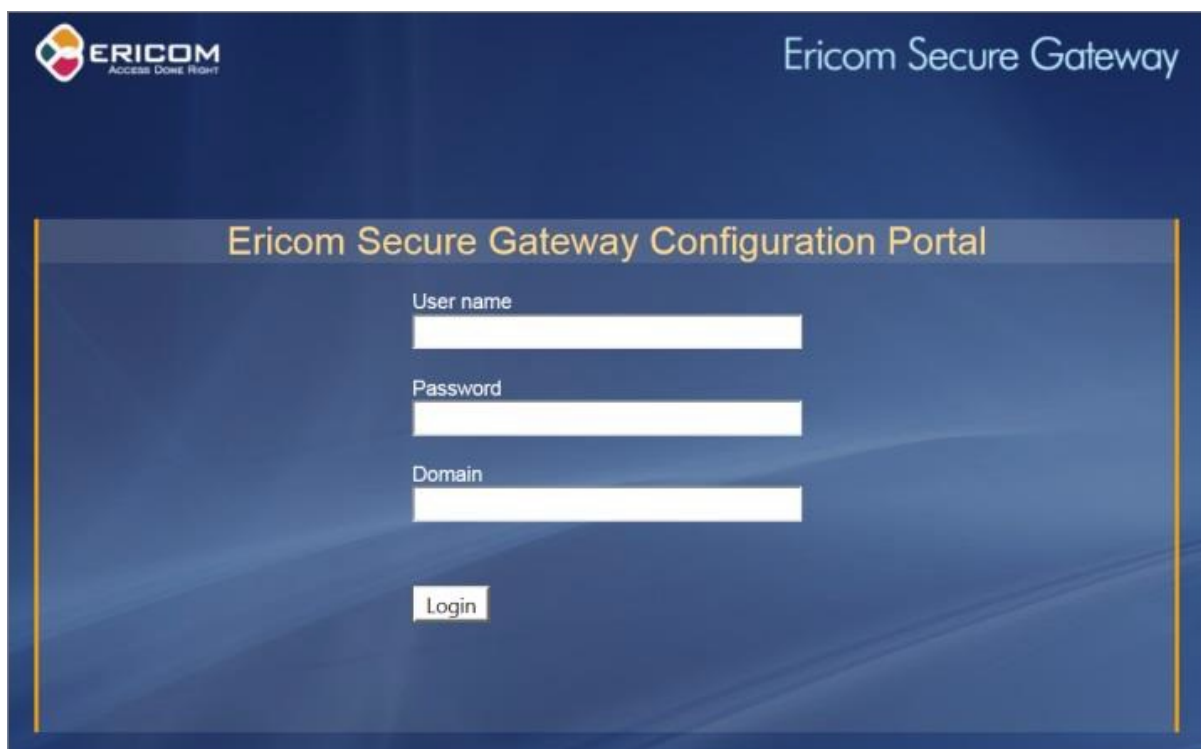


## 4.2.3 Configuration Portal

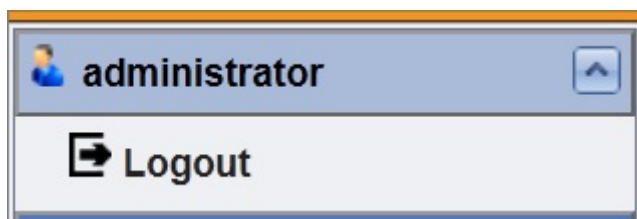
Ericom Secure Gateway(ESG) は、管理者が関連する設定変更を実行できる Configuration Portal を備えています。これらの設定の大部分は、インストール・プロセス中に設定したものです。Configuration Portal ページにアクセスするには、Web ブラウザを使用して Secure Gateway の設定 URL に移動します:

https://<ESG サーバのアドレス>:<ポート番号>/admin

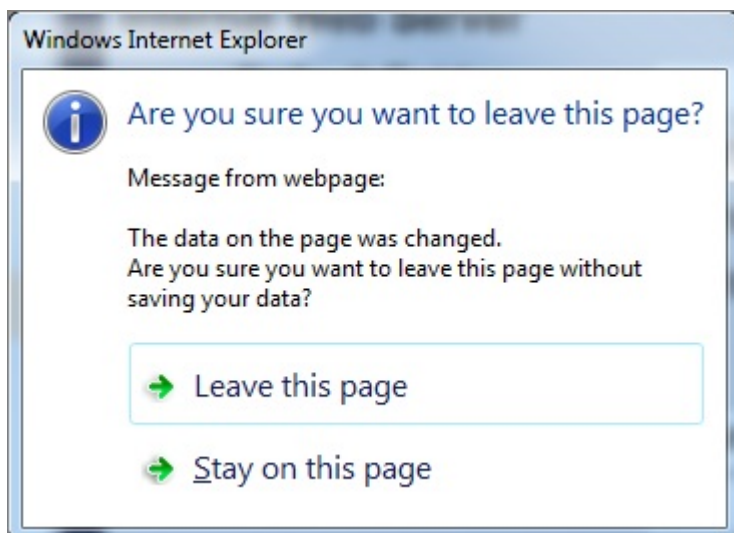
ESG サーバ上のローカル Administrators グループのメンバーであるいずれかのユーザでログインします。すべてのログインは、Ericom Secure Gateway のログ・ファイルにて監査されます。セキュリティで保護されたアクセスを確実にするために、強固なパスワードを使用することを管理者に注意喚起してください。



Configuration Portal からログアウトするには、Logout ボタンを押します。

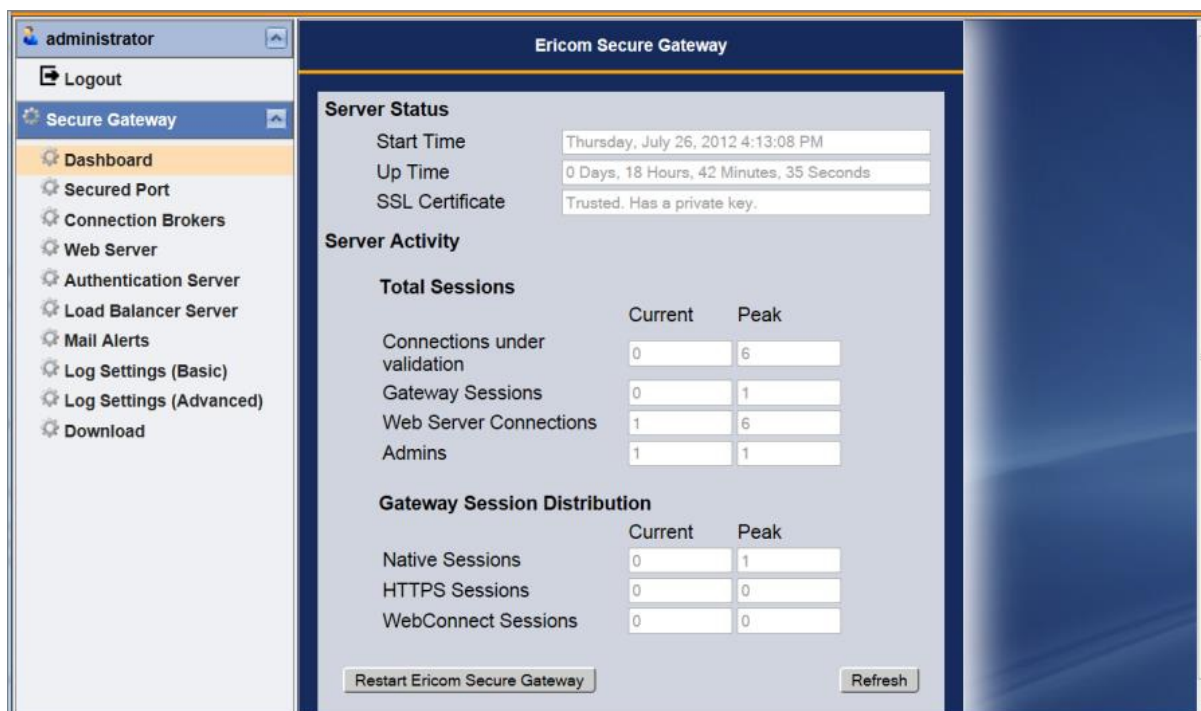


設定を変更した場合、Save ボタンを押します。Save ボタンを押さずに違うページを選択した場合、警告ダイアログが表示されます。変更をキャンセルして続行する場合には、Leave this Page をクリックします。現在のページに戻り変更を保存するには、Stay on this page をクリックします。



## Dashboard

ESG Configuration Dashboard には、Ericom Secure Gateway の動作に関連する役立つ統計情報が表示されます。このページを使用して、サーバの稼働時間、SSL 証明書の状態、セッション・アクティビティの確認や、Ericom Secure Gateway サーバの再起動を実行できます。



## メール・アラート

特定のシステム・イベント時に、E メール・アラートを送信するよう Ericom Secure Gateway を設定できます。メール・アラートを設定するには、E メール・サーバの SMTP 情報を入力します。次に、メール・アラート送信のトリガとなるパラメータをチェックします。

設定を適用するには、Save または Save and Test Mail Settings をクリックします。

The screenshot displays the configuration page for Mail Alerts in the Ericom Secure Gateway. The interface is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes options like Dashboard, Secured Port, Connection Brokers, Web Server, Authentication Server, Load Balancer Server, Mail Alerts (highlighted), Log Settings (Basic), Log Settings (Advanced), and Download. The main configuration area is titled 'SMTP Server Settings' and contains several sections: 'SMTP Server Settings' with fields for Address (mail.test.com), Port (25), User Name, Password, and a 'Secured' checkbox; 'Email Settings' with fields for From (ESG Service), To (administrator@test.com), and Subject Prefix (Ericom Secure Gateway mail alert:); and 'Alerts' with checkboxes for Gateway Status (Started, Stopped, Crashed, Failed bind to port) and 'Unable to connect to:' (Host, External Web Server, VMware View Server, WebConnect Server, Authentication Server, Load Balancer Server). At the bottom, there are buttons for 'Save and Test Mail Settings', 'Save', and 'Cancel'. A note at the top of the main area states 'Fields marked with \* are mandatory'.

その他の設定ページについては、次の章で取り上げます。

## 4.2.4 ポートと SSL 証明書

Ericom Secure Gateway には、自己署名証明書が備えられています。一部の Web ブラウザでは、自己署名証明書の検出時にセキュリティの警告が表示される場合があります。この警告を除くには、信頼された証明書をインストールします。信頼された証明書は、信頼された証明機関 (GoDaddy など) から購入する必要があります。証明機関により返される「.CER」ファイルには、秘密鍵が含まれていないことが一般的です。「.CER」ファイルは、秘密鍵を持つ「PFX」に変換する必要があります。通常これは、元の CSR を作成したシステム (例: IIS) 上で実行します。「PFX」を作成する際は、新たに入力したパスワードのメモを取り、証明書をエクスポート可能に設定します。

Ericom Secure Gateway では、Windows 証明書ストア (コンピュータ・アカウント) でその証明書が使用されます。証明書の追加、確認または変更するには、以下を実行します。



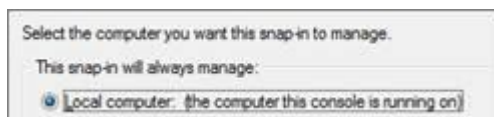
### Tips:

Ericom Secure Gateway サーバで CSR を作成する手順は「APPENDIX」- 「[Ericom Secure Gateway の CSR 作成 \(ページ 183\)](#)」を参考にしてください。  
他の方法で作成した「PFX」をお持ちの場合は、下記手順から証明書のインストールが可能です。

1. 「mmc.exe」を実行します
2. ファイル | スナップインの追加/削除 に移動します
3. 証明書を追加し、コンピュータ アカウント を選択します。



4. ローカル・コンピュータ を選択します



5. 完了 をクリックし、OK をクリックします。
6. 証明書 | 個人 | 証明書 フォルダに移動し、Secure Gateway に使用できるすべての利用可能な証明書を確認します。



7. 信頼された証明書を Secure Gateway に使用する場合、その証明書を Secure Gateway の証明書と同じ場所に保存します (個人 | 証明書)。



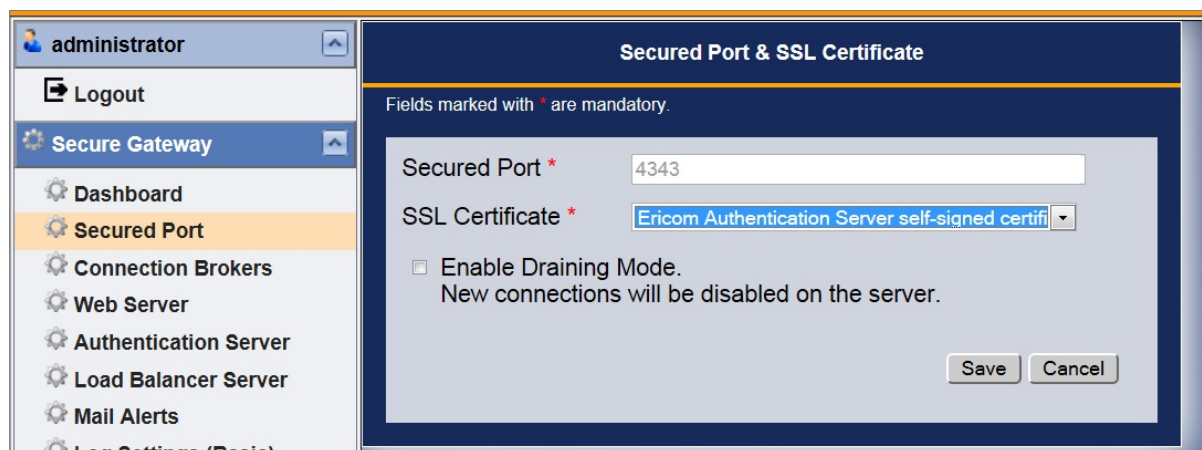
8.1 以下の Ericom Secure Gateway では、ゲートウェイの設定ファイル EricomSecureGateway.exe.config で設定する一意の拇印を使用して証明書が識別されます。

```
<add key="CertificateThumbprint" value="<信頼された証明書の値をここに入力します>" />
```

8.5 以降のバージョンをご利用の場合は、Ericom Secure Gateway で使用する証明書の設定は、後述の「セキュリティで保護されたポートと SSL 証明書を設定する」の画面で設定してください。

## セキュリティで保護されたポートと SSL 証明書を設定する

Secure Gateway で使用するポートを変更するには、「Secured Port and SSL Certificate」ページを使用します。設定の前に、目的のポートがサーバで使用中でないことを確認してください。Netstat ユーティリティを使用して、ポートのステータスを確認します。ESG で使用する SSL 証明書を選択します。ESG を本番環境で使用する場合、信頼された証明書を使用することを強くお勧めします。Dashboard ページから、選択した証明書が信頼されたものであることを確認します。



## 信頼された証明書を手動で設定する



注意:

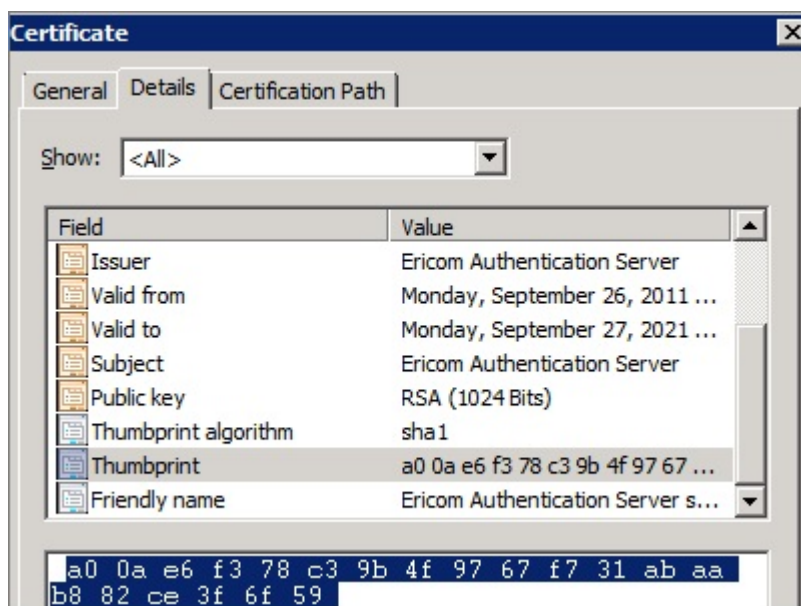
8.5 以降をご利用の場合は、上記「セキュリティで保護されたポートと SSL 証明書を設定する」の画面から証明書を設定してください。

信頼された証明書を Secure Gateway で使用するには、以下の 2 つの手動設定の方法があります。

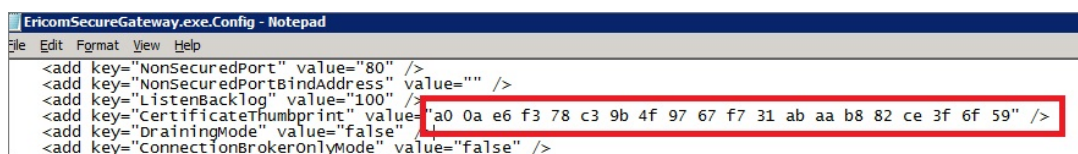
方法 1: 「EricomSecureGateway.exe /import\_cert」を実行し、Windows ストアから証明書を選択します。次に、その証明書の拇印を設定ファイルにインポートします。

方法 2: 以下の方法を実行して、拇印の値を設定ファイルに追加します:

1. 証明書の 詳細 タブに進み、拇印をハイライトします。



- CTRL-C を押し、コピーします。
- OK をクリックし、ダイアログを閉じます。
- EricomSecureGateway.exe.Config ファイルを開きます。
- 既存の拇印を削除し、CTRL-V を押し、新しい拇印をファイルにコピーします。すべてのスペースは無視されます。



- ファイルを保存すると、新しい拇印が使用されるようになります。Secure Gateway サービスを再起動すると、新しい証明書がすぐに適用されます。

拇印を手動で入力することも可能です。



注意:

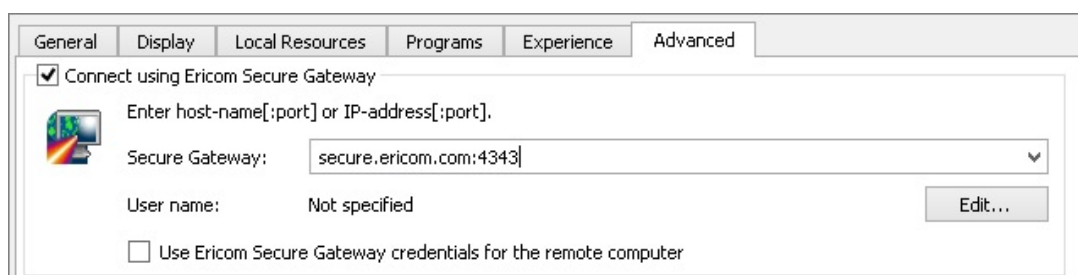
Secure Gateway サーバの DNS アドレスは、証明書の名前と一致する必要があります。一致しない場合、接続時に以下のエラー・メッセージが表示されます:

**Connection failed - verify that the Ericom Secure Gateway is running and reachable**

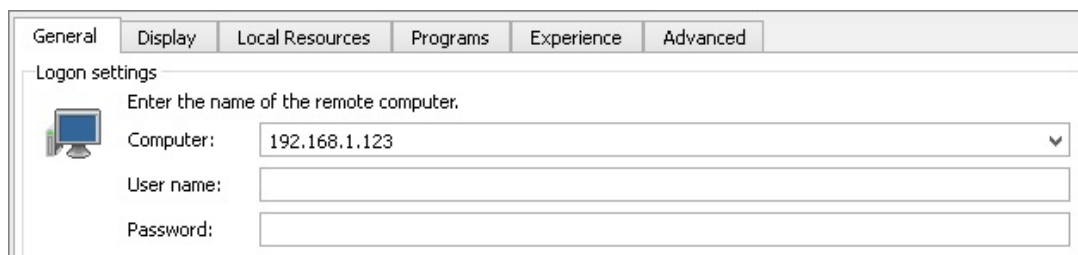
## 4.2.5 BLAZE クライアントの設定

Ericom Blaze クライアントでは、Secure Gateway を使用した Blaze サーバへの接続がサポートされています。Secure Gateway とともに使用するために Blaze クライアントを設定するには、以下を実行します：

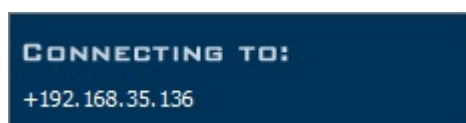
1. RDP ホスト上に Blaze Server 2.x をインストールして実行中であることを確認します。
2. Blaze クライアントを起動し、詳細 タブに移動します。「Connect using Ericom Secure Gateway」(Ericom Secure Gateway を使用して接続) をクリックし、Secure Gateway サーバのアドレスとポートを入力します (アドレス:ポート)。このアドレスは、Blaze クライアントから到達可能なものとする必要があります。



3. 一般 タブに移動し、Secure Gateway から見た場合の Blaze サーバのアドレス (通常は内部アドレス) を入力します。



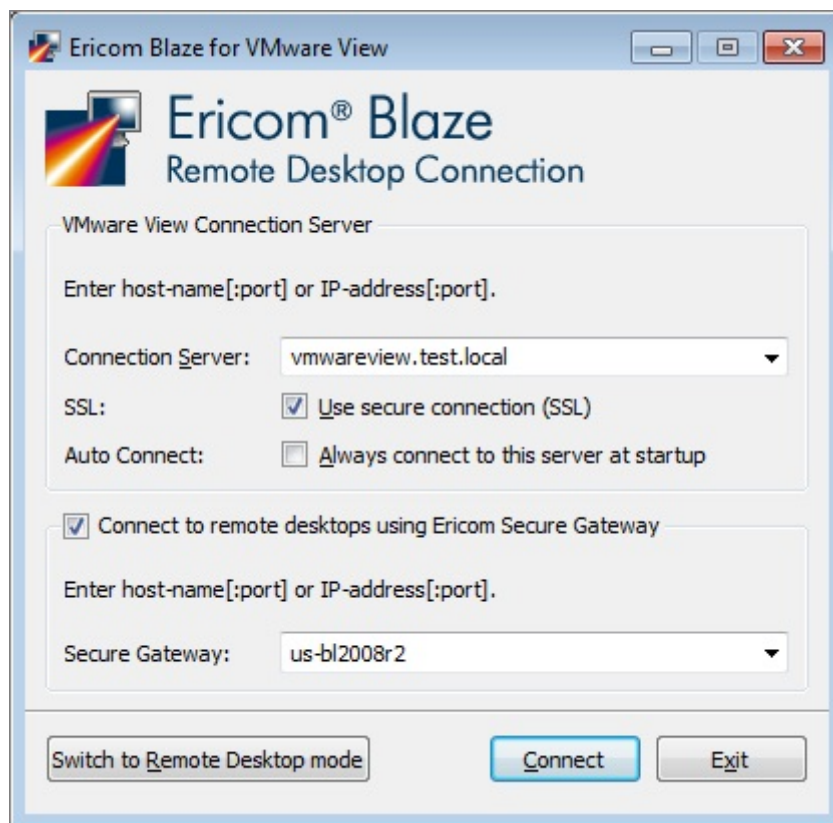
4. 「接続」をクリックします。Secure Gateway を使用して Blaze クライアントをリモート・デスクトップに接続する場合、Blaze 接続パナーの宛先アドレスに「+」がプレフィックスとして表示されます。



## VMware View 接続

Ericom Secure Gateway を使用して、Blaze クライアントを実行中のリモート・システムから VMware View で管理された仮想デスクトップへの接続をセキュリティで保護することができます。このようなシナリオでは、VMware View Security Server の代わりに Ericom Secure Gateway を使用します。VMware View Security Server を削除する必要はなく、標準の VMware View クライアントとの使用向けに保持できます。

Secure Gateway の使用を有効にするには、「Ericom Secure Gateway を使用して接続」チェックボックスをオンにし、リモート接続に使用する Ericom Secure Gateway のアドレスを指定します。ポートが 443 以外の場合 (例: us-bl2008r2:4343)、明示的に指定します。



## ■ フェイルオーバー・ゲートウェイを設定する

複数の Ericom Secure Gateway を、AccessNow Web クライアントと Blaze クライアントにおけるフェイルオーバー・チェーンとして設定することができます。これにより、プライマリのゲートウェイが使用できない場合に自動的に代替ゲートウェイとして使用され、Secure Gateway 機能の冗長性が提供されます。リストの最初の Secure Gateway への接続が失敗すると、リクエストはリストの次のサーバへ自動的にリダイレクトされます。このリストに制限はありません。

Secure Gateway のフェイルオーバー・リストを指定するには、各ゲートウェイのアドレスをセミコロン (「;」) 区切りで入力します。

以下は、サーバのリストのサンプルです:

**Us-bl2008r2;securegateway.ericom.com;192.168.0.3:4343**

プライマリ・ゲートウェイは、ポート 443 を介した「Us-bl2008r2」です。

2 番目の Secure Gateway は、ポート 443 を介した「securegateway.ericom.com」です。

3 番目の Secure Gateway は、ポート 4343 を介した「192.168.0.3」です (443 以外のポート値を使用する場合、明示的に指定する必要があります)。

**注意:**

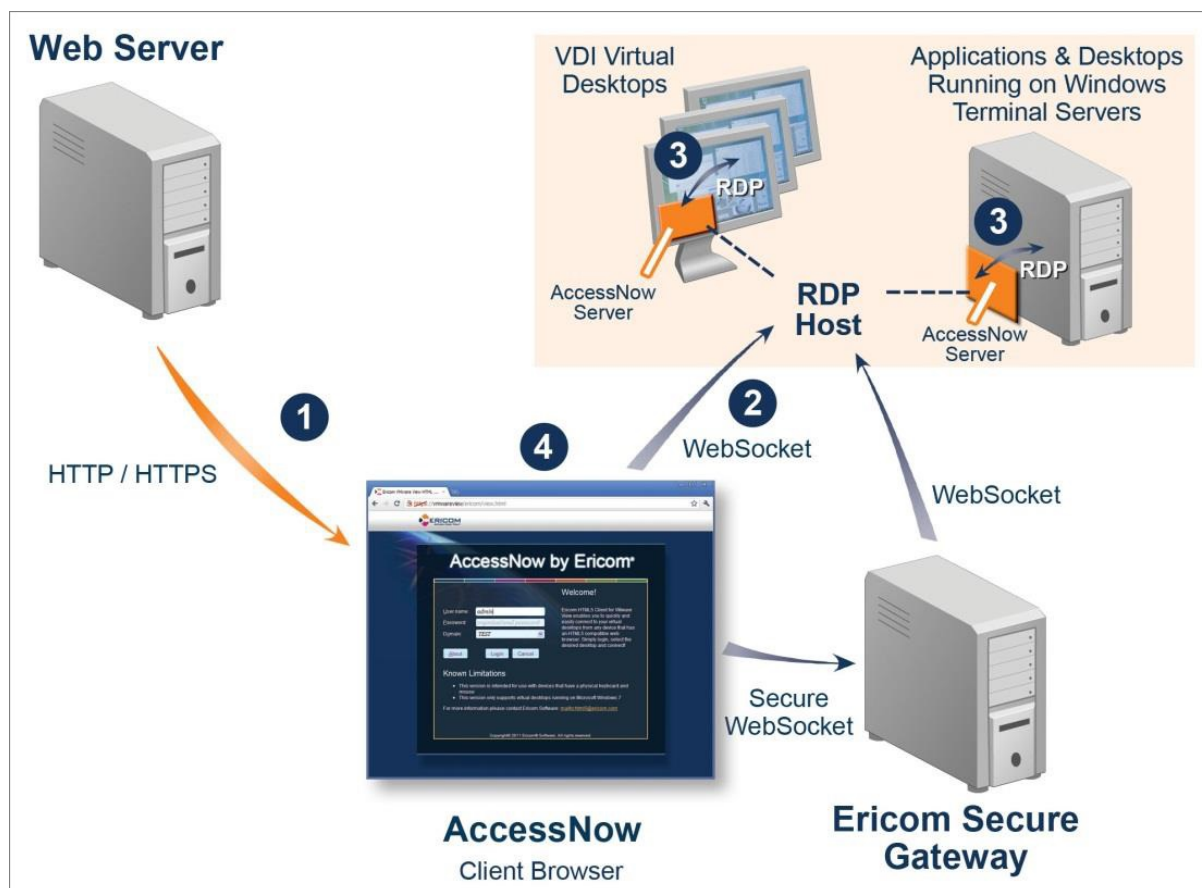
高速なログイン時間を確実に提供するため、リストの上位のサーバの稼働時間を管理してください。

