Ericom Connect®

バージョン 7.6.1

目次

目次 2

1 はじめてみる 16

1.1 Ericom Connect®とは? 16

先進のグリッド・アーキテクチャ 16

簡単なエンドユーザ・アクセス 18

Web ベースの管理 18

強力な起動分析(Launch Analysis) 19

役割ベースの分類 19

ビジネス・インテリジェンス 20

1.2 要件 20

1.2.1 SQL データベース 20

1.2.2 Active Directory 22

1.2.3 デスクトップ/セッション ホスト 22

1.2.4 Windows 2008 R2/2012 R2 23

1.2.5 信頼された証明書 23

1.2.6 DNS とポート 24

1.3 インストーラの使用 26

1.3.1 プロダクション・インストーラ 28

1.3.2 PoC インストーラ 30

1.3.3 RemoteAgent インストーラ 31

1.4 インストール後の手順 34

1.4.1 Connect Configuration Tool 34

1.4.2 Configuration Analyzer 35

1.4.3 グリッドの初期化 37

1.4.4 管理コンソール 40
1.4.5 ConnectCLI を使用する 41
1.4.6 ESG の設定 41
1.4.7 証明書の設定 42
1.4.8 管理者ユーザの追加 43
1.4.9 ドメインの追加 44
1.4.10 ホスト・システムの追加 44
1.4.11 アプリケーションとデスクトップの公開 46
1.4.12 接続のテスト 49

1.5 ConnectCLI リファレンス 50
1.5.1 基本的な使用方法 50
1.5.2 システム構成 52
1.5.3 グリッド・コンポーネントの構成 53
1.5.4 リモート・ホストの構成 55
1.5.5 高度な設定 56
1.5.6 アイコンの構成 57
1.5.7 ライセンス 58
1.5.8 エンドユーザ情報 59
1.5.9 Active Directory の構成 59
1.5.10 ConnectCLI 管理者の資格情報の設定 60
1.5.11 テナント設定 60
1.5.12 切断されたサービス・コンポーネントのマーク 62
1.5.13 RemoteAgent を切断する 62
1.5.14 SQL データベースのバックアップ/リストア 63
1.5.15 古いデータベースのデータを消去する 65
1.5.16 ライセンスのリカバリ 66
1.5.17 デスクトップのタイトル・ラベルを変更する 67

1.6 ライセンス 68
1.6.1 管理コンソールでのアクティベーション 69

1.6.2 ConnectCLI でのアクティベーション 71
1.6.3 入手可能なエディション 72
1.6.4 Connect に含まれる AccessNow と Blaze 72

1.7 Connect のアンインストール 72

2 管理コンソールの使用方法 73

2.1 管理コンソールへのサインイン 73
ユーザ・インターフェース言語の選択 75

2.2 管理コンソールを使用する 76
ナビゲーション・パネル 77
プライマリ・パネル 77
「詳細」パネル 78
一覧オブジェクトの展開と折りたたみ 78
ツールチップ(ツールヒント) 79
継承の切り替え 79

2.3 ダッシュボード 81
システムヘルス 81
ステータス・インジケータ 82
アクティブリソースのステータス 84
最近のセッション 84
Connect ステータス 85
リソース・サーバのステータス 85

2.4 ユーザ 86
情報 87
セッション 87
リソース 89
起動分析 89

2.5 レポート ... 91
カテゴリ ... 93

2.6 公開 ... 96
2.6.1 リソース ... 96
2.6.2 グループ ... 102

2.7 システム ... 106
2.7.1 ホスト ... 106
2.7.2 グループ ... 108

2.8 サービス ... 111
接続サービス一覧表 ... 111
詳細情報 ... 112

2.9 システム構成 ... 113
デフォルト： 要件 ... 113
デフォルト： 詳細タブ ... 113
設定 システム設定 ... 113
セカンダリ設定 ... 113
RADIUS ... 114
ログの設定 ... 116
役割 ... 116

2.10 テナント ... 118
デフォルト： 要件 ... 118
デフォルト： 詳細タブ ... 118
設定 : テナント設定 ... 118
設定 : RADIUS ... 119
役割 ... 119

2.11 詳細タブの設定 ... 119
サードパーティ・ソリューションの有効化 ... 119

キーボード・ロケールの自動切り替え 120

2.12 正規表現の使用 122

3 エンドユーザ・ガイド 124

3.1 AccessPortal(Web) 126

3.1.1 使用方法 126

3.1.2 AccessPortal メニュー・バー 131

3.1.3 複数タブの使用 137

3.1.4 RDP の推奨設定 138

3.2 AccessPad(ネイティブ) 139

3.2.1 ダウンロード場所 140

3.2.2 使用方法 140

3.2.3 AccessPad メニュー・バー 142

3.2.4 ローカル・デスクトップ・アイコン 143

3.2.5 ローカルのスタート・メニュー・アイコン 144

3.2.6 ローカル Windows からの SSO 144

3.2.7 AccessPad Uniprint バンドル (Windows) 146

3.2.8 AccessPad Uniprint バンドル (Mac) 147

3.2.9 AccessPad (Linux) 148

3.3 AccessToGo Connect (モバイル) 150

3.3.1 ダウンロードできる場所 150

3.3.2 使用方法 150

3.4 シングル・サインオン(SSO)のオプション 152

3.4.1 直接起動用の SSO インターフェース 152

3.4.2 キオスク端末での SSO ページ 154

3.4.3 AccessPortal 用 SSO インターフェース 155

3.5 エンコードされた AccessPad アイコンの配置 156

既知の動作 159

3.6 Web サイトからのアプリケーションの起動 160

3.6.1 インストール 161

3.6.2 エンコードされた URL を作成する 162

3.6.3 カスタム URI を作成する 164

3.6.4 URI を使用するためのホスト Web ページを構成する 164

3.6.5 ブラウザの警告メッセージ 165

3.6.6 既知の動作 166

3.7 エンドユーザ・ポイントのカスタマイズ 166

3.7.1 AccessPad の事前構成アドレス 167

3.7.2 AccessPad SSO と URI コマンド・ライン 168

3.7.3 独自の AccessPad 設定のパッケージ化 168

3.7.4 AccessPortal 169

3.7.5 RADIUS マルチファクターのプロンプト 169

3.7.6 独自の AccessPad ログイン・バナー画像 171

3.8 パスワードの変更 173

3.9 フォルダの構造 174

4 展開ガイド 176

4.1 データ・モデルの理解 176

4.1.1 継承階層 176

4.1.2 システム・オブジェクト 177

4.1.3 グループ・オブジェクト 178

4.1.4 リソース・オブジェクト 179

4.1.5 ユーザ・オブジェクト 180

4.2 バインド要件の理解 180

4.2.1 AD を経由してデスクトップとユーザをバインドする 181

4.2.2 デスクトップからのシームレス・アプリケーション 183
4.2.3 切断のステータス 183
4.2.4 公開グループをポータル・タイプにバインドする 184
4.2.5 ESG 階層 186

4.3 ビジネス・ロジック・サービスの理解 186
4.3.1 Connect BL サーバ 186
4.3.2 データ・パーティション 187
4.3.3 データの分散 189
4.3.4 高可用性の実装 190
4.3.5 2 台のサーバ構成(例) 192
4.3.6 複数パーティション・コピーの構成 193

4.4 Connect での Active Directory の使用法 194
4.4.1 認証プロセス 195
4.4.2 認証の詳細 196
4.4.3 最初の ActiveDirectorySets の作成 197
4.4.4 複数の Active Directory の使用 198
4.4.5 Active Directory ConnectCLI の使用法 199
4.4.6 ネストされた AD グループのサポート 205
4.4.7 要件と既知の問題 205

4.5 アップグレードと再展開 206
4.5.1 アンインストール手順 206
4.5.2 再展開の手順 208
4.5.3 RemoteAgent のアップグレード 209
4.5.4 SQL DB からの再展開 210
4.5.5 以前のバージョンへのロールバック 211

4.6 マルチテナント機能 212
4.6.1 共有 Active Directory モデル 213
4.6.2 専用 Active Directory モデル 214

4.6.3 マルチテナント機能のベスト・プラクティス 215
4.6.4 テナントの作成 216
4.6.5 テナントの管理 216
4.6.6 テナントにホストを追加する 217
4.6.7 テナント設定 218
4.6.8 ESG の設定 218

4.7 Ericom Analytics 221
4.7.1 ビルトインのビジュアル化機能 222
4.7.2 インストールのトラブルシューティング 224

4.8 RemoteAgent の展開を自動化する 224

4.9 RemoteAgent(Win) を使用してサーバを複製する 226

4.10 LUS 設定 - マルチキャストが無効化されている場合 227

4.11 LUS 設定 – 混合モード 229

4.12 ワークステーション OS でのアプリケーションの展開 229

4.13 .BAT バッチファイルの公開 230

4.14 Linux 前提条件の設定 231
4.14.1 Ubuntu のアップグレードとアップデート 231
4.14.2 Linux Ericom RDX のインストール 232
4.14.3 XFCE4 のインストール 233
4.14.4 ActiveDirectory サポート(Likewise)を追加する 235
4.14.5 ActiveDirectory サポート(Pbis)を追加する 237
4.14.6 DNS の構成 237

4.15 Linux アプリケーションとデスクトップの展開 238
4.15.1 前提条件 238
4.15.2 Ericom RemoteAgent for Linux のインストール 239

4.15.3 AccessServer for Linux 240
4.15.4 Ericom RemoteAgent for Linux の実行と構成 241
4.15.5 Linux RemoteAgent アクション・コマンド 242
4.15.6 Linux デスクトップを公開する 243
4.15.7 Linux アプリケーションを公開する 243
4.15.8 Linux でのセッション共有 244
4.15.9 アプリケーションとしての Linux デスクトップ 246
4.15.10 Linux セッションでの印刷 247
4.15.11 Linux セッションでのオーディオ 248
4.15.12 Linux RemoteAgent をアンインストールする 248
4.15.13 AccessPortal の設定 249

4.16 Windows RDS でのセキュアなブラウジング 249
4.16.1 Windows RDS サーバの構成 250
4.16.2 Web サイト・アクセス用にブラウザを公開する 250
4.16.3 EricomLaunch.js ファイルの構成 252
4.16.4 Web ページへの URI の追加 252
4.16.5 AccessPad URI の使用方法のサンプル HTML: 253

4.17 Linux Ubuntu でのセキュアなブラウジング 254

4.18 ロード・バランサ Ping ポイント 255

4.19 ESG 経由での管理者ページの公開 255

4.20 Qualys のグレードを A に向上する 255

4.21 ワークステーションでのセッション・フォロー 257

4.22 セッション・ホスト機能を構成する 258
4.22.1 AccessNow 用の Scale-to-Fit 機能を使用する 258
4.22.2 構成済みのカスタム・ホスト名を使用する 259
4.22.3 TsAgent による切断したセッションのログオフ 260

4.22.4 「ログオフ」遅延秒数を使用する ... 260
4.22.5 TsAgent によるログオフ ... 262
4.22.6 TSagent VBS のスクリプト ... 262
4.22.7 XenApp サーバからの公開 ... 264
4.22.8 RDSH 上の App-V クライアントの公開 ... 266
4.22.9 セッション共有 ... 267

5 エコシステムガイド ... 269

5.1 Amazon AWS での展開 ... 269
5.1.1 概要 ... 269
5.1.2 AWS RDS SQL データベースを使用する ... 270
5.1.3 AWS RDS Microsoft SQL を使用する ... 272
5.1.4 Business Logic マシンのインストール ... 273
5.1.5 RDS ターミナル・サーバの設定 ... 274
5.1.6 Ericom Secure Gateway のインストール ... 275
5.1.7 ELB と DNS の設定 ... 277
5.1.8 Ericom Connect AMI の準備 ... 278

5.2 Microsoft Azure Cloud での展開 ... 278
5.2.1 概要 ... 278
5.2.2 要件 ... 279
5.2.3 Business Logic マシンのインストール ... 279
5.2.4 Microsoft Azure SQL の使用 ... 280
5.2.5 RDS ターミナル・サーバの設定 ... 281
5.2.6 Ericom Secure Gateway ... 281
5.2.7 エンドポイントの設定 ... 283
5.2.8 負荷分散の設定 ... 283
5.2.9 Traffic Manager の設定 ... 285
5.2.10 高可用性と負荷分散の構成 ... 286
5.2.11 Ericom Connect イメージの準備 ... 287

5.2.12 イメージからの作成 287
5.2.13 ホストへの遅いログインの解決 288

5.3 RSA SecureID RADIUS 二要素認証 288
5.3.1 RSA RADIUS の設定 288
5.3.2 エージェント・ホスト設定 289

5.4 SecurEnvoy RADIUS 二要素認証 290
5.4.1 SecurEnvoy RADIUS の設定 290
5.4.2 エージェント・ホスト設定 292

5.5 Duo RADIUS 二要素認証 294
5.5.1 Duo RADIUS の設定 294
5.5.2 DUO プロキシの構成 294
5.5.3 エンドユーザ・アクセス 295

5.6 AccessPortal での OneLogin SSO 296
5.6.1 システム構成 297

5.7 Juniper SSL VPN を使用した展開 299
5.7.1 リバース・プロキシの構成 301
5.7.2 SSO の設定 302

5.8 F5 SSL VPN での展開 303
5.8.1 オプション 1: リバース・プロキシ 304
5.8.2 オプション 2: リライタ 307
5.8.3 SSO の設定 313

6 サポート・ガイド 315

6.1 Ericom Connect に関する法律上の注意事項 315

6.2 用語集 317

6.3 リリース・ノート 321

6.3.1 Ericom Connect v7.6.1 321
6.3.2 Ericom Connect v7.6.0 323
6.3.3 Ericom Connect v7.5.2 326
6.3.4 Ericom Connect v7.5.1 327
6.3.5 Ericom Connect v7.3.0 329
6.3.6 Ericom Connect v7.2.0 332
6.3.7 Ericom Connect v7.1.0 334
6.3.8 Ericom Connect v7.0.2 335
6.3.9 Ericom Connect v7.0.1 335
6.3.10 Ericom Connect v7.0.0 336

6.4 サーバ・サイドの FAQ 338

6.4.1 Ericom Connect のインストール用にサーバを検証する 338
6.4.2 IPv6 マシンをグリッドに参加させる 338
6.4.3 ホストの IP アドレスの変更 338
6.4.4 最初の Connect 管理者を割り当てることができない 339
6.4.5 グリッド・コンポーネントに同じバージョンを使用する 339
6.4.6 古いバージョンのグリッドとの互換性がない RemoteAgent 340
6.4.7 SQL での Windows 認証 341
6.4.8 ビルトイン証明書の復元 341
6.4.9 AccessPortal HTTP ポイントの無効化 341
6.4.10 AccessServer ポートの変更 341

6.5 サーバ・サイドの既知の動作 342

6.5.1 Database Server User は英語の名前である必要があります 342
6.5.2 レポート: Access Server フィルタには RemoteAgent が必要です。 342
6.5.3 クロス・ドメイン・グループはサポートされません 342
6.5.4 レポートの結果における負の数 343
6.5.5 信頼された証明書によるページの中断 343
6.5.6 EUWS グローバル証明書の問題 343
6.5.7 RemoteAgent が存在しない場合のセッション・リダイレクト 344
6.5.8 Cloud DB での Configuration Analyzer のエラー 344
6.5.9 サービスの再起動後に管理者がオフラインとなる 345
6.5.10 RemoteAgent WMI エラー 345

6.5.11 セッションの ClientName の CC# とは 346
6.5.12 ファームと NLA で IP アドレスを使用する 346
6.5.13 IPv4 または IPv6 の使用(どちらか一方のみ)..... 347
6.5.14 ユニバーサル・アプリケーションを公開できない 347
6.5.15 Ericom Analytics でデータベースを読み込むことができない..... 348
6.5.16 Windows 7 のセッション・シャドウイング..... 350
6.5.17 MS ユニバーサル/Metro アプリケーションの公開..... 350
6.5.18 SQL データベースの資格情報を変更する 351
6.5.19 最小パスワード長 352

6.6 エンドユーザのトラブルシューティング 352
6.6.1 MSTSC/RDP を使用したテスト 352
6.6.2 ポート接続の確認..... 352
6.6.3 接続タイムアウト..... 353
6.6.4 AccessPortal の変更時のブラウザ・キャッシュのクリア..... 353
6.6.5 IE で 検索テキストを選択できない..... 354
6.6.6 Firefox 上の AccessPortal のスクロールが遅い..... 354
6.6.7 新規ユーザのログインが切断される..... 354
6.6.8 印刷アドオンでの印刷ができない 355
6.6.9 AccessNow タブレットの解像度が 800x600 に設定される 355
6.6.10 Firefox 44 で音声が出力されない..... 356
6.6.11 USB ドライブのリダイレクト..... 356
6.6.12 iOS 上の AccessNow は 1 つのファイルアップロードのみ 356

6.7 認証のトラブルシューティング 357
6.7.1 ログイン: ドメインの定義..... 357
6.7.2 ログイン: ユーザ・ログオン名の定義..... 357
6.7.3 認証サーバのエラー 358
6.7.4 Windows 8/2012 でのログイン・フォーマットの問題 358
6.7.5 SSL ネゴシエーションの失敗 359
6.7.6 Windows 2012 での RDP アクセス許可の問題 360