プライマリ・サーバが使用できない場合、エンドユーザのログインにかかる時間が長くなります。

これは、ログイン・プロセスにおいて、フェイルオーバー・サーバへの接続を試行する前にプライマリ・サーバがタイムアウトするのを待つことが必要となるためです。

## 4.2.6 Ericom AccessNow HTML5 クライアントの設定

Ericom Secure Gateway を使用することで、AccessNow クライアントと AccessNow サーバ間のセキュリティで保護された接続を提供することができます。下図は、これらのコンポーネントがどのように連携するかを示しています：



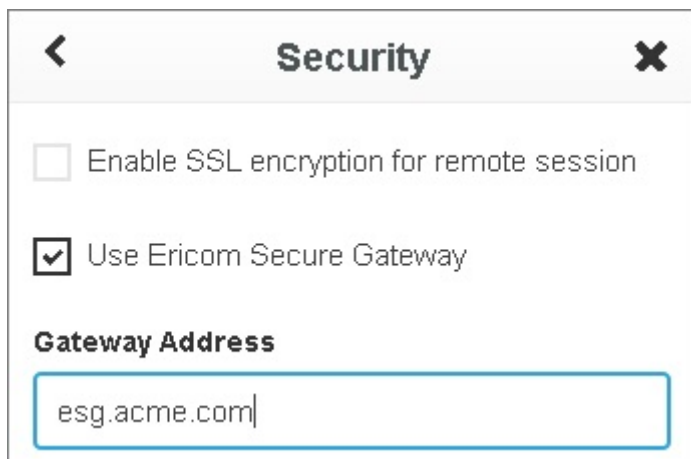
この構成では、Ericom Secure Gateway へのセキュアな WebSocket 接続が AccessNow サーバによって常に確立されます。次にゲートウェイにより AccessNow サーバへの WebSocket 接続が確立されます。

ゲートウェイと AccessNow サーバ間の WebSocket 接続は、AccessNow クライアントの設定に基づいて、セキュリティ保護される場合とされない場合があります (AccessNow Web 設定の Enable SSL を確認してください)。

- Enable SSL encryption for desktop session
- RDP Compression and Acceleration

### 設定

AccessNow での Ericom Secure Gateway の使用を有効にするには、設定 ボタンをクリックします。セキュリティに移動し、Ericom Secure Gateway の使用 チェックボックスをオンにし、ゲートウェイ・アドレスを入力します：



AccessNow スタンドアロンと ESG を使用する場合は、AccessNow サーバ のアドレスは、エンド・ユーザのデバイスからではなく、ESG サーバから認識されるサーバのアドレス (通常は AccessNow サーバの内部アドレス) を入力する必要があります。RDP ホストの値も同様に入力する必要があります。

ESG を使用する場合、常に AccessNow サーバの値を入力することを強くお勧めします。(値を入力しない場合、URL で使用したアドレスの値が使用されることに注意してください)

AccessNow for VMware View での Ericom Secure Gateway の使用を有効にするには、デスクトップのリストの下部にある Ericom Secure Gateway の使用 チェックボックスをオンにし、ゲートウェイ・アドレスを入力します。

## ■ ESG セッション Cookie

ESG によってクライアントのブラウザに AccessNow ページ が配信される際に、セッション Cookie が生成されます。ESG 自体により配信されるページ (Web サーバとして機能する場合) とトンネルして通過するページ (プロキシとして機能する場合) の両方で、セッション Cookie が生成されます。セッション Cookie 名は ESG\_GWID となり、ページが ESG により配信されたものか ESG を通過したものであるかを特定するために使用できます。

The screenshot shows the 'Cookies' tab in a browser's developer tools. A table lists several cookies. The 'ESG\_GWID' cookie is highlighted with a red box. The table has columns for Name, Value, Domain, Path, Expires, Size, and HttpOnly.

Name	Value	D...	...	Expires...	S...	H
EAN_endURL	#	u...	/...	Session	11	
EAN_id		u...	/...	Session	10	
EAN_name		u...	/...	Session	12	
EAN_resolu...	browser	u...	/...	Session	21	
ESG_GWID	9CC86C54-83B1-49EC-B...	u...	/	Session	44	



注意:

これはセッション Cookie であるため、ブラウザを閉じるまで存続します。そのため、ESG と別の Web サーバの両方で同一のアドレスを使用する場合（例：Access Server または IIS を使用する）、ユーザがブラウザを閉じることなくその 2 つをスイッチすると、ESG\_GWID<sub>□</sub> →クッキーは引き続き存在します。これにより、そのページが ESG により配信されていない場合でも、ESG<sub>□</sub> →により配信されたものであるとクライアントを混乱させる可能性があります。

AccessNow クライアントでは、ページが ESG を使用して配信されたものであるかを特定するために、ESG\_GWID Cookie の存在が使用され、それに従い動作が調整されます:

- config.js で ゲートウェイ・アドレス を指定していない場合、URL アドレスが 詳細 ダイアログの ESG アドレスとしてクライアントで表示、使用され、Ericom Secure Gateway の使用 チェックボックスがデフォルトでオンになります。
- UI、config.js または API を介して ゲートウェイ・アドレス を指定せず、Cookie が存在する場合、URL アドレスが ESG アドレスとしてクライアントに使用されます。
- ゲートウェイ・アドレス を指定し、そのゲートウェイ・アドレスが URL アドレスと同一であるが、Cookie が存在しない場合、クライアントによりゲートウェイ・アドレスの設定は無視され、代わりにダイレクト 接続が実行されます。

## AccessNow での セッション Cookie と PowerTerm WebConnect

PowerTerm WebConnect(PTWC) と使用する際、環境変数 SecureGatewayExternalAddress が空で SecureGatewayEnabled アドレスが 1(有効化)である場合、URL アドレスが ESG アドレスとしてクライアントに使用されます。SecureGatewayExternalAddress を定義した場合、そちらが優先されます。

変数名	値
SecureGatewayEnabled	1
SecureGatewayExternalAddress	

このメカニズムを使用して、PTWC の SmartInternal 機能を AccessNow 接続でシミュレートできます (現在、AccessNow では PowerTerm WebConnect の SmartInternal 機能はサポートされていません)。この機能を有効にするには、次を設定します:

- SecureGatewayEnabled を 1 にします。
- SecureGatewayExternalAddress を目的の ESG アドレスとするか、ユーザが URL で指定するアドレスを使用するには空のままにします。
- SmartInternalIsGateway を 0 にするか、空のままにします (デフォルトは 0)。ESG を通過しないすべての AccessNow 接続は、ダイレクト モードで動作するようになります。ESG を通過するすべての AccessNow 接続には、セッション Cookie が存在するため、Gateway モードが使用されるようになります。
- 配信された接続を SmartInternal に設定します。



Requirements	network reconnect, but adds additional load on the WebConnect Server. See the Administrator's Manual for more information.
<b>Connection Types</b>	
Servers	
Owner	
Information	
	Connection Type
	<input type="radio"/> Public      Establish Direct connection between clients and hosts, unless clients request Reconnect. If a client requests Reconnect then Gateway will be used for it.
	<input checked="" type="radio"/> Smart Internal      Use Direct connections for clients that are in the same subnet as the PowerTerm WebConnect server. Otherwise, use Gateway.

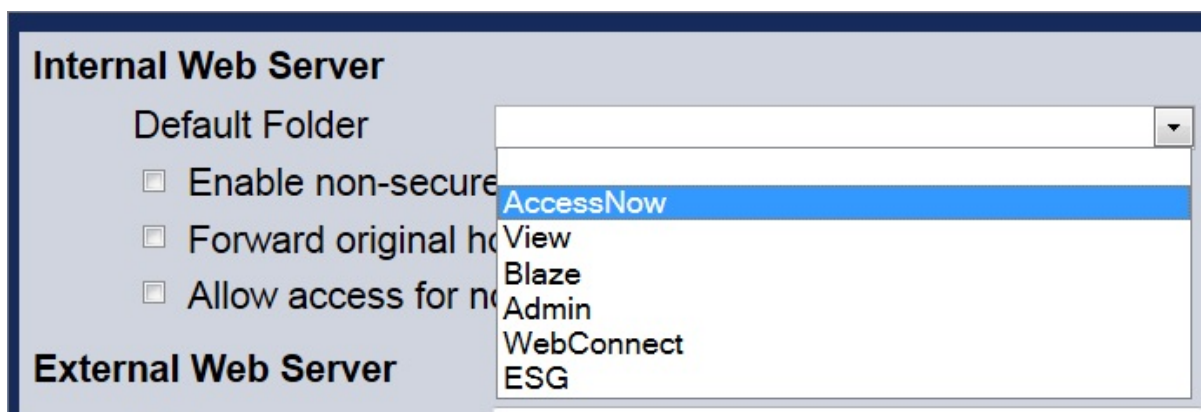
## 4.2.7 ビルトインの Web サーバ

### 内部 Web サーバ

Ericom Secure Gateway には、Web サーバが組み込まれています。この Web サーバを使用して、次の Ericom 製品向けの Web ページをホストできます: Ericom AccessNow、Ericom AccessNow for VMware View および Ericom Blaze。ビルトインの Web サーバは無効にできず、Ericom Secure Gateway のポートが常にリッスンされます。Web サーバを設定するには、Configuration Tool を開き、Web Server に移動します。



ドロップダウン・ボックスをクリックし、ビルトインの Web サーバのデフォルト URL となる必要がある Ericom コンポーネントを選択します。Save をクリックします。ユーザが URL のルート・パスに進んだ場合、選択したコンポーネントが使用されます。



例えば、AccessNow を選択した場合、ユーザが `https://<ESG サーバのアドレス>:<ポート番号>/` に移動すると、URL は自動的に以下のアドレスにリダイレクトされます:

`https://<ESG サーバのアドレス>:<ポート番号>/accessnow/start.html`



注意:

Ericom に関連しないページのホストに ESG を使用できますが、これは公式にサポートされていません。  
ホストする Web ページは、基本的な静的コンテンツとする必要があります。

## 外部 Web サーバ

Ericom Secure Gateway には、Web サーバ・プロキシが組み込まれています。この Web サーバを使用して、Ericom PowerTerm WebConnect の Web ページをプロキシすることができます。ESG をプロキシとして使用するには、PowerTerm WebConnect の Web サーバの Address と Port を入力します。



注意:

Ericom に関連しないページのプロキシとして ESG を使用できますが、これは公式にサポートされていません。  
ESG を介してプロキシする Web ページは、基本的な静的コンテンツとする必要があります。

## Web サーバに接続する

Secure Gateway Web サーバを介して Ericom リソースへ接続するには、ブラウザを開いて目的の URL に移動します。Secure Gateway でポート 443 以外を使用している場合、URL でポートを明示的に指定する必要があります。例:

`https://myserver:4343/accessnow/start.html`

デフォルトで、以下の URL を使用できます。

Ericom Secure Gateway の ウェルカム ページ	https://server:port/ または  https://server:port/welcome.html
Ericom AccessNow	https://server/accessnow/start.html
Ericom AccessNow for VMware View	https://server/view/view.html
Ericom PowerTerm WebConnect (プロキシ・モード)	https://server/webconnect/start.html
Ericom Blaze (Ericom Blaze クライアントのダウンロード)	https://server/blaze/blaze.exe

## ■ HTTP リダイレクト

Ericom Secure Gateway Web サーバは、デフォルトでポート 80 をリッスンします。これにより、サーバへの HTTP 参照は、自動的に HTTPS の URL にリダイレクトされます。例えば、ユーザが `http://server.test.local/view/view.html` を入力した場合、Web サーバによりこのリクエストが受け入れられ、ユーザは自動的に `https://server.test.local/view/view.html` にリダイレクトされます。

この機能は、ポート 443 が Secure Gateway によりリッスンされている場合のみ動作します。他のポートを使用するよう設定されている倍、HTTP 自動リダイレクトはサポートされません。この機能を有効にするには、以下の設定をオンにします:

Enabled non-secured port for HTTPS auto-redirect:

**Enable non-secured port for HTTPS auto-redirect**

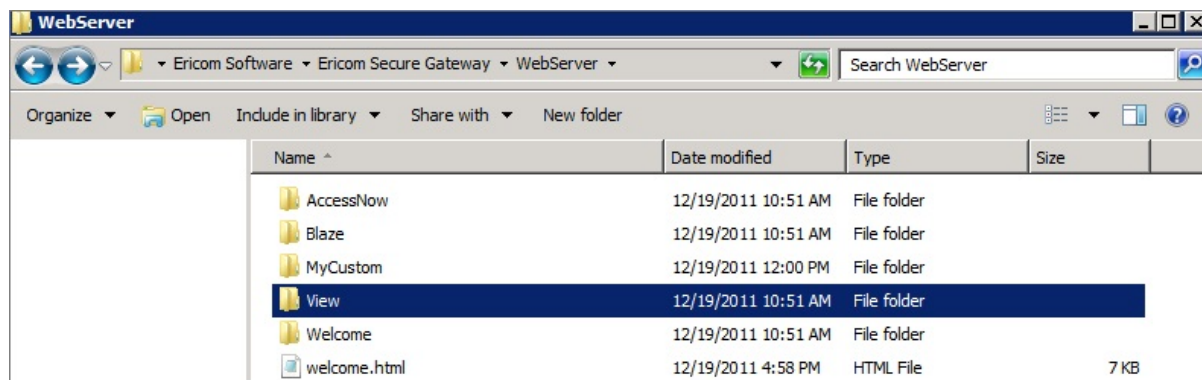
EricomSecureGateway.exe.Config ファイルでこの機能を設定するには、以下を使用します:

```
<add key="EnableNonSecuredPortForHttpsAutoRedirect" value="false" />
```

## 高度な設定

変更を加える前に、バージョン 8.1 以下をご利用の場合は現在の EricomSecureGateway.exe.config ファイルを、バージョン 8.5 以降をご利用の場合は EricomSecureGateway.config ファイルをバックアップしてください。

ビルトイン Web サーバの設定を構成するには、テキスト・エディタを使用して EricomSecureGateway.exe.config (または EricomSecureGateway.config) を開きます。WebServer ディレクトリの各フォルダにはデフォルトのドキュメントが割り当てられている場合があります、エンド・ユーザがアクセスできないよう制限されていることもあります。



例えば、下記の設定を使用すると、以下が構成されます:

- View フォルダをデフォルトのフォルダとして設定する
- view.html を View フォルダのデフォルトのドキュメントとして設定する
- ディレクトリにリストされていないフォルダへのアクセスを制限する
- AccessNow、Blaze および MyCustom フォルダへのアクセスを拒否する

※ 8.1 以下のバージョンをご利用の場合

```
<internalWebServerSettings>
```

```
<Folders default_folder="View" allow_access_for_non_listed_folders="false">
```

```
<add folder_name="AccessNow" default_page="start.html" allow_access="false"/>
```

```
<add folder_name="View" default_page="view.html" allow_access="true"/>
```

```
<add folder_name="Blaze" default_page="blaze.exe" allow_access="false"/>
```

```
<add folder_name="MyCustom" default_page="hello.html" allow_access="false"/>
```

```
</Folders>
```

```
</internalWebServerSettings>
```

※ 8.5 以降のバージョンをご利用の場合

```
<Property name="FolderList" type="list(WebServerFolder)">
  <Value>AccessNow,start.html,False</Value>
  <Value>Blaze,blaze.zip,False</Value>
  <Value>Admin,login.html,True</Value>
  <Value>WebConnect,start.html,True</Value>
  <Value>ESG,,True</Value>
</Property>
```

※ 上記のように、アクセスを制限するものには「False」を設定します。

## ■ リストにないフォルダへのアクセスを防止する

ESG WebServer フォルダに、サブフォルダを追加することができます。追加したサブフォルダは、internal-WebServerSettings リストにない場合でもアクセス可能です。internalWebServerSettings リストで明示的に定義していないフォルダへのアクセスを防止するには、Allow access for non-listed folders のチェックボックスをオフに設定します (または、allow\_access\_for\_non\_listed\_folders="false"を設定します)。

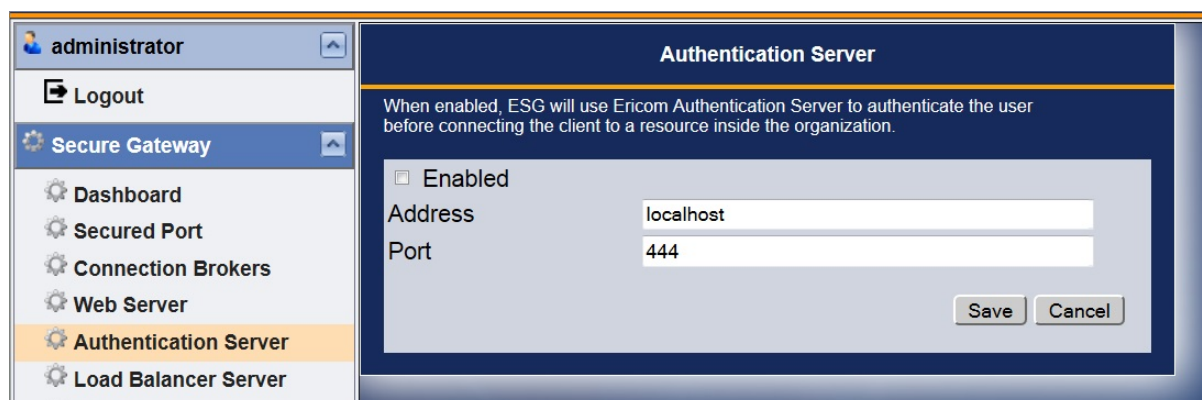
Allow access for non-listed folders

## 4.2.8 ビルトインの 認証サーバ

Ericom Secure Gateway には、認証サーバが備えられています。認証サーバにより、エンド・ユーザが内部リソース (ターミナル・サーバ、AccessNow サーバなど) にコンタクトする前に認証を行うセキュリティ・レイヤーが提供されます。認証サーバは、主にスタンドアロン・クライアントとともに使用され、PowerTerm WebConnect および VMware View コネクション・ブローカーとは使用されません。

認証サーバは、ユーザを認証するドメインのメンバーであるサーバにインストールします (PowerTerm WebConnect ブローカーを使用する場合を除く)。認証サーバは、1 度に 1 つのドメイン用としてのみ設定することができます。

認証サーバの設定を変更するには、Configuration ページを使用します:



設定内容は、ファイル EricomAuthenticationServer.exe.config に保存されています。ユーザが構成可能な設定は <appsettings> セクションにあり、下記の表に定義が記載してあります。

設定	説明
Port	認証サーバによりリスンされるポートの数値です。同じポートがシステム上の他のサービスに使用されていないことを確認してください。ポートの競合は、認証サーバの動作に障害を発生させます。
BindAddress	認証サーバをバインドするアドレス
CertificateThumbprint	認証サーバで使用するSSL証明書の拇印。自己署名証明書がインストールされ、デフォルトで使用されます。
LogStatisticsFreqSeconds	サービスの動作をログに記録する間隔

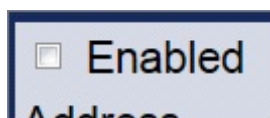


注意:

認証サーバを有効にすると、ドメイン・ユーザのみを認証できます。ローカル・システム・ユーザ（管理者など）は、認証サーバを介してログインできません。

## ■ ブローカーでの認証サーバを無効化する

すべてのアクセスがコネクション・ブローカーを経由し、スタンドアロン・クライアント (Blaze クライアントなど) から接続しない場合、認証サーバを無効にする必要があります。設定ページで Enabled のチェックボックスをオフにし、認証サーバを無効にします。



コネクション・ブローカーだけに使用する認証サーバを設定するには、8.1 以下のバージョンをご利用の場合は EricomSecureGateway.exe.config に以下の変更を適用します:

1. 「AuthenticationServer」 | 「Enabled」を **false** に設定します



```
<externalServersSettings>
  <AuthenticationServer>
    <add key="Enabled" value="false"/>
    <add key="Address" value="192.168.1.100"/>
  </AuthenticationServer>
</externalServersSettings>
```

2. 「Appsettings」 | 「ConnectionBrokerOnlyMode」を **true** に設定します

```
<add key="DrainingMode" value="false" />
<add key="ConnectionBrokerOnlyMode" value="true" />
<add key="LogStatisticsFreqSeconds" value="60" />
```

8.5 以降のバージョンをご利用の場合は、EricomSecuregateway.config に以下の変更を適用します:

1. 「<Section name="AuthenticationServer">」の下記を false に設定します。

```
<Property name="Enabled" type="bool" value="false" />
```

2. 「<Section name="Security">」の下記を true に設定します。

```
<Property name="ConnectionBrokerOnlyMode" type="bool" value="true" />
```

これにより、Secure Gateway を介したスタンドアロン・クライアントからのすべての接続が禁止され、コネクション・ブローカーを介したログインがすべてのユーザに強制されます。

## ■ PowerTerm WebConnect の推奨

ビルトインの認証サーバにより、基本的なセキュリティが提供されます。認証サーバの認証元となるドメインのメンバーである任意のユーザがログイン可能になります。ログインを許可するユーザの管理を強化するには、Ericom PowerTerm WebConnect を使用してください。

## 4.2.9 コネクション・ブローカー

このページを使用して、ESG で使用するコネクション・ブローカーのアドレスとポート設定を入力します。現在、PowerTerm WebConnect と VMware View の 2 つのブローカーがサポートされています。

The screenshot shows the 'Connection Brokers' configuration page in the Ericom Secure Gateway interface. The left sidebar shows the user 'administrator' and a navigation menu with 'Secure Gateway' selected. The main content area has a title 'Connection Brokers' and a note: 'When both address and port are specified, ESG can act as a proxy to the Connection Broker. In such setup, the Connection Broker server can reside behind the firewall.' Below this, there are two sections: 'WebConnect Server' and 'VMware View Server'. The WebConnect Server section has 'Address' set to 'localhost' and 'Port' set to '4000'. The VMware View Server section has 'Address' set to '192.168.35.205' and 'Port' set to '443', with a checked 'SSL' checkbox. At the bottom, there is an unchecked checkbox labeled 'Only allow connections from a connection broker. Deny connections from standalone clients.' and 'Save' and 'Cancel' buttons.

コネクション・ブローカーを介した接続のみを許可するには、Deny connections from Standalone clients を選択します。スタンドアロンの Blaze および AccessNow クライアントを介した接続試行は拒否され、管理されたブローカーを介した認証がすべてのユーザに必要とされます。

PowerTerm WebConnect または VMware View サーバのアドレスは、ESG サーバから到達可能なアドレスに設定する必要があります。ping と telnet コーティリティを使用し、ESG とコネクション・ブローカー・サーバの接続を確認してください。

## PowerTerm WebConnect 6.0 の設定

PowerTerm WebConnect 6.0 クライアント・コンポーネントは、Ericom Secure Gateway に対応しています。通常 Secure Gateway は DMZ 上にインストールされ、PowerTerm WebConnect に関連するすべての通信の単一ポート・プロキシとして機能します。これは、外部ファイアウォール上で 1 つのポートのみ開放する必要があることを意味します。Secure Gateway により、関連するすべての通信がそのポートを介して安全にトンネルされます: PowerTerm WebConnect (4000)、RDP (3389)、Blaze (3399)、AccessNow (8080)、HTTP (80)、HTTPS (443)、エミュレーション (80)、SSH (22) など。

Secure Gateway での PowerTerm WebConnect の使用を設定するには、以下の 2 つの手順を実行します:

1. Secure Gateway を有効化するために、PowerTerm WebConnect の管理コンソールで 3 つの環境変数を設定します。
2. (オプション) PowerTerm WebConnect アドレス用に外部から Secure Gateway をポイントするために使用する、Secure Gateway 「sg」固有の Application Zone、Application Portal および AccessToGo クライアントを設定します。Secure Gateway はブローカー・サーバのプロキシとして機能します。

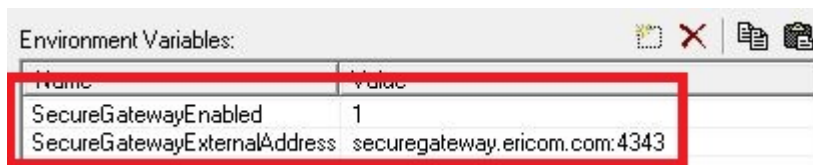
3. (オプション) ブローカーを介した接続と介さない接続 (Blaze クライアントなど) の両方に Secure Gateway を使用する場合、スタンドアロン・クライアント向けのセキュリティを確保するために認証サーバが必要になります。

#### ブローカーの 3 つの ESG 変数を設定する

PowerTerm WebConnect Administration Tool を開き、Server | Configuration に移動します。環境変数の一覧をスクロール・ダウンし、Secure Gateway に関連する設定に移動します:

SecureGatewayEnabled	1 - 有効 0 - 無効 (ゲートウェイ・モードを指定した場合、ブローカーに組み込まれている代替サービス・ゲートウェイが使用されます)
SecureGatewayExternalAddress	Ericom クライアントから到達可能となる Secure Gateway サーバのアドレスとポートこのアドレスとポートは、ESG を介して接続するエンド・ユーザから到達可能なものとする必要があります。
SmartInternalIsGateway	AccessNow と AccessToGo では、SmartInternal の自動検出がサポートされていません。 SmartInternal の初期設定では、これらのクライアントに対してデフォルトで自動的にダイレクトが使用されます。すべての SmartInternal 接続にゲートウェイの使用を強制するには、この値を 1 に設定します。

以下の例では、すべての Ericom クライアントは次のアドレスで Secure Gateway に接続します: securegateway.ericom.com (ポート 4343 経由)



注意:

Secure Gateway で信頼されて証明書を使用している場合、IP アドレスではなく、SecureGateway の DNS アドレスを入力してください。信頼された証明書からアドレスのドメイン名が認識可能である必要があります。

SmartInternalIsGateway を 1 に設定した場合、接続のゲートウェイ設定を SmartInternal に設定すると、すべての Access コンポーネント (AccessNow、AccessPad および AccessToGo) によりゲートウェイ・モードが使用されます。



注意:

現在、Access コンポーネントでは SmartInternal 機能がサポートされていません (今後のリリースで利用可能となります)。

クライアント・ファイルを設定する

WebConnect をデフォルトの ESG Web サーバ・フォルダとして設定した場合、デフォルトのページにより sgstart.html が指されます。



この設定は、8.1 以下のバージョンをご利用の場合は EricomSecureGateway.exe.config ファイルの folder\_name="WebConnect" で変更することができます:

```
<add folder_name="WebConnect" default_page="sgstart.html" allow_access="true" />
```

8.5 以降のバージョンをご利用の場合は、EricomSecureGateway.config ファイルの下記 value で変更することができます:

```
<Property name="DefaultFolder" type="string" value="WebConnect" />
```

PowerTerm WebConnect ブローカー上の Application Zone と Web ポータル・ページのファイルの「sg」バージョンでは、PowerTerm WebConnect 用の Secure Gateway をポイントするように設定することが必要になる場合があります。



注意:

アドレス内部と外部のユーザ向けに同一アドレス (例: sg.acme.com) を使用する場合、sg.  
 ↳acme.com 用の  
 外部 DNS により Secure Gateway の外部 IP/アドレス (例: ポート 443 を転送するファイ  
 アウォールのアドレス) が  
 参照され、内部 DNS により Secure Gateway の内部 IP/アドレスが参照されることを確認し  
 てください。

### オプションの「/websocket」パラメータ

Secure Gateway でポート 443 を使用する場合、一部のトラフィックがファイアウォールによりフィルタされる可能性があります。接続の問題を防ぐためには、Secure Gateway を経由するすべての TCP トラフィックを許可するよう外部向けファイアウォールを設定します。

HTTP/HTTPS フィルタリングを無効化できないファイアウォールでは、パラメータ /websocket を追加し、Websocket を使用するよう PowerTerm WebConnect を設定します。

### Application Zone の設定

デフォルトでは、URL のアドレスとポートが sgapplicationzone.html に使用されます。ほとんどの場合、このページをカスタマイズする必要はありません。ただし、ハードコートした値を「server:」と「port」の変数に設定することができます。

この例では、PowerTerm WebConnect サービスに接続するために、sgapplicationzone.html により 外部 Secure Gateway アドレスがポート 4545 上で指されています (securegateway.ericom.com:4545)。

```

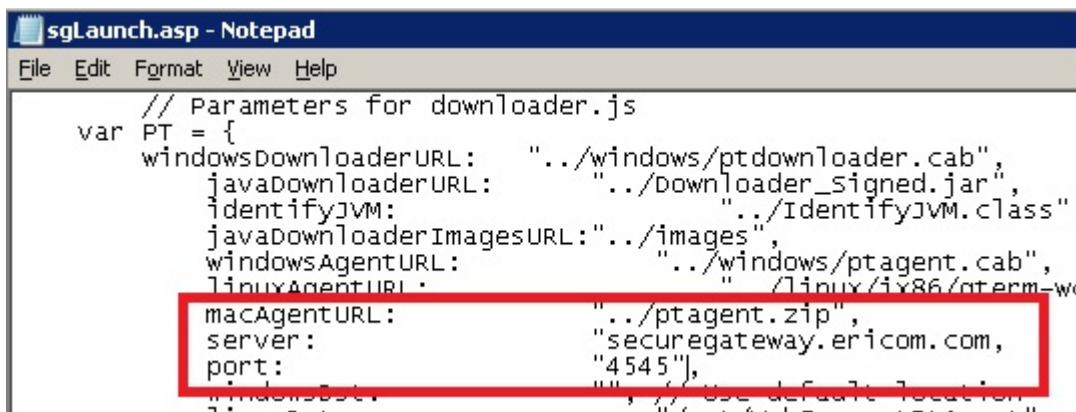
sgApplicationZone.html - Notepad
File Edit Format View Help
identifyJVM: "IdentifyJVM.class",
javaDownloaderImagesURL: "images",
windowsAgentURL: "./windows/ptagent.cab",
linuxAgentURL: "./linux/ix86/qterm-wc.zip",
macAgentURL: "/ptagent.zip"
server: "securegateway.ericom.com",
port: "4545",
windowsDist. // use default location
  
```

Websocket モードを有効にするには、パラメータ /websocket を追加します。

```
+ " /websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

### Web ポータル - sgLaunch.asp の設定

デフォルトでは、URL のアドレスとポートが sgLaunch.asp に使用されます。ほとんどの場合、このページをカスタマイズする必要はありません。sgapplicationzone.html と同様に、ハードコートした値を「server:」と「port」の変数に設定することができます。



```

sgLaunch.asp - Notepad
File Edit Format View Help
// Parameters for downloader.js
var PT = {
  windowsDownloaderURL:  "../windows/ptdownloader.cab",
  javaDownloaderURL:    "../Downloader_Signed.jar",
  identifyJVM:          "../IdentifyJVM.class",
  javaDownloaderImagesURL:"../images",
  windowsAgentURL:     "../windows/ptagent.cab",
  linuxAgentURL:       "../linux/ix86/pterm-wc",
  macAgentURL:         "../ptagent.zip",
  server:               "securegateway.ericom.com",
  port:                 "4545",
  windowsExt:           "", // Use default location
  linuxExt:             "" // Use default location
}

```

Websocket モードを有効にするには、パラメータ /websocket を追加します。

```

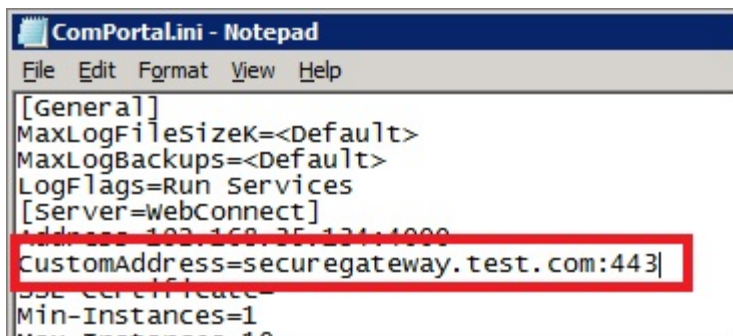
+ " /websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";

```

### Web ポータル Comportal.INI の設定

PowerTerm WebConnect サーバと IIS を別々のマシンで実行中の場合、Secure Gateway のアドレスとポートをポイントするよう ComPortal.INI を設定します。この設定では、Launch.asp または sgLaunch.asp ファイルを変更する必要はありません。

以下の例では、PowerTerm WebConnect サービスにアクセスするために、Secure Gateway をポイントするよう Comportal.INI を設定しています。



```

ComPortal.ini - Notepad
File Edit Format View Help
[General]
MaxLogFileSizeK=<Default>
MaxLogBackups=<Default>
LogFlags=Run Services
[Server=webConnect]
Address=192.168.25.134:1000
CustomAddress=securegateway.test.com:443]
UseCertificate=
Min-Instances=1
Max-Instances=10

```

Websocket モードを有効にするには、Launch.asp または sgLaunch.asp ファイルにパラメータ /websocket を追加します:

```

+ " /websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";

```

### AccessToGo クライアントの設定

Secure Gateway を使用したりリモート・アクセス用に PowerTerm WebConnect を設定すると、AccessToGo の接続が可能になります。AccessToGo を使用して PowerTerm WebConnect に接続するには、以下の手順を実行します:

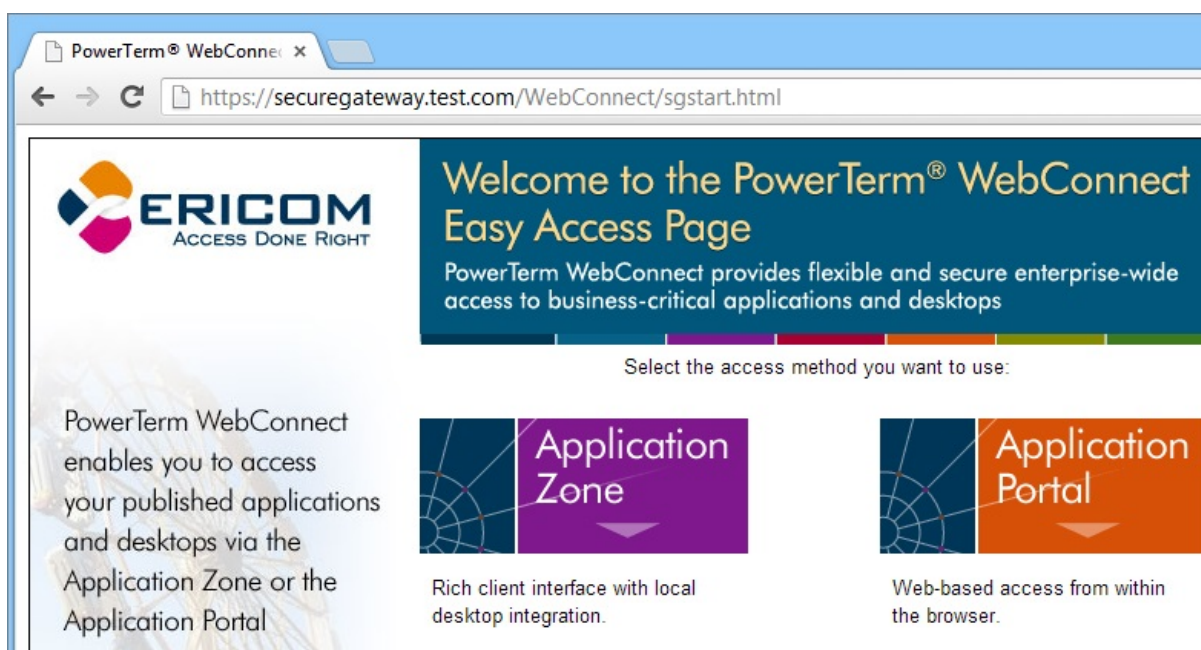
1. AccessToGo アプリをダウンロードします
2. 新しい PowerTerm WebConnect 接続を作成します
3. サーバの項目にサーバのアドレスとポートを入力します (例: securegateway.test.com:443)
4. OK をクリックし、接続 をタップして起動します

### Secure Gateway を使用して接続する

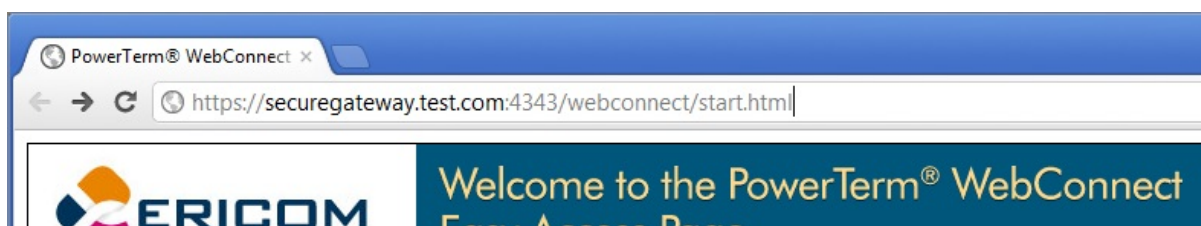
PowerTerm WebConnect 用に適切に Secure Gateway を設定すると、Secure Gateway の URL にユーザがダイレクトされます。ユーザは <https://securegateway.test.com>(または http) を入力します:



ページは自動的に次にリダイレクトされます: <https://securegateway.test.com/WebConnect/sgstart.html>



Secure Gateway は Web サーバへのプロキシとして機能するため、すべてのサブフォルダとファイル名はそのままになります (例: /webconnect/sgstart.html) ポート 443 以外を Secure Gateway として使用する場合、URL で明示的に指定する必要があります (例: 「:4343」)







注意:

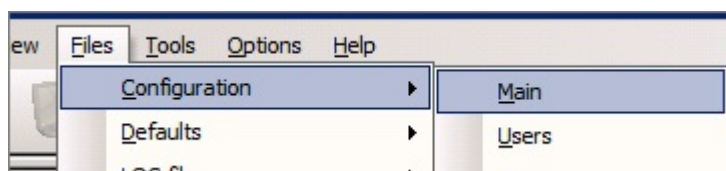
接続ユーザが Secure Gateway を使用して PowerTerm WebConnect に接続する際、すべての SmartInternal 接続で自動的に ゲートウェイ モードが使用されます。ダイレクト接続は影響を受けません。

## 認証サーバの設定

PowerTerm WebConnect を単独で使用する場合、認証サーバは必要ありません。これを設定するには、セクション「ブローカーでの認証サーバを無効化する」を参照してください。

ただし、その環境でスタンドアロン・クライアントも使用する場合、同一サーバ上で PowerTerm WebConnect と Secure Gateway を動作させる必要があります。特定の認証サーバを使用するよう PowerTerm WebConnect を設定するには、以下の手順を実行します:

1. PowerTerm WebConnect の管理ツールに移動します
2. Files | Configuration | Main



3. ファイルの末尾に移動し、「Authentication Server」のセクションを探します以前のバージョンの ptserver.ini ファイルをインポートした場合、このセクションは存在しない場合があります、その場合はセクションを作成する必要があります。
4. 認証サーバを実行する場所のアドレスを設定します以下の例では、認証サーバは 192.168.0.2 上で実行されています

```
[Authentication Server]
```

```
Address= 192.168.0.2
```

```
Port= 444
```

```
CertificateDnsIdentity=
```

```
MaxClockSkewMinutes=180
```

5. Secure Gateway の設定ファイル (EricomSecureGateway.exe.config) において、<externalServersSettings> | AuthenticationServer に移動し、手順 4 で設定した値と同じになるよう Address の値を設定します

```
<externalServersSettings>
```

```
<AuthenticationServer>
  <add key="Address" value="192.168.0.2"/>
  <add key="Port" value="444"/>
```

## ESG の手動設定

設定 GUI を使用した方法に加え、バージョン 8.1 以下をご利用の場合は EricomSecureGateway.exe.config ファイルを手動で編集することで、インストール・プロセス中に構成した設定を変更することができます。以下は、アドレス 192.168.35.134 の PowerTerm WebConnect(PTWC) サーバと動作するように Secure Gateway を設定するサンプルです:

```
<WebConnectServer>
  <add key="Address" value="192.168.1.134"/>
  <add key="Port" value="4000"/>
</WebConnectServer>
<WebServer>
  <add key="Address" value="192.168.1.134"/>
  <add key="Port" value="80"/>
  <add key="SecuredConnection" value="false"/>
</WebServer>
```

バージョン 8.5 以降をご利用の場合は、EricomSecureGateway.config ファイルの以下の設定を変更することで設定可能です。

```
<Section name="WebConnectServer">
  <Property name="Address" type="string" value="192.168.1.134" />
  <Property name="Port" type="int" value="4000" />
</Section>
<Section name="ExternalWebServer">
  <Property name="UrlServicePointsFilter" type="UrlServicePointsFilter"
value="&lt;UrlServicePointsFilter /&gt;" />
  <Property name="UrlDefaultServicePoints" type="list(string)">
    <Value>http://192.168.1.134:80/</Value>
  </Property>
```

</Section>

## 4.2.10 高度な設定

Secure Gateway に関連する変更可能なすべての設定は、EricomSecureGateway.config ファイルにあります。このファイルは、テキスト・エディタで開くことができるテキスト・ファイルです。変更後、反映にはサービス再起動が必要です。

### ホワイトリスト・セキュリティ

ホワイトリスト機能が Ericom Secure Gateway 7.6.1 で追加されました。

次の 3 つのタイプのホワイトリストを設定可能です: エンド・ユーザのアドレスと範囲、リレー・サーバのアドレスと範囲、およびターゲット・ホストのアドレスと範囲。リレー・サーバは、エンド・ユーザとターゲット・ホスト (例: Ericom AccessServer) 間の通信を中継する Ericom のコンポーネントです。IPv4 アドレスと IPv6 アドレスがサポートされています。

すべてのホワイトリストは、デフォルトでは無効化されています。1 つのタイプのホワイトリストを有効化するには、有効化の設定を「false」から「true」に変更します。

例:

```
<add key="ClientWhitelistByIPAddressesEnabled" value="false" />
<add key="ClientWhitelistByIPAddressesEnabled" value="true" />
```

アドレスは、標準的なフォーマット (例: 192.168.1.1) で入力し、セミコロン (;) で区切ります。

アドレスの範囲は、低い方の IP、文字「-」、および高い方の IP を使用します。例: 192.168.1.1-192.168.255.255

すべての設定オプションの一覧は以下のとおりです:

```
<Visitor>
  <add key="HandshakeTimeoutSeconds" value="60" />
  <add key="ClientWhitelistByIPAddressesEnabled" value="false" />
  <add key="ClientWhitelistAllowedIPv4Addresses" value="" />
  <add key="ClientWhitelistAllowedIPv6Addresses" value="" />
  <add key="RelayServerWhitelistByIPAddressesEnabled" value="false" />
  <add key="RelayServerWhitelistAllowedIPv4Addresses" value="" />
  <add key="RelayServerWhitelistAllowedIPv6Addresses" value="" />
  <add key="TargetHostRestrictedToRelayServerIPEnabled" value="false" />
  <add key="TargetHostWhitelistByIPAddressesEnabled" value="false" />
  <add key="TargetHostWhitelistAllowedIPv4Addresses" value="" />
  <add key="TargetHostWhitelistAllowedIPv6Addresses" value="" />
</Visitor>
<Admin>
```

```

<add key="InactivityTimeoutMinutes" value="5" />
<add key="WhitelistByIPAddressesEnabled" value="true" />
<add key="WhitelistAllowedIPv4Addresses" value="" />
<add key="WhitelistAllowedIPv6Addresses" value="" />
</Admin>

```



注意:

「ClientWhitelistByIPAddressesEnabled」と管理ホワイトリスト設定は、以前のバージョンでは「LockdownAllowed\*\*\*\*」アドレスとして存在していました。現在これらの設定を構成している場合、新しい値にパラメータをコピーしてください。

## ■ HTTP/HTTPS 通信をブロックする

AccessNow の通信に Websocket のみを使用するよう Ericom Secure Gateway に強制するために、HTTP/HTTPS を無効にすることができます。設定ファイルで<Section name="Http">設定に移動し、最初のキー「Enabled」を「false」から「true」に設定します。

```

<Section name="Http">
  <Property name="Enabled" type="bool" value="false" />
  <Property name="ClientPullDataTimeoutSeconds" type="int" value="30" />
  <Property name="ServerPushDataTimeoutSeconds" type="int" value="10" />
</Section>

```

## ■ セッション Cookie タイムアウトの設定

バージョン 7.6.1 では、Websocket が確立された際の最初のアップグレード・コールを保護するために、クライアント・セッション Cookie が追加されました。また、アップグレード・リクエストと一緒にトークンも送信されます (このアプローチは、XSRF 攻撃から保護するために設計されています)。この Cookie は、ESG\_CSID として識別され、設定可能な時間の間有効となります。

Cookie のタイムアウトは、以下のようにファイルで設定します:

```

<add key="ClientSessionCookieTimeoutMinutes" value="0" />

```

ユーザが接続を試行し ((Websocket や HTTPS が有効化されている場合、それらを介して)、Cookie の有効期限が切れている場合、接続が拒否され、ユーザはページをリロードしてログインを再試行する必要があります。

Cookie のタイムアウト時間は、同一デバイスでそのページを開いたすべてのアクティブなブラウザで認識されます。例えば、ユーザが Firefox を使用してページを開き、それを閉じ、そのページを Chrome で開いた場合、タイムアウト時間のカウントダウンは、Firefox で残されていた時間から再開します。

セッション Cookie のリースの詳細な流れは以下のとおりです：

- 最初にエンド・ユーザのブラウザがページをリクエストした際、ESG に Cookie がキャッシュされます
- Cookie のリース期間は、「ClientSessionCookieTimeoutMinutes」に基づいて定義されます
- リースはブラウザではなく、ESG(サーバ)側で維持されます。そのため、すべてのブラウザはエンド・ユーザのデバイスからの 1 つのブラウザとして扱われます。
- Cookie の値とリースは、クライアント (IP アドレス) ごとです。そのため、同じユーザ・デバイスの複数のブラウザからは、同一の Cookie とリースが使用されます。
- Cookie のリース期間は、ページが取得されるたびに延長されません。設定された時間後にのみ期限切れになります。
- ユーザは、それぞれの期限切れの後にページをリロードして ESG にコンタクトすることが必要になります。

## ■ 同一生成元の検証 (AccessNow のみ)



注意：

この機能は、AccessNow のみで使用されます。同時に他の Ericom クライアント (例: [Blaze](#) クライアント) を使用している場合、この機能を有効化しないでください。

バージョン 7.6.1 では、信頼できる発信元とホスト・アドレスを設定するための 2 つのホワイトリスト・パラメータが追加されました。ホワイトリストを設定するには、設定ファイルを開き、「sessions Settings | ビジター」の次の場所に移動します：

- OriginHttpHeaderWhitelistAddresses
- HostHttpHeaderWhitelistAddresses

Websocket のアップグレード・メッセージ上に「OriginHttpHeaderWhitelistAddresses」が設定されているかが ESG によりチェックされます。「発信元」HTTP ヘッダがメッセージに存在する場合、それが信頼できるアドレスのリストにあることが確認されます。そうでなければ、「参照元」HTTP ヘッダがメッセージに存在するかがチェックされます。存在する場合、それが信頼できるアドレスのリストにあることが確認されます。一致するものが存在しない場合、Websocket のアップグレード・リクエストは ESG により拒否されます。

次に、「HostHttpHeaderWhitelistAddresses」が設定されているかが ESG によりチェックされます。「ホスト」HTTP ヘッダがメッセージに存在する場合、それが信頼できるアドレスのリストにあることが確認されます。一致するものが存在しない場合、WebSocket のアップグレード・リクエストは ESG により拒否されます。

両方のテストを通過した場合、ESG により接続が受け入れられます。

## ■ HTTP セキュリティヘッダーを設定する

HTTP セキュリティヘッダーは、EricomSecureGateway.Config file で設定されています。

※ 8.5 以降のバージョンをご利用の場合は、EricomSecureGateway.config で設定されています。

X-Frame-Options の値を設定するには、次を編集します: `<Property name="XFrameOptions" type="string" value="" />`

コンテンツセキュリティポリシーの値 (すなわち、X-Content-Type-Options: nosniff) を設定するには、次を編集します:

`<Property name="ContentSecurityPolicy" type="string" value="" />`

Access Control Allow Origin の値を設定するには、次を編集します: `<Property`

`name="AccessControlAllowOrigin" type="string" value="*" />`


## ■ 高可用性

Secure Gateway レイヤーに高可用性を備えるには、2 つ以上の Secure Gateway をインストールし、それらへのアクセスを管理するサードパーティの冗長なロード・バランサを使用してください。


ロード・バランサにより、エンド・ユーザの接続向け 1 つのアドレスが提供されます。リクエストがロード・バランサに到着すると、ビルトインの重み付け基準に基づいて利用可能な Secure Gateway にリクエストがリダイレクトされます。基本的なラウンド・ロビン式ロード・バランサも使用できますが、Secure Gateway がアクティブであるかが検出されない場合があります。

## ■ Qualys A グレードのための設定

Windows 2012R2 サーバにインストールされたバージョン 7.5 以降の Ericom Secure Gateway は、Qualys ( <https://www.ssllabs.com/ssltest/> ) の A グレードを達成します (2017 年 8 月時点で確認済み)。信頼された証明書と Nartac の無償 IIS Crypto ツール ( <https://www.nartac.com/Products/IISCrypto> ) も必要となります。ESG をインストールした後、自己署名証明書よりも優先して信頼された証明書を使用するように設定します。ワイルドカード証明書の使用は、低い Qualys グレードをもたらす可能性があることに注意してください。次に、以下のように IIS Crypto を使用して RC4 暗号および Diffie-Helman 鍵共有を無効化します



IIS Crypto 2.0



---

Schannel

Cipher Suites

Templates

Site Scanner

**Schannel**

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

Protocols	Ciphers	Hashes	Key Exchanges
<input checked="" type="checkbox"/> Multi-Protocol Unified Hello	<input checked="" type="checkbox"/> NULL	<input checked="" type="checkbox"/> MD5	<input type="checkbox"/> Diffie-Hellman
<input checked="" type="checkbox"/> PCT 1.0	<input checked="" type="checkbox"/> DES 56/56	<input checked="" type="checkbox"/> SHA	<input checked="" type="checkbox"/> PKCS
<input checked="" type="checkbox"/> SSL 2.0	<input checked="" type="checkbox"/> RC2 40/128	<input checked="" type="checkbox"/> SHA 256	<input checked="" type="checkbox"/> ECDH
<input checked="" type="checkbox"/> SSL 3.0	<input checked="" type="checkbox"/> RC2 56/128	<input checked="" type="checkbox"/> SHA 384	
<input checked="" type="checkbox"/> TLS 1.0	<input checked="" type="checkbox"/> RC2 128/128	<input checked="" type="checkbox"/> SHA 512	
<input checked="" type="checkbox"/> TLS 1.1	<input type="checkbox"/> RC4 40/128		
<input checked="" type="checkbox"/> TLS 1.2	<input type="checkbox"/> RC4 56/128		
	<input type="checkbox"/> RC4 64/128		
	<input type="checkbox"/> RC4 128/128		
	<input checked="" type="checkbox"/> Triple DES 168		
	<input checked="" type="checkbox"/> AES 128/128		
	<input checked="" type="checkbox"/> AES 256/256		

Set Client Side Protocols

RC4 と Diffie-Helman 鍵共有を必要とするサーバ上のその他のアプリケーションが影響を受けることに注意してください。ベストプラクティスとして、最高のパフォーマンスと安定性のために Ericom Secure Gateway はサーバ上の主要なアプリケーションである必要があります。

IIS Crypto の変更後にサーバを再起動し、Qualys の Web サイトで ESG の URL をテストします。「A」グレードの結果となるはずですが。

**SSL Report:** [REDACTED]

Assessed on: Tue, 08 Aug 2017 19:04:48 UTC | HIDDEN | [Clear cache](#) [Scan Another »](#)

**Summary**

Overall Rating

A

Certificate	<div style="width: 100%; height: 10px; background-color: green;"></div>
Protocol Support	<div style="width: 95%; height: 10px; background-color: green;"></div>
Key Exchange	<div style="width: 90%; height: 10px; background-color: green;"></div>
Cipher Strength	<div style="width: 90%; height: 10px; background-color: green;"></div>

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

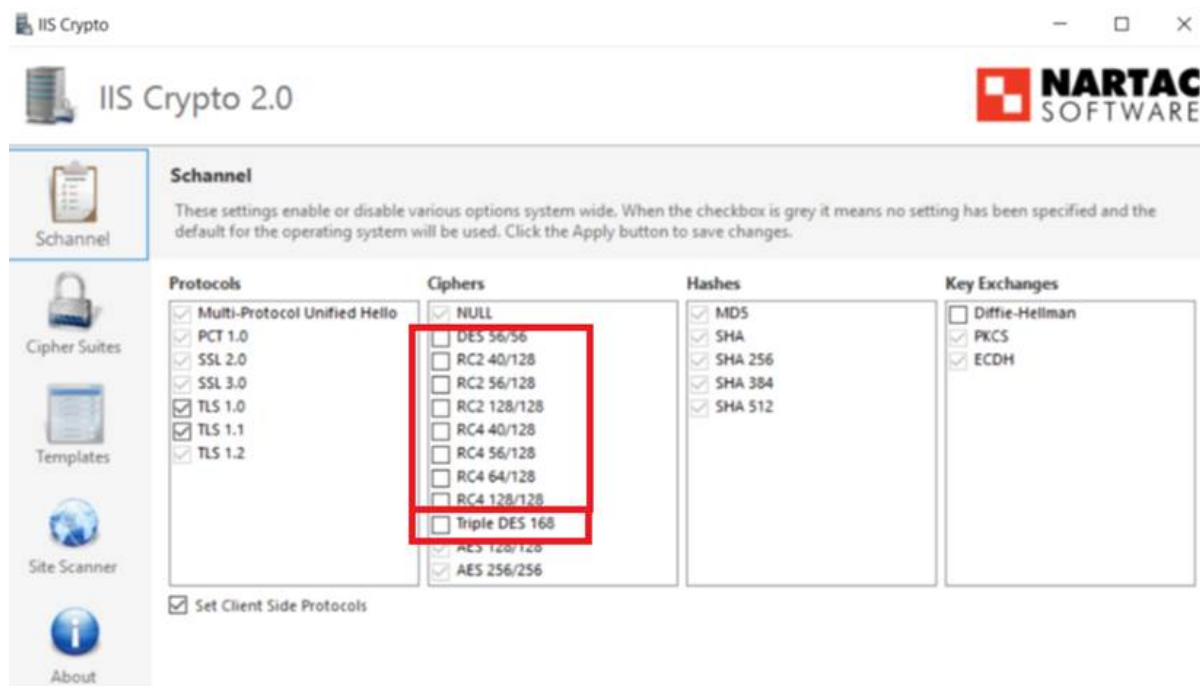
## ■ SWEET32 に対する保護

Ericom Secure Gateway は、SWEET32 へのセキュリティ保護対策が施されたオペレーティング・システムに対応しています。SWEET32 に対する保護の基本的なステップは、トリプル DES を無効化することです。これは Nartac の IISCrypto を使用して実行できます。システムを用意にロールバックできるよう、変更を適用する前にシステムのバックアップやスナップショットの作成を忘れないでください。



## ■ SSL Medium Strength Cipher Suites Supported に対する保護

Ericom Secure Gateway は、「SSL Medium Strength Cipher Suites Supported」へのセキュリティ保護対策が施されたオペレーティング・システムに対応しています。この脆弱性に対する保護の基本的なステップは、すべての下位ビット暗号 (RC2 および RC4) を無効化することです。これは Nartac の IISCrypto を使用して実行できます。例えば、Nartac の IISCrypto を使用して、以下を設定した後にオペレーティング・システムを再起動します。



また、上記の画像は、トリプル DES を無効化することによる SWEET32 の対策も示しています。システムを用意にロールバックできるように、変更を適用する前にシステムのバックアップやスナップショットの作成を忘れないでください。

## ■ PTWC での DMZ の設定

デフォルトでは、インターネット経由で ESG を介して接続するユーザは、ESG のアドレスを使用していると PowerTerm WebConnect サーバにより識別されます。DMP IP レンジを SmartInternalIpRanges 変数で設定している場合、これは SmartInternal の動作を妨げる場合があります。

例:

- ESG: 10.75.4.1
- PTWC: 10.75.1.1
- End User: 10.10.50.50

PTWC の SmartInternalIpRanges に「10.10」を追加した場合、ユーザは PTWC によって「10.10.50.50」ではなく「10.75.4.1」(ESG アドレス)として認識されます。そのため、ユーザの接続はダイレクト・モードではなく、引き続きゲートウェイ・モードとなります。PTWC に適切にエンド・ユーザの IP アドレスを認識させるには、index.asp と applicationzone.html の PRAM リストにパラメータ /websocket を追加します。

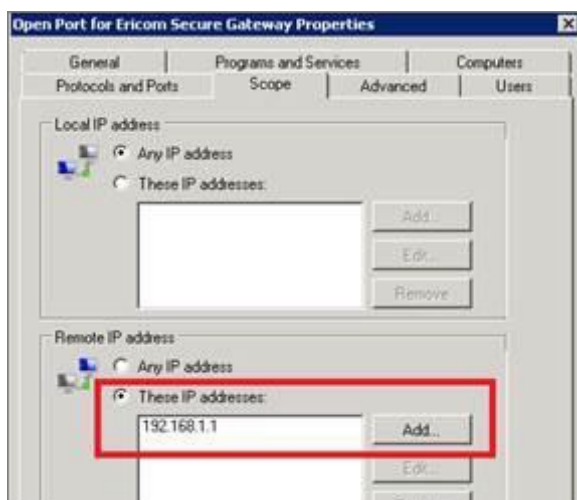


注意:

AccessToGo、AccessPad、および AccessNow では、SmartInternal 機能は完全にはサポートされていません。これらのクライアントでは、SmartInternalIsGateway 変数を使用してゲートウェイの動作を管理する必要があります。

## ESG とのアクセスを制限する

ESG とターミナル・サーバへの着信接続を制限するには、Windows ファイアウォールの スコープ の規則を使用します。ESG への着信接続を制限するには、Ericom Secure Gateway 用のポート規則に移動します。スコープ タブをクリックし、ESG へのアクセスを持たせるシステムまたはアプライアンスのアドレスを入力します。以下の例では、「192.168.1.1」からの接続のみが ESG ポートを介して接続できます。



ターミナル・サーバ上の着信接続を ESG のみに制限するには、目的のポートに同様のスコープの規則を設定します:

- 3389: 標準の RDP ポート
- 8080: AccessNow/Blaze のポート

## ログ・ファイルのサイズを変更する

デフォルトのログ・ファイルのサイズは 32 MB です。この上限に達した場合、新しいファイルが生成されます。この値を変更するには、.config ファイルを編集し、logSettings セクションの LogSizeMB の設定を変更します。目的のサイズ (MB 単位) に値を変更し、新しい値が反映されるようサービスを再起動します。サービスを再起動するごとに、新しいログ・ファイルが生成されます。

## SSO フォームの POST

POST がサポートされているサードパーティの認証エンティティ (SSL VPN など) を使用する場合、ユーザは認証済みの資格情報を使用して AccessNow セッションにシングル・サインオンすることができます。この機能には、ESG が必要です。


認証エンティティに、POST URL を入力するフィールドがあります。目的の製品の SSO URL を入力します:

AccessNow: <https://esg-address/accessnow/sso>

AccessNow for VMware View: <https://esg-address/view/sso>



注意:

両方のケースで、各デフォルト・ページ (start.html と view.html) へのリクエストが ESG  により自動的にリダイレクトされます。

フォームに以下のフィールドを追加します:

- name="autostart" value="yes"
- name="esg-cookie-prefix" value="EAN\_"
- name="username"
- name="password"
- name="domain"

以下は、Juniper SSL VPN での例です:

**Autopolicy: Single Sign-on**

Use this autopolicy to automatically pass user credentials to the Web application.

Basic Auth  
 NTLM  
 Remote SSO

POST the following data

Resource : \*

Post URL: \*

Deny direct login for this resource  
 Allow multiple POSTs to this resource

Delete

<input type="checkbox"/>	Label	Name	Value	User modifiable?
<input type="checkbox"/>				Not modifiable
<input type="checkbox"/>	cookie-prefix	esg-cookie-prefix	EAN_	Not modifiable
<input type="checkbox"/>	Username	login	<USER>	Not modifiable
<input type="checkbox"/>	Password	password	<PASSWORD>	Not modifiable
<input type="checkbox"/>	autostart	autostart	yes	Not modifiable
<input type="checkbox"/>	anserveraddress	address	192.168.0.88	Not modifiable

値「esg-cookie-prefix」により、フォームの AccessNow Cookie のプレフィックスが定義されます。これは、AccessNow の接続のための必須項目です。ターゲットが相対 URL の場合、パスの「/sso」の部分が置き換えられます。ターゲットが完全な URL の場合、現在のパスが完全に置き換えられます。

値を POST するためのページのサンプル