6.8 パラメータ値とエラーコード 361

6.8.1 パラメータの説明と値 361

6.8.2 エラーコードの定義 365

6.9 テクニカル・サポートのお問い合わせ先 368

オンライン・フォーラム 368

Email/お電話 368

1 はじめてみる

1.1 Ericom Connect®とは?

Ericom Connect® は、様々なホスト・アプリケーションとデスクトップへのアクセスを管理する、エンタープライズ向けのコネクション・ブローカーです。 リモート・デスクトップ・セッション・ホスト(ターミナル・サーバ)、仮想および物理ワークステーションのプラットフォームがサポートされています。

Ericom Connect は、あらゆる規模の組織において、強固かつユーザ・フレンドリーな方法で、仮想化されたアプリケーションやデスクトップを迅速に展開することを可能にします。 エンドユーザは、公開されたアプリケーションやデスクトップ、ドキュメントに次のような様々なクライアント・デバイスから接続できます: Windows®、Linux、 Mac OS X、タブレット、スマートフォン、Chromebook、 各種シンクライアント・デバイス。さらに、Ericom Connect は、社内・社外どちらのアクセスにも暗号化された接続を提供します。(現在、クライアント・デバイスは限定的な対応となっています)

先進のグリッド・アーキテクチャ

Ericom Connect には、高可用性、高スケーラビリティ、パフォーマンスの向上を実化するグリッド・テクノロジーが使用されています。グリッド・プラットフォームの分散化の性質により、何千ものホスト・サーバや何十万ものユーザ・セッションをサポートするスケーリ

ングが可能になります。 すべてのビジネス・ロジック、状態情報、動作状態は、グリッドの各メンバーに共有されます。

グリッドは、Connect のインストール・プロセスの一部として作成と設定が行われます。 このプロセスは以下から構成されています:

- データベースの初期化
- ビジネス・ロジック・サービスの設定および起動
- システムのブートストラップ
- その他のグリッド・コンポーネントの起動

グリッドは「グリッド名」によって識別されます。すべてのコンポーネントは特定のグリッド名で登録されます。同一ネットワーク上の各グリッドは、一意の名前を与えられる必要があります。デフォルトの名前は「EricomConnect」です。

グリッドのメンバーには、以下が含まれます:

- プロセッシング・ユニットサーバ(Processing Unit Server)
- Ericom Secure Gateway(ESG)
- 管理 Web サービス(Admin Web Services)
- クライアント Web サービス(Client Web Service)
- RemoteAgent Web サービス
- RemoteAgent (Windows のみ)

AccessPortal は Connect の一部としてインストールされますが、グリッドのメンバーではなく、AccessPad や AccessToGo のネイティブ・クライアントでもありません。

簡単なエンドユーザ・アクセス

エンドユーザは、何種類かの Ericom ポータル・インターフェースを使用して、Ericom Connect へのサインインと公開されたリソースを起動できます。

- AccessPortal は、Connect へログインして割り当てられたリソースを表示するための Web ベースのポータルです。 リソースを起動すると、該当するアプリケーションまたはデスクトップが AccessNow により Web ブラウザに表示されます。 HTML5 対応ブラウザが必要です。
- AccessPad は、Connect にログインして割り当てられたリソースを表示するためのネイティブ・クライアントです。 リソースを起動すると、該当するアプリケーションまたはデスクトップが、Connect サーバの設定を使用して AccessPad により表示されます。このクライアントでは Blaze のアクセラレーションおよび非アクセラレーションのモードがサポートされています。
- AccessToGo は、Connect へログインして割り当てられたリソースを表示するためのモバイル・アプリです。 リソースを起動すると、該当するアプリケーションまたはデスクトップが、Connect サーバの設定を使用して AccessToGo により表示されます。このアプリでは Blaze のアクセラレーションおよび非アクセラレーションのモードがサポートされています。

Web ベースの管理

すべての管理と監視は、単一の使いやすい Web ベースのインターフェースから実行します。複数の Active Directory アカウントに管理者

のアクセス権を割り当てることができます。 Web インターフェースはすべてのブラウザでサポートされ、複雑なプラグインやインストーラは必要ありません。

強力な起動分析(Launch Analysis)

この独自の起動分析は、アプリケーションやデスクトップへのユーザの接続をプロアクティブに分析する強力なツールです。 これにより、管理者は管理コンソールを使用して、すべてのユーザの接続プロセスのイベントごとの詳細な情報を得ることができます。詳細な情報を使用して接続を分析することで、問題の根本原因を検出し修正できる可能性が大幅に向上します。 これは、手動のトラブルシューティングとエンドユーザの混乱を減らすことにつながります。 また、このツールはリモート画面共有ができないタブレットなどのデバイス上での問題を対処するのに役立ちます。

役割ベースの分類

Ericom Connect では、様々な用途に対応するためにグループの概念が使用されています。 すべての公開されたリソースは、「公開」グループに割り当てられた後、所有者から Active Directory(ユーザ、グループなど)へ割り当てられます。その後、各「公開」グループは 1 つまたは複数の「システム」グループに割り当てられます。その「システム」グループには、アプリケーションやデスクトップを実行するシステムが含まれています。「システム」グループにより、類似したロールを持つサーバとワークステーションを、割り当て用のグループに分類できます。

ビジネス・インテリジェンス

Ericom Connect では、リソースの使用状況についての詳細な情報を管理者とビジネス・マネージャに提供するために、すべてのユーザとセッションのアクティビティのログが取得されます。このようなデータは以下の様な多くの用途で役立ちます:

- アプリケーションとデスクトップのサブスクリプション・ベースの利用追跡
- ユーザの生産性の監視
- システムのワークロードと健全性の測定
- 問題解決 (接続性、割当て、エラーなど)

1.2 要件

1.2.1 SQL データベース

Ericom Connect には、すべてのシステム情報を格納するための Microsoft SQL が必要です。 SQL Server 2012 または SQL Express 2012 (またはそれ以降) が利用可能である必要があります(Connect サーバ・コンポーネントと同一マシン上にある必要はありません)。SQL は、すべてのグリッド情報を格納するために使用されますが、グリッドの動作に必須ではありません。

グリッドの各サーバにより、データベース情報のキャッシュが保持されます。SQL データベースとの接続が中断された場合、Ericom Connect サーバによりデータベースのインメモリ・バージョンが使用され動作が継続されます。 エンドユーザにダウンタイムは発生しま

せんが、管理コンソールの「レポート」機能は使用できなくなります。SQL Server への接続が復元されると、すべてのキューのメッセージが送信され、ログが再開されます。

Connect では、Windows 認証または SQL 認証を使用してデータベースに接続できます。グリッドの初期化(Ericom Connect Configuration Tool)中に適切なオプションを選択してください。Windows 認証には、Connect Processing Unit Service が適切な資格情報で実行されている必要があります。

インストール後:

- データベースの「TCP/IP」を有効化していることを確認してください(「SQL Server 構成マネージャ」 | 「SQL Server ネットワークの構成」 | 「SQL server のプロトコル」 | 「TCP/IP」を有効化する必要があります)。
- SQL Server Browser サービスを起動します(既に自動で実行されている必要があります)
- Windows 認証を使用しない場合、SQL 混合 モードの認証を有効にします。

構成:

- データベース作成のために SA ユーザが使用されます
- 現在ログインしているユーザが Windows 認証に使用されます
- 指定した資格情報が SQL 認証に使用されます
- Connect データベースの読み込み/書き込み/更新のために、サーバユーザが Connect サービスにより使用されます

- Connect サービスの資格情報が Windows 認証により使用されます(サービスの資格情報が明示的に指定されている場合のみ)
- Connect のインストールにより、このユーザへ SQL 権限が付与されます。
- SQL ユーザにより、指定した資格情報が使用されます(ユーザが存在しない場合、作成されます)

1.2.2 Active Directory

Ericom Connect は、ユーザ認証のためにマイクロソフトの Active Directory と統合されています。 Connect のローカルとドメインの権限を持つサービス・アカウントの使用をお勧めします(初期の Connect 管理者ユーザとして)。

ユーザが Ericom Connect へサインインする際には:

- ユーザに指定されたドメインが使用されます。
- ドメインが指定されない場合、システムのデフォルトのドメインが使用されます。

1.2.3 デスクトップ/セッション ホスト

Ericom Connect により、Connect 環境へ登録されているすべてのリソース・ホスト・システム(例:ターミナル・サーバ・セッション・ホスト)が管理されます。 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:

- Windows 2008 ターミナル・サーバ、またはそれ以上
- Windows 7 ワークステーション、またはそれ以上

- ホスト上で RDP が有効にされ利用可能

Ericom で使用する適切なポートを ローカルの Windows ファイアウォールで設定してください(例:ポート 8080 の新規の着信の規則を作成する)。

ユーザが RDP を使用してデスクトップまたはサーバへ接続できるよう、ターミナル・サーバ上のリモート設定を行ってください。

1.2.4 Windows 2008 R2/2012 R2

Ericom Connect には、Windows 2008R2 または 2012 R2 が必要です。サーバには以下のハードウェア・スペックをお勧めします:

- 4 コア
- 8 GB RAM
- 4GB のハードディスク空き容量
- SQL データベースを同一マシンで実行する場合(例: PoC 用)、8 コアと 16 GB RAM を推奨します。

1.2.5 信頼された証明書

各 Connect マシン上に信頼された証明書を配置することをお勧めします。 ワイルドカード証明書がサポートされています。 Ericom Secure Gateway の証明書は、システムの外部 DNS 名と一致させる必要があります。

1.2.6 DNS とポート

Ericom Connect には、ネットワーク上で DNS (ドメイン・ネーム・サービス) が利用可能であることが必要です。Ericom Connect Remote Agents により、Ericom グリッドへ接続する際のアドレス解決のために DNS が使用されます。

Ericom Connect の展開には、ネットワーク上で特定のポートが利用可能であることが必要です。 以下の表では、Connect または Connect 環境で一般的に使用されるポートを示しています。 これらのポートは、「着信を開放する側」の欄で指定されたシステム上で利用可能であることが必要です。 これらのポート値がデフォルトから変更されている場合、それらもファイアウォール上で調整する必要があります。SQL サーバとグリッド・コンポーネントを分離しているグリッドでは、SQL サーバ上で SQL 着信ポート(1433)を開放する必要があります。

Ericom のコンポーネントで使用されるデフォルト・ポート

ポート番号	使用	着信を開放する側
443	Ericom Secure Gateway	ESG サーバ
443	RemoteAgent (タイプ 2) Web サービス	Web サービス・ノード
8011	HTTPS 経由の End User Web インターフェース	クライアント Web サービス(Connect サーバ)
8022	Administrator Web Interface	管理 Web サービス

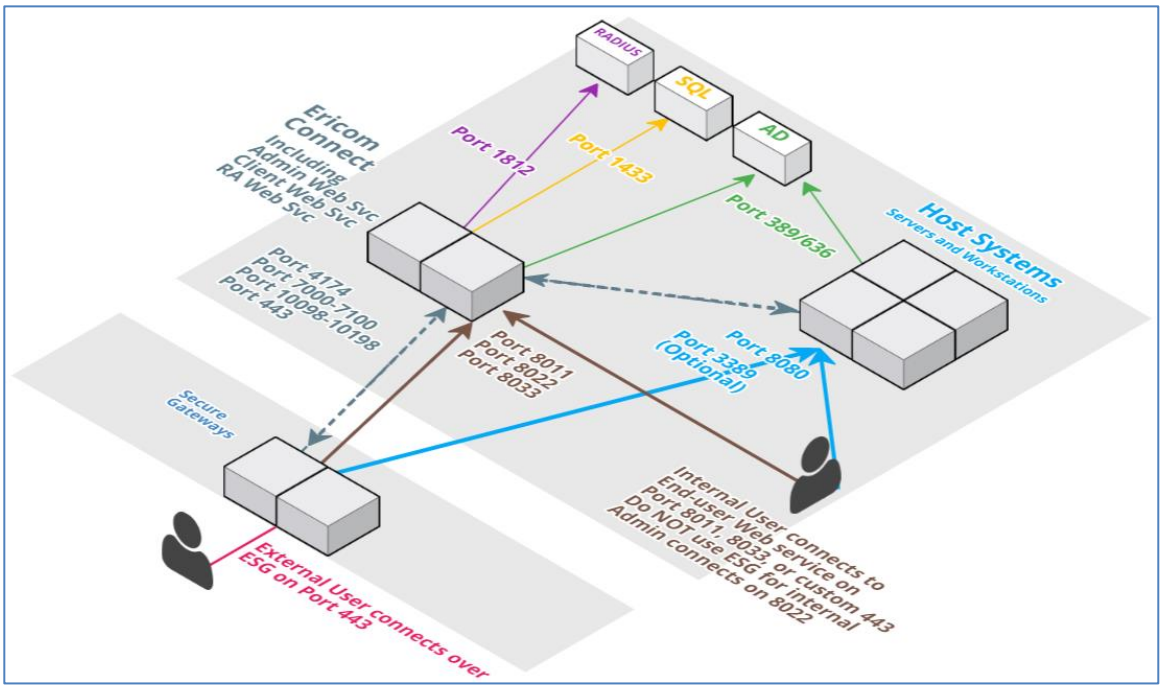
		(Connect サーバ)
8033	HTTP 経由の End User Web Interface	クライアント Web サービス(Client Web Service) (Connect サーバ)
8080	AccessServer Session Communication	TS/RDS
4174	グリッド通信(LUS)	すべてのグリッド・ノード (ESG/Connect サーバ)
7000-7100	グリッド通信	すべてのグリッド・ノード (ESG/Connect サーバ)
10098-10198	グリッド通信	すべてのグリッド・ノード (ESG/Connect サーバ)

一般的に Ericom Connect と組み合わせて使用されるアプリケーションとサービスにより使用されるデフォルト・ポート(これらのポートは、環境でカスタマイズされている場合は異なる可能性があります)。

ポート番号	**使用**	**着信を開放する側**

1433	SQL Server	SQL Server
1812	RADIUS 二要素認証(デフォルト)プロコトル	RADIUS サーバ
3389	Microsoft RDP	TS/RDS(オプション)
389/636	LDAP/S-LDAP	AD サーバ

Ericom Connect 環境でのポート設定のサンプル:



1.3 インストーラの使用

利用可能なインストーラは以下のとおりです:

名前	説明

プロダクション・インストーラ (EricomConnect.exe)	本番環境または高度な環境のためのインストーラです。 このインストーラを使用して、各グリッド・コンポーネントを個別にインストールできます。 Windows 2008 R2 または 2012 R2 が必要です。
EricomPoC (EricomConnectPOC.exe)	概念実証(Proof of Concepts)用のインストーラです。 このインストーラには SQL Express が含まれています。 Windows 2008 R2 または 2012 R2 が必要です(日本では同梱していません)。
RemoteAgent x64 (EricomConnectRemoteHost_x64.exe)	Windows 2008 R2、2012R2、Windows 7 x64 およびそれ以上のオペレーティング・システム用の RemoteAgent インストーラです。 AccessServer が含まれています。
RemoteAgent 32 (EricomConnectRemoteHost_x86.exe)	Windows 2008 と 32 bit Windows オペレーティング・システム 用の RemoteAgent です。 AccessServer が含まれています。
AccessPad (Windows、Mac、Linux)	Windows と Mac のオペレーティング・システム用の AccessPad ネイティブ・クライアントのインストーラです(Mac 版 AccessPad は日本では将来のバージョンで対応予定)。
AccessToGo (ストアからダウンロード)	Android と iOS 用のモバイル・クライアントです。

1.3.1 プロダクション・インストーラ

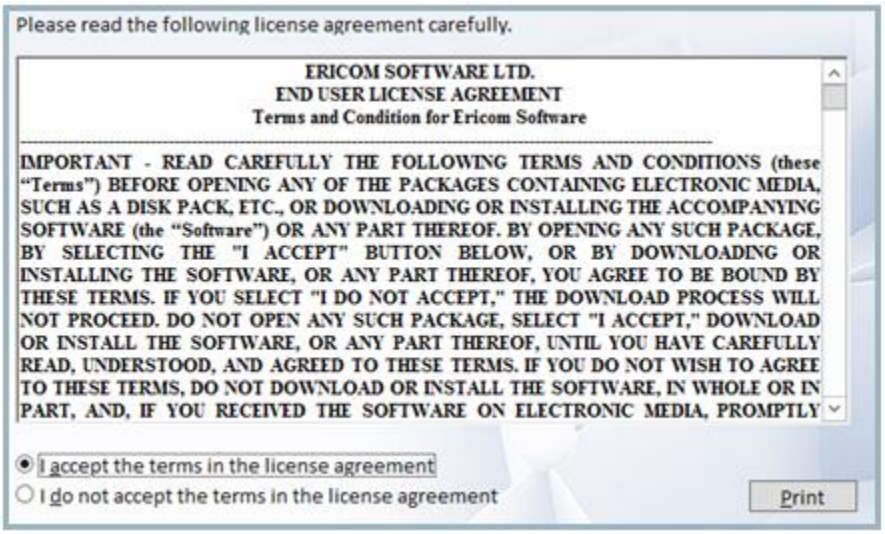
1.3.1.1 アーキテクチャ

このインストーラを使用して、管理者は個別のグリッド・コンポーネントを専用のサーバへインストールできます。 本番運用のシナリオでは、一般的に Ericom Secure Gateway(ESG)をネットワークの末端にある専用サーバで実行します。 セッション・ホストとワークステーション上で RemoteAgent を実行します。このインストーラは単一サーバへの展開に使用できますが、SQL データベースは含まれていません。

1.3.1.2 インストール手順

EricomConnect.exe インストーラを実行して、各ダイアログの手順に従います。

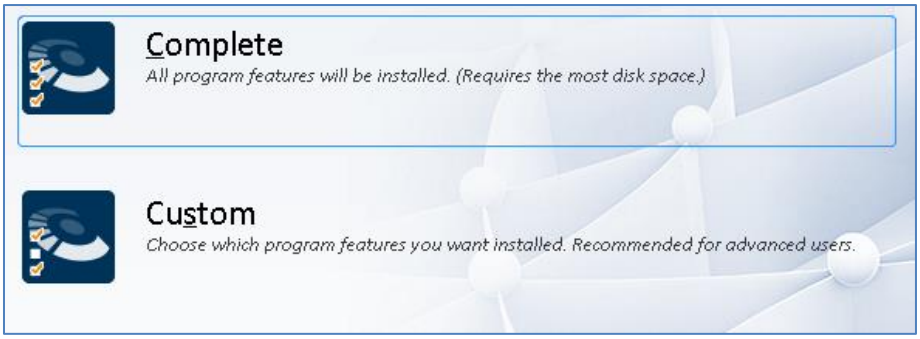
License Agreement(使用許諾契約)を確認し、同意してください。



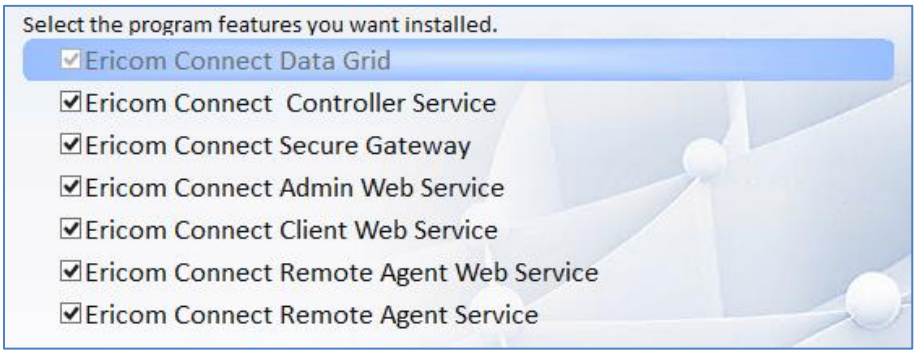
インストール方法を選択します:

Complete: サーバにすべてのコンポーネントをインストールします。

Custom: サーバにインストールするコンポーネントを選択できます。



「Component Selction」ダイアログにおいて、サーバへインストールするコンポーネントを選択します。



「Finish」ボタンをクリックすると、インストール後の設定のために Ericom Configuration Tool が自動的に起動します。

1.3.2 PoC インストーラ

1.3.2.1 アーキテクチャ

PoC(Proof of Concept: 概念実証) インストーラは、SQL Express を含むすべての必要なコンポーネントをインストールするために設計されています。 このインストーラは、簡単に展開できるよう設計され、インストール・プロセスでのユーザ操作を最小限にするよう設計されています。

1.3.2.2 インストール手順

EricomConnectPoC.exe インストーラを実行し、「Next」をクリックしてインストールを開始します。

このインストーラを使用時には、ユーザ・プロンプトは表示されません。インストールの完了後、システムを利用できるようになります。

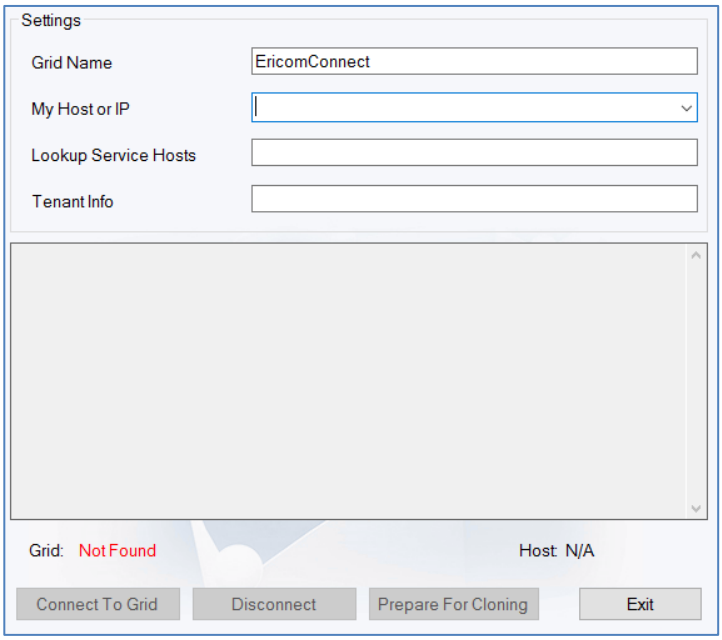
インストール中にユーザ・プロンプトは表示されません。 インストールの最後に「Finish」ボタンをクリックすると、インストール後の設定用に「Ericom Configuration Tool」が自動的に起動します。

1.3.3 RemoteAgent インストーラ

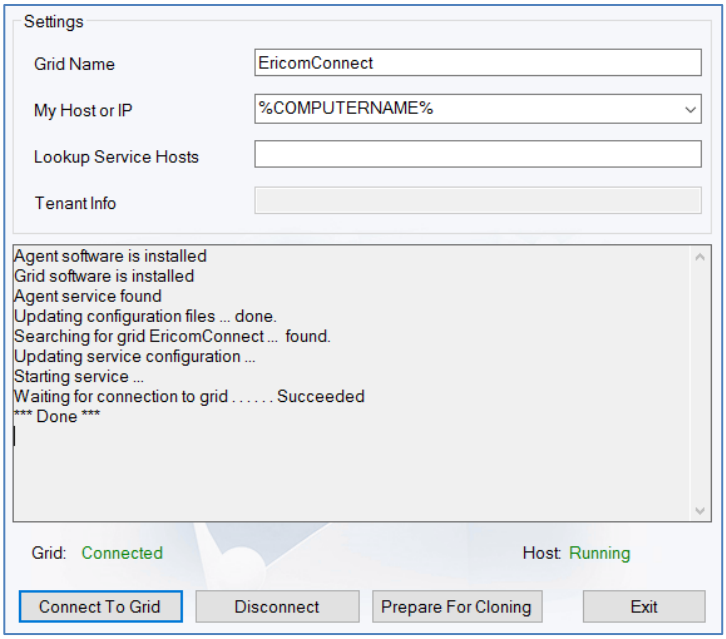
EricomConnectRemoteHost_x64.exe インストーラ(32 bit または旧型の x64 オペレーティング・システムの場合は EricomConnectRemoteHost_x86.exe)を実行します。 このインストーラにより RemoteAgent(タイプ 1)コンポーネントのみがインストールされます。 インストールが完了すると、設定ダイアログが表示されます。必要なパラメータを入力します:

- Grid Name (グリッド名)

- My Host or IP - グリッド上のシステムの識別用。 ネットワーク上で認識可能かつ一貫性のある値を使用します。
- Lookup Service Hosts (ルックアップ・サービス・ホスト)
- Tenant Info (テナント情報)



グリッドへの接続が成功すると、画面下部のステータスで「Grid」が「Connected」と表示され、「Host」が「Running」と表示されます。



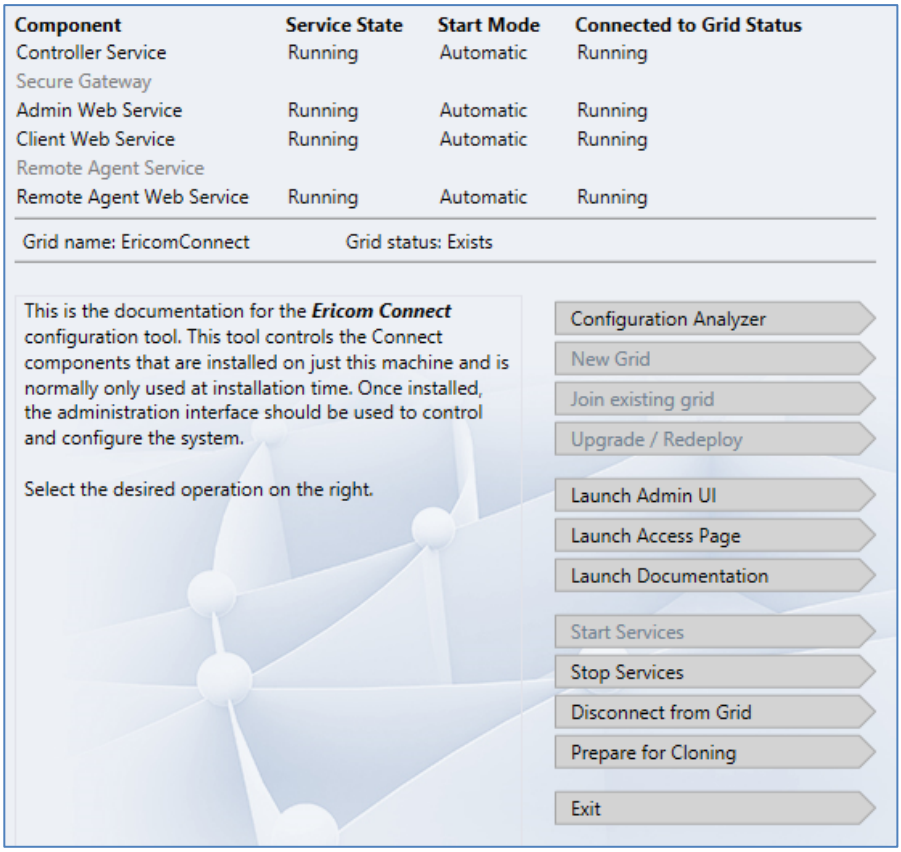
注意: RemoteAgent をアンインストールすると、自動的にグリッドから切断されます。

RemoteAgent for Linux の展開方法については、「展開ガイド」の Linux セクションを参照ください。

1.4 インストール後の手順

1.4.1 Connect Configuration Tool

インストールが完了すると、Ericom Configuration Tool が自動的に起動し、 「コンポーネント・ステータス」画面が表示されます:



上部のステータス領域では、現在のサーバ上の Connect コンポーネントの状態が表示されます。 「Connected to Grid」の欄では、コンポーネントが正常にグリッドへ接続されているかどうかが表示されます。「Configuration Analyzer」ボタンをクリックして、Ericom グリッドを使用するためのパラメータを入力します。 「Configuration

Analyzer」によりパラメータの検証が行われた後、グリッド作成のために Configuration Tool にパラメータが渡されます。

Configuration Tool は、次のようにしてコマンド・プロンプトから実行可能です:

“<ドライブ>:\Program Files\Ericom Software\Ericom Connect Configuration Tool\EricomConnectConfigurationTool.exe”.

次の方法で実行することもできます:

「Start "config" /w “<ドライブ>:\Program Files\Ericom Software\Ericom Connect Configuration Tool\EricomConnectConfigurationTool.exe”」

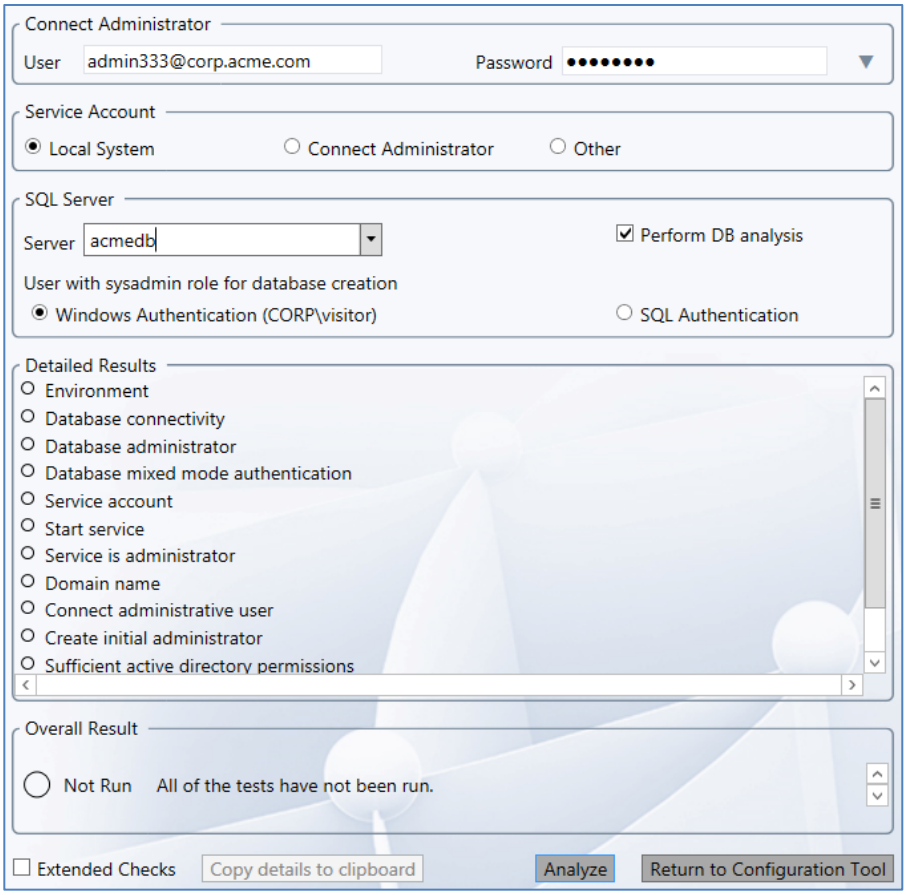
この呼び出しは、インストールが完了するまで**待機**状態となります。

すべてのオプションを表示するには、以下を実行します:

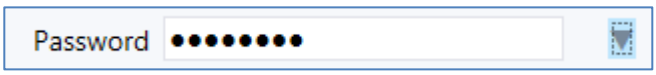
EricomConnectConfigurationTool /?
デフォルトでは、現在のディレクトリ内に「EricomConnectConfiguration.log」という名前でログ・ファイルが作成されます。

1.4.2 Configuration Analyzer

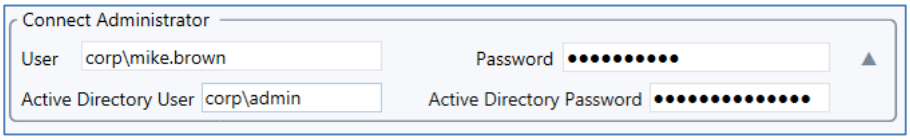
Ericom Connect Configuration Analyzer は、Configuration Tool から利用可能で、Connect で使用する様々なパラメータを検証するために使用します。 これは、Ericom Connect システムの初期化が失敗した場合に、不適切な設定の原因を特定するのに役立ちます。



一部の Active Directory(例: 匿名アクセスなし) では、Ericom Connect 管理者としてアカウントを追加するための AD 資格情報が必要となる場合があります。 AD にアクセスするための資格情報を特定するには、パスワード入力欄の右にあるドロップ・ダウンの矢印をクリックします。



Ericom Connect 管理者用に使用する資格情報と Active Directory へのアクセスが許可された AD アカウントを入力します。

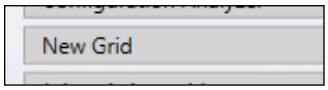


「Analyze」ボタンを押すと、システムの初期化に使用される設定パラメータの検証が行われます。

Configuration Analyzer を Configuration Tool とは別のスタンドアロンのツールとしてダウンロードすることもできます。 これは、Ericom Connect をインストールする時間と労力をかける前に、Ericom Connect で使用するサーバを検証するのに役立ちます。