```
<form name="cookieform" method="post" action="/AccessNow/sso"><p>
<!-- <form name="cookieform" method="post" action="/view/sso"><p> -->
アドレス: <input type="text" name="address"/><br/>
<!-- RDP Host: <input type="text" name="fulladdress"/><br/> -->
ユーザ名: <input type="text" name="username"/><br/>
パスワード: <input type="password" name="password"><br>
ドメイン: <input type="text" name="domain"><br>
Ericom Secure Gateway を使用: <input type="checkbox" name="use_gateway" value="true"><br>
ゲートウェイ・アドレス: <input type="text" name="gateway_address"/><br/>
接続時にプログラムを起動: <input type="checkbox" name="remoteapplicationmode"
value="true"><br>
プログラムのパス: <input type="text" name="alternate_shell" size="256"><br>
<input type="hidden" name="autostart" value="true"/>
<input type="hidden" name="esg-cookie-prefix" value="EAN_"/>
<input type="submit"/>
</p></form>
```

POST の値を受け取るページのサンプル

```
<body>
<%
Response.Write ("アドレス:"& Request.Form("address") &"<br>")
Response.Write( "fulladdress: " & Request.Form("fulladdress") &"<br/>")
Response.Write ("ユーザ名:"& Request.Form("username") &"<br>")
Response.Write ("パスワード:"& Request.Form("password") &"<br>")
Response.Write ("ドメイン:"& Request.Form("domain") &"<br>")
Response.Write( "autostart: " & Request.Form("autostart") &"<br/>")
Response.Write( "esgcookieprefix: " & Request.Form("esg-cookie-prefix") &"<br/>")
Response.Write ("Ericom Secure Gateway を使用:"& Request.Form("use_gateway") &"<br>")
Response.Write( "ゲートウェイ・アドレス:" & Request.Form("gateway_address") &"<br/>")
Response.Write( "接続時にプログラムを起動: " & Request.Form("remoteapplicationmode") &"<br/>")
Response.Write( "プログラムのパス: " & Request.Form("alternate_shell") &"<br/>")
%>
</body>
```

---

## 2008R2 上の ESG には TLS 1.0 が必要

ESG v9.0 以降では、ベストプラクティスにあわせて TLS 1.0 は無効化されています。Windows 2008R2 サーバには、TLS 1.0 が必須です。Ericom は、2016 などの新しいオペレーティング・システムを利用して ESG を実行し、TLS 1.0 を無効化されたままにすることを推奨しています。ただし、2008R2 を使用が必要である場合、次のファイルを編集して手動で TLS 1.0 を有効化できます:

<drive>\Program Files (x86)\Ericom Software\Ericom Secure Gateway\EricomSecureGateway.Config  
SslProtocolsWithClient と SslProtocolsWithHost の両方に文字列「Tls,」を追加します。

例:

- <Property name="SslProtocolsWithClient" type="SslProtocols" value="Tls, Tls11, Tls12" />
- <Property name="SslProtocolsWithHost" type="SslProtocols" value="Tls, Tls11, Tls12" />

## 4.2.11 テクニカル・サポート

### AccessNow の一般的なエラー・メッセージ

ほとんどの最新のブラウザでは、暗号化されたセッションを確立する際に、信頼された証明書が要求されます。

「Failed to connect using both WebSockets and HTTPS」(Websocket と HTTPS の両方を使用した接続に失敗しました) というエラーがユーザに表示された場合、ESG サーバ上の証明書に問題がある可能性があります。

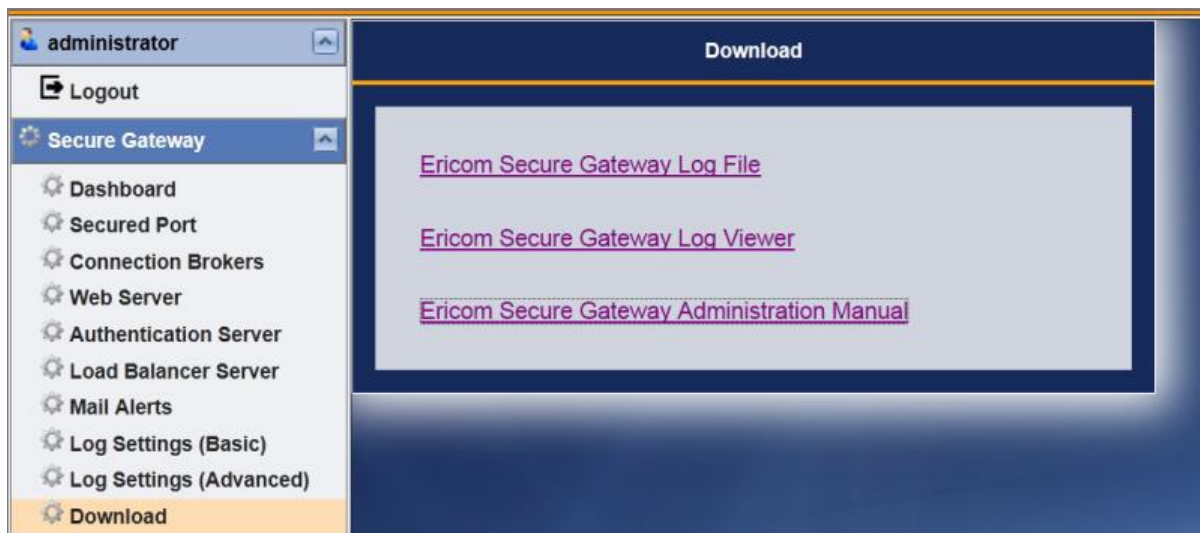
ESG の指定に使用しているアドレスを確認してください。アドレスが IP アドレスの場合、それが証明書と一致しないため、問題を引き起こす可能性があります:

IP アドレスを使用するのではなく、ESG に設定した信頼された証明書と一致するドメイン名を使用してください。

例えば、「192.168.1.111」を使用するのではなく、そのドメイン名 `esg.test.com` を使用してください。さらに、「`esg.test.com`」または「`*.test.com`」と一致する ESG 上に、信頼された証明書をインストールしてください。

### ログ・ファイルの取得

テクニカル・サポートを依頼する際、ESG ログが必要とされる場合があります。設定ページの Download から、現在のログ・ファイルを取得することができます。実際のログ・レベルは、2つのログ・ページから設定できます。どの設定を有効にするかについては、Ericom のサポート・エンジニアにご相談ください。



ログ・ファイルには特別なビューアが必要です。そのビューアは Download ページ からダウンロード可能です。完全なログ・フォルダーは、以下のようなパスにあります: `C:\Program Files (x86)\Ericom Software\Ericom Secure Gateway\Logs`

### HTTP/HTTPS フィルタリングを無効にする

一部のタイプのネットワーク・トラフィックがファイアウォールにブロックされることがあります。大部分のファイアウォールのポート 443 は、HTTP(および HTTPS) ベースの通信用に確保されています。大部

分のファイアウォールは、非 HTTP トラフィックをフィルタで除外する規則が適用されています。Secure Gateway にルーティングされる対象によって、ファイアウォール上で HTTP フィルタリングを無効化が必要となる場合があります。

Ericom Secure Gateway では、様々な種類のトラフィックをプロキシすることができます。一部は HTTP ベースであり、そうでないものもあります。Web Application Portal と AccessNow を一緒に使用する場合のみ、HTTP フィルタリングを無効にする必要がなくなります。

以下のテーブルは、接続方法により使用されるプロトコルを示しています:

接続の種類	使用されるプロトコル
Web Application Portal へのログイン	HTTP/HTTPS
AccessToGo へのログイン	HTTPS
Application Zone へのログイン	TCP
AccessNow の RDP セッション	HTTPS (Secure Gateway が必要)
AccessToGo RDP または Blaze のセッション	TCP
RemoteView RDP または Blaze のセッション	TCP

## ■ Admin Configuration Portal のアイドル・タイムアウト

Admin Configuration Portal のデフォルトのアイドル・タイムアウトは、5 分間です。これを変更するには、EricomSecureGateway.exe.config ファイルを編集し、sessionsSettings/Admin/InactivityTimeoutMinutes を設定します。

## 4.3 AccessToGo 管理者ガイド

### 4.3.1 Ericom Access To Go ユーザマニュアル

#### 概要

Ericom AccessToGo は、対応する携帯電話やタブレット・デバイスから Windows デスクトップやアプリケーションにリモート接続する機能をエンドユーザに提供します。

Ericom Connect および WebConnect Client は AccessToGo と同じエンジンとインターフェースを使用していますが、管理対象ブローカーのアクセスに特化しています。詳細については、AccessToGo の利用と Connect/WebConnect の設定に関するセクションを参照してください。

Ericom Blaze Client は AccessToGo と同じエンジンとインターフェースを使用していますが、Blaze のアクセスのみに特化しています。詳細については、AccessToGo の利用と Blaze の設定に関するセクションを参照してください。Ericom Blaze Client には、AccessServer 7.3 以上が必要です。テクニカル・サポートに関する質問または依頼については、[mobile@ericom.com](mailto:mobile@ericom.com) まで E メールでお問い合わせください。

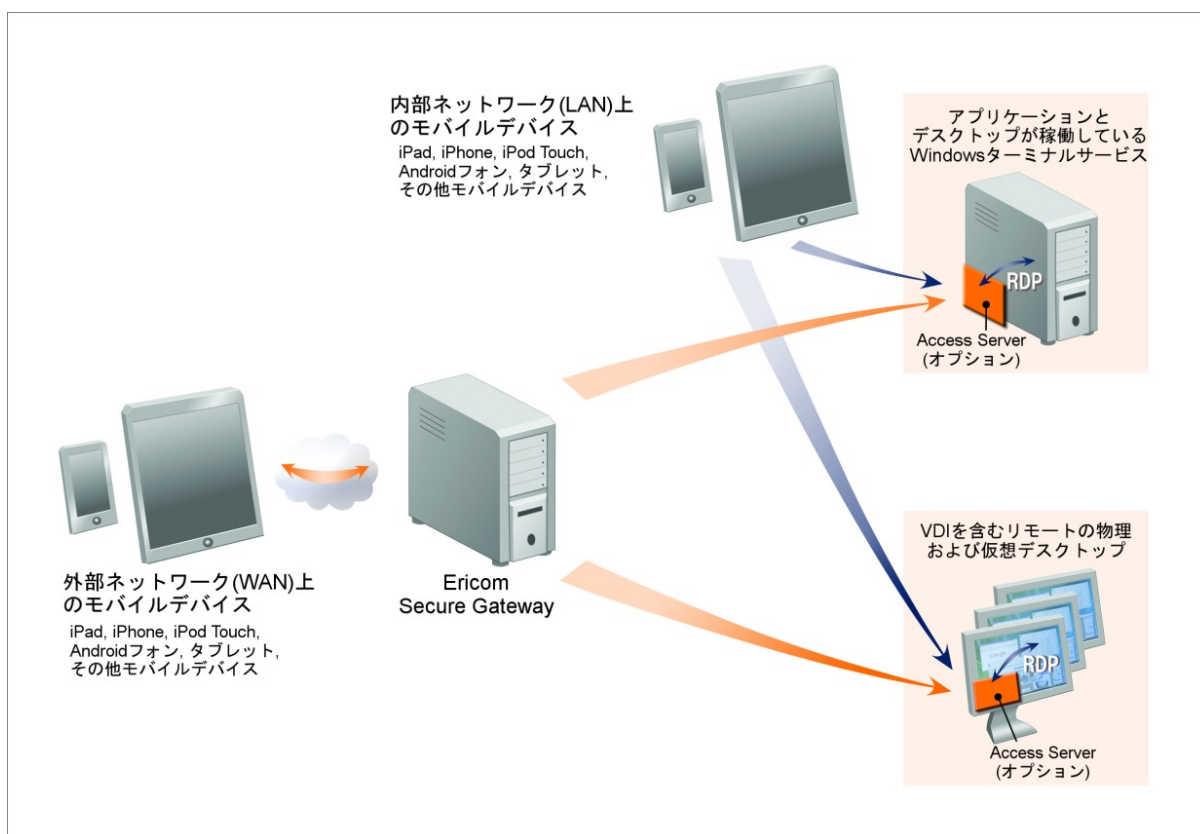
#### アーキテクチャ

Ericom AccessToGo はインストール可能な 3 つのコンポーネントにより構成されています。

1. ダウンロード可能なクライアント
2. (オプション) RDP アクセラレーションと圧縮のための Access Server
3. (オプション) デスクトップやアプリケーションへの安全かつ暗号化されたリモート・アクセスを提供する Secure Gateway サービス

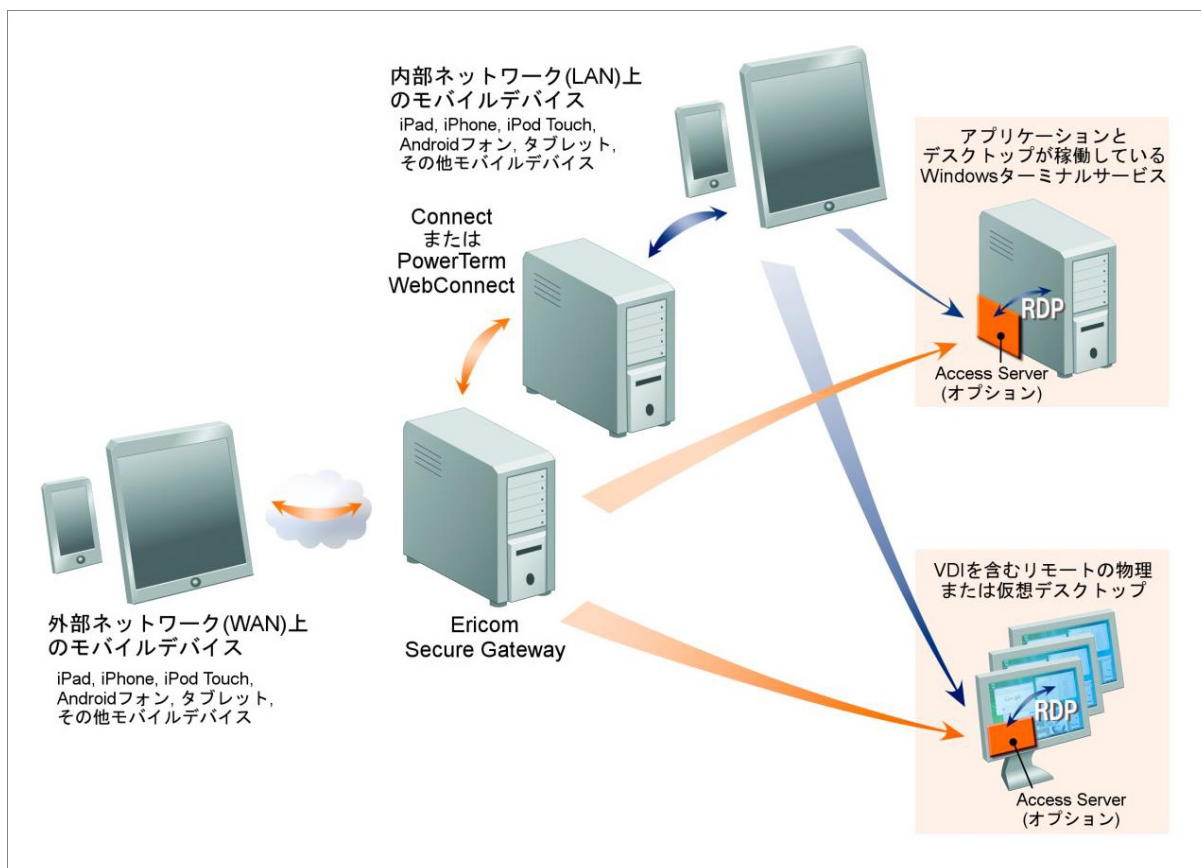
この図は、AccessToGo のコンポーネントがどのように連動するかを示しています。オレンジ色の矢印はリモート接続を示し、青色の矢印は内部接続を表しています。





1. エンドユーザは、対応する携帯電話やタブレット上で Ericom AccessToGo を起動します。AccessToGo に接続用パラメータを入力します。
2. AccessToGo は、対象の RDP ホストに対して RDP または Blaze 接続を試みます。
  - (a) オプションの Ericom Secure Gateway を使用している場合、AccessToGo セッションは、セキュアなポート (デフォルトは 443) を介して接続されます。
3. Blaze を有効化している場合、Access Server は AccessToGo セッションを受け入れ、RDP をアクセラレートします (デフォルトでは 8080 ポートを介して)。Blaze を有効化していない場合、AccessToGo は直接 RDP によって受け入れられます (デフォルトでは 3389 ポートを介して)。

この図は、AccessToGo の各コンポーネントと Ericom Connect または PowerTerm WebConnect ブローカーがどのように連動するかを示しています。オレンジ色の矢印はリモート接続を示し、青色の矢印は内部接続を表しています。



### Blaze RDP 圧縮とアクセラレーション

Ericom AccessToGo には、RDP 圧縮とアクセラレーションを行う Ericom の Blaze テクノロジーが搭載されています。このテクノロジーにより、低速ネットワーク接続を介したリモートデスクトップのパフォーマンスが向上します。アクセラレートされたセッションは、高度なグラフィック画像やアニメーションを含むコンテンツを閲覧する際にも役立ちます。

このテクノロジーには 3 つの主要機能が備わっています。

- 画像圧縮
- パケット・シェーピング
- 全フレームのレンダリング

画像の圧縮は、クライアントがレンダリングを行う前に画像を圧縮することを意味します。圧縮のレベルは、ユーザーが選択したアクセラレーション/品質のレベルに左右されます (規定値は管理者による設定も可能です)。

パケット・シェーピングは、ネットワークの利用状況やパフォーマンスを向上するためにネットワークメッセージを最適化します。

全フレームのレンダリングは、標準の RDP のようなブロック単位ではなく、全体として表示がアップデートされることを意味します。この点は、動画の視聴や、遅いネットワーク接続を使用する際に特に違いが現れます。その他の最適化機能を合わせて活用し、ローカルのデスクトップの機能性により近い、スムーズな表示を実現しています。

## 4.3.2 はじめてみる

### 前提条件

エンドユーザと リモートデスクトップの間のセッション通信には RDP が使用されるため、RDP ホスト上で RDP アクセスを有効化する必要があります。

- 対象とする RDP ホストへの RDP 接続が許可されていることをネットワーク管理者に確認します。
- 対象とする PC で RDP を有効化します。「コントロールパネル | システム | リモート設定」に進みます。「リモートデスクトップ」から、「リモートデスクトップを実行しているコンピュータからの接続を許可する」を選択します。NLA は現在サポートされていないため、3 番目の設定は選択しないでください。
- 「ユーザの選択」ボタンをクリックし、リモート接続を許可するユーザを追加します。「OK」をクリックします。
- システムの Windows ファイアウォールによって RDP 接続が許可されていることを確認します (デフォルトのポートは 3389)。Ericom が提供するプロトコルを使用している場合、8080 も開く必要があります。

RDP ポートを介して 対象の PC への受信接続を許可するよう、ネットワークまたはルータのファイアウォールを設定します。

### デバイスの要件

AccessToGo を使用するには、デバイスに少なくとも 512 MB の RAM が搭載されている必要があります。V9.2 では以下のオペレーティング・システムがサポートされています:

- Apple iOS(iPadOS) 11.x, 12.x, 13.x
- Android OS 6, 7, 8, 9

### AccessToGo をダウンロードする

デバイスのマーケットプレイス (例: Google Play Store や Apple App Store) で Ericom を検索し、目的のアプリを選択します。

- AccessToGo
- Ericom Connect Client
- Ericom WebConnect Client
- Ericom Blaze Client

アプリケーションをダウンロードすると、デバイスのアプリケーション一覧にアイコンが表示されます。アイコンをタップすると、アプリケーションが起動します。

AccessToGo(RDP、Blaze、および PowerTerm WebConnect および Ericom Connect アクセスが含まれます):



Ericom Connect Client (Ericom Connect アクセスのみが含まれます):



Ericom WebConnect Client (PowerTerm WebConnect アクセスのみが含まれます):

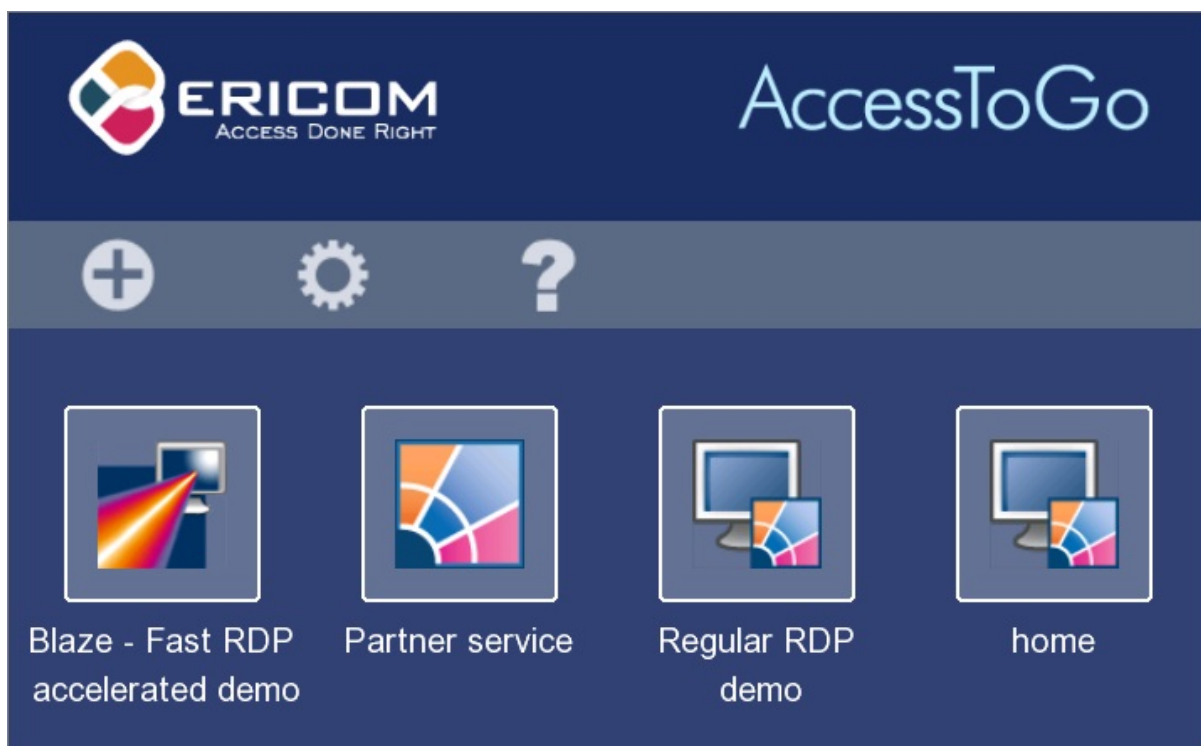


Ericom Blaze Client (Ericom Blaze のアクセラレートされた RDP アクセスのみが含まれます):



## ■ 接続リスト

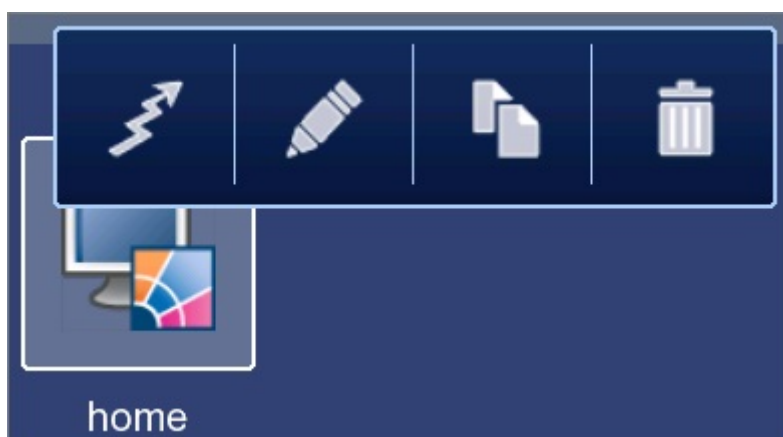
Ericom AccessToGo を起動すると、接続リストが表示されます。このリストには、保存されたすべての接続が表示されます。米国にある Ericom のデモサーバーに接続するための 2 つのサンプル接続も含まれています。RDP ホストに接続する際、一方の接続では標準の RDP が使用され、もう一方では Ericom の Blaze RDP アクセラレーションが使用されます。既存の接続と同じ名前で作成した場合、混乱を避けるために自動的に別な名前に置き換えられます。



目的の接続を押すか、タップするか、クリックして、接続を起動します。

## ■ 接続のオプション

既存の接続をコピー、編集、削除することができます。接続に対する操作を行うには、操作メニューが表示されるまで目的の接続を押し続けます。



ボタン	機能	説明
	接続	設定したパラメータを使用して接続します。
	編集	既存の接続パラメータを編集します。
	コピー	既存の接続をコピーします。
	削除	接続を削除します。

## ■ オンライン・ヘルプ

AccessToGo のオンライン・マニュアルを参照するには、「オンラインヘルプ」ボタンをタップします。



## ■ 新しい接続を作成する

AccessToGo の接続一覧画面で、「新しい接続」ボタンをクリックします。



いくつかのオプションを選択することができます。 目的の接続タイプを選択し、接続パラメータを入力します。

接続タイプ	説明
RDP (フリー)	標準の RDP を使用して RDP ホストに接続します。ホスト上で RDP を有効化してください。
Blaze	RDP ホストに AccessServer 7.3 以上がインストールされている必要があります。低速ネットワーク接続を介してグラフィックス (動画、写真など) を表示する RDP 画面をアクセラレートします。詳細については、 <a href="http://www.EricomBlaze.com">www.EricomBlaze.com</a> を参照してください。
Ericom Connect	仮想アプリケーションとデスクトップにアクセスするために、Ericom Connect ブローカーに接続します。
PowerTerm Web-Connect (VDI/TS)	仮想アプリケーションとデスクトップにアクセスするために、PowerTerm WebConnect ブローカーに接続します。





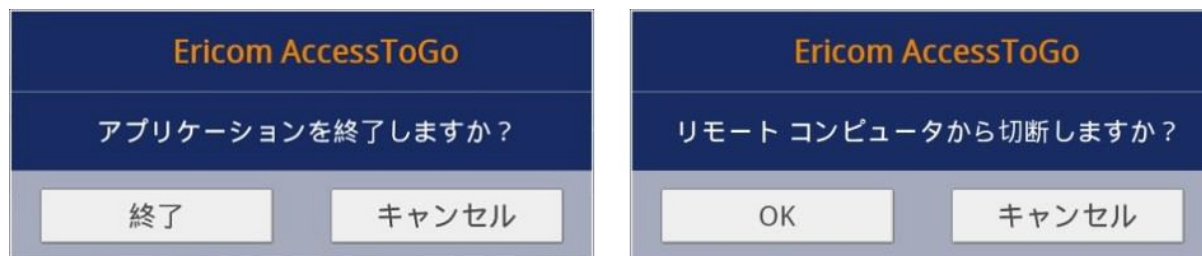
## ■ 接続パラメータ

接続パラメータ	
接続名	設定中の接続用のカスタマイズ可能なラベル。
サーバ	RDP が有効化されている接続先システムのアドレス。
ユーザ名	RDP ホストにログインするためのユーザの資格情報。オプションとしてドメインの詳細を含む事も可能です。(例: domainuser.)Ericom SecureGateway を使用する場合、このフィールドは必須です。それ以外の場合このフィールドはオプションです。指定されない場合、ユーザは RDP ホストにより資格情報が要求されます。
パスワード	ユーザ名に対応するパスワード。
Ericom Secure Gateway の使用	有効化すると、AccessToGo は指定された Ericom Secure Gateway を使用してリモートデスクトップに接続します。
新規 Gateway	リモート接続用に Ericom Secure Gateway を設定し、選択します。
Blaze - RDP アクセラレーション	オンの場合、セッションでの品質損出のある画像圧縮を有効にします。品質損失/アクセラレーションの