1.4.3 グリッドの初期化

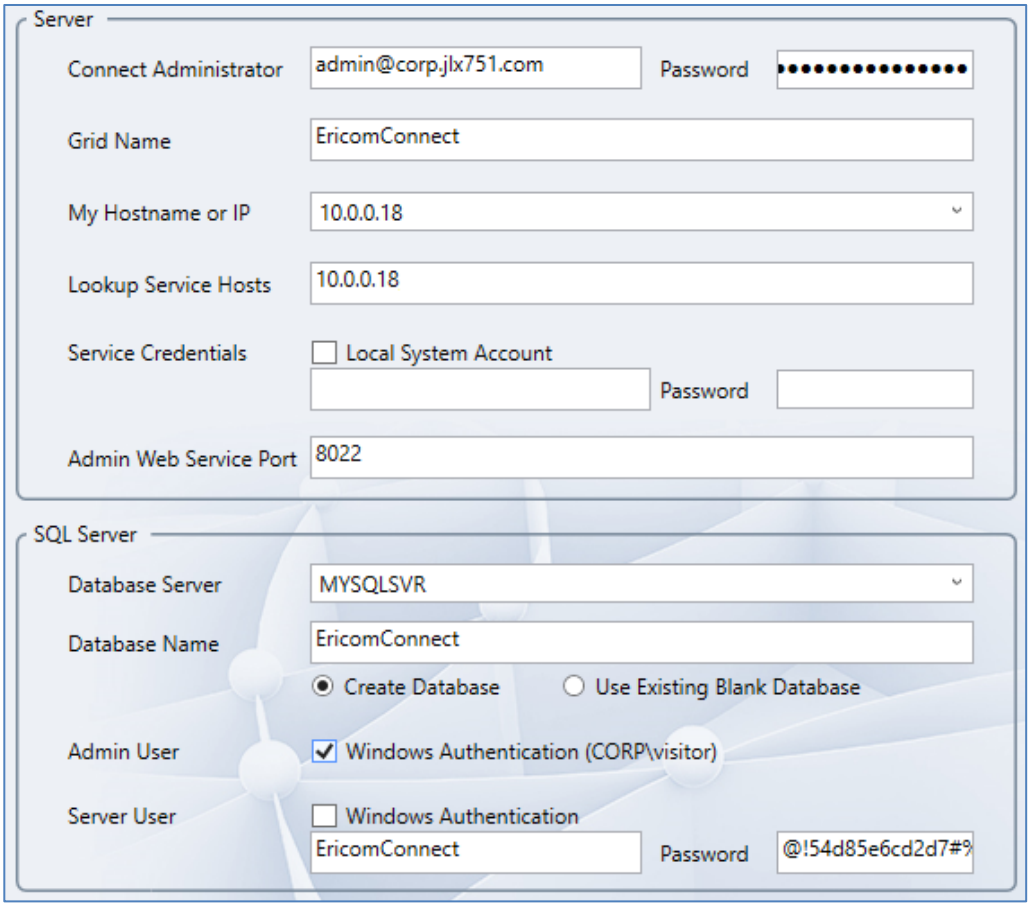
新規の複数サーバ展開の最初のサーバか、単一マシン用の展開の場合、「New Grid」オプションを選択します。



例えば、10 台のマシンに展開する場合、最初のサーバに「New Grid」オプションを選択し、他の 9 台のサーバでは「Join existing grid」を選択します。

「New Gird」を選択する前に「Configuration Analyzerr」を起動しなかった場合、警告メッセージが表示されます。 「New Grid」の前に「Configuration Analyzer」を起動することは必須ではありませんが、お勧めします。

「New Grid」オプションを選択すると、「Create New Grid」画面が表示されます:



この画面には 2 つのセクションがあります: 「Server」と「Database」

「Server」セクションでは、以下のフィールドへの入力が必要です:

- Connect Administrator と Password – 最初の Ericom Connect 管理者ユーザ資格情報
- Grid Name - Connect グリッド の名前
- My Host or Ip - 参照に使用されるローカル・アドレス
- Lookup Service Hosts (LUS) - グリッドの自動選択を許可するには空白のままにします。または、検索サービスのホストとして指定するサーバのアドレスを入力します。 一つのグリッドの展開に

つき少なくとも 2 つ持つことをお勧めします。 指定する LUS システムには静的 IP アドレスが与えられている必要があります。 LUS の設定は、すべてのグリッド・システム上で同一である必要があります(必須ではなく推奨)。

- Service Credentials - サービス用の Windows アカウントまたはビルトインのシステム・アカウントを使用します。 Windows アカウントを使用する場合、ユーザはローカル管理者である必要があります。
- Admin Web Service port – Admin Web Service(AWS)に使用するポート値。

「データベース」セクションでは、以下のフィールドへの入力が必要です。

- Database Server - SQL Server の名前。リストから選択、または完全なアドレスを入力します。
- Database Name - Connect 用に作成するデータベースの名前
- Create Database – Ericom Connect によってデータベース・サーバに新たなデータベースが作成されます(ユーザに権限がある場合)
- Use Existing Database – データベース・サーバ上に作成済みのデータベースを使用します。 構成済みのデータベース資格情報には、データベースへのアクセス権が必要です。
- Admin User - SQL SA データベース管理者ユーザ(定義する方法については必要に応じて Microsoft SQL ドキュメントを確認してください)を入力するか、「Windows Authentication」を使用する

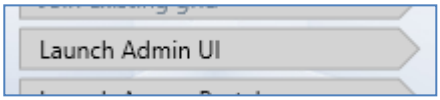
ためにチェックボックスをオンにします。「Windows Authentication」を使用する場合、設定したユーザに SQL データベースの作成と変更するためのアクセス権が与えられていることを確認してください。 この手順には「Windows Authentication」をお勧めします。

- Server User - データベース用の管理者ユーザを設定する(事前設定値を使用している場合、データを記録)か、Windows アカウントを使用します。

すべてのフィールドへの入力の完了後、「Initialize database and start services」をクリックします。 グリッドが初期化されシステムの準備が完了すると、使用可能になった新しい機能(例:(Launch Admin UI、Stop Service など)が Configuration Tool に表示されます。

1.4.4 管理コンソール

Connect Web ベース管理コンソールを起動するには、「Launch Admin UI」ボタンをクリックします(コンソールはシステムのデフォルトのブラウザを使用して起動されます)



新規グリッドの作成時に使用した管理者アカウントで管理コンソールへログインします。

管理コンソールは次の URL を使用して直接起動することもできます:

https://<サーバアドレス>:8022/Admin

1.4.5 ConnectCLI を使用する

付属する ConnectCLI ツールを使用して、コマンド・ライン・パラメータ経由で Ericom Connect の設定を実行することも可能です。

ConnectCLI ツールを使用するには:

- Windows のコマンド・プロンプト(cmd.exe)を開きます
- 「< Ericom Connec へのパス >\Ericom Connect Configuration Tool\」に移動します
- 「ConnectCLI リファレンス」のセクションに記載されているパラメータを使用して ConnectCLI.exe を実行します。
- ConnectCLI を実行するには、Ericom Connect の管理者ログインが必要です(各コマンドの実行時に管理者の資格情報が要求されます)

このツールは、以下の「インストール後」セクションの機能を設定するために使用します。

1.4.6 ESG の設定

ESG では、443 ポートがデフォルトで使用されています。 デフォルトのポートを変更するには、「サービス」に移動して「ESG サービス」編集ボタンをクリックします。

その後、「設定 |ネットワーク | セキュアポート」からポート値を変更します。

次の ConnectCLI コマンドを使用して ESG を設定することもできます:

- ポート値が 443 以外とする場合は、ポートを設定します。 例えば、ポートを 8443 に設定する場合:
  ConnectCLI EsgConfig common Network$SecuredPort=8443

```
> connectcli esgconfig common Network$SecuredPort=8443
Network$SecuredPort <= 8443
```

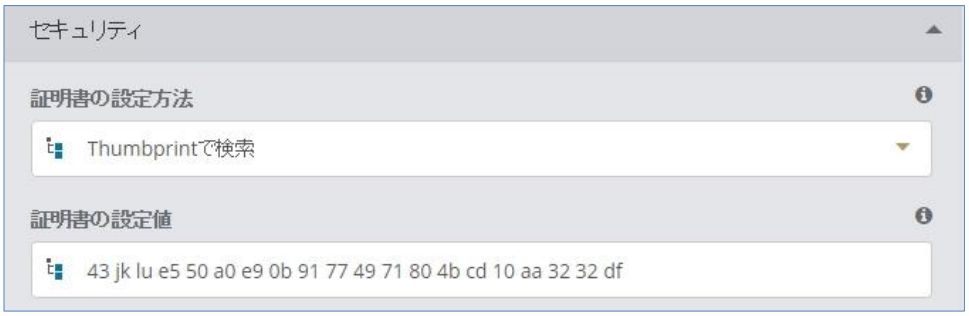
1.4.7 証明書の設定

管理コンソールまたは ConnectCLI コマンドを使用して Ericom Connect で証明書を設定できます。

管理用 GUI

「接続サービス」へ移動し、対象サービスの設定ボタン(歯車のアイコン)をクリックします。 サーバ名の隣にある設定ボタンをクリックして、サーバ・レベルで証明書を設定できます。または、サービス・レベル(例: ESG サービス)の設定ボタンをクリックし、グローバル・レベルで設定することも可能です。

証明書の設定に移動し、「証明書の設定方法」および「証明書の設定値」を設定します。



ConnectCLI を使用した方法

以下の ConnectCLI コマンドを使用して、システムの証明書を設定します:

- 使用可能な証明書の一覧を確認する(この一覧に表示される証明書のみが使用できます): **ConnectCLI ConfigureCertificates**

ESG 用の証明書を設定(外部アクセス用):

- ConnectCLI ConfigureCertificates /noaws **/esg** /noeuws FindByThumbPrint <thumbprint>

  ESG(内部アクセス用)を使用しない Admin Web Service および End User Web サービス 用の証明書の設定:

- ConnectCLI ConfigureCertificates **/aws** /noesg **/euws** FindByThumbPrint <thumbprint>

設定する証明書は各サーバの名前と一致させる必要があります。 証明書はシステム上に「エクスポート可能」としてインストールする必要があります。 ワイルドカード証明書がサポートされています。

EsgHostAddress に IP アドレスを設定する際は注意してください。アドレスが設定した証明書と一致しない場合、ブラウザによりクロスドメイン(CORS)の問題として処理され、接続が許可されません。

1.4.8 管理者ユーザの追加

管理コンソールを使用して管理者を追加することができます。「設定(またはテナント) | 役割」に移動し、既存の管理者レベルの役割にユ

ーザを追加するか、希望する管理者権限を持つ新たな役割を作成します。

ConnectCLI を使用して管理者を追加することもできます。:

- ConnectCLI AdminUsers add <user または group> < ドメイン> < ユーザまたはグループ名>
- 例: ConnectCLI AdminUsers add user test.local *admin@test.local*

1.4.9 ドメインの追加

Ericom Connect では、複数ドメインの使用がサポートされています。Active Directory ドメイン を個別のビジネス・ユニットや顧客で使用している場合に使用されることがあります。 Active Directory ドメインを追加するには、次の ConnectCLI コマンドを使用します:

ConnectCLI ActiveDirectories add **test.local**
(「test.local」には追加するドメイン名を入力します)

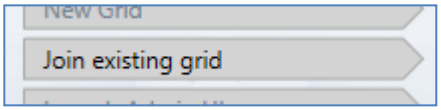
1.4.10 ホスト・システムの追加

グリッドにサーバやワークステーションを追加するには、対象とするシステムに Ericom RemoteAgent MSI をインストールします。RemoteAgent には以下の 2 つのタイプがあります:

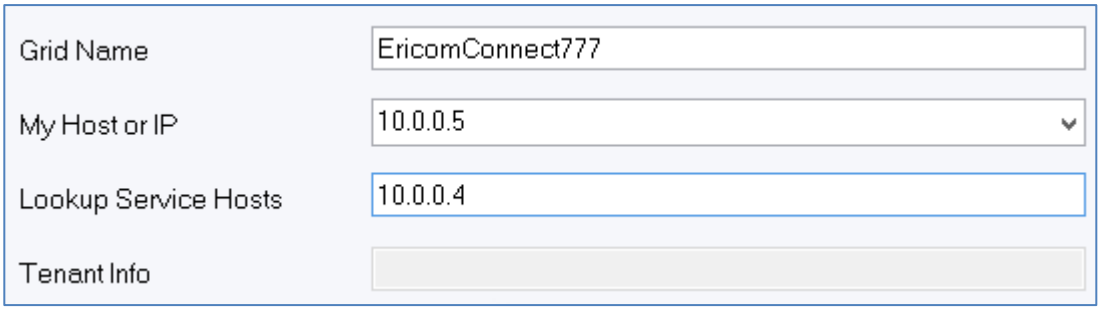
- RemoteAgent (x64) - すべての x64 Windows オペレーティング・システムで使用します(Windows 2008R2 Server 以上、 または Windows7 x64 以上)
- RemoteAgent (32 64) - すべての 32 bit Windows オペレーティング・システムおよび Windows 2008R2 と Windows 7 以前の x64 Windows オペレーティング・システムで使用します。
- RemoteAgent for Linux – Ubuntu Linux 14.04.3 以降を実行しているシステムではこちらを使用してください。 Linux の機能の詳細については、展開ガイドの Linux のセクションを参照してください。

エージェントのインストールが完了すると、Ericom Connect Configuration Tool が起動されます。

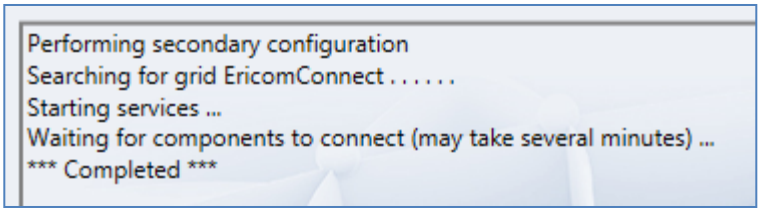
「Join existing grid」をクリックしてシステムを Connect グリッドへ追加します。



Connect グリッドの詳細を入力します。



「OK」をクリックし、グリッドへの登録を開始します。 このプロセスは、約 4 ~ 8 分 かかる場合があります。



1.4.11 アプリケーションとデスクトップの公開

まず管理コンソールのナビゲーション・パネルで「公開」をクリックします。

「リソース」を選択し、「アプリケーション追加」または「デスクトップ追加」を選択します。

アプリケーションを公開するには、完全なパスを入力するか、対象のサーバ上をクリックして、スタート メニューから一つを選択します。

リソースを公開すると、自動的に「All Resources」という名前の「公開」グループに割り当てられます。

デフォルトでは、「All Resources」グループにはユーザやグループが割り当てられていません。 所有者を割り当てるには、「基本」タブでグループのリンクをクリックします。

1.4.11.1 Active Directory ユーザまたはグループの割り当て

割り当てを行うリソースを選択します。

リソースの「詳細」パネル(基本タブ)から、希望する「公開」グループをクリックします:

このアクションにより、選択したグループの「プロパティ」に移動します。

「ユーザ」タブを選択し、「Active Directory オブジェクトを追加」をクリックし、AD ユーザやグループ・オブジェクト、または「Everyone」をグループに割り当てます。 初期状態では、各グループにオブジェクト割り当てられていません。

「Everyone」を使用すると、システムへの接続を許可されているすべてのユーザにリソースが割り当てられます。

「公開」グループにリソースが割り当てられ、「公開」グループがユーザ(またはユーザのグループ)に割り当てられると、使用可能になります。

すべての「公開」グループにはデフォルトで全システムが割り当てられます(「システム」グループ「All remote hosts for Root」が割り当てられます)。

1.4.11.2 「システム」グループの割り当て

「公開」グループの所有権を割り当てた後、「システム」タブをクリックします。このリソースの起動用に利用可能とするサーバとデスクトップを割り当てるために、「システム」グループを追加します。 各サーバとデスクトップは、エンドユーザがアクセスできるように、「公開」グループのメンバーにする必

要があります。

追加されたすべてのサーバとデスクトップは、自動的にビルトインのグループ「All remote hosts for Root」に追加されます。

利用可能な「システム」グループを「公開」グループに追加するには、「システムグループを追加」をクリックします。

選択した「システム」グループを「公開」グループから削除するには、「システムグループを削除」をクリックします。

1.4.12 接続のテスト

Connct 環境が構成されると、エンドユーザ側のテストの準備ができた状態になります。 サポートされている Ericom エンドユーザ・アクセス方法をテストする前に、管理コンソールの「システムヘルス」を参照し、すべてのシステムが正常(赤いステータスではない)ことを確認してください。

Ericom Connect に含まれる 3 つのエンドユーザ・アクセス方法で Ericom Connect をテストするには「エンドユーザ ガイド」を参照してください: : AccessPortal、AccessPad、および AccessToGo。

1.5 ConnectCLI リファレンス

Ericom Connect CLI は、一部の特徴と機能を設定するためのコマンド・ライン・インターフェースを提供します。 ConnectCLI へのデフォルトのパスは次のとおりです: 「< Ericom Connect へのパス>\Ericom Connect Configuration Tool\」 Ericom Connect の一部の設定と機能は、コマンド・ライン・ツール「 ConnectCLI.exe」以外からは設定ができません。

一部の ConnectCLI コマンドは、実行前に Ericom Connect 管理者の認証を必要とします。これは、セキュリティ上の理由のための設計です。

便宜上、以下のコマンド・ライン・セッションを使用して Ericom Connect 管理者資格情報をコマンド・ライン・セッションに保存します。これにより、複数のコマンドを実行する際に再入力する必要がなくなります。

- set EC_ADMIN_USER=<admin user>
- set EC_ADMIN_PASSWORD= < admin password>

1.5.1 基本的な使用方法

ConnectCLI <コマンド名> [/オプション値] ... [引数 ...] - 各コマンドでは、異なるオプションと引数のセットを使用可能です。

ConnectCLI /? - 使用可能なすべてのコマンドを一覧表示します。

ConnectCLI /?? 変数、引数などを含むより詳細な形式で、使用可能なコマンドを一覧表示します。

ConnectCLI /? and /?? 7.6.0 以降のバージョンでは、ConnectCLI /? および /?? にオプションの検索文字列を使用することが可能です。例: ConnectCLI /?remote は、文字列「remote」を含むすべてのコマンドを返します。

ConnectCLI コマンド名 /? - 特定のコマンドの詳細を表示します。

ほとんどのコマンドで、Connect の管理者の資格情報やグリッド名が必要です。 これらをオプションとして渡すために、環境変数を使用します。 オプション名と、対応する環境変数は以下のとおりです:

- /adminUser <ユーザ名> EC_ADMIN_USER
- /adminPassword <パスワード> EC_ADMIN_PASSWORD
- /gridName <グリッド名> EC_GRID_NAME (使用中のコンピュータに Connect component がインストールされている場合、設定済みのグリッド名がデフォルトで使用されます)

コマンド名とオプション名では大文字と小文字は区別されません。 オプション名は、一意のプレフィックスを使用して短縮できます。

例えば、オプション「/adminUser」と「/adminPassword」では、「/adminU」や 「/adminUser」 または「/adminUs」を使用できます。

オプション名「/admin」は、一意のプレフィックスではないため使用できません。

資格情報が要求される状態において指定されていない場合、各 ConnectCLI コマンドでプロンプトが表示されます。

1.5.2 システム構成

ConnectCLI Version - Ericom Connect のバージョンが表示されます

ConnectCLI SystemConfig - システム構成のパラメータを確認または設定します。 引数なしの場合、すべての設定が表示されます。 引数を指定すると、指定した値にプロパティが設定されます。

ConnectCLI SystemConfig プロパティ=値 - 1 つまたは複数の構成パラメータを設定します。

ConnectCLI SecondarySystemConfig - セカンダリ構成パラメータの確認または設定に使用します(通常は使用しません)。引数なしの場合、すべての設定が表示されます。 引数を指定すると、指定した値にプロパティが設定されます。

ConnectCLI ConnectionConfig - 共通接続(Blaze ファイル)オプションを設定または表示します。 これは、このパラメータを上書きしていないすべてのリソースとグループに影響します。

ConnectCLI BindingConfig - 共通のバインド(制限)オプションの設定または確認を行います。 これは、このパラメータを上書きしていないすべてのリソースとグループに影響します。

ConnectCLI TwoFactorConfig - 2 要素設定のパラメータを設定または確認します。

1.5.3 グリッド・コンポーネントの構成

ConnectCLI EuwsConfig - インスタンスの一覧表示、一般的な設定の表示と確認、インスタンス構成パラメータの確認と設定を行います。

ConnectCLI EuwsConfig List - 現在実行中のすべてのエンドユーザ Web サービスを一覧表示します。 ここでの「ID」は、インスタンス構成の取得/設定に使用されます。

ConnectCLI EuwsConfig Common - インスタンスで上書きされていない場合には、すべての EUWS に適用されている共通の構成パラメータが表示されます。

ConnectCLI EuwsConfig common プロパティ=値- 1 つまたは複数の一般的な構成パラメータを設定します。

ConnectCLI EuwsConfig <id> - 特定の EUWS 用のインスタンス特有のプロパティが表示されます。 EuwsConfig List コマンドでの ID を使用します。

ConnectCLI EuwsConfig <id> プロパティ=値 - 特定の EUWS 用の 1 つまたは複数のインスタンス特有のプロパティを設定します。 EuwsConfig List コマンドでの ID を使用します。

ConnectCLI EsgConfig - インスタンスの一覧表示、共通設定の確認と設定、インスタンス構成パラメータの確認と設定を行います。

ConnectCLI AwsConfig - インスタンスの一覧表示、共通設定の確認と表示、インスタンス構成パラメータの確認と設定を行います。

ConnectCLI RemoteAgentConfig - インスタンスの一覧表示、共通設定の確認と表示、インスタンス構成パラメータの確認と設定を行います。

ConnectCLI GridInfo - 次の情報が表示されます: Business Logic components と Databese Sync components(ミラー・サービス)、パーティションのステータス、バックアップの割り当て、コンテナ(GSC)のステータス。

出力のサンプル:

```
EricomConnectBusinessLogic Intact; Partitions=2; Backups=1; MaxInstancesPerMachi
ne=0
EricomConnectMirrorService Intact; Partitions=1; Backups=0; MaxInstancesPerMachi
ne=0

CONNECT3DBVM.corp.jlx3.com
  GSC 1
    EricomConnectBusinessLogic Patition 1 [Primary]
  GSC 2
    EricomConnectBusinessLogic Patition 2 [Primary]
  GSC 3
    EricomConnectBusinessLogic Patition 2 [Backup 1]
  GSC 4
    EricomConnectBusinessLogic Patition 1 [Backup 1]
  GSC 5
    EricomConnectMirrorService Patition 1 [Primary]
```

各マシンには、5 つのコンテナがあります。

ConnectCLI SetGridParameters - グリッド・パラメータを設定するために使用します。 新しいパラメータを定義する場合、指定した値が使用可能であるかどうかの検証がこのコマンドにより行われます。 使用可能である場合、サンプルの展開が表示され、確認プロンプトが表示されます。

使用法:

ConnectCLI SetGridParameters #partitions #backups #gscPerMachine #maxInstPerMachine

式は次のようになっています: (バックアップ数 + 1)* パーティション数 + 1 = コンテナ数 (コンテナ = GSC)

「SetGridParameters」を使用してシステムを構成した後、パーティションの値を変更した場合は、設定を有効にするためにすべてのグリッド・コンポーネントを再起動します。

「SetGridParameters」を使用してシステムを構成した後、バックアップの値を変更した場合は、設定を有効にするために全ての Business Logic Controller サーバを再起動します。

1.5.4 リモート・ホストの構成

オプションは、グリッド・コンポーネントの構成と同じです。

ConnectCLI RemoteHostConfig - インスタンスの一覧表示、共通設定の確認と表示、インスタンス構成パラメータの確認と設定を行います。 例: **ConnectCLI RemoteHostConfig info** <guid> - ホストに関する追加情報を表示します。

ConnectCLI GetHostIdentifyingInfo - システム上で認識されているホスト名とアドレスを表示します。

ConnectCLI RemoteHostGroupMembers - 利用可能なシステム(ホスト)グループの一覧表示またはシステム・ホストの追加や削除を行います。

ConnectCLI RemoteHostGroups - システム(ホスト)グループの一覧表示、作成、削除を行います。

ConnectCLI SystemInfo <address> - Ericom Connect に登録されたすべてのシステム(ホスト)の詳細な仕様が表示されます。

ConnectCLI RemoteHostConfig common WebServerAddressList=https://<サーバ 1>:8044,https://<サーバ

2>:8066 - RemoteAgent Web サービス用に指定したアドレスを RemoteAgent が使用するよう設定します(タイプ 2 の RemoteAgent のみに適用)。 これらの値をサーバ・サイドで設定すると、クライアント・サイドの設定は上書きされます。

1.5.5 高度な設定

ConnectCLI SetLogLevel - すべてのコンポーネント(Server、ESG、EUWS、AWS、RA)のログ・レベルを、指定したレベルに設定します。 デフォルトのレベルは警告です。この設定は個々のコンポーネント設定コマンドで行うことができます。

ConnectCLI ConfigureCertificates - (現在のマシン上で)利用可能なすべての証明書の表示、または ESG、EUWS、AWS 用の共通の証明書を設定します。設定は他のコマンドでも行うことができます。

この設定により、すべてのインスタンスに対してグローバルな証明書を設定します。 EsgConfig、EuwsConfig と AwsConfig コマンドを使用して、インスタンスごとに証明書を設定することも可能です。

ConnectCli ConfigureCertificates reset - デフォルトの自己署名証明書を使用するように**すべての**コンポーネントをリセットします。

ConnectCLI DeleteCertificates - ローカルの証明書ストアから証明書を削除します。

ConnectCLI DeleteConnectCertificates - システムからすべての Ericom 自己署名証明書を削除します。

ConnectCLI ImportReportDefinitions - 新しいレポート定義をインポートします。

ConnectCLI ServerSideTimings - サーバ・サイドのパフォーマンス・タイマーを表示します。

ConnectCLI EncryptSsoPassword - SSO インターフェースで使用するための暗号化されたパスワードを作成します。 パラメータとしてパスワードを入力していない場合、プロンプトが表示されます。このコマンドには管理者の認証が必要です。

引数: 暗号化するパスワードを入力します

ConnectCLI ImportLanguageFiles - 言語ファイルをインポートします。

ConnectCli TechnicalSupport [GetConfigurationProperties, SetAllServicesAsStopped, QueuedLogMessages, cbMonitor, expirePassword, changePassword,clearAutoDeletes, gridMonitor, multiValidate, dbgmon]

ConnectCli technicalSupport dbgmon - すべてのデバック・メッセージを高度なデバックで使用するコンソール・ウィンドウに送信します。

1.5.6 アイコンの構成

ConnectCLI SetIcon - 公開済みのリソースにカスタム・アイコンを設定します

引数リストの形式は次のとおりです:

[/SaveIcon <ファイル名
>] <FileWithIcon> [<ResourceNameRegex>]

FileWithIcon: (任意の拡張子を使用した)任意のファイルのパス。 ファイルのアイコン(Windows エクスプローラで表示されるアイコン)が一致したリソースと関連付けられています。

ResourceNameRegex: 設定するアプリケーション名にマッチする正規表現(標準の Connect 式言語を使用)。 ここでは、大文字と小文字が区別されます。 正規表現に複数のアプリケーションがマッチする場合、それらが一覧表示され、確認が要求されます。

/SaveIcon <filename>: アイコンは指定されたファイル名で保存されます(拡張子は強制的に「.ico」になります)。 これは、アイコンを常設として設定せずに、どのアイコンを使用するかを検証するために使用できます。

テナントのアプリケーションのアイコンを設定するには、「/tenant」パラメータを追加します。 例えば、次のコマンドにより、公開済みの「Browser」アプリケーションにおいて、テナント名「tenant1」のアイコン・ファイル「firefox2.ico」が使用されるよう設定します。

ConnectCLI SetIcon /tenant tenant1 c:\firefox2.ico Browser

1.5.7 ライセンス

ConnectCLI GetLicenseInfo - Ericom に送信されライセンス発行に使用されるデータを生成します。

ConnectCLI ImportLicense - Ericom から受信したライセンスをシステムにインポートします。

1.5.8 エンドユーザ情報

ConnectCLI ResourceTree - ユーザが利用可能なすべてのアプリケーションが表示されます。

ConnectCLI LaunchAnalysis - ユーザがアプリケーションの起動を試行した際に何が発生するかが表示されます。

1.5.9 Active Directory の構成

ConnectCLI ActiveDirectories - エンドユーザに使用されている Active Directory アクティブ・ディレクトリのセットにおいて、管理者が一覧表示、追加、削除を行うことを許可します。

ConnectCLI ActiveDirectories list - 設定済みの Active Directory が一覧表示されます

ConnectCLI ActiveDirectories add test.local –「test.local」AD を追加します

ConnectCLI ActiveDirectories remove test.local -「test.local」 AD を削除します

ConnectCLI UserActiveDirectoryInfo user@test.local - Active Directory から「user@test.local」についての情報が表示されます。

ConnectCLI ActiveDirectories /nonStandardUpnSuffixes upntest.local modify test.local - 標準外の UPN サフィックスドメインを設定し、これらのドメイン・サフィックスでユーザがログインできるようにします。

ConnectCLI ActiveDirectories /adUser mike@test.local /adPassword Hello1 add test.local

- adUser「mike」を指定し、adPassword「Hello1」を Ad「test.local」へ追加します。

より詳細な使用法については、展開ガイドの Active Directory ConnectCLI の使用法のセクションを参照してください。

1.5.10 ConnectCLI 管理者の資格情報の設定

ConnectCLI では、各実行に管理者の資格情報が必要となります。 時間を節約するには、「set」を使用して、管理者の資格情報を環境変数として設定可能です。 コマンドのサンプルは次のとおりです:

C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>set ec_admin_user=john.doe@acme.com
C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>set ec_admin_password=MyP@s$w0rd

1.5.11 テナント設定

ConnectCLI tenant /? – テナント設定に関連するすべてのコマンドが表示されます。

ConnectCLI tenant list – 設定済みのすべてのテナントが表示されます

ConnectCLI tenant /tenantUrlPrefix acme add company1 – 識別子「company1」とプレフィックス「acme」を使用して新しいテナントを作成します。 プレフィックスは管理コンソールへのログインに使用され、テナントの URL として使用されます(例: acme.serviceprovider.com)。

ConnectCLI TenantConfig - テナント設定パラメータを表示または設定します。引数なしの場合、すべての設定が表示されます。 引数を指定すると、指定した値にプロパティが設定されます。

ConnectCLI EndUserTenantReassign <user> <tenant> - 新しいテナント「<tenant>」に既存のユーザ「<user」の再割り当てを行います。

ConnectCLI ActiveDirectories /tenant TenantA add company1.com – Active Directory「company1.com」をテナント「TenantA」に割り当てます。

1.5.12 切断されたサービス・コンポーネントのマーク

サービス・コンポーネントの一覧を表示するには次を実行します:

ConnectCLI Services list -

「切断」のためのコンタクトを失ったすべてのサービスをマークするには次を実行します:

ConnectCLI Services cleanup PermanentlyDisconnected (or TemporarilyDisconnected) – サービスを切断された状態に設定します。

このコマンドは「接続不可」状態のものだけが設定され、停止しているサービスへの設定は行われません。

バージョン 7.5 で非推奨のコマンド(上記のコマンドを使用してください):

ConnectCLI AwsConfig|EuwsConfig|EsgConfig|BLServiceConfig|RemoteAgentConfig list

ConnectCLI StandaloneServerSetState PermanentlyDisconnected id1 id2 …

1.5.13 RemoteAgent を切断する

RemoteAgent(サーバおよびワークステーション)の一覧を表示するには次を実行します:

ConnectCLI Systems list - 「切断」するためのコンタクトを失ったすべての RemoteAgent をマークするには、次を実行します:

ConnectCLI Systems cleanup PermanentlyDisconnected (または TemporarilyDisconnected)

バージョン 7.5 で非推奨のコマンド(上記のコマンドを使用してください):

ConnectCLI RemoteAgentConfig の一覧

ConnectCLI RemoteHostSetState PermanentlyDisconnected id1 id2 …

1.5.14 SQL データベースのバックアップ/リストア

データベースをバックアップするには次を使用します:

:ConnectCLI BackupDatabase /databaseServer <サーバ名> /databaseName <DB 名> [/databaseUser <ユーザ>] [/databasePassword] /noconfirm backupFileName.bak

データベースをリストアするには次を使用します:

ConnectCLI RestoreDatabase /databaseServer <サーバ名> /databaseName <DB 名> [/databaseUser <ユーザ>] [/databasePassword] /noconfirm backupFileName.bak

この 2 つのコマンドは、「backupFileName」にコピーを保存することで SQL Server データベースのバックアップ/リストアを行います。 「/databaseServer」と「/databaseName」を指定する必要があります。 「 /databaseUser」を指定していない場合、データベースへの接続時に Windows 認証が使用されます。 /noconfirm が指定されていない場合、既存のバックアップ・ファイルまたはデータベースを上書きする前に、確認が要求されます。

- バックアップ・ファイルを保存する場所が必要です。
- システムの実行中にバックアップが実行される場合があります。
- 万が一バックアップ作業中にエラーが発生した場合でも、稼働中のデータベースは影響を受けず、データは失われません。 その場合はもう一度バックアップ作業を試みます。

これらの作業を問題なく実施するために、データベースで SQL コマンド「backup database」がサポートされている必要があります。 これは SQL Server と SQL Server Express に該当し、クラウド・ベースの Amazon と Azure SQL のプロバイダには該当しません。

さらに、現在のユーザがデータベースのバックアップ・ディレクトリへのアクセス権を持っている必要があります。 通常、ディレクトリは次のようになります:
「"C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup」

サーバがリモート・マシン上にある場合、ユーザが UNC パス経由でのディレクトリへのアクセス権を持つ必要があります。 例えば次のようになります: \\サーバ\C$\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup

リストアは 2 つ方法のいずれかで実行できます。

- データベースが破損し、同一のデータベース・サーバとデータベース名でバックアップからリストアする必要がある場合:
  - すべての Connect グリッドのサービスを停止します
  - データベースをリストアします

    - サービスを起動します
- データベースは、再配置または名前の変更が行われた状態になります
    - すべてのグリッド・マシンで「Disconnect from Grid(グリッドからの切断)」を実行します
    - 「Redeploy(再展開)」を実行します
    - いかなる状況でも、実行中の Connect システムに対してはリストアを実行しないでください。 実行した場合、システムが破損する可能性があります。

リストア作業中にエラーが発生した場合、データベースが破損します。この事態が発生した場合、破損したデータベースを削除し、リストア作業を再度試行してください。

1.5.15 古いデータベースのデータを消去する

ConnectCLI コマンドを使用して、指定したデータ以前のログメッセージを削除することができます。 デフォルトの期間は 90 日間です。以下の 2 つのコマンドを使用できます:

- ConnectCli DeleteOldLogMessages [オプション]*
- ConnectCli DeleteOldLogMessagesDb [オプション]*

DeleteOldLogMessages は、Connect サーバからデータベース化された接続情報を取得します。DeleteOldLogMessagesDb は、コマンド・ラインからそれを実行します。 メッセージが削除されると、データベースの容量が圧縮されます。オプションの一覧を確認するには、