127度合いは、ドロップ・ダウン・リストを使用して指定できます。

## ■ 接続の切断と終了

アクティブなセッションを切断したり、Android デバイス上の AccessToGo アプリケーションを終了したりするには、デバイスの「戻る」ボタンを押してください。切断または終了を確認するためのプロンプトが表示されます。



## ■ Ericom Secure Gateway を設定する

Secure Gateway は、AccessToGo アプリケーションから社内の RDP ホストへの暗号化されたリモート・アクセスを提供するために使用されます。Secure Gateway は、以下のモードで使用できます: RDP および Blaze。Ericom Connect と PowerTerm WebConnect の接続では、それらのアドレスとして Secure Gateway が使用されます (ESG を PowerTerm WebConnect サービスに対してのリバース・プロキシとして設定している場合)。

Secure Gateway は、接続の「オプション」から有効化することができます。



1. Secure Gateway の使用を有効化するには、「Ericom Secure Gateway の使用」をオンにしてください。
2. 次に、Ericom Secure Gateway をタップして、設定済みの Secure Gateway を選択します。
3. 新しい Secure Gateway を追加するには、「新規 Gateway」ボタンをタップし、必須項目への入力を行います。

項目	説明
サーバ	Secure Gateway サーバのアドレス
接続ポート	Secure Gateway サービスでリスニングしているポート値
ユーザ名	Secure Gateway への認証に使用するユーザ名
パスワード	Secure Gateway の認証に使用するパスワード

4. 目的の Secure Gateway をタップし、有効化します。



**注意:**

デフォルトのゲートウェイ・ポートは 443 です。Secure Gateway でカスタム・ポートをリスニングしている場合、「接続ポート」パラメータに正しい値を入力してください。

---

### 4.3.3 AccessToGo を使用する

---

#### AccessToGo ツールバー

AccessToGo ツールバーは、セッションが確立された後に、デスクトップまたはアプリケーションの下部に表示されます。Android ベースのデバイスで AccessToGo ツールバーを表示するには、デバイスのメニュー・ボタンを押します (通常は一番左側のボタンです)。接続時にツールバーを表示するには、設定に進み、「Always」をオンにします。



ボタン	機能	説明
	スクリーン上のマウス	スクリーン上のマウスを表示/非表示にします。
	スクリーン上のタッチパッド・マウス	スクリーン上のタッチパッド・マウスを表示/非表示にします。
	スクリーン上のキーボードの表示	スクリーン上のキーボードを表示します。
	ズーム・イン/ズーム・アウト	スクリーンのズーム・イン/ズーム・アウト操作
	リモート・マウス・モード (デフォルトで有効)	有効な場合、すべてのマウスの動作やジェスチャはリモート・セッション内に適用されます。例えば、源氏亜の表示をズーム・アウトするジェスチャは無効になります。ローカル画面をスクロールするには、タップした状態を0.5秒間保持した後、指を動かします。
	スクロール・ホイール・モード	このモードを有効化している場合、画面上で指を上下にスライドすることにより、スクロールホイールの動作を再現することができます。
	追加メニューの表示	ジェスチャの設定な

## 指をマウスとして使用する

ユーザは、自分の指を使用してマウスを操作することができます。ユーザが画面上の一部をタップすると、クリックのインジケータが表示されます。このインジケータは、セッションでマウスのクリックが実行された場所の点と、指のタップを示す円により構成されます。

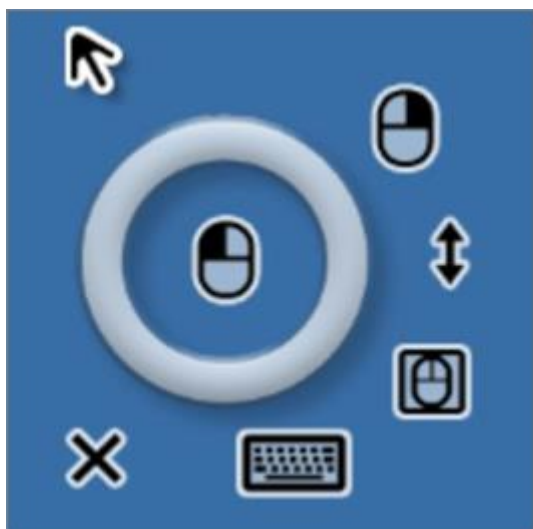
右クリックを実行するには、画面をタップし、ホールドします。右クリックのインジケータが円になってから指を離すことで、右クリックを実行します。

## スクリーン上のマウスを使用する

スクリーン上のマウスは、リモート・セッションを操作する上で役立つ機能を提供します。マウスが有効であるかどうかに関わりなく、ユーザは自分の指を使用してセッションを操作することができます。

操作	指のジェスチャ
左クリック	シングル・タップ (一度だけタップ)。
右クリック	シングル・タップ + ホールド。

フルスクリーン上のマウスのアイコン:



スクリーン上のマウスが有効な場合、以下の機能を利用可能です。

アイコン	機能	説明
	マウス/左クリック	このアイコンをタップすると左クリックが実行されます。マウスのポインタをドラッグするには、このアイコンを押したままにします。
	ポインタ	このアイコンは、マウスのポインタを表します。
	右クリック	このアイコンをタップすると、マウスのポインタの位置で右クリックが実行されます。
	スクロール・ホイール・モード	このモードを有効化している場合、画面上で指を上下にスライドすることにより、スクロールホイールの動作を再現することができます。
	リモート・マウス・モード	有効な場合、すべてのマウスの動作やジェスチャはリモート・セッション内に適用されます。例えば、現在の表示をズーム・アウトするジェスチャは無効になります。ローカル画面をスクロールするには、タップした状態を0.5秒間保持した後、指を動かします。

## ■ スクリーン上のタッチパッド・マウスを使用する

タッチパッド・マウスは、デバイスの画面をタッチパッドとして使用することを可能にします。タッチパッドを有効化している場合、ユーザは画面の任意の領域をタップして、マウスを操作することができます。指をスライドさせるだけで、画面でマウスを動かすことができます。指は直接マウスの上にある必要はありません。マウスをタップしてホールドすると、右クリックが実行されます。タッチパッドを有効化している場合でも、ズーム・インやズーム・アウトの動作を実行することができます。

タッチパッドのマウス・ボタン:






キーボード・ツールバーを使用する

AccessToGo には、より強化されたキーボード機能が含まれています。スクリーン上のキーボードを有効化している場合、以下の操作が利用可能です。





アイコン	説明
	<p>高度なキーボード・キーを表示します: ファンクション・キー、矢印キー、キーの組み合わせ (例: CTRL+ALT+DEL) など。このキーを押すことで、OS の仮想キーボードと高度なキーの切り替えも実行できます。</p>
	<p>ESC キーをシミュレートします。</p>
	<p>TAB キーをシミュレートします。</p>
	<p>CTRL キーをシミュレートします。アクティブな場合には、緑のライトが点灯します。</p>
	<p>ALT キーをシミュレートします。アクティブな場合には、緑のライトが点灯します。1回 ALT キーを押すと、ALT キーが「ホールド」されます。もう一度キーを押すと、ALT キーが「タップ」されます。</p>
	<p>Windows キーをシミュレートします (Windows スタート・メニューを表示しま</p>
	<p>135す)。 スクリーン上の PC</p>

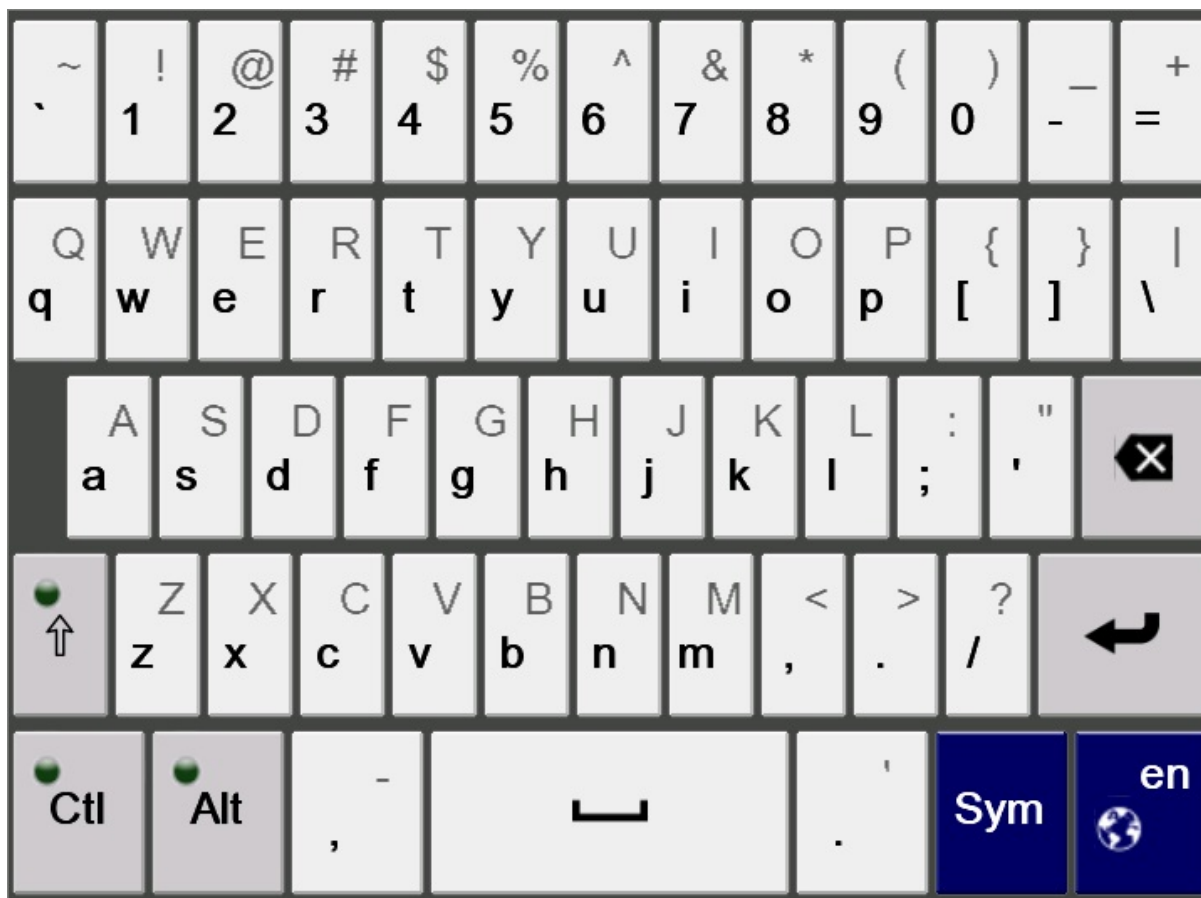
## ■ スクリーン上のキーボードを使用する

スクリーン上のキーボード・ボタンを押すと、AccessToGo キーボードが表示されます。AccessToGo キーボードは、追加のキーと機能を提供し、Windows ベースのアプリケーションでタイピングする際に、より優れたユーザ・エクスペリエンスを提供します。

スクリーン上のキーボード・ボタン:



AccessToGo キーボード:



## ■ スクリーン上のファンクション・キーを使用する

スクリーン上のファンクション・キーボード・ボタンを押すと、AccessToGo ファンクション・キーボードが表示されます。ファンクション・キーボードは、ファンクション・キーや一般的な Windows キーの組み合わせ、スクロール・キーを提供し、Windows ベースのアプリケーションやデスクトップでタイピングする際に、より優れたユーザ・エクスペリエンスを提供します。

スクリーン上のファンクション・ボタン:



AccessToGo ファンクション・キーボード:

F1	F2	F3	F4	F5	F6	Ctl+Tab	Ctl+F4
F7	F8	F9	F10	F11	F12	Alt+Tab	Alt+F4
Ctl+Z	Ctl+Alt	Ctl+Esc	Home	▲	PgUp	Del	
Ctl+X	Ctl+C	Ctl+V	◀	Ins	▶	ⓧ	
↑	Ctl + Alt + Del		End	▼	PgDn	↶	

## リモート・セッションの PPI 解像度を使用する

エンドユーザ・デバイスとユーザの好みの多様化に対応する上で、リモートデスクトップやアプリケーションを起動する際に、最適な解像度で作業できるようにすることが重要になっています。

デフォルトでは、画面サイズが7インチ未満のデバイス向けの PPI は 190 です。画面サイズが7インチ以上のデバイス向けの PPI は 170 です。これらの設定によりデバイスの画面サイズに合った最適な解像度を提供することができますが、ユーザが独自の PPI 値を選択することを望む場合もあります。お使いのデバイスに最適な解像度で表示するために PPI 機能を使用する方法については、「設定」のセクションを参照してください。

## デバイスとホストの間でテキストをコピー/貼り付けする

AccessToGo では、コピー/貼り付け機能のために、テキストのみのクリップボードがサポートされています。クリップボードはデフォルトで有効化されており、設定の「クリップボードを有効にする」(Enable Clipboard) をオフにすることで無効化できます。

デバイスとホスト間のコピー/貼り付け  
を有効にする



この機能を有効化している場合、双方向のコピー/貼り付け機能がサポートされます。つまり、ローカル・デ

デバイスから AccessToGo セッションへのコピー/貼り付け、また AccessToGo セッションからローカル・デバイスへのコピー/貼り付けが可能です。

以下の例では、リモートの AccessToGo セッションからローカル・デバイスのブラウザにコピー/貼り付けする操作が示されています。

リモートの AccessToGo セッションでコピーを実行します：



目的のテキストがクリップボードにコピーされた後、ローカル・アプリケーションに切り替えてペーストを実行します。これにより、選択したテキストがクリップボードからコピーされます。



注意：

一部のデバイスでは、ローカル・アプリケーションへの切り替えにより AccessToGo セッションが終了する場合があります。

## 物理キーボードとマウスを使用する

物理的な入力/出力デバイスは、オペレーティング・システムにより処理され、アプリケーションにより直接処理されることはありません。物理的な入力/出力デバイスを使用する場合、AccessToGo は、オペレーティング・システムから受け取った内容に基づいて物理キーボードやマウスからの入力を受け入れます。右シフトなど物理キーボードの一部のキーは、オペレーティング・システムによってサポートされていないため、正常に動作しない場合があります(そのようなキーは同じデバイス上のすべてのアプリケーションにおいて正常に動作しません)。

## 物理キーボードを有効化する

Bluetooth キーボードなどの物理キーボードは、セッションが確立した直後に使用できない場合があります (デバイスにより異なります)。セッションの接続後にキーボードが機能しないデバイスでは、AccessToGo のデバイス・キーボードを有効化して (以下のボタンをタップ)、入力を試みてください。



注意:

物理マウスを使用する場合、右のマウス・ボタンは Android 4.0 以上を搭載しているデバイスのみでサポートされます。

Apple iOS デバイス上でテスト済みの Bluetooth キーボード:

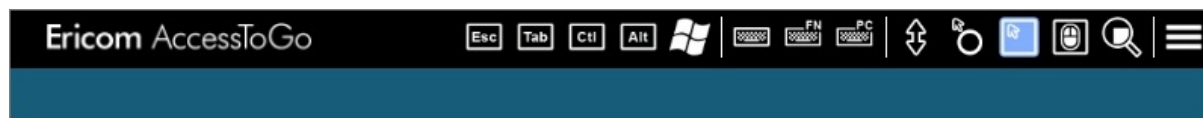
Logicool KEYS-TO-GO キーボード、バッファロー iPad Air 専用 Bluetooth キーボード BSKBB25

※ iOS 用 Bluetooth キーボードは英語配列のみサポートしております。Android デバイスの Bluetooth キーボード接続での日本語入力はサポートしていません。

## ■ タブレット・ファンクション・バーを使用する

タブレット・ファンクション・バーは、アクティブ・セッション中によく使用されるキー (ESC、TAB、CTRL、ALT、Windows) や機能 (スクリーン上のマウスの表示など) を表示します。このバーは、「設定」の「上部バーの有効化」をオフにすることで無効化できます。

AccessToGo は、起動時にデバイスがタブレットであるかどうかを識別します。AccessToGo の表示領域が 5.5 インチ以上あるデバイスはタブレットとして識別され、デフォルトでアクティブなセッションの上部にタブレット・ファンクション・バーが表示されます。5.5 インチ以下の場合はスマートフォンとみなされ、設定メニューで「上部バーの有効化」をオンにしている場合でも上部のファンクションバーは表示されません。



ボタンをタップしてホールドすると、そのボタンの用途の簡単な説明が表示されます。

アイコン	機能	説明
	Esc	Escape キー
	Tab	Tab キー
	Ctrl	Control キー
	Alt	Alt キー
	Windows キー	Windows キーを実行します
	デバイス・キーボード	テキスト入力用のデバイス・キーボードを表示/非表示とします。
	ファンクション・キーボード	特殊キーやキーの組み合わせを実行するためのファンクション・キーボードを表示/非表示とします。
	PC キーボード	テキスト入力用の PC キーボードを表示/非表示とします。この機能は、一般的な PC キーボードのレイアウトに似ています。
	スクロール・ホイール・モード	このモードを有効化している場合、画面上で指を上下にスライドすることにより、スクロールホイールの動作を再現することができます。セッション・ディスプレイの移動やパンはできません。
	スクリーン上のフローティング・マウス	スクリーン上のマウスを表示/非表示とします。フローティングマウスによる操作のみがセッション内に適応されます。セ

## 拡張メニューを使用する

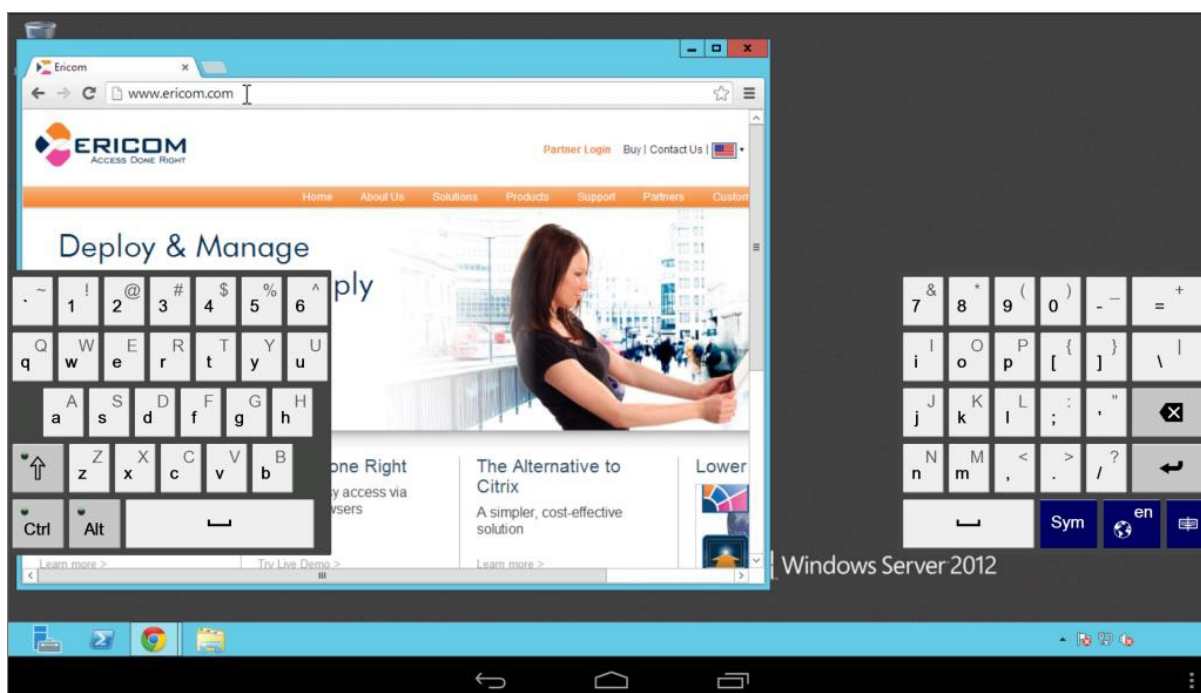


拡張メニューは、AccessToGo ツールバーやタブレットバーより利用可能で、以下の追加機能を提供します。

	現在のキーボード・ロケール	現在のキーボード・ロケールの言語を表示します。
	ジェスチャの設定	サポートされているジェスチャについて、目的の機能を設定します。
	リモート PPI	アクティブなセッション中に PPI を設定します。リモート・セッションは自動的にサイズが調整されます。
	スクリーン上のヘルプ	スクリーン上のヘルプ・ダイアログ表示します。
	セッションを閉じる	現在のセッションを閉じて、前のメニューに戻ります。

## タブレット向け分割キーボードを使用する

AccessToGo には、分割 PC キーボードを使用する機能が含まれています。この PC キーボード・モードは、仮想キーボードをより人間工学的にし、エンドユーザがデバイスを手に持った状態で親指でタイピングできるようにするために設計されています。



分割キーボードを無効化する

分割 PC キーボードを無効化してフル PC キーボード・モードに切り替えるには、右下にあるこちらのボタンをタップします:



## ■ テキスト入力時のキーボードの自動表示と配置

テキスト入力フィールドを利用しやすくするために、AccessToGo ではビルトインのキーボードが画面上に自動的に表示・配置されます。テキスト・フィールドからフォーカスが外れた場合、キーボードは自動的に閉じられます。一部のアプリケーションは、AccessToGo によってテキスト・フィールドを検知できない使用で開発されているため、この機能が動作しない場合があります。



タブレット上で分割キーボードを有効化している場合、この動作は適用されません。

注意:

キーボードの自動表示と配置を無効化する

「設定」メニューから「言語とキーボード」に進み、「キーボードの自動表示」をオフにします。



## ■ マルチタッチ

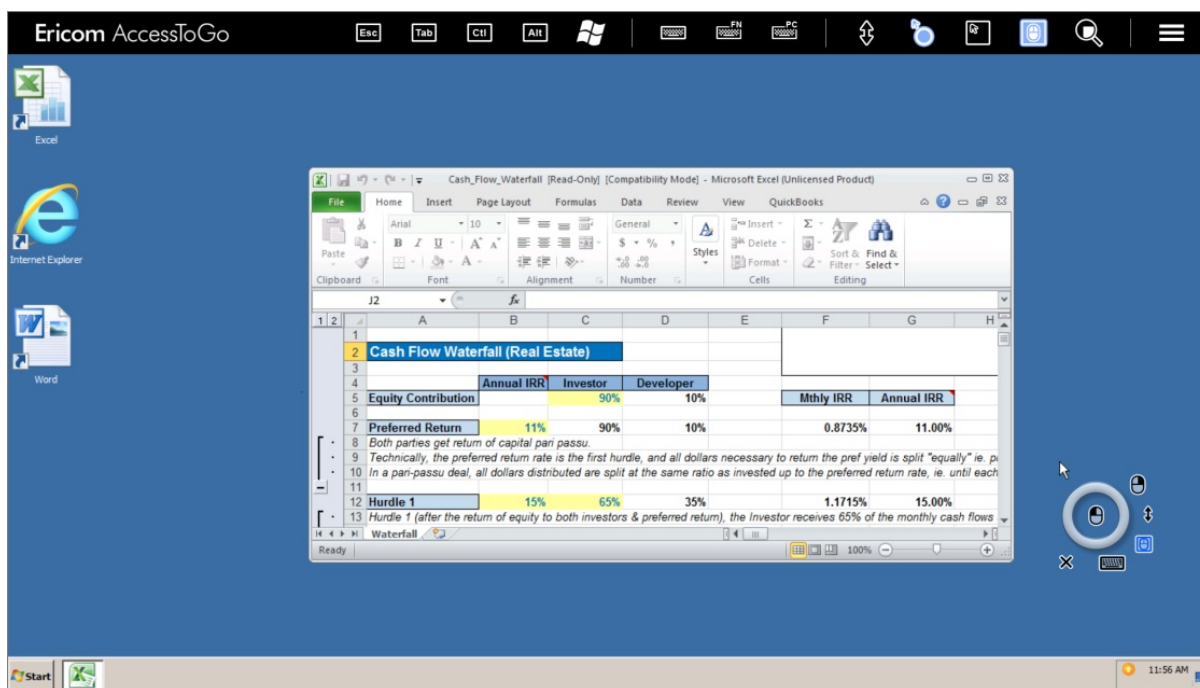
マルチタッチは、Windows 8 および Windows Server 2012 以上でサポートされる RDP の機能です。マルチタッチを有効化している場合、対応アプリケーションにおいて、コンテキストに関連するマルチフィンガー・ジェスチャを利用できるようになります。例えば、Excel を使用する際、ユーザは 2 本指のジェスチャを使用して、デスクトップ全体を拡大せずに Excel ドキュメントを拡大/縮小できます。また、上下にスワイプするマルチフィンガー・ジェスチャを使用して、ユーザはデスクトップを移動せずに Web ブラウザのページをスクロールできます。マルチタッチがサポートされているサーバに接続する際、マルチタッチが利用可能であることをユーザに通知するメッセージが画面上に表示されます。マルチタッチを有効化している場合、マルチタッチ・モードを有効化/無効化するためのオプションがセッション・メニューに表示されます。

マルチタッチ・モードでジェスチャを使用する際、画面上にマルチタッチ・アイコンが表示されます。

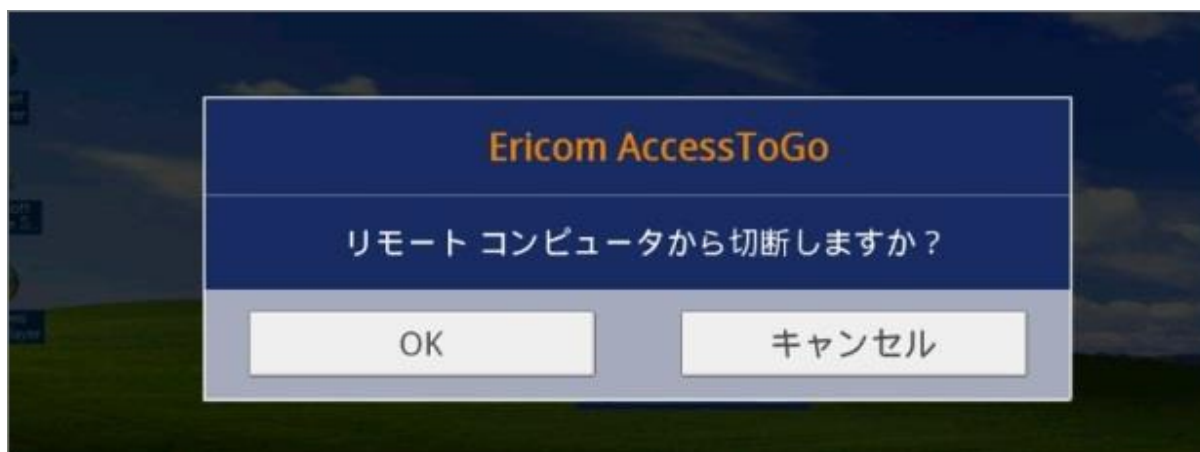


### 4.3.4 デSKTOPへの接続

接続パラメータを設定した後、必要に応じて接続を保存します。「接続」ボタンを押して接続を開始します。ログインが成功すると、DESKTOPに接続されます。AccessToGoによりマウスのボタンとキーボードのイベントが読み取られ、それらがRDPホストへ転送されます。デバイスがタブレットとして認識された場合、以下のようにアプリケーションの上部にAccessToGoツールバーが表示されます。



アクティブ・セッションを切断するには、デバイスの「戻る」ボタンを押します。切断のリクエストを確認するプロンプトが表示されます。切断コマンドは、Windowsのスタート・メニューから実行することもできます。



Blaze RDP アクセラレーション接続を有効化するには、オプションの Access Server を RDP ホストにインストールする必要があります。以下の RDP ホストがサポートされています：

Windows 7、8.1、10、2008、2008 R2、2012R2、2016。



注意:

Blaze モードを使用するには、RDP ホスト上に AccessServer 7.3 以上が必要です。古いバージョンの Blaze Server がインストールされている場合、接続が RDP プロトコルにフォールバックします。

## ■ 自動角度調整と自動サイズ調整

フルスクリーン・セッションの間、デバイスの向きが変更された場合に新しい解像度をサポートするために、AccessToGo は画面サイズを自動調整することができます (自動回転機能が有効化されている場合)。この機能を有効化するには、アプリケーションの設定に進み、「タブレット回転時の全画面リサイズ」設定をオンにします。



### 4.3.5 アプリケーションへの接続

デスクトップ全体ではなくアプリケーションのみを起動するには、「接続」パラメータの「プログラム」パラメータを設定します。

プログラム・パラメータ	
起動時に次のプログラムを起動する	接続時に RDP ホスト上の特定のプログラムのみを起動するように接続を設定します。
パスとファイル名	RDP ホストで起動されるアプリケーションへのパス。アプリケーションが適切にインストールされていることを確認してください。
次のフォルダで開始する	アプリケーションの作業フォルダへのパス。

アプリケーションが有効化され、「起動時に次のプログラムを起動する」で設定されている場合、セッションが接続された後そのアプリケーションのみが表示されます。起動したアプリケーションによってセッション全体の領域がカバーされ、リモートデスクトップは表示されません。



リモート・アプリケーションはターミナル・サーバに接続する場合にのみ動作します。この機能は、Windows ワークステーションのオペレーティング・システム (例: Windows 7) では利用できません。

Windows 2008 ターミナル・サーバー (および 2008 R2RDS) では、サーバで RemoteApps を有効化する必要があります。起動するアプリケーションは、「RemoteApp プログラム」の許可リストに追加する必要があります。

RemoteApp プログラム		RemoteApp プログラムの追加(D)	引数
名前		RD Web アクセスに表示する(S)	無効
ペイント		RD Web アクセスに表示しない(I)	
PowerTerm Terminal Serv		rdp ファイルの作成(C)	制限なし
PowerTerm Terminal Serv		Windows インストーラー パッケージの作成(W)	制限なし

RemoteApp にアプリケーションを追加するには、以下の手順に従ってください:



TS/RDS を使用して起動可能とする目的のアプリケーションを選択します:



目的のアプリケーションを追加した後、エンドユーザーに公開する前に、AccessToGo を使用して接続をテストします。

---

### 4.3.6 リモート・アクセス の設定

---

AccessToGo は、RDP をサポートするすべての Windows ベースの PC へのリモート・アクセス用ソリューションとして使用することができます。一部の Windows オペレーティング・システムでは、受信 RDP セッションがサポートされていません (例: Windows 7 Home)。基本的なリモート・アクセス接続を導入するために必要な手順は以下の通りです:

1. 対象とする PC への リモート RDP 接続が許可されていることをネットワーク管理者に確認します。一部の組織では、組織の PC への RDP 接続が禁止されています。
2. エンドユーザ・デバイス (例: iPad) に AccessToGo をインストールします。
3. 対象とする PC で RDP を有効化します。「コントロールパネル | システム | リモート設定」に進みます。「リモートデスクトップ」から、「リモートデスクトップを実行しているコンピュータからの接続を許可する」を選択します。NLA は現在サポートされていないため、3 番目の設定は選択しないでください。
4. 「ユーザの選択」ボタンをクリックし、リモート接続を許可するユーザを追加します。「OK」をクリックします。
5. PC の Windows ファイアウォール によって受信 RDP 接続が許可されていることを確認します (デフォルトのポートは 3389)。
6. RDP ポートを介して 対象の PC への受信接続を許可するよう、ネットワークまたはルータのファイアウォールを設定します。

7. 対象の PC のアドレスに接続するよう AccessToGo を設定します。接続がリモートで行われる場合、受信接続を対象の PC にポート転送するルールが設定されているファイアウォール/ルータの外部アドレスを指定します。
  
8. オプションの Access Server を RDP アクセラレーションのために使用している場合、Blaze ポートは 8080 であることに注意してください。
  
9. オプションの Ericom Secure Gateway をリモート接続用に使用している場合、ネットワーク・ファイアウォール上でポート 443(RDP ポートではなく)が必要となります。Secure Gateway のポート値は変更することができます。詳細については、Ericom Secure Gateway の資料を参照してください。



---

### 4.3.7 管理対象ブローカーのアクセスの設定

---

AccessToGo を使用して、Ericom Connect または PowerTerm WebConnect 接続ブローカーを介してホストされているアプリケーションやデスクトップに接続できます。 リモート・セッションへのリモート・アクセスを導入するために必要な手順は以下の通りです:

1. 対象とするリモート RDP ホストへの RDP 接続が許可されていることをネットワーク管理者に確認します。
2. 対象とする PC で RDP を有効化します。「コントロールパネル | システム | リモート設定」に進みます。「リモートデスクトップ」から、「リモートデスクトップを実行しているコンピュータからの接続を許可する」を選択します。NLA は現在サポートされていないため、3 番目の設定は選択しないでください。
3. 「ユーザの選択」ボタンをクリックし、リモート接続を許可するユーザを追加します。「OK」をクリックします。
4. システムの Windows ファイアウォール によって受信 RDP 接続および/または Blaze 接続が許可されていることを確認します (デフォルトのポートはそれぞれ 3389、8080 です)。
5. RDP ポートを介して 対象の PC への受信接続を許可するよう、ネットワークまたはルータのファイアウォールを設定します。
6. エンドユーザ・デバイス (例: iPad) に AccessToGo をインストールします。

7. Ericom Connect または WebConnect サーバのアドレスに接続するよう AccessToGo を設定します。Connect 向け 8011 以外、WebConnect 向けに 4000 以外を使用する場合、ポートを明示的に指定します (例 : 192.168.1.1:443)。
  
8. リモート接続用に オプションの Ericom Secure Gateway を使用している場合、その外部アドレスとポート 443 を指定します (PowerTerm WebConnect のポートではなく)。Secure Gateway は、PowerTerm WebConnect サーバへのリバース・プロキシとして動作します。Secure Gateway のポート値を変更することが可能です (デフォルトは 443)。詳細については、Ericom Secure Gateway のドキュメントを参照してください。
  
9. Ericom Connect または PowerTerm WebConnect へのログインに使用するオプションのユーザ名とパスワードを設定します。

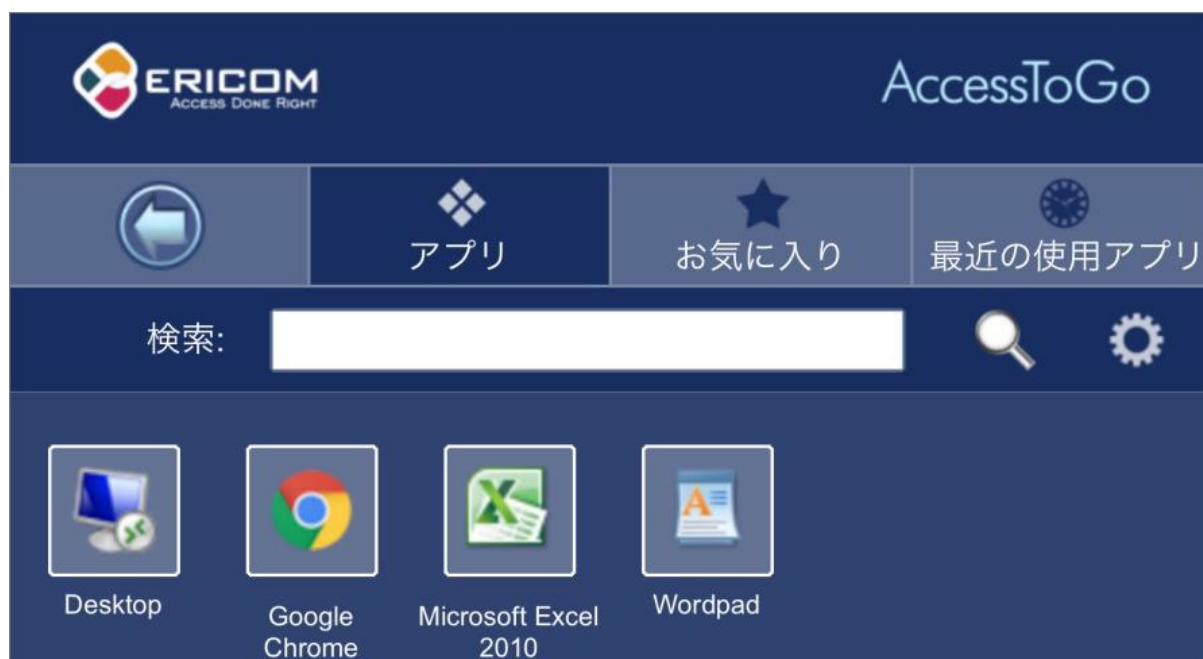


注意:

PowerTerm WebConnect の「SmartInternal」設定を使用するには、サーバ上で次の環境変数を設定する必要があります: SmartInternalIsGateway を 1 とする

## ■ ユーザ・インターフェースを使用する

ブローカーを介した環境への接続が正しく認証された後、Ericom Connect および WebConnect のインターフェースが表示されます。



ユーザが選択可能な 4 つのタブのオプションがあります。

機能	説明
	ログアウトします。
	割り当てられたすべての公開アプリケーションとデスクトップを表示します。
	ユーザがお気に入りとしてマークした、割り当てられた公開アプリケーションとデスクトップを表示します。
	最近使用した割り当てられた公開アプリケーションとデスクトップを表示します。
	自動 PPI リサイズなどの AccessToGo の機能を設定するために設定用ページにアクセスします。
	検索機能で使用するキーワードをこのフィールドに入力します。検索ボタンをタップして検索を開始します。
	検索フィールドに入力したキーワードに関連する公開された接続を検索します。例えば「pa」を入力すると、「Paint」、「WordPad」、「Space」
	などが返されます。

オプションメニューを表示するには、接続をタップしてホールドします。

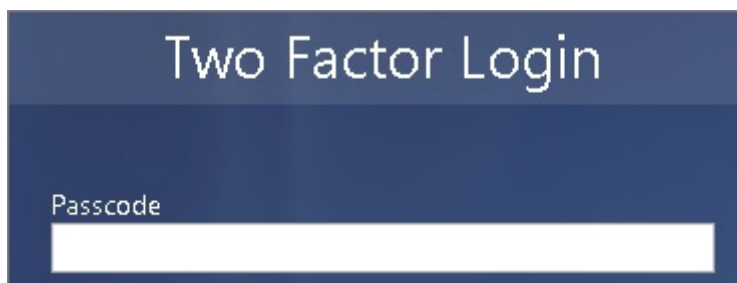


機能	説明
	接続を起動します。
	接続をお気に入りに追加します。

接続を検索するには、検索フィールドにキーワードを入力し、検索アイコンをタップします。この検索に基づいて、関連する接続が一覧表示されます。

## ■ 二要素認証のサポート

二要素認証が有効化されている Ericom Connect または PowerTerm WebConnect 6.0 環境に接続する場合、最初のパスワード・ログインの後に、第 2 要素を求めるダイアログが表示されます。



ユーザは、タイピングまたは「ペースト」機能を使用して、第 2 認証要素を入力できます。クリップボードにコピー済みの文字列をペーストするには、テキスト・フィールドをタップしてホールドしてペースト機能を使用するか、「ペースト」ボタンを使用します。

第 2 要素の認証に成功すると、リソースのリストが表示されます。認証が失敗した場合、再度認証を試みることができます。

## ■ 管理対象のアクセス許可

管理対象クライアントを使用する場合、AccessToGo アプリケーションで定義されている様々な設定は、コネクション・ブローカー (例: Ericom Connect) で定義されている設定によって上書きされます。例えば、デバイスとホスト間でのコピー/ペーストが Ericom Connect で設定されている場合、ローカル設定は適用されま

せん。このルールの例外は、デスクトップのサイズ/解像度です。ATG 設定は常に適用されるため、ユーザーは最適な設定を選択できます。

バージョン 9.x 以降では、Ericom Connect ブローカーで設定を行うと、アプリ内でローカルに保存されているパスワードは削除されます (「構成」 | 「設定」 | 「セカンダリ設定」または「テナント設定」 | 「パスワードの保存を許可」)。

---

## 4.3.8 設定

---

AccessToGo アプリケーションの設定を行うには、接続リスト画面で「設定」ボタンをクリックします。



利用可能な設定は、以下のカテゴリに分類されています:外観、ジェスチャ、言語とキーボード、接続、バージョン。

## ■ 外観

上部バーの有効化	接続時に、画面上側にツールバーを表示します。
常にバーを下に表示	接続時に、画面下側にツールバーを表示します。
タブレット回転時の全画面リサイズ	デバイスが自動回転をサポートしている場合にデバイスの向きが変わると、向きが変化した後の新しい解像度をサポートするために、AccessToGo はセッションに再接続します。この機能は、接続がフルスクリーン・モードである場合のみ動作します。
クリックアニメーションの有効化	オンにしている場合、ユーザが AccessToGo セッション内でシングル・クリックやダブル・クリック(長いシングル・タップ)を実行した際、アニメーションが表示されます。
フルスクリーン上でのリモート・マウス・モード	仮想キーボードが開いていない場合に、リモート・マウス・モード開きます(ユーザが画面上を移動できるようにするため)。
OS 通知バーを表示	AccessToGo 起動中、デバイス (iPad 等) の上部通知バーを表示します。





## 言語とキーボード

ユーザインターフェース言語	AccessToGo アプリケーションのインターフェース言語を変更します。
初期設定キーボードタイプ	ネイティブ・デバイスのキーボードまたは PC キーボードのキーボード・レイアウトを選択します。
拡張キーボード言語選択	AccessToGo で使用する PC キーボードの言語を選択します。
リモートキーボードで使用する言語	使用するキーボードの言語ロケールの地域を選択します。これは、リモート RDP セッションで 사용되는のと同じ言語に設定する必要があります。
キーボードのスキャンコードの使用	キーボードのスキャン・コード・モードを有効化します。この設定は、一部のオペレーティング・システムやアプリケーション向けに有効化する必要があります。デスクトップ・セッションまたはアプリケーションで文字入力ができない場合、この設定を有効化してみてください。
キーボードの自動表示	テキスト・フィールドにフォーカスした際に、自動的にキーボードを表示し、テキスト・フィールドを配置する機能を有効化/無効化します。

## 接続

デバイスとホスト間のコピー/貼り付けを有効にする	デバイスとホスト間のコピー/貼り付けを許可する機能を有効化/無効化します。
接続中断時の再接続	セッションの再接続を有効化するには、この設定をオンにします。
接続タイムアウト	このタイムアウト時間内に接続ブローカーへの接続が確立できない場合、AccessToGo は接続の試行を停止します。これは Ericom Connect にも当てはまります。
リモートコンピュータからの切断を確認	オンにすると、ユーザがセッションを切断しようとした際に、確認のプロンプトが表示されます。

## バージョン

製品のバージョン	バージョン番号とビルド
デバイス	デバイス ID
OS バージョン	オペレーティング・システムの種類とバージョン
利用可能 RAM	デバイスの利用可能な RAM
設定のリセット	アプリケーションの設定をデフォルトに戻します
デバック・ログ	Ericom のテクニカル・サポートにリクエストされた場合に有効化します
サポートの要請	※こちらを利用する場合は、弊社サポートセンターからご案内致しますので、それまでは設定不要で問題ありません。

## ジェスチャ

生産性を高めることを目的として、AccessToGo では手のジェスチャがサポートされています。サポートされているジェスチャは、特定の動作を実行するために設定することができます。

ジェスチャを変更するには、「設定」メニューに移動して、「ジェスチャ」をタップします。



「変更」ボタンをタップして、目的のジェスチャを変更します。



以下の画像は、デフォルトのジェスチャの設定を示しています。



アクティブ・セッション中にメニュー内の、「ジェスチャの設定」をタップすることで、ジェスチャを設定することもできます。



注意:

AccessToGo 3.5 以上を初めて開く際、2本指でのタップを新しいズーム機能として選択するためのプロンプトが表示されます。ズーム・ジェスチャを使用するには、「はい」をクリックします。



### 4.3.9 URL スキーム

URL スキームは、事前設定されたアプリケーションやデスクトップ・セッションを AccessToGo を使用して起動するために簡単な方法を提供します。URL スキーム「ericom」または「mrdp」を使用して、AccessToGo の接続を自動的に起動することができます。AccessToGo では URL スキームとして「ericom」を使用し、サブエディション (Blaze、Connect、WebConnect) では「mrdp」を使用します。構文は両方とも同じです。URL スキームで参照されている .rdp または .blaze 設定ファイルをユーザが選択 (またはクリック) すると、AccessToGo はその設定ファイルの内容に従ってセッションを起動します。



注意:

AccessToGo をすでに実行中に URL リンクをクリックすると、AccessToGo アプリケーションへの切り替えのみが起こります。リンク先で定義されている設定を読み込むために、URL を起動するには AccessToGo を実行していない状態でなければなりません。

URL スキームを使用して AccessToGo セッションを起動するには、以下の 3 つの方法があります:

1. HTTP/HTTPS を用いて .rdp または .blaze ファイルを起動する URL スキームを使用する (iOS と Android でサポートされています)。

例 (サブエディションを使用している場合は、「ericom」を「mrdp」に置き換えてください): `<a href="ericom://http://www.test.com/myconnection.rdp">Connect to RDP Demo from WWW </a>`  
`<a href="ericom://https://www.test.com/myconnection.blaze">Connect to Blaze Demo from WWW </a>`

2. デバイスの Ericom フォルダ内の .rdp または .blaze ファイルを起動する URL スキームを使用する (Android のみでサポートされています)。

例: `<a href="ericom://myconnection.rdp">Connect to RDP Demo from root folder </a>`

3. デバイスのサブ・フォルダから .rdp または .blaze ファイルを起動する URL スキームを使用する (Android のみでサポートされています)。

例: `<a href="ericom://sdcard/myconnection.blaze">Connect to Blaze Demo from subfolder </a>`

### .rdp ファイル または .blaze ファイルを作成する

AccessToGo で使用するために .rdp または .blaze ファイルを作成する最善の方法は、Ericom の Web サイトから Ericom Blaze Client をダウンロードすることです。Blaze Client を使用して接続をテストした後、「名前を付けて保存 (Save As)」の操作を実行して、設定を設定ファイルに保存します。.rdp または .blaze ファイルの任意の設定を構成するには、「設定ファイルのパラメータの定義」の表を参照してください。

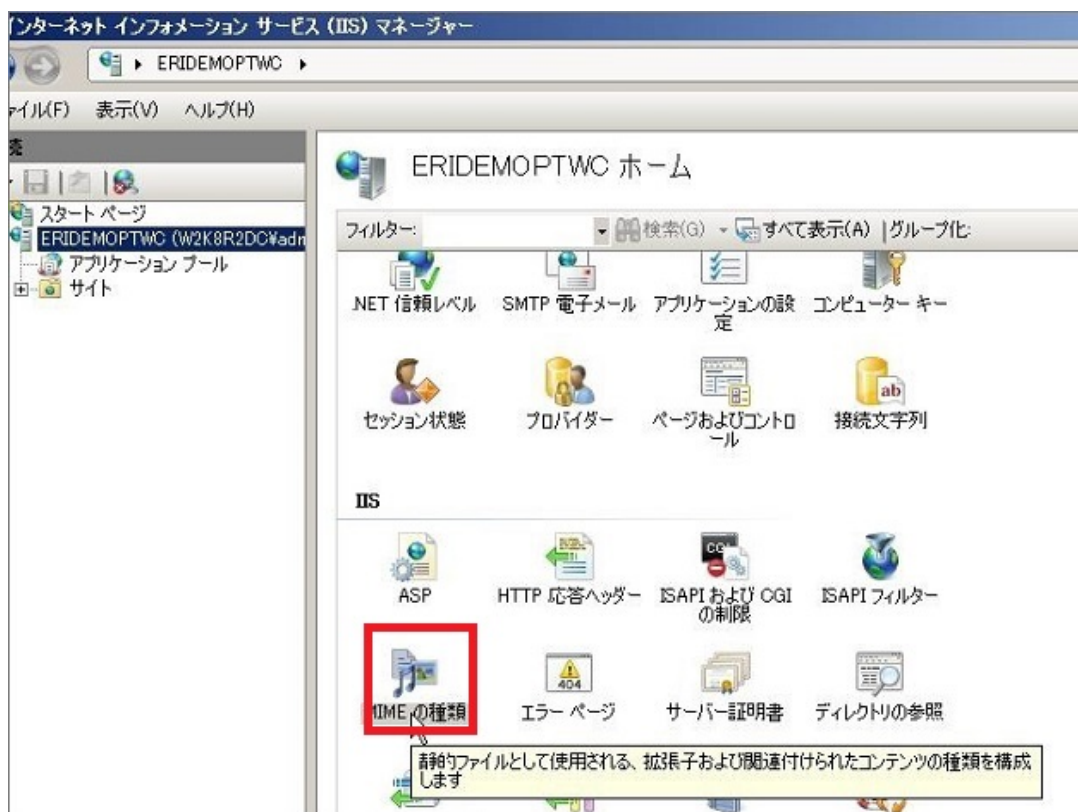
バージョン 8.1 以前ではパスワードを保存した .rdp または .blaze ファイルを、あるマシンから別のマシンに転送できませんでした。これは .rdp または .blaze ファイルが生成されたシステムにバインドされていることを確認するためのセキュリティメカニズムでした。8.2 から汎用的な .rdp または .blaze ファイルを作成し、始点以外のシステムで使用することが出来ます。これは URL スキームで使用するために保存されたパスワードを持つ .rdp または .blaze ファイルを公開するために必要です。汎用的なファイルを作成する

には、-generic-configuration パラメータを使用して Blaze.exe を起動します。次に、Blaze.exe を使用して URL スキームで使用される .rdp または .blaze ファイルを保存します。

## ■ MIME タイプを Web サーバに追加する

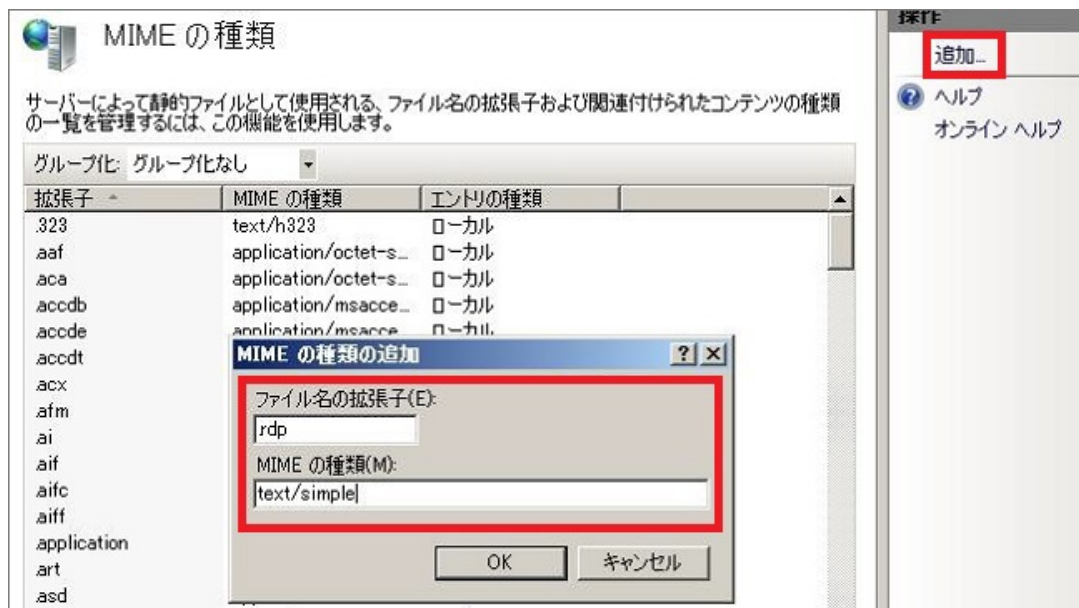
AccessToGo の URL スキームを使用するには、URL リンクをホストしている Web サーバに MIME タイプを追加する必要があります。以下は、Microsoft IIS 7 でこれを実行する方法です：

1. IIS マネージャに進み、「MIME の種類」を開きます。

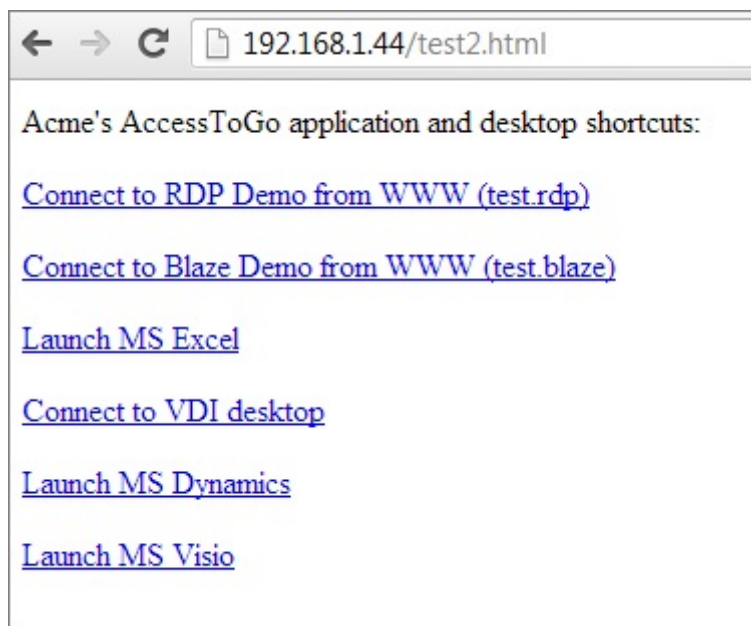


2. 「操作 | 追加」をクリックし、新しい MIME の種類を入力します。

- (a) ファイル名の拡張子: .rdp
- (b) MIME タイプ: text/simple
- (c) ファイル拡張子: .blaze 用にもう 1 つ作成します。



3. AccessToGo がインストールされているデバイスのウェブブラウザを使用して、構成済みのリンクを含む Web ページにアクセスします。そのリンクをクリックすると、設定済みのパラメータを使用して AccessToGo が自動的に起動します。



## 設定ファイルのパラメータの定義



一部の設定 (例: 印刷) は、AccessToGo では使用されていません。

注意:



パラメータ	タイプ	デフォルト	説明
alternate shell	s	なし	ターミナル・サービスのセッションで使用するシェルを設定します。これは、program.exe などの代替シェルを設定したり、ユーザがターミナル・サーバにログインした際に実行するアプリケーションを設定したりするために使用することができます。 サンプル値: c:temptest.exe
audiomode	i	2 (Blaze) 0 (AccessNow)	0: このコンピュータで再生する 1: リモート・コンピュータで再生する 2: 再生しない
auto connect	i	-	使用されていません。