/? を使用します。 デフォルトでは、**レポート**レベルのログメッセージはレポート機能を維持するために削除されません。

ConnectCLI コマンドを使用して、指定したデータ以前のデータベース・**セッション**・データを削除することができます。 デフォルトの期間は 90 日間です。 以下の 2 つのコマンドを使用できます:

- ConnectCli DeleteOldSessions [オプション] *
- ConnectCli DeleteOldSessionsDb [オプション] *

DeleteOldSessions は、Connect サーバから DB 接続情報を取得します。DeleteOldSessionsDb は、コマンド・ラインからそれを実行します。 これにより、いくつかのテーブルが消去されます。 オプションの一覧を確認するには、/? を使用します。

1.5.16 ライセンスのリカバリ

オフラインの Ericom Connect システムにライセンスをインポートすることが可能です。 これにより、異なるグリッド名および Active Directory を持つライセンスを設定できます。

ライセンス要求のデータを生成するには -

ConnectCLI GetLicenseInfoRecovery gridName domainName outputFileName.xml

ライセンスをインポートするには -

ConnectCLI InstallLicenseRecovery /databaseServer <DB サーバ> /databaseName <DB 名> [/DatabaseUser user] [/DatabasePassword pwd] license.xml

管理者ユーザを追加するには -

ConnectCLI AddAdminRecovery /databaseServer < DB サーバ>

/databaseName <DB 名> [/DatabaseUser user]

[/DatabasePassword pwd] license.xml newAdminUser [password]

パスワードはアカウントの検証に使用され、保存はされません。

1.5.17 デスクトップのタイトル・ラベルを変更する

デスクトップ・セッションのタイトル・バーに含まれるラベル・テキストを変更する(IP アドレス、Blaze クライアント・ラベル、アクセラレーション・ラベルを入れ替える)には、次のコマンドを使用します:r

ConnectCli ConnectionConfig title="Custom Title Label"

使用法: ConnectCLI ConnectionConfig [オプション]* [prop=val or prop=@filename] ...

r 共通接続(Blaze ファイル)のオプションを設定または確認します。これは、このパラメータを上書きしていないすべてのリソースとグループに影響します。

/adminUser <string> []

ユーザ名 (env = EC_ADMIN_USER)

/adminPassword <string> []

パスワード (env = EC_ADMIN_PASSWORD)

/tenant <string>　　[rooturl]

テナント (env = EC_ADMIN_TENANT)

/gridName <string>　　[ECPRE1a]

使用するグリッド名 - (EC_GRID_NAME)

/locators <string>　　[10.0.0.12:4174]

グリッドを探すために使用する場所

/[no]ShowInheritance　[False]
/[no]techSupport　　[False]

より詳細な情報は、テクニカル・サポートまでお問い合わせください。

1.6　ライセンス

各 Connect グリッドでは、30 日間、50 同時ユーザの評価版ライセンスが提供されます。 イニシャル・ライセンス情報の抽出と新しいライセンスのインポートは、管理 GUI または ConnectCLI コマンドを使用して実行できます。 追加のグリッドの実装(例:テスト用)には、別のライセンスが必要になります(こちらについては、Ericom の担当者までお問い合わせください)。

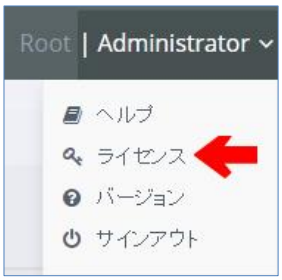
公開済みのリソースを Connect 経由で起動する際、ライセンスが利用可能である必要があります。 Connect を介して開始されるすべてのリモート・セッション(新規または再接続)は、このライセンスの下のユーザとしてカウントされます。

ポータル・セッション(AccessPortal、AccessPad、AccessToGo)のログインはライセンスとしてカウントされず、それらから起動されたリソースのみがカウントされます。

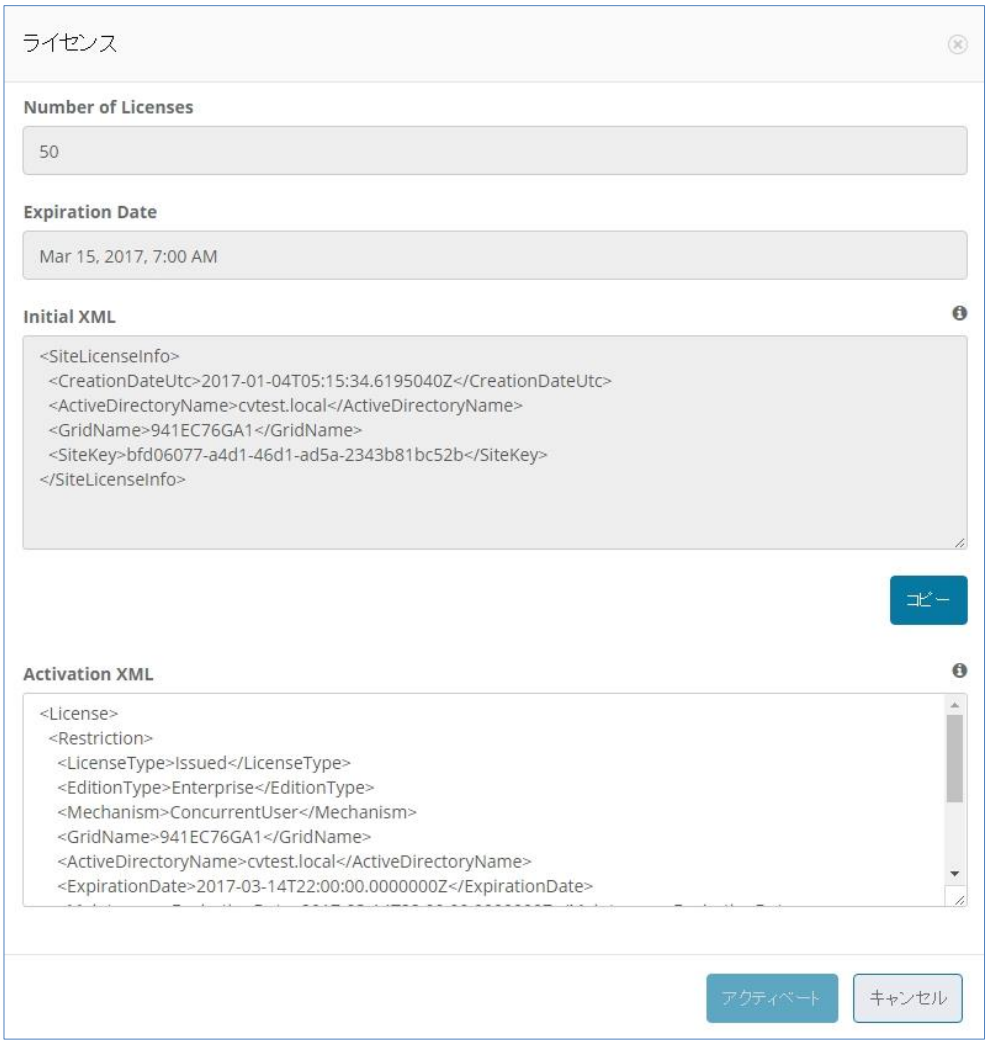
1.6.1 管理コンソールでのアクティベーション

アクティベーションまたは延長のために Ericom にイニシャル・キーを送信するには:

- 管理コンソールにログインします
- 「設定」 | 「ライセンス」 に移動



以下のウィンドウが表示されます:



- 「Initial XML」をコピーして Ericom に送信します
- Ericom が新しいキーを生成します。キーを表示ウィンドウの下部のセクションにコピーし、「アクティベート」を押します。これで、新しいライセンスが有効になります。

1.6.2 ConnectCLI でのアクティベーション

アクティベーションまたは延長を ConnectCLI を使用して実行することが可能です:

- 「ConnectCLI GetLicenseInfo >info.xml」を実行します
- 「info.xml」ファイルを Ericom に送信します。
- Ericom が新しいキーを生成し、「license.xml」という名前のファイルでライセンスが返信されます。

Ericom からライセンス・ファイルを受け取り、そのファイルをシステムにインポートします。 ライセンスの内容は以下の構造となっています:

```
<License>
 <Restriction>
  <LicenseType>string</LicenseType>
  <EditionType>string</EditionType>
  <GridName>string</GridName>
  <ActiveDirectoryName>string</ActiveDirectoryName>
  <ExpirationDate> string</ExpirationDate>
  <MaintenanceExpirationDate>string</MaintenanceExpirationDate>
  <NumberOfSessions>number</NumberOfSessions>
  <Id>string</Id>
 </Restriction>
 <Signature>string</Signature>
</License>
```

ファイルを受け取ったら、次の ConnectCLI コマンドを実行してライセンスをインポートします:

「ConnectCLI ImportLicense <license.xml へのパス>」

1.6.3 入手可能なエディション

Ericom Connect は様々なエディションが入手可能です。 Ericom Web サイトの表を使用して、エディションの違いを参照してください: http://www.ericom.com/connect-feature-matrix.asp

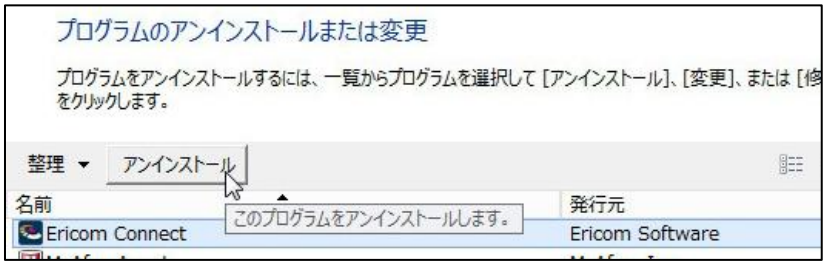
カスタムの機能セットも入手可能です。 詳細については、Ericom の販売代理店にお問い合わせください。

1.6.4 Connect に含まれる AccessNow と Blaze

Ericom Connect のライセンスには、Ericom AccessNow HTML5 と Blaze アクセラレーションのテクノロジーが含まれています。 これらのテクノロジーを使用するために追加コストは必要ありません。

1.7 Connect のアンインストール

Ericom Connect Configuration Tool を起動して、グリッドから切断します。ツールを終了し、システムの「プログラムの追加と削除」機能を使用して Connect をアンインストールします。



2 管理コンソールの使用方法

2.1 管理コンソールへのサインイン

Web ベースの管理コンソールを起動するには、以下の方法があります:

- Ericom Connect Configuration Tool を起動し、メイン・メニューから「Launch Admin UI」を押します。
- 次の URL を使用します: https://サーバアドレス:8022/Admin/

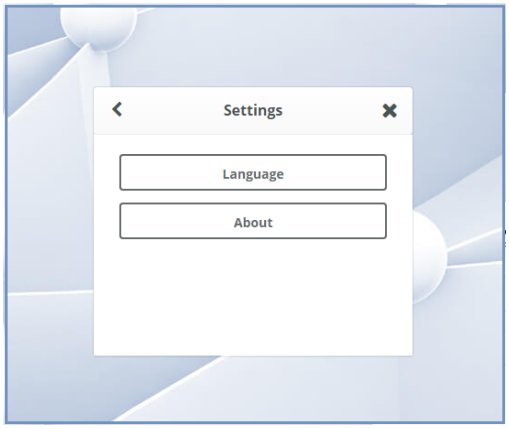
管理コンソールへサインインするための初期アクセス権は、グリッド作成用に設定された管理者ユーザに付与されます。

Web インターフェースは、水平解像度 1366 ピクセルに最適化されています。

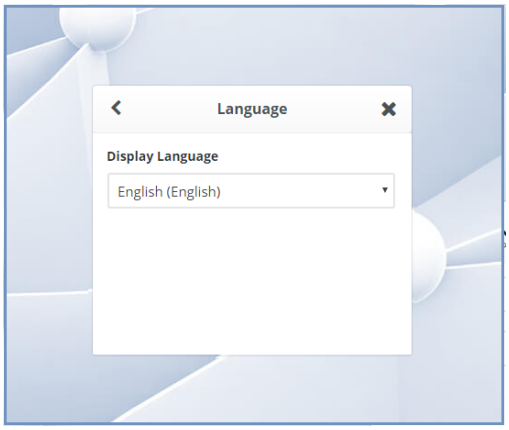
バージョン 7.6 以前の Ericom Connect ユーザは、次のアドレスに移動して旧バージョンの管理コンソールにアクセスできます: https://<サーバアドレス>:8022/Admin/classic.html

ユーザ・インターフェース言語の選択

管理コンソールのユーザ・インターフェース言語を変更するには、右上のコンテキスト・メニューをクリックして、設定画面を開きます:

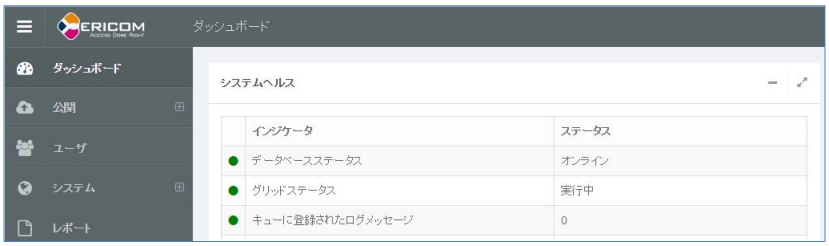


言語オプションを選択します



一覧から目的の言語を選択すると、選択した言語がユーザ・インターフェースに使用されます。

日本語を使用する例:

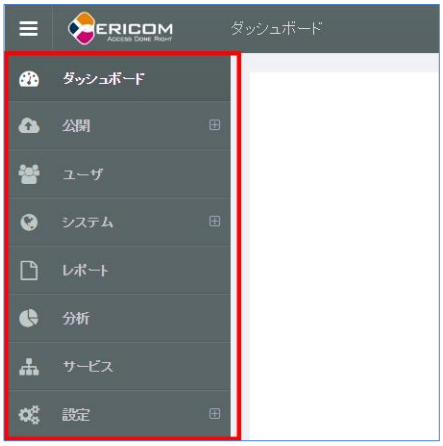


Ericom connect の一部のデフォルト・ オブジェクトは英語で作成されており(例: : 「All Resources」や「All Hosts group」)は翻訳されません。 これらのテキストをローカル言語に変更するには、オブジェクトのプロパティに移動し、ローカル言語で任意のテキストを入力します。

2.2 管理コンソールを使用する

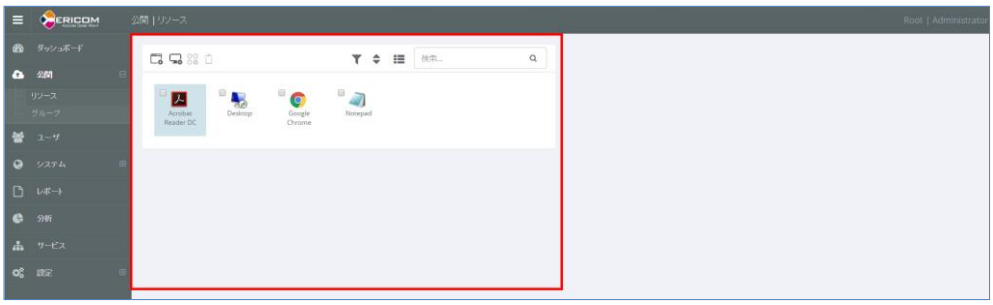
この Web ベースの管理コンソールは、以下のパネルで構成されています:

ナビゲーション・パネル



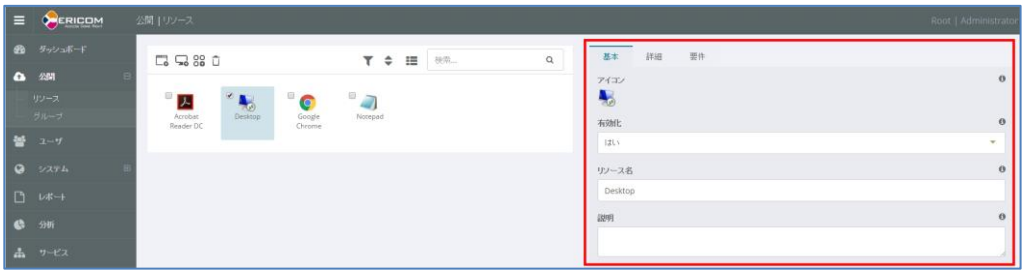
ナビゲーション・パネルはコンソールの左端にあります。このパネルでは、管理コンソールで使用可能なカテゴリや機能が表示されます。カテゴリの中には、サブ・セクションが含まれていることを示す小さな矢印が右側に表示されるものがあります。カテゴリ名を押して展開すると、サブ・セクションが表示されます。もう一度押すと、サブ・セクションの一覧が閉じます。 垂直解像度が低いモニタでは、スクロール・バーが表示されます。

プライマリ・パネル



このパネルはコンソールの中央エリアにあります。このパネルでは、選択したカテゴリに関連する高度な情報および設定が表示されます。一部のカテゴリ(例えば「ダッシュボード」)では、「プライマリ」パネルはワイドに表示され、その他のカテゴリ(例えば「リソース」)では、「詳細」パネルが「プライマリ」パネルに含まれます。