autoreconnection enabled	i	1	接続が切断した際に再接続を試みます。
bitmapcachepersistenable		-	使用されていません。

パラメータ	タイプ	デフォルト	説明
connect to console	i	0	0: 仮想セッションに接続する 1: コンソール・セッションに接続する
desktopheight	i	600	セッションのデスクトップの高さ (ピクセル単位)
desktopwidth	i	800	セッションのデスクトップの幅 (ピクセル単位)
disable cursor setting	i	-	使用されていません。
disable full window drag	i	0: Blaze 1: AccessNow	1: セッションでのドラッグ操作中、ウィンドウの内容の表示を無効にする
disable menu animation	i	0	1: セッションにおけるメニューのアニメーションを無効化する
disable themes	i	0	1: セッションにおけるテーマの使用を無効化する

パラメータ	タイプ	デフォルト	説明
disable wallpaper	i	0	1: セッションにおける壁紙を無効化する
displayconnectionbar	i	1	1: フルスクリーン・セッションにおいて、接続バーを表示する
domain	s	-	1: フルスクリーン・セッションにおいて、接続バーを表示する
full address	s	-	サーバの IP アドレス/名前 (およびオプションのポート値) サンプル 値:192.168.1.1:3389
keyboardhook	i	2	標準的な Windows キーの組み合わせの適用先。 0: ローカル・コンピュータ上 1: リモート・コンピュータ上 2: フルスクリーン・モードのみ
maximizeshell	i	-	使用されていません。
password 51	b	-	使用されていません。

パラメータ	タイプ	デフォルト	説明
port	i	3389	使用されていません。
redirectcomports	i	-	使用されていません。
redirectdrives	i	-	使用されていません。 代わりに 「drivestoredirect」を 参照してください。
redirectprinters	i	0	0: リダイレクトし ない 1: セッションでクラ イアント・プリンタ をリダイレクトする 2: blaze 汎用プリン タ・ドライバを使用し てリダイレクトする
redirectsmartcards	i	0	1: セッションでクラ イアント・スマート・ カードをリダイレク トする (.NET のみ)。 現在は Linux バー ジョンのみです。
screen mode id	i	2	1: ウィンドウ 2: フルスクリーン
server port	i	-	使用されていません。

パラメータ	タイプ	デフォルト	説明
session bpp	i	32	すべてのオプションがサポートされています:8、15、16、24、32。
shell working directory	s	-	代替シェルを指定している場合の作業ディレクトリ: サンプル値: c:temp
smart sizing	i	-	使用されていません。
username	s	-	ログインに使用するユーザ名 サンプル値: administrator
winposstr	s	-	使用されていません。
allow font smoothing	i	1	1: フォント・スムージングを有効化する
redirectclipboard	i	1	0: 無効 1: 有効
prompt for credentials	i	0	0: 無効 1: 有効

パラメータ	タイプ	デフォルト	説明
session sharing	i	1	0: 無効 1: 有効
connection type	i	6	1: モデム 2: 低速 3: サテライト 4: 高速 5: WAN 6: LAN
drivestoredirect	s	-	リダイレクトするドライブ: ローカル・ディスク (C:): CD-ROM/DVD Drive (D:)
dirstoredirect	s	-	リダイレクトするフォルダ: 「デスクトップ」、「マイドキュメント」(および Windows 以外の「メディア」フォルダ)。
use multimon	i	0	0: 現在の値 1: マルチモニタを使用する 2: マルチモニタに拡張する #: # 枚のモニターを使用する

パラメータ	タイプ	デフォルト	説明
remoteapplicationmode	i	1	使用されていません。
allow desktop composition	i	2	使用されていません。
compression	i	-	使用されていません。
disable cursor setting	i	-	使用されていません。
bitmapcachepersistenable		-	使用されていません。
redirectposdevices	i	-	使用されていません。
authentication level	i	-	使用されていません。
negotiate security layer	i	-	使用されていません。
gatewayhostname	s	-	使用されていません。
gatewayusagemethod	i	-	使用されていません。
gatewaycredentialssource		-	使用されていません。
gatewayprofileusagemethod		-	使用されていません。

---

パラメータ	タイプ	デフォルト	説明
promptcredentialonce	i	-	使用されていません。
audiocapturemode	i	-	使用されていません。
videoplaybackmode	i	-	使用されていません。
use redirection server name	i	-	使用されていません。

- Ericom パラメータ



パラメータ	タイプ	デフォルト	説明
blaze version	s	-	バージョン番号 サンプル値:2.1
blaze acceleration	i	1	0: 無効 1: 有効
blaze image quality	i	40	Blaze の品質 (100 – ロスレス、95 – 最高 度、75 – 高度、40 – 良、20 – 並 )。
Blaze password	s	-	暗号化されたパス ワード
html password	s	-	暗号化されていない パスワード
wc password	s	-	CryptUnprotectData を使用して復号化し ます。
x password	s	-	XTEA を使用して復 号化します
Use Ericom Secure Gateway	i	0	0: 無効 1: 有効
Use Secure Gateway	I		
		1750	0: 無効 1: 有効

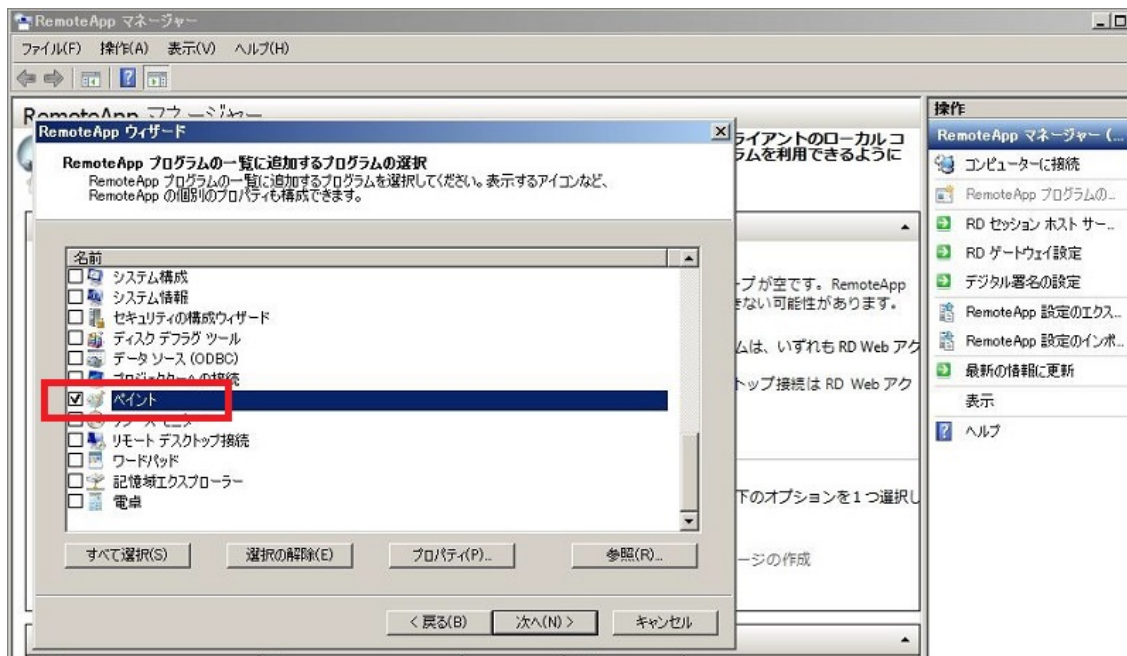
以下の設定は、スクリーンショット実行時の制御で使用されます。

パラメータ	タイプ	デフォルト	説明
atg screen capture blocking (Android)	i	0	(1: 有効、0: 無効) これは、Android デバイス上でのスクリーン・キャプチャを制御します。有効にした場合、スクリーン・キャプチャは取得できません。また Android 端末上にキャプチャできなかったという Android が発行するメッセージが表示されます。パラメータの記載が無い場合、またはパラメータの値が Null の場合、ともにスクリーンショットは取得可能となります。
atg screen capture notification (iOS)	i	0	(1: 有効、0: 無効) これは、iOS デバイス上でのキャプチャ通知を有効/無効にします。
atg screen capture notification text (iOS)	s	-	これは、スクリーン・キャプチャが検出された後にユーザに表示するテキストです。日本語メッセージを表示するには、設定ファイル (.blaze ファイル) を UTF-8 で保存する必要があります。atg screen
		177	capture notification (iOS) で 1 が指定されていても、このパラメータが指定され

## URL スキームを使用してアプリケーションを起動する

ターミナル・サーバ/リモートデスクトップ・サーバからアプリケーションのみを起動するために URL スキームを使用する場合、目的のアプリケーションを「RemoteApp プログラム」リストに追加します。

以下の画像は、MS ペイントを許可されたアプリケーションリストに追加する方法を示しています：



.rpd または .blaze ファイルで、以下のパラメータが設定されていることを確認します：

- remoteapplicationmode:i:1
- alternate shell:s:mspaint
- (オプション) shell working directory:s:

## URL スキームを介してスクリーンショットをブロックする (Android)

URL スキームを介して Android 版 AccessToGo (8.1.2 以上) を起動した場合、スクリーンショットの操作をブロックするよう指定することができます。スクリーンショットのブロックを有効化するには、.blaze ファイルに atg screen capture blocking を追加して有効にします。

ユーザが AccessToGo (Android) アプリケーションで標準のスクリーンショット操作を実行すると、スクリーンショット操作がブロックされていることを示すメッセージが表示されます。このメッセージはオペレーティング・システムにより生成されるものであるため、設定変更することはできません。

## スクリーンショットについてアプリケーションに通知する (iOS)

iOS 版 AccessToGo (8.1.2 以上) では、スクリーンショット操作が実行された際に Web サーバへ通知を送信する機能をサポートしています。AccessToGo は、利用可能なパラメータ (通常は時間とデバイスのアドレス等) を Web POST を使用してサーバ・アドレスとポートに送信します。URL の構文は次の通りです (HTTPS または HTTP)：

**https://host:port/page?param1=value1&param2=value**

(URL の末尾に"?"をつけ、その後にパラメータを記述します)

POST を作成する場合

- URL のデータ部分が body に送信されます。
- データ以外の部分は header に送信されます。

スクリーンショット操作が実行された際、.blaze ファイル内のパラメータの atg screen capture url で指定された URL に対し、次の内容で Web POST されます。

- 指定 URL の 先頭のスキーム名 (http または https) から "?" までが Web POST 先の URL (Request ヘッダー) となります。
- 指定 URL の パスにおいて "?" で連結されたパラメータ部があれば、最初に登場した "?"以降が Web POST の Body 部パラメータとなります。

また、指定されたパラメータの他に、次の 2 つのパラメータが追加されます。

- LocalTime . . . iOS デバイスのタイムスタンプ
- Product . . . ATG バージョン情報

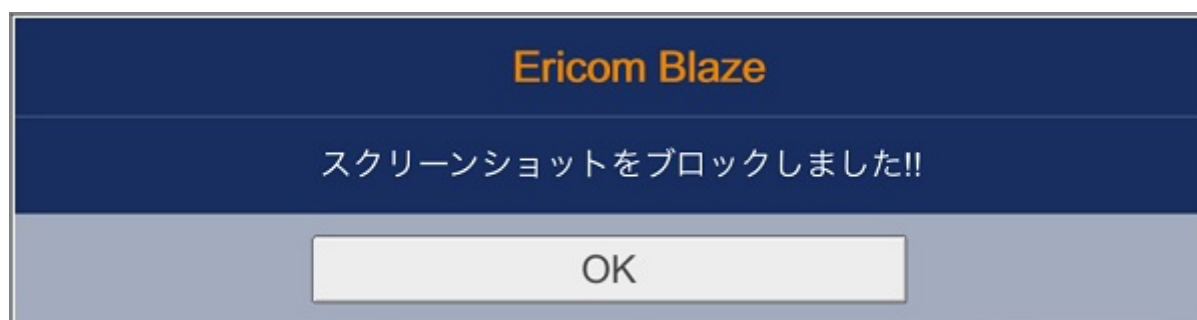
ユーザが LocalTime と Product の取得内容をカスタマイズするための仕組みはありません。

この機能は、Blaze または RDP ファイルの 3 つの設定を使用して設定します:

- atg screen capture notification:i:1
- atg screen capture notification text:s:
- atg screen capture url:s:

ユーザが AccessToGo(iOS) アプリケーションで標準のスクリーンショット操作を実行すると、「atg screen capture notification text」に定義されたテキストのメッセージが表示されます。

例えば、次のように設定します: atg screen capture notification text:s:スクリーンショットをブロックしました!! スクリーンショットをキャプチャしようとしたときにこのメッセージを表示します。



日本語メッセージを表示する場合は Blaze または RDP ファイルを UTF-8 フォーマットで保存する必要があります。

## 4.3.10 テクニカル・サポート

### 接続の確認

接続上の問題が発生している場合、AccessToGo アプリケーションと RDP ホスト間のすべてのファイアウォールで適切なポートが設定されていることを確認してください。

RDP:3389

Blaze:8080 (3.x 以前のバージョンでは 3399)

Secure Gateway:443

アドレスとポートの接続を確認するには、デバイスに Telnet アプリをダウンロードして、ターゲットのアドレスとポートへの接続を試みます。「Connection Refused」メッセージが返される場合、接続は利用できない状態となっています。

### URL スキームが機能しない

URL スキームで AccessToGo が起動するものの、設定済みのパラメータを使用して接続が行われない場合、以下を確認してください:

- AccessToGo がすでに実行されていない
- RDP ファイルで定義されている RDP ホストのアドレス (DNS 名がデバイスで正しく解決できることを確認してください)。
- Ericom Blaze Client(無料ダウンロード) を使用して、背邸ファイル (.rdp または . blaze) を再作成します。これにより、すべてのパラメータが正しく定義されます。入力ミスがある場合、ファイルが無効になります。

### RDP SSL を無効にする

Access Server には、RDP ホスト上で有効にするためのネイティブ RDP へのアクセスが必要です。このため、RDP Security Layer を SSL へ変更しないでください。RDP Security Layer の設定は変更せず、ビルトインの AccessNow SSL 暗号化または Secure Gateway を使用して SSL 暗号化を追加します。



## PTWC や ESG での SSL 認証エラー

Ericom Connect または PowerTerm WebConnect (PTWC) へのアクセス用に Ericom Secure Gateway と AccessToGo を使用する場合、信頼された証明書を ESG にインストールするのが一般的です。サードパーティのプロバイダが発行する信頼された証明書をリクエストする場合、カスタム CSR をプロバイダに送信する必要があります。

AccessToGo を適切にサポートするには、CSR を作成する際に以下を設定します:暗号化サービスプロバイダ (CSR) の「詳細」セクションで、「秘密鍵」のオプションを変更します。デフォルトでは、これは「Microsoft Strong Cryptographic Provider (Signature)」に設定されています。これを、「Microsoft RSA SChannel Cryptographic Provider (Encryption)」に変更します。



CSR が適切に設定されていない場合、イベント・ビューアに「The client and server cannot communicate, because they do not possess a common algorithm」(共通アルゴリズムがないため、クライアントとサーバが通信できません) というエントリが表示されます。このエラーが表示された場合、ESG 用に新しい証明書を生成する必要があります。

## タブレットモード (上部バー) を使用できない

AccessToGo は 5.5 インチのディスプレイの場合にデバイスをタブレットとみなします。古い AccessToGo iOS バージョンではデバイス名が「iPad」の場合にタブレットモードが有効になりました。v8.1.2 以上の AccessToGo iOS では起動時に、5.5 インチ (またはそれ以上) のディスプレイの場合にタブレットモードを有効にします。



## 第 5 章

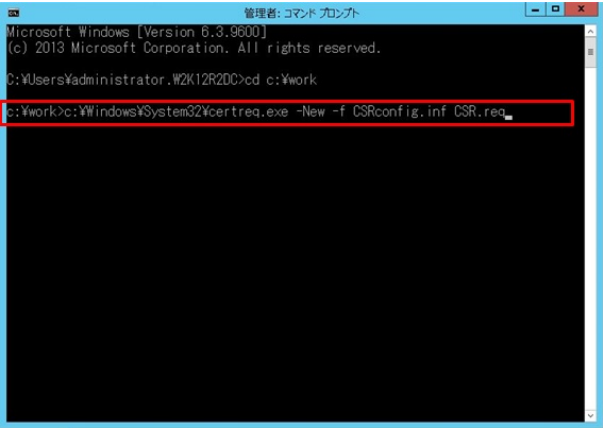
# APPENDIX

## 5.1 Ericom Secure Gateway の CSR 作成

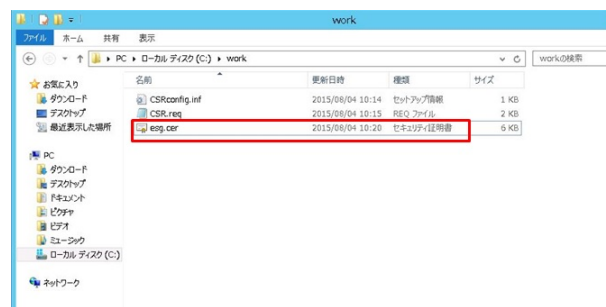
### **5.1.1 CSR の作成と証明書のインストール**

---

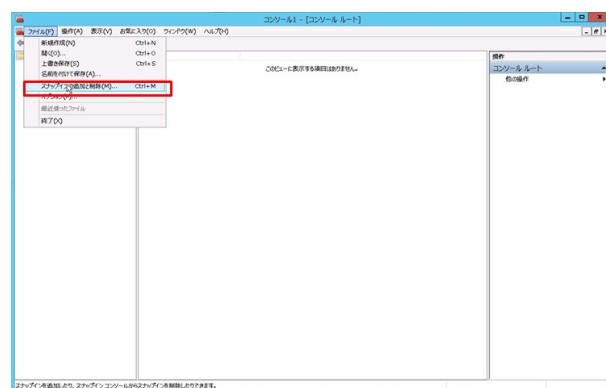
ESG サーバ上で証明書発行に必要な CSR の作成と、証明書のインストールを実施します。

<p>1. CSR 発行用の inf ファイルを作成します。本資料では ESG サーバ上に c:\work\CSRconfig.inf として作成し、保存しています。</p> <p>※ Subject および Extentions の dns は環境に合わせて変更してください。</p> <p>※ CSR の Subject 属性の中で「O=XXXXX Co.,Ltd.」のようにカンマを含む値を記述して CSR を作成すると証明書が発行されない場合があります。</p> <p>カンマ記号を利用する場合は以下のように CSR の記述を変更して下さい。</p> <ul style="list-style-type: none"> <li>・ Subject 属性の値の中の各要素を区切る文字をカンマからセミコロン (;) に変更</li> <li>・ Subject 属性の直後の行に「X500NameFlags = 0x40000000」の記述を追加</li> </ul>	<pre>[NewRequest] Subject = "C=JP,ST=Tokyo,L=Chiyoda-ku,O=K.K.Ashisuto,CN=esg.ashisuto.co.jp" Exportable = TRUE Hashalgorithm = sha256 KeyLength = 2048 KeySpec = 1 KeyUsage = 0xA0 MachineKeySet = True ProviderName = "Microsoft RSA SChannel Cryptographic Provider" ProviderType = 12 RequestType = PKCS10  [EnhancedKeyUsageExtension] OID=1.3.6.1.5.5.7.3.1  [Extensions] 2.5.29.17 = "{text}" _continue_ = "dns=esg.ashisuto.co.jp&amp;"</pre>
<p>2. c:\windows\certreq.exe を利用し、CSR の発行を行います。</p> <p>コマンド例&gt;</p> <pre>c:\windows\system32\Certreq.exe -New -f CSRconfig.inf CSR.req</pre>	

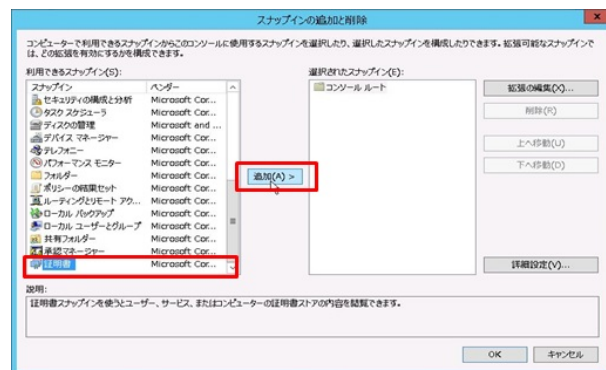
3. 作成した CSR を認証局へ送り署名をしてもらいます。署名済みの証明書を受け取ったら ESG サーバの適当なフォルダへ証明書を配置し、次の手順へすすみます。

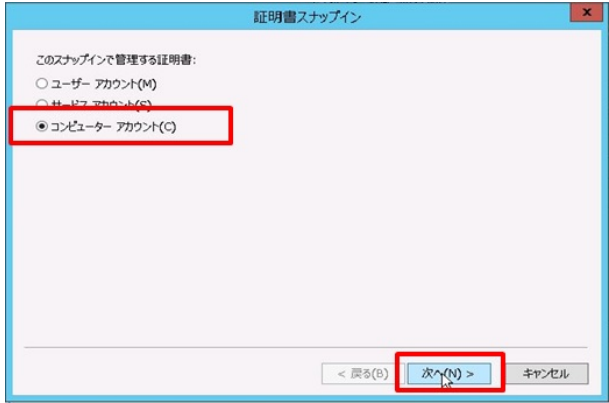
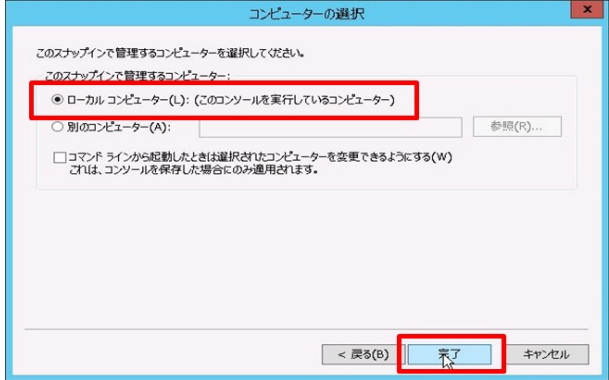
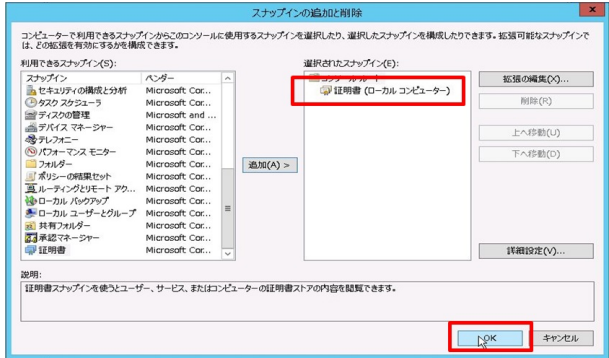


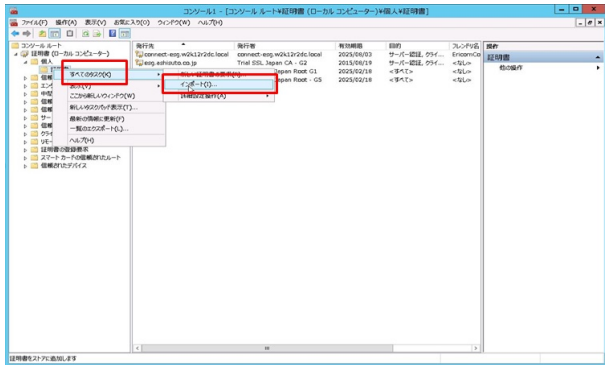
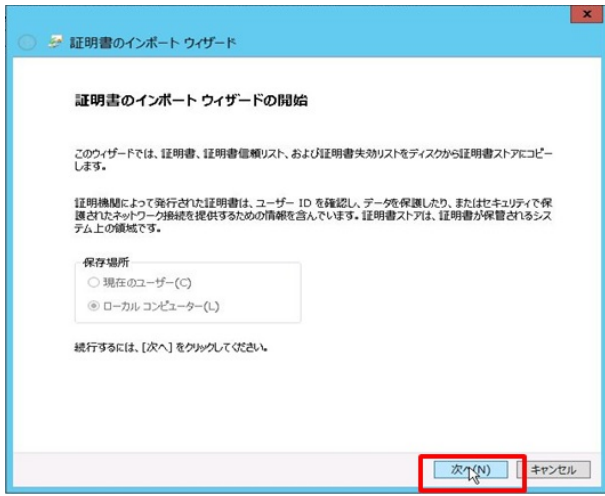
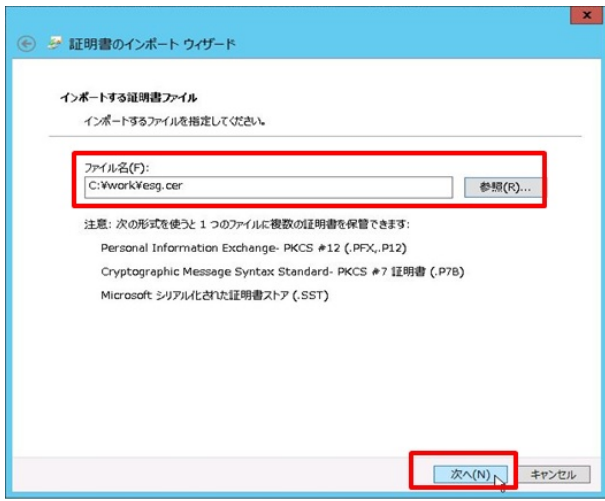
4. MMC を起動し、「スナップインの追加と削除」をクリックします。



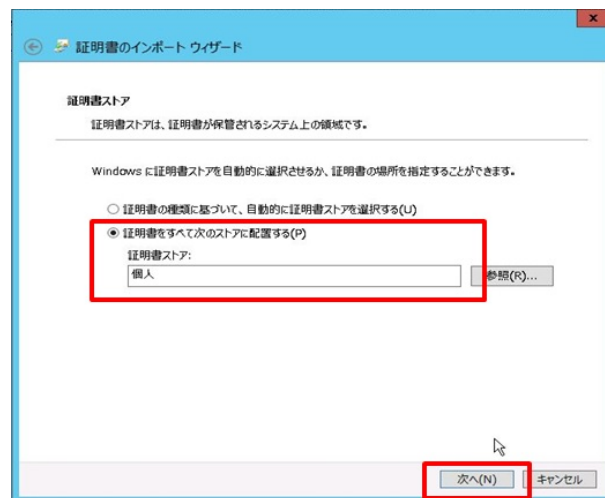
5. 「証明書」を選択し「追加」をクリックします。



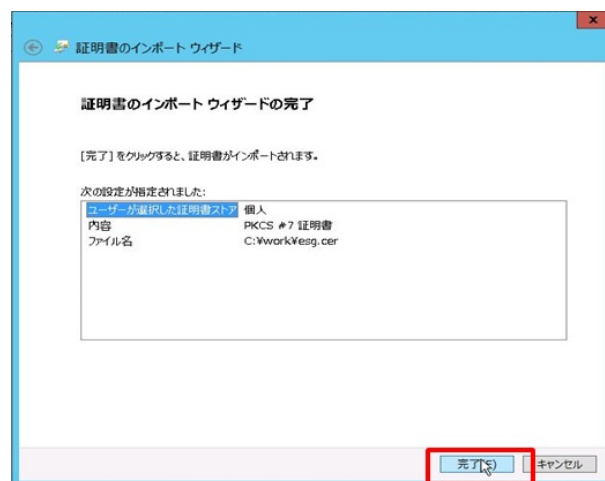
<p>6. 「コンピューターアカウント」を選択し「次へ」をクリックします。</p>	
<p>7. 「ローカルコンピューター」を選択し「完了」をクリックします。</p>	
<p>8. 「証明書 (ローカルコンピューター)」が表示されたことを確認し、「OK」をクリックします。</p>	

<p>9. 「個人」 - 「証明書」を右クリックし、「すべてのタスク」から「インポート」をクリックします。</p>	
<p>10. 「証明書のインポートウィザード」が起動したら [次へ] クリックします。</p>	
<p>11. [参照] をクリックし、「ファイル名」に発行された署名済み証明書のパスを設定して [次へ] をクリックします。</p>	

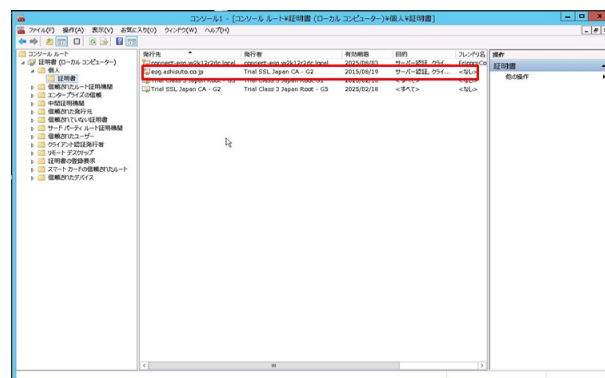
12. 「証明書ストア」に「個人」が表示されていることを確認し、[次へ] をクリックします。



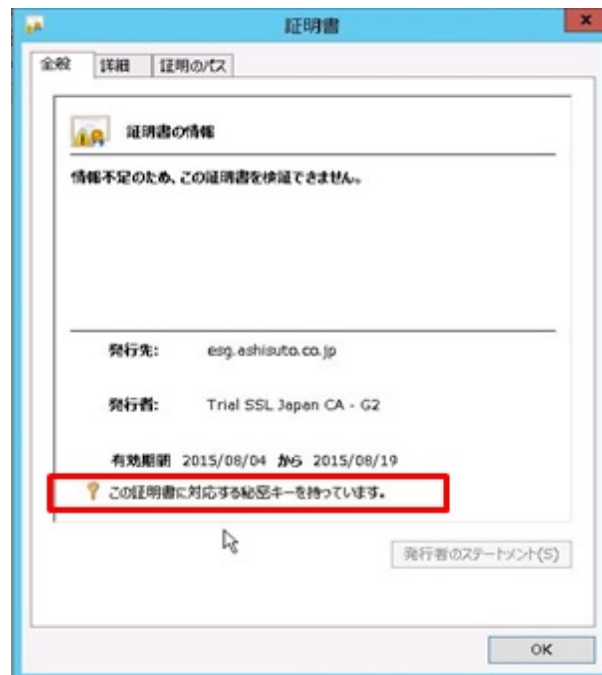
13. [完了] をクリックします。



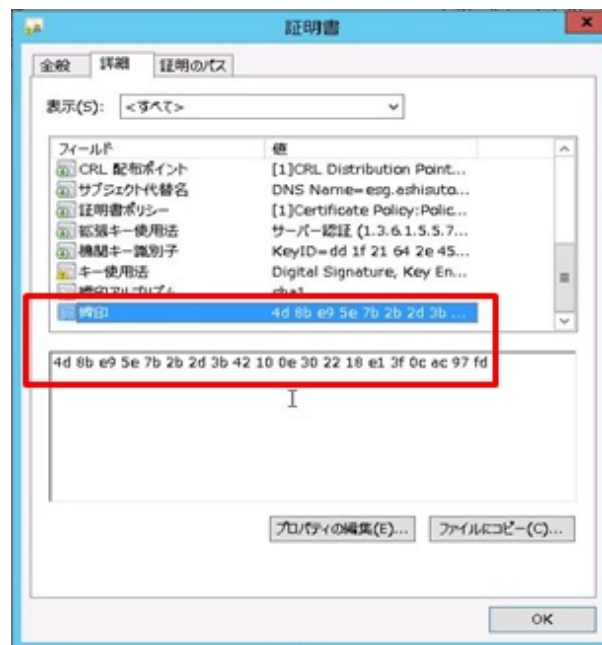
14. 証明書がインポートされたことを確認します。



15. 証明書をダブルクリックし、秘密鍵が存在することを確認します。



16. 「詳細」タブを開き、「拇印」の文字列を確認し、控えておきます。





作成した証明書を Ericom SecureGateway に適用する手順は「Secure Gateway 管理者ガイド」- 「ポートと SSL 証明書 (ページ 78)」を参照してください。

**Tips:**



## 5.2 Blaze Client / AccessNow 利用時のエラー

Blaze Client やブラウザ (AccessNow) からの AccessServer へのログイン時、また、公開アプリケーションや公開デスクトップへの接続時にエンドユーザに表示されるエラーを記載しております。



**注意:**

ご利用の Blaze Client や AccessServer のバージョンによって、表示されるメッセージが異なる場合があります。下記はエンドユーザに表示されるエラーの一部となりますので、下記以外のエラーが表示されることもあります。下記にないエラーが表示され Blaze Client や AccessServer の利用ができない場合は、弊社サポートセンターへお問い合わせください。

内容	Blaze	AccessNow
接続ユーザー名が間違っている場合	Your Username or Password are either incorrect or expired. If this problem persists, please contact your system administrator - (error 0x22)	The remote host requires (NLA) Network Level Authentication. Please make sure that Username and Password are entered
接続ユーザのパスワードが間違っている場合	Your Username or Password are either incorrect or expired. If this problem persists, please contact your system administrator - (error 0x22)	Your Username or Password are either incorrect or expired. If this problem persists, please contact your system administrator - (error 0x22)
AD がダウンしている場合	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator

ADのユーザーが無効化されている場合	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator
ADのユーザオブジェクトのパスワードがブランクの場合	The remote host requires (NLA) Network Level Authentication. Please make sure that Username and Password are entered	The remote host requires (NLA) Network Level Authentication. Please make sure that Username and Password are entered
(AccessServerのOSが参照している)DNSサーバがダウンしている場合	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator	Your Password is either expired or must be changed before logging on the first time. Please update your password. If this problem persists, please contact your system administrator
AccessServer サービスがダウンしている場合	Unable to connect to Ericom Access Server 「<AccessServer アドレス:3399>」	※ AccessNow ログイン画面へアクセスできない。
ClientPC - AccessServer間で必要なポートで疎通できない場合	Unable to connect to Ericom Access Server 「<AccessServer アドレス:3399>」	※ AccessNow ログイン画面へアクセスできない。

---

AccessServer の証明書が破損している場合	Unable to connect to Ericom Access Server 「<AccessServer アドレス:3399>」	※ AccessNow ログイン画面へアクセスできない。
AccessServer ライセンスが期限切れの場合	Licensing Error : Check with your System Administrator (Error code:BLZ-10)	Licensing Error : Check with your System Administrator (Error code:AN-10)

## 5.3 サポートポリシー

### 5.3.1 対象製品（アクセスプロダクトの定義）

このルールについては以下の 4 製品にのみ適用対象となります。

- PowerTerm WebConnect
- Connect
- Blaze
- AccessNow

### 5.3.2 バージョンレベルの定義

以下の三種類のバージョンレベルのリリースがあります。各バージョンレベルがリリースされると、赤字の番号が更新されます。

- メジャーバージョンレベル：x .x.x
- マイナーバージョンレベル：x. x .x 機能拡張と不具合修正が含まれます
- サービスリリースレベル :x.x. x 不具合修正リリースのみが含まれます

### 5.3.3 リリースとサポートの前提

- Ericom 製品 アクセスプロダクトは約 3 ヶ月に 1 回のサイクルでマイナーバージョンが、約 1 年に 1 回のサイクルでメジャーバージョンがリリースされます。
- 正式リリースの案内は、パートナーメルマガ/パートナー Web/当ページおよび Ericom 製品オンラインドキュメントのサポート状況一覧/サポートメルマガにて告知します。

### 5.3.4 サポートポリシー

- **EOS (End of Support)**

- 問合せは対応はマイナーバージョンリリース後 5 年間受け付けます。この日付以降は開発元である Ericom 社への問い合わせや調査協力が要請できなくなり、アシストで保有するナレッジからの回答のみの提供になります。
- 不具合に対しての修正は最新バージョンに対してのみに提供されます。上位バージョンにバージョンアップすることで著しい不都合が生じる場合は、サービスリリースが作成される可能性があります。

### 5.3.5 コンポーネント間のバージョン互換性

- Ericom 製品では、バージョン互換性をコンポーネント単位でサポートしています。
- 各製品におけるコンポーネントは、可能な限り同一バージョンをご利用いただくことを推奨します。
- 互換性の対象製品は Ericom Connect および Blaze となります。
- Ericom 製品は、ver.8.0 以降で後方互換がサポートされます。
  - － 例: AccessPad 8.0 利用時に Connect Server 8.2 への接続をサポート
  - － 例: Blaze Client 8.1 利用時に Access Server 8.2 への接続をサポート
- Ericom 製品は、ver.8.5 より前方互換および後方互換をサポートします。
  - － 例: RemoteAgent 8.5 利用時に Connect Server 8.0 への接続をサポート
  - － 例: Blaze Client 8.5 利用時に Access Server 8.1 への接続をサポート
- Ericom 製品は、同一メジャーバージョン間であれば、マイナーバージョンが異なるコンポーネントを組み合わせる利用することがサポートされます。
- Ericom 製品 ver.9.0 および 9.1 においても 8.x との互換性がサポートされています。<sup>\*1</sup>

コンポーネントとは Ericom Connect の場合、以下の 3 つを指します。

- Connect Server
- RemoteAgent
- AccessPad

[注記] Client Web Service, Admin Web Services, RemoteAgent Web Service, Ericom Connect Secure Gateway は Connect Server に含まれると見なすため、Connect Server と同一のバージョンを利用していることが前提となります。



参考:

Ericom Connect で利用している TSAgent および Access Server については RemoteAgent に含まれていると見なすため、RemoteAgent と同一のバージョンを利用していることが前提となります

Blaze の場合、以下の 2 つを指します。

- Access Server
- Ericom Blaze Client

### 5.3.6 販売ポリシー

- 新規購入時はアシストのリリース最新バージョンが提供されます。
- 追加購入時はリリース後 5 年以内であれば現利用バージョンと同一を提供します。

<sup>\*1</sup> 例外として RemoteAgent 9.0(Type1) から Connect Server 8.0/8.1/8.2/8.5 への接続は未サポートとなります。

### 5.3.7 サポート状況一覧

製品	バージョン	EOS (End Of Support) *3
Blaze	2.2	2014年11月1日
	2.5	2014年11月1日
	3.1	2019年1月23日
	3.2	2019年3月27日
	3.4	2019年8月12日
	7.0	2020年4月1日
	7.1	2020年6月22日
	7.2	2020年9月1日
	7.3	2020年11月16日
	7.5.1	2021年3月24日
	7.6	2021年11月16日
	7.6.1	2021年11月16日
	8.0	2022年4月27日
	8.1	2022年7月5日
	8.2*2	2022年10月25日
	8.5	2023年9月5日
	9.0	2023年11月14日
	9.1	2024年1月15日
	9.2	2025年3月10日
	9.4	2025年10月18日
	9.5	2026年2月5日

## 5.4 サポート / お問い合わせ先

### 5.4.1 アシスト サポートセンター

サポートセンターでは Ericom 製品に関する技術的なご質問にお答えしております。ご利用に際しては、お手元のサポート契約書類をご確認いただき、サポート ID をご準備の上、書類に記載されたお問い合わせ先へご連絡願います。

\*3 この日付以降は開発元である Ericom 社への問い合わせや調査協力が要請できなくなり、アシストで保有するナレッジからの回答のみの提供になります。

\*2 Ericom Blaze 8.2 はダブルブラウザソリューション環境でのみ提供されています。

## 製品お問い合わせ時のテンプレートご利用のお願い



お願い:

E-mail、Ashisuto Web Support Center(AWSC) よりお問い合わせいただく際は、ご契約時に送付させていただきました資料に記載されております問い合わせテンプレートを是非ご利用ください。問題の早期解決とお客様環境情報把握を目的としております。全てにご記入いただく必要はございませんが、不足している情報については、サポート対応の中で随時確認させていただきます。

## Ashisuto Web Support Center(AWSC) アカウント登録のお願い



お願い:

弊社では Ashisuto Web Support Center(AWSC) をご用意しており、Web からのお問い合わせや、お客様に有益な技術情報の提供も行っております。主に下記のようなコンテンツをご利用いただけます。

- Web からのご質問のご登録と更新、履歴管理
- 製品技術ナレッジ (FAQ) の参照
- 技術ドキュメントの参照

AWSC サイトでは、現在いただいているお問い合わせのステータス管理や過去お問い合わせの履歴参照等の仕組みをご用意しております。AWSC サイトをご利用いただく際には、アカウント (AID) の登録が必要です。1つのサポート ID に対して AID の登録数制限はございませんので、複数人でアカウントを作成いただき、関係者間での情報共有基盤としてもご利用いただけます。また、FAQ や技術資料は、毎月更新され、お客様が製品を最大限ご活用いただけるように積極的な情報提供を行っておりますので、是非 AWSC サイトにて AID をご登録の上、ご利用ください。

AWSC のご利用は、下記サイトより AID を作成の上、ご利用ください。

- AWSC ログインに必要な AID の作成、AWSC ご利用方法について  
[https://www.ashisuto.co.jp/support/awsc\\_entry.pdf](https://www.ashisuto.co.jp/support/awsc_entry.pdf)
- AWSC ログインについて <https://support.ashisuto.co.jp/>

## 5.4.2 ライセンス発行、見積、契約に関するお問い合わせ窓口

ライセンスや追加ライセンスご検討時の見積、ご契約内容の照会等につきましては、下記窓口を別途用意しておりますので、こちらをご利用ください。

- ライセンスの新規発行、再発行窓口 ライセンスキーの発行 (再発行) に関しては、下記窓口までご連絡ください。

[eri\\_key@ashisuto.co.jp](mailto:eri_key@ashisuto.co.jp)

- ライセンス追加のご検討やお見積に関する窓口

[sk\\_info@ashisuto.co.jp](mailto:sk_info@ashisuto.co.jp)

- ご契約内容、保守契約期間や費用に関するお問い合わせ窓口

担当営業、もしくは弊社サポートセンターまでお問い合わせください。

### 5.4.3 Ericom 製品向けサポート用ログ収集スクリプト

サポートセンターでは調査を円滑に進めるために Ericom 製品を利用する環境向けにログ収集 Powershell スクリプトを用意しております。サポート問い合わせを行う際に、事前に取得いただくと調査を円滑に進めることが可能となります。

- 対象製品

- Ericom Connect 8.1 以上
- Ericom AccessNow 8.1 以上
- Ericom Blaze 8.1 以上
- ダブルブラウザ連携キット (WBrowserLauncher 8.1 以上、KOTOMINE 1.3 以上)

- 対応 OS

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019
- Windows 10

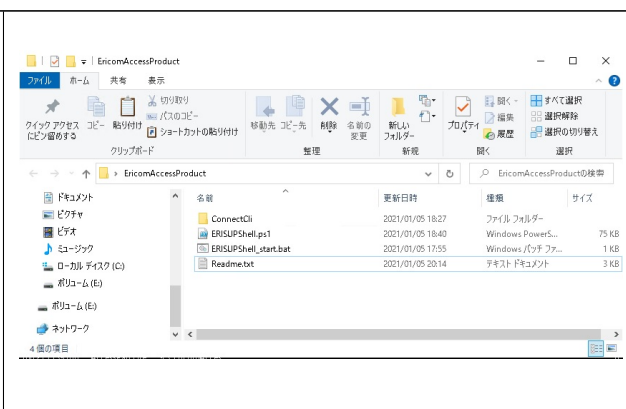
- ダウンロード こちらよりダウンロードください。

※利用方法については、ダウンロードした ZIP に Readme.txt が含まれております。

以下、ログ採取スクリプトの利用手順となります。

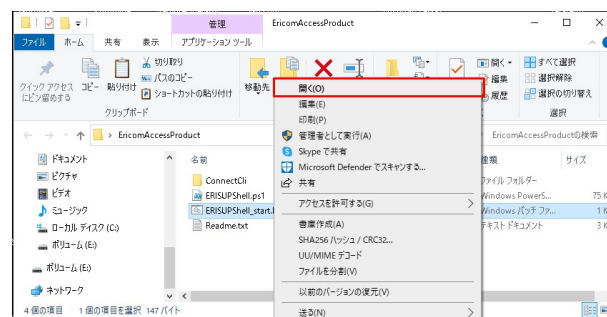
1. ダウンロードした ZIP ファイルを任意の場所に保存して解凍します。

ZIP より解凍した EricomAccessProduct フォルダを開きます。





2. ERISUPShell\_start.bat を右クリックして「開く」をクリックします。



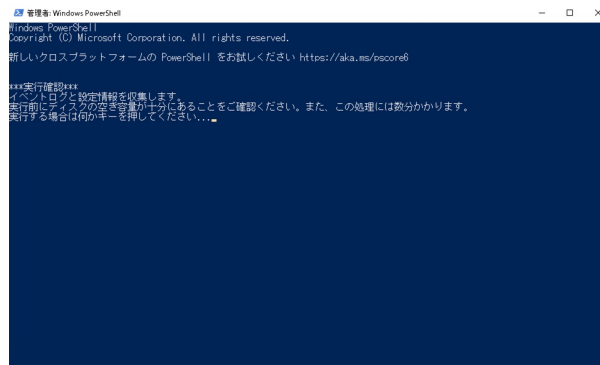
3. 別ウィンドウにて「ERISUPShell.ps1」が実行された際に、以下のような「ユーザアカウント制御」の確認画面が表示された場合には「はい」を選択して処理を進めてください。



※実行ユーザに管理者権限がない場合には、以下のような画面が表示されます。管理者権限を持つユーザ名とパスワードを入力して「はい」を選択して処理を進めてください。



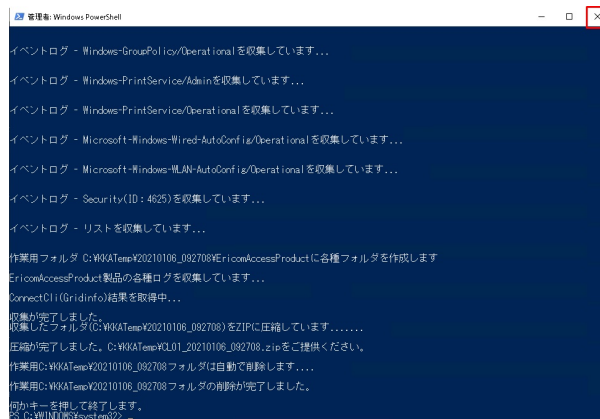
4. 別ウィンドウにて「ERISUPShell.ps1」が実行されると以下のメッセージが表示されます。「何かのキー」を押してログ収集を開始してください。



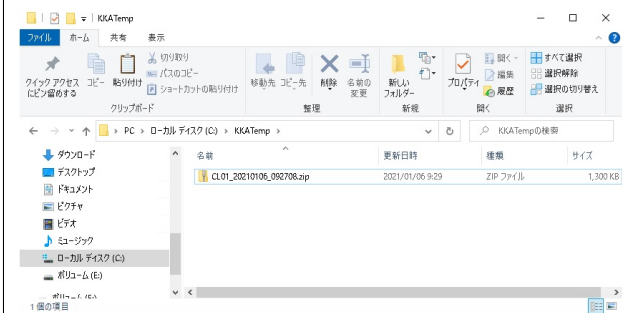
※ログ収集中は以下のような画面となります。



6. ログ収集が完了すると以下のようなメッセージが表示されます。「何かのキー」を押してログ収集を終了してください。Powershell ウィンドウは自動で閉じませんので「×」で閉じてください。



7. 収集された [C:KKATemp ホスト名\_実行日時 (YYYYMMDD\_hhmmss).zip] をアシストサポートセンターへご提供ください。



## 第 6 章

# 法律に基づく告知および免責事項

本ドキュメントは、明示的かつ適切に認められたユーザを支援することのみを目的としたもので、株式会社アシスト（以下「当社」）により随時、変更または撤回されることがあります。

本ドキュメントの所有権は 当社および各製品のメーカー各社に属します。

当ドキュメントに記載されているソフトウェアおよびドキュメント自体は、ライセンス契約の下で提供されています。各社の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、複製、開示、変更することはできません。

ここに記載されている情報は、告知なく変更されることがあり、「現状のまま」として提供され、誤りがないことを保証されていません。

ここで挙げられている例の一部は、例示のためのみにて提供され、特に記載のない限り架空のものです。実際の関係や関連性について推測されるもの、または推測されるべきものではありません。

当ドキュメントからリンクやバナーなどによって他のサイトに移動された場合、移動先サイトで提供される情報、サービス等について一切の責任を負いません。

Ericom<sup>®</sup>、Ericom Connect<sup>®</sup>、PowerTerm<sup>®</sup> は、Ericom Software の登録商標（米国）です。Ericom Blaze<sup>™</sup>、Ericom AccessNow<sup>™</sup>、Ericom AccessToGo<sup>™</sup>、Ericom Shield<sup>™</sup>、PowerTerm WebConnect<sup>™</sup> は、Ericom Software の商標です。その他の名称はそれぞれの所有者の商標である場合があります。