「詳細」パネル



このパネルは、一部のカテゴリでコンソールの右側に表示されます。表示される場合、このパネルには「プライマリ」パネルで選択したアイタムの追加情報および設定機能が含まれます。

一覧オブジェクトの展開と折りたたみ

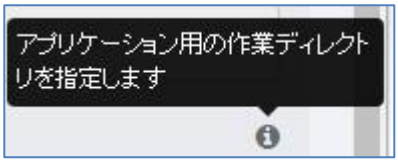
管理コンソールの一部のオブジェクトは、関連付けられた矢印アイコンをクリックして、展開または折りたたむことができます。 通常このようなオブジェクトは、同一カテゴリの追加オブジェクトの一覧です。

「展開」 - 現在は折りたたまれた状態で、内容のオブジェクトは非表示となっています。 内容の追加オブジェクトを表示するには、アイコンをクリックして「展開」モードに入ります。

「折りたたみ」- 現在は展開し、内容のすべてのオブジェクトが表示されています。 内容のオブジェクトを非表示にするには、アイコンをクリックして「折りたたみ」モードに入ります。

ツールチップ(ツールヒント)

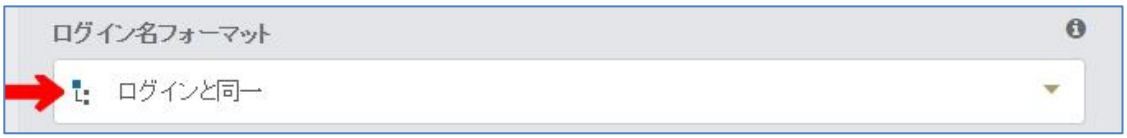
「詳細」パネルで一部の設定の上にマウス・カーソルを置くと、機能の目的や詳細な設定を説明するツールチップのメッセージが表示されます。



継承の切り替え

それぞれの設定には、別のレイヤーから値を継承できます。 「継承の切り替え」ボタンを使用して、継承された値を継承するか「ローカル」値を設定するかを管理者が選択できます。 Connect で継承を操作する方法の詳細については、「展開ガイド」の「継承階層」を参照してください。

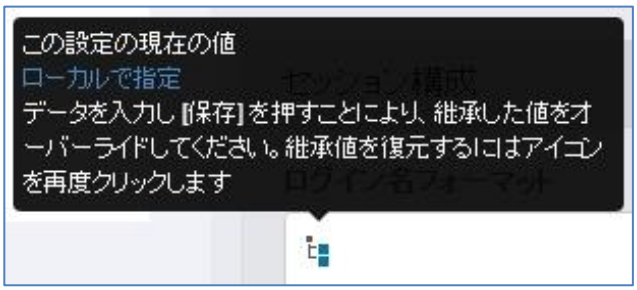
継承ボタンの例:



2.2.1.1 **ローカル値の指定**

対象の設定を構成し、ローカル値を使用するように「継承」ボタンを設定します:

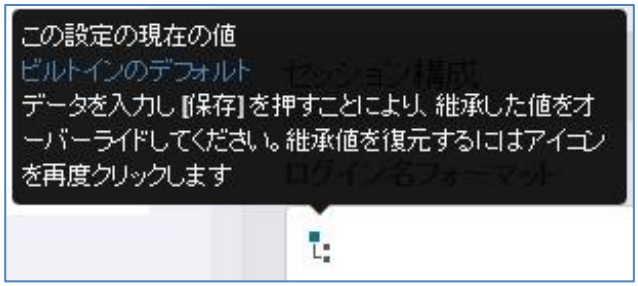
ローカル値が使用されていることをツールチップから確認できます。



2.2.1.2 **継承された値の使用**

継承された値を使用するように「継承」ボタンを設定します:

継承された値が使用されていることをツールチップから確認できます。



2.3 ダッシュボード

「ダッシュボード」はウィジットで構成されています。 各ウィジェットには、システムの健全性、ユーザ・アクティビティおよびリモート・ホスト・データに関連する有用な情報が表示されます。

システムヘルス

このウィジェットは、Connect システムの健全性に関連する有用な情報を提供します。 システムに問題がある場合、まずこの場所でエラーと警告を確認してください。このウィジェットには以下のデータが含まれます:

- データベースステータス
- グリッドステータス
- キューに登録されたログメッセージ
- データベース使用量(最大サイズ)
- RemoteAgent（Windows）バージョンステータス
- RemoteAgent（Linux）バージョンステータス
- アクティブ・セッション(Connect 以外のリモート・セッションは含まれていません)
- 切断済みセッション(Connect 以外のリモート・セッションは含まれていません)
- ライセンスステータス
- ライセンスの有効期限
- ターミナル・サーバ(数)
- デスクトップ(数)

- 公開アプリケーション(数)
- テナント

システムヘルス

	インジケータ	ステータス
●	データベースステータス	オンライン
●	グリッドステータス	実行中
●	キューに登録されたログメッセージ	0
●	データベース使用量(最大サイズ)	80MB/10240MB 1%
●	RemoteAgent(Windows)バージョンステータス	全て最新
	RemoteAgent(Linux)バージョンステータス	ホストは登録されていません
	アクティブセッション	0
	切断セッション	0
●	ライセンスステータス	0/50 0%
●	ライセンスの有効期限	2017年3月15日 7:00
●	ターミナルサーバ	ターミナルサーバの使用数(無制限):3
●	デスクトップ	デスクトップの使用数(無制限):0
●	公開アプリケーション	アプリケーションの使用数(無制限):4
●	テナント	0/1000 0%

ターミナル(RDS)サーバとワークステーションの状態を監視するには、「システム」|「登録済み」に進みます。

ステータス・インジケータ

緑: 正常 - 通常動作

黄色: 動作可能警告 - 動作可能、ただし注意が必要です

赤: 早急な対応が必要です - 動作不可または切迫した問題があります。

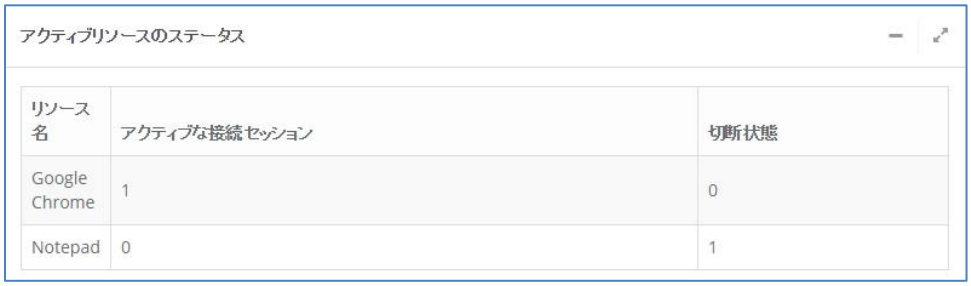
インジケーター	**測定基準**
データベースの使用率	緑: 0-74% の使用率 黄色: 75-89% の使用率 赤: 90-100% の使用率 インジケーターなし: 不明 75% では警告ログのみ。76% 以上では保存。 90% ではレポート・ログのみ。91% 以上では保存。 95% では監査ログのみ。96% 以上では保存。 ログメッセージの優先順位は次のとおりです（最低から最高の順）: 冗長、デバッグ、情報、警告、エラー、レポート、深刻、監査。 ユーザのセッション情報が常に保存されます。
RemoteAgent (Windows のみ)	緑: すべての Windows RA が最新です。 黄色: いずれかの Windows RA が v7.6 未満の場合。 赤: いずれかの Windows RA が v7.5 未満の

	場合。
RemoteAgent（Linux）	緑: すべての Linux の RA が最新です。 赤: いずれかの Linux RA が 7.5.1.9573 未満の場合。

アクティブリソースのステータス

各リソースの以下のデータが表示されます:

- リソース名
- アクティブな接続セッション(Connect 経由で開始されたこのリソースのセッション数。Connect 以外の RDP セッション数を含みません)
- 切断状態



アクティブリソースのステータス

リソース名	アクティブな接続セッション	切断状態
Google Chrome	1	0
Notepad	0	1

最近のセッション

各セッションの次のデータが表示されます:

- サーバ名
- ユーザ名

- プリンシパル名
- アプリケーション
- ステータス起動時間

最新の起動情報

サーバ名	ユーザ名	プリンシパル名	アプリケーション	ステータス	起動時間
ec76all1	user01	user01@cvtest.local	Notepad	アクティブ	Jan 04, 2017, 3:45:37 PM
ec76rdsw2k8r2-1	user03	user03@cvtest.local	Google Chrome	アクティブ	Jan 04, 2017, 3:45:10 PM
ec76all1	user01	user01@cvtest.local	Acrobat Reader DC	アクティブ	Jan 04, 2017, 3:43:45 PM

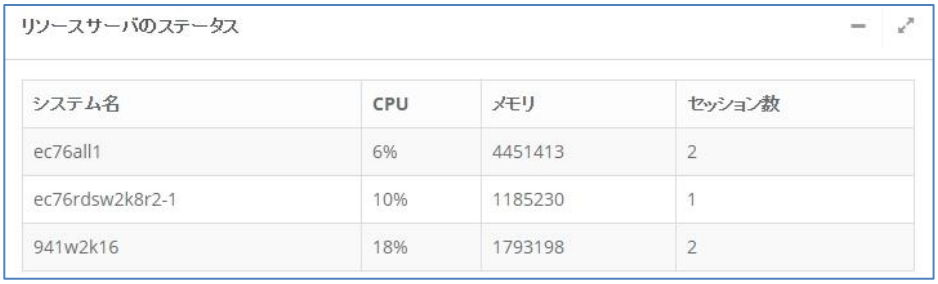
Connect ステータス

サーバが起動された日時が表示されます。

リソース・サーバのステータス

各リモート・サーバとワークステーションの以下のデータが表示されます:

- システム名
- CPU(パーセント)
- メモリ
- すべてのセッションの合計(Connect および Connect 以外のセッションが含まれます)

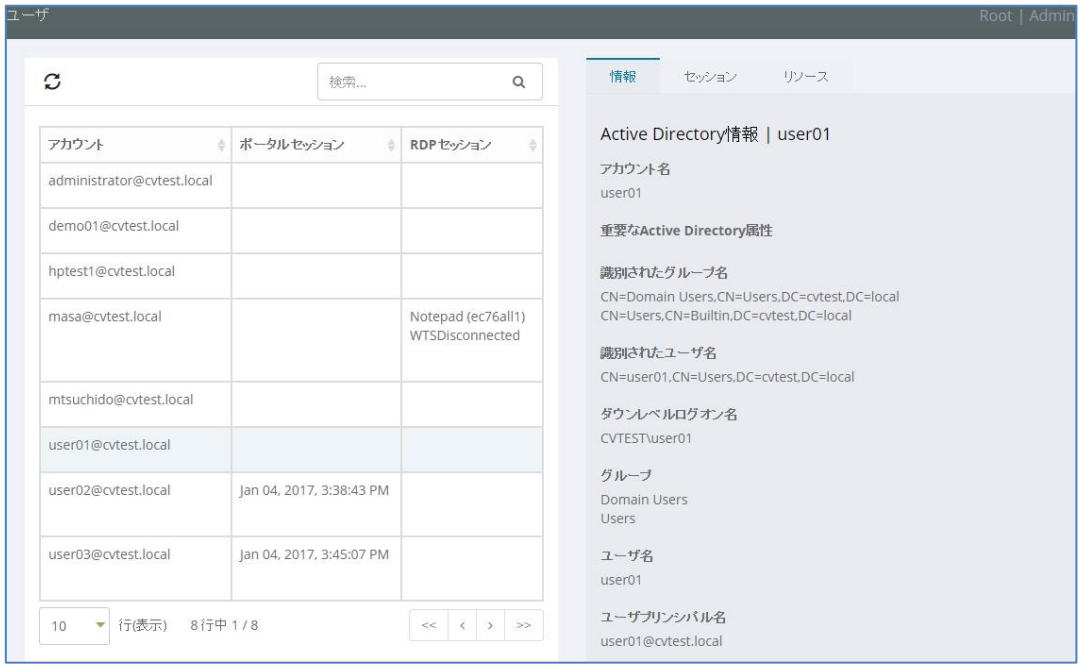


システム名	CPU	メモリ	セッション数
ec76all1	6%	4451413	2
ec76rdsw2k8r2-1	10%	1185230	1
941w2k16	18%	1793198	2

2.4 ユーザ

ユーザ・セクションには、Connect にログインしたすべてのユーザが表示されます。「プライマリ」パネルには、各ユーザが Portal と Connect で開始したアクティブな RDP セッションの一覧が表示されます。

詳細なユーザ・データを表示するには、ユーザ・アカウントをクリックします。関連する情報が詳細パネルに表示されます。



情報

「詳細」パネルの中にあり、選択したユーザの以下の情報が表示されます:

- Active Directory 情報 - Active Directory から取得したユーザ・アカウントの詳細。

セッション

「詳細」パネルの中にあり、次の 2 つのセクションで構成されています: エンドユーザのセッション情報およびリモート セッションの情報

エンドユーザのセッション情報のセクションには、選択したユーザの各セッションについての以下の詳細が表示されます:

- エンドユーザのセッション詳細
- ESG 情報
- クライアント・アドレス
- ポータルの情報

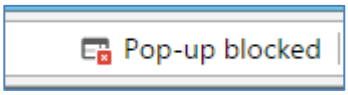
リモート セッション情報のセクションには、選択したユーザのアクティブ・セッションと、各セッションに適用することが可能な操作が表示されます。 アクティブ・セッションに対して操作を実行するに

は、目的のセッションを選択し、操作をクリックします。 以下の操作が可能です:

- ログオフ
- 切断
- リセット
- メッセージの送信
- シャドウ（管理および閲覧オプション）

セッション・シャドウは、マイクロソフトのビルトイン・テクノロジーを利用して HTML5 を使用する際のシャドウイングを行う技術を提供します。これにより、管理者がエンドユーザのセッションを閲覧することが可能になります。 管理者がセッションをシャドウイングする際には、ユーザのセッションをシャドウイングするための資格情報が必要です(例: ユーザのワークステーション上のローカル管理者権限)。 ドメイン・アカウントを使用する場合、ユーザ名または FQDN にドメイン・プレフィックスを入力します。

管理者セッションはブラウザの新規タブで開くため、セッションのシャドウイングを起動するためにポップアップ・ブロッカーを無効化する必要があります。



セッション・シャドウの動作には リモート・デスクトップ・セッション・ホスト(RDSH)が使用されます。RDS CAL が必要となる場合があります。 RDSH ホスト上のセッションをシャドウイングする場合、管理者セッションは同じシステムから起動します。 ワークステーションまたは VDI インスタンスでセッションをシャドウイングする場合、ランダムに選択された RDSH システムから管理者セッションが起動します。 利用可能な RDSH システムが存在しない場合、シャドウ機能は失敗します。

リソース

「詳細」パネルの中にあり、選択したユーザに割り当てられたすべてのアプリケーションが表示されます。リソースの起動分析を開始するには、リソースをクリックします。

起動分析

エンドユーザの選択からリソースの起動までの接続プロセス全体をトレースします。このツールは、接続に関する問題の解決に役立ちます。

起動分析は、異なる Ericom Connect ポータルタイプを使用してシミュレートすることができます。 目的のポータルのタイプを設定するには、次の場所へ移動します: 「設定 | 設定 | セカンダリ設定タブ | 起動分析のポータルタイプ」 (テナントユーザ向けは次の場所へ移動します: 「テナント」 | 「設定」 | 「設定タブ」 | 起動分析のポータルタイプ)

2.5 レポート

「レポート」セクションは、内部に格納されたデータに基づいたレポートを生成するために使用します。 これは、すべての Connect サービスのアクティビティを詳細なレベルで監視する強力な機能です。

「カテゴリ」- ソートに使用する高レベルの区分

「レポート」- 選択した「カテゴリ」に基づく詳細なエリア。 使用可能なオプションは、選択した「カテゴリ」により異なります。

「デフォルト」ボタン - すべてのフィールドをリセットし、デフォルトに戻します

「CSV へエクスポート」ボタン - CSV 形式のファイルにレポート出力データを保存します。

「実行」ボタン - 設定したパラメータに基づいた新しいレポートを生成します。 デフォルトでは出力は常に「タイムスタンプ」でソートされます。ソート条件として使用するには、1 つの列のタブをクリックします(例:「優先度」)

「フィルタ」- カスタム・レポートに表示される必要な情報を絞り込むために使用します。 使用可能な「フィルタ」オプションは、選択された「カテゴリ」と「レポート」により異なります。

「結果」- 設定した「カテゴリ」、「レポート」、「フィルタ」に基づいたデータの出力を表示します。

カテゴリ

システムヘルス(「システム構成」の役割が必要)

- エラー時間別サービスステータス

システムヘルス

- エラー
- 起動要求の有効期限

リソースバインディング

- リソースバインディングの失敗
- リソースバインディングの失敗
- ホストごとのリソースバインディング

- リソースバインディングの詳細

ユーザ

このカテゴリでは、エンドユーザおよびライセンス使用状況を追跡するための以下のレポートが使用可能です。

- エンドユーザ: ユーザのログイン回数、リモートセションの回数、テナント名、初回ログイン時間を表示します
- エンドユーザセッション: ユーザ・セッションの情報(ソース IP、セション終了時間、セッション終了理由、クライアントタイプ、クライアントバージョン)を表示します。
- リモートセッション: ユーザのリモートセッションの詳細(起動したアプリケーション名、サーバ名、セッション終了時間、セション終了理由、再接続と切断の数)を表示します。
- リモートセッション(日ごと)
- 失敗したログイン: 失敗したログイン(ユーザ名、時間、エラー・メッセージ、テナント URL)を表示します。
- セッションの操作: ユーザ・セッションの管理アクションを追跡します: ログオフ、切断、リセット、メッセージ送信、セション・シャドウイング

アプリケーション

このカテゴリでは、公開済みリソースの起動を追跡するための以下のレポートが使用可能です:

- トップアプリケーション - 起動されたすべてのアプリケーションを表示します。最もよく起動されたものが上部に表示されます。
- トップアプリケーション(日)
- トップアプリケーション(週)
- トップアプリケーション(月)
- トップアプリケーション(年)
- トップアプリケーション(曜日)

システム

このカテゴリでは、Connect サーバのモニタリング用に以下のレポートを利用できます(情報はサーバ名に基づいてフィルタされて表示されます):

- サーバごとの起動: 各リモートサーバホストの起動回数
- サーバログメッセージ: ログからの様々なテクニカルデータを表示します
- システム管理者のサーバログメッセージ

メンテナンス

このカテゴリでは、データベースの特性を追跡する以下のレポートを利用できます:

- テーブルサイズ: すべてのデータベーステーブルおよびそれらの容量の使用状況が表示されます

- データベース情報： SQL Server のバージョン、エディション、サーバ名、データベース名、最大サイズ、および現在のデータベースサイズ

テクニカル・サポート

このカテゴリでは、様々なタイプのログを追跡するために以下のレポートが使用可能です:

- すべてのログメッセージ(sysadmin)
- エラー(sysadmin)
- すべてのログメッセージ(tenant)
- メッセージタイプ
- ESG セッションログ

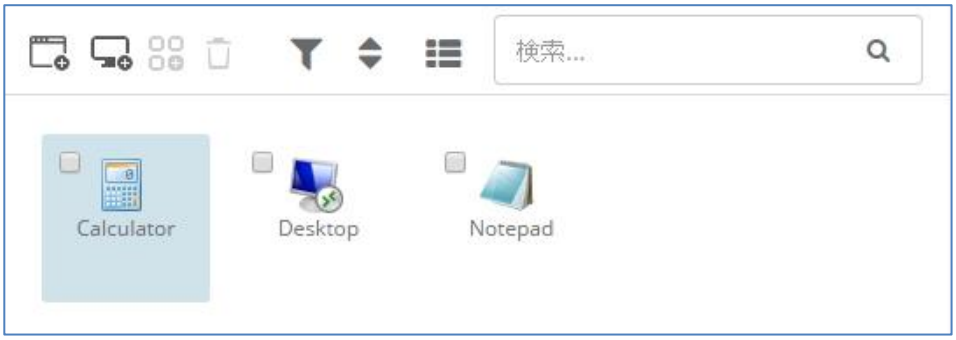
2.6 公開

「公開」セクションは、公開アプリケーションとデスクトップ(リソースとも呼ばれます)の追加、削除および管理を行うために使用します。「プライマリ」パネルにリソースの一覧が表示されます。「詳細」パネルでは、現在の設定が表示され、継承された値を上書きできます。

2.6.1 リソース

「プライマリ」パネルには、「アプリケーション追加」、「デスクトップ追加」、「グループに追加」、「削除」の機能が表示されます。

リソースを追加すると、一覧エリアに表示されます。



アプリケーションやデスクトップを追加すると、自動的にデフォルトの「All Resources」グループに割り当てられます。 リソースは「公開」グループにのみ割り当てが可能で、 Active Directory オブジェクトへ直接割り当てることはできません。 リソースを既存のグループまたは新しいグループに追加するには、「グループに追加」ボタンを選択します。

アプリケーションの追加

この機能を使用して、アプリケーションを選択するダイアログを開きます。 以下のオプションがあります:

- 「サーバへの完全なアプリケーションのパスを入力」- リモート・ホスト上のアプリケーションファイル(.EXE、.LNK、または . BAT)への完全なパスが必要です。 リモート・ホストの Windows の「ファイル名を指定して実行」コマンドを使用して、パスが有効であることを確認してください。 対

象のアプリケーションが起動すれば、パスは Connect での使用に有効です。

- 「選択したサーバからアプリケーションを選択」 - 選択したサーバ上で使用可能なアプリケーションのリストが一覧表示されます。 公開するには、希望するアプリケーションを一覧から「選択」します。

すべてのホスト上の公開アプリケーションを参照するには、「すべてのホストを検索」をクリックします。 Ericom Connect は、対象のアプリケーションが含まれるホストのみからアプリケーションを起動します。 例えば、「すべてのホストを検索」を選択し、「メモ帳」を追加した場合 - ユーザが「メモ帳」を起動すると、Ericom Connect は メモ帳がインストールされているホストのみから選択が行われます(「すべての」ホストからの選択は行われません)

アプリケーションを追加すると、「プライマリ」パネルに表示されます。

デスクトップの追加

この機能を使用して、リソースの一覧に新しいデスクトップのアイコンを追加します。

デスクトップ・リソースにより、リソースに割り当てたグループの「システム」からデスクトップ・セッションが開始されます。

「Active Directory 属性アドレス」でユーザアドレスを含む AD 属性を入力すると、デスクトップ・リソースの宛先アドレスを Active Directory から取得することができます。 詳細については、「展開ガイド」の「AD を経由してデスクトップとユーザをバインドする」を参照してください。

グループに追加

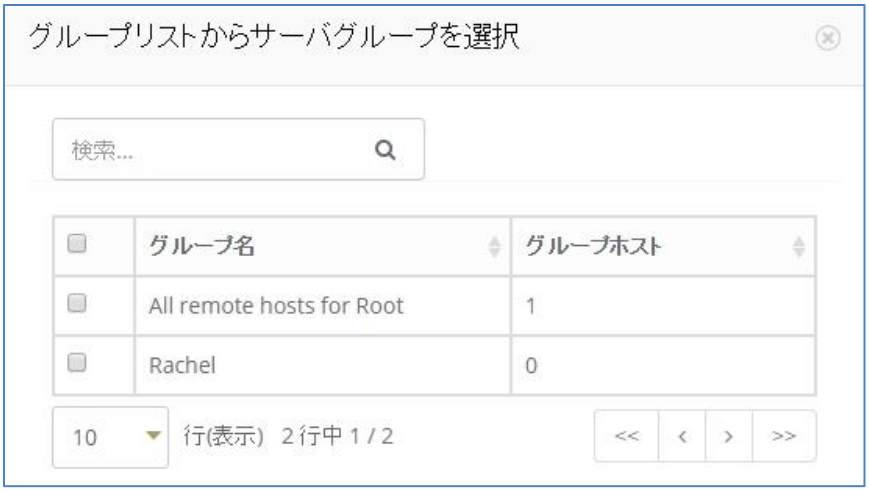
すべての公開アプリケーションとデスクトップを「公開」グループに割り当てる必要があります。 「公開」グループを使用して、グループ・レベルで以下の設定を構成できます:

- 詳細設定
- システム・グループ

公開グループの追加

「公開」グループの所有権を割り当てた後、「システム」と「システムグループを追加」をクリックすると、このリソースで起動可能なサーバとデスクトップが割り当てられます。 各サーバとデスクトップは、エンドユーザからアクセスできるように、「システム」グループのメンバーである必要があります。

そのリソースに「システム」グループを追加するには、「システムグループを追加」をクリックします。



削除

削除する対象のリソース(複数可)を選択します。 Connect からリソースを削除するには、「削除」ボタンを押します。 この操作は元に戻すことができませんので、リソースを削除する際は注意してください。

表示オプション

リソース・エリアは、グリッドやビュー表示にできます。

フィルタ

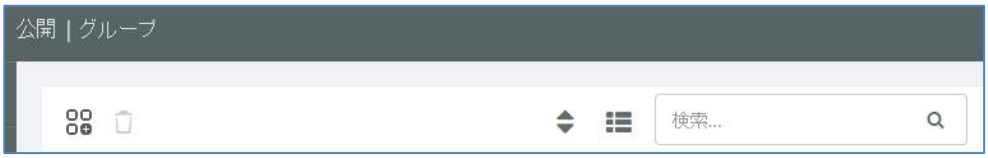
アプリケーションまたはデスクトップのリソースのみを表示するには、「フィルタ」ボタンを使用します。

ソート

リソースがグリッド表示されている場合、次のオプションによりソートが可能です:名前順、追加日時順、変更日時順。

2.6.2 グループ

このセクションでは、新しいグループの作成および既存の「公開」グループの表示と管理ができます。このグループには、グループのユーザが利用可能となるリソースが含まれています。



グループの作成

管理者が新しい「公開」グループを作成できます。管理者は「新しいグループを作成」ウィンドウで、新しい名前を入力し、新しいグループに追加するリソース(リソース・エリアで利用可能なリソースから)を選択できます。

グループの削除

管理者はグループを削除できます。 この操作は、単一または複数のグループに対して行うことができます。 この操作は元に戻すことができません。

表示オプション

グループは、グリッドまたは一覧の 2 つのオプションで表示できます。

ソート

グループを名前(昇順/降順)でソートが可能です。

プロパティ

以下の 5 つのタブがあります:

- 「基本」
- 「リソース」
- 「詳細」
- 「ユーザ」
- 「システム」

各設定には、その目的を説明するツールチップがあります。継承された値は、新しい値を入力し「継承の切り替え」ボタンを押すことで上書きできます。

2.7 システム

2.7.1 ホスト

「プライマリ」パネルには、すべてサーバとワークステーションとその IP アドレスおよびエージェントのステータスが表示されます。

青色のタイトル・バーの「編集」ボタンをクリックして、グローバル・レベルでプロパティを変更できます。

- システム名には、システムの DNS 名が表示されます。
- IP アドレスには、Connect により認識されたシステムの IP アドレスが表示されます。
- AccessServer には、システムの AccessServer エージェントのステータスが表示されます。

- RemoteAgent には、システムの RemoteAgent のステータスが表示されます。
- RemoteAgent には以下の 2 つのタイプがあります: タイプ 1 はグリッドへ接続され、Type 2 では Web サービスを使用します。

2.7.1.1 グループに追加

一覧表から新規または既存のグループへのサーバの追加を行うことが可能です。

2.7.1.2 詳細情報

「詳細」パネルには、テーブルに表示される各サーバとワークステーションの詳細な情報が表示されます。詳細な情報には以下のタブが含まれています

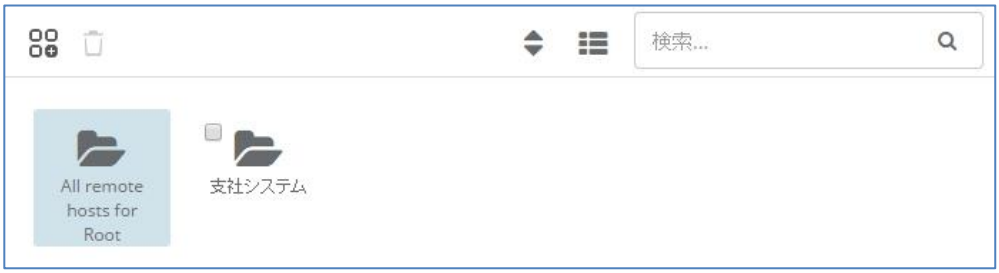
- 「ステータス」

- 「設定」
- 「ログ」

それぞれのタブの各プロパティには、項目を説明するツールのヒントがあります。

2.7.2 グループ

このセクションでは、新しいグループの作成、システムの既存グループの表示と管理ができます。 すべてのサーバとワークステーション(システム)は、「公開」グループに割り当てるために、「システム」グループのメンバーとする必要があります。



2.7.2.1 グループの作成

「グループ作成」をクリックして、Connec 環境のメンバーとなる登録システムを編成します。

グループ名を入力し、「作成」をクリックします。

2.7.2.2 グループの削除

管理者はグループを削除できます。この操作は、単一または複数のグループに対して行うことができます。 この操作は元に戻すことができません。

2.7.2.3 表示オプション

グループは、グリッドまたは一覧の 2 つのオプションで表示できます。

2.7.2.4 ソート

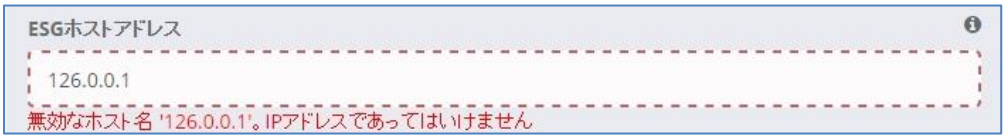
グループを名前(昇順/降順)でソートが可能です。

2.7.2.5 プロパティ

- 「基本」- グループの基本的なプロパティが表示されます

「基本 | ESG ホストアドレス」- システムのこのグループからのセッション起動を許可された、ESG のアドレスを入力します。

DNS アドレス(エイリアス) の入力が必要です(例: both usa.acme.com)。 IP アドレスは使用できません(例: 「126.0.3.32」 は使用できません) この機能により、ESG 経由で接続するユーザによるアプリケーションまたはデスクトップの起動でローカル・ホスト・システム・グループが確実に使用されるようになります。



- 「システム」- グループに含まれるすべてのシステムが一覧表示されます

2.8 サービス

接続サービス一覧表

「プライマリ」パネルには、すべての Connect グリッド・コンポーネント、その IP アドレスとステータスが表示されます。

各サービス・タイプのプロパティをグローバル・レベルで変更するには、サーバ・タイトル・バーの「編集」ボタンをクリックします。

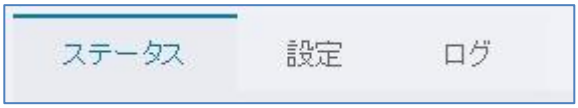
各サービス・インスタンスのプロパティの設定は、各行をクリックするか、ConnectCLI を使用して実行します。

例えば、特定の ESG の証明書を変更するには、**Connectcli EsgConfig list** を実行し、対象の ESG の GUID を探します。

-
```
C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>Connectcli EsgConfig list
Connect Admin User: visitor
Password: ************
97cb65d9-2f8b-4e0e-a7d0-9e789ea47129 GATEWAY
```
- 次に、その GUID を「instanceId」として使用し、証明書の「find」メソッドを設定します。**Connectcli EsgConfig instanceId Security$CertificateFindBy=<on of the FindByXXX values>**
- その後、GUI を使用して実際の証明書パラメータを設定します。**Connectcli EsgConfig instanceId Security$CertificateFindValue=<the value>**

詳細情報

「詳細」パネルには、各 Connect コンポーネント・サーバの詳細なプロパティが表示されます。



「ステータス」タブには、選択したコンポーネント・サーバのステータス情報が表示されます。「ログ」タブには、選択したコンポーネント・サーバから生成されたログ・データが表示されます。

「設定」タブには、選択したコンポーネント・サーバに設定可能なパラメータが表示されます。例えば、このタブでサービスのデフォルトのポートの設定を行います。

2.9 システム構成

デフォルト： 要件

このセクションでは、「要件」タブのデフォルトをシステム・レベルで設定します。同じ設定を同様にグループまたはリソース・レベルで定義できます。

デフォルト： 詳細タブ

このセクションでは、「詳細」タブのデフォルトをシステム・レベルで設定します。 同じ設定を同様にグループまたはリソース・レベルで定義できます。

設定 システム設定

このセクションでは、管理 UI の言語およびタイムアウト間隔などのシステム・レベルの各種パラメータを設定します。

セカンダリ設定

このセクションには、「root」テナント用の追加の構成設定が含まれています。例えば、「クライアントログイン有効化」や「マイ デスクトップの Active Directory 属性」などがあります。 テナントを構成すると、このセクションは自動的に「テナント設定」となり、含まれる設定はテナントごとに定義されます。

RADIUS

このセクションでは、RADIUS 二要素ベース認証と Ericom Connect を使用する場合の RADIUS 設定を構成します。

RADIUS を有効化 - RADIUS 二要素認証を有効化するには、「はい」に設定します。

RADIUS サーバアドレス - RADIUS サーバのアドレスを入力します。

RADIUS ポート - RADIUS サーバのポートを入力します。デフォルトは 1812 です。

RADIUS 共有鍵 - RADIUS サーバ上で設定されている共有鍵を入力します

RADIUS タイムアウト(秒) - RADIUS サーバとの通信のタイムアウトを設定します。

RADIUS 再試行 - 接続が失敗した場合の、RADIUS サーバの再試行の回数を設定します。

RADIUS デフォルト・ドメイン - ユーザ名が完全修飾ドメインでない場合に、ユーザ名に追加するデフォルトのドメインを指定します。一部の RADIUS サーバにより同様の機能が提供される可能性があることに注意してください。 デフォルトのドメインが「@」で始まる場合、次の形式が使用されます:「ユーザ@ドメイン」

デフォルトのドメインが「\」で終わる場合、次の形式が使用されます:「ドメイン\ユーザ」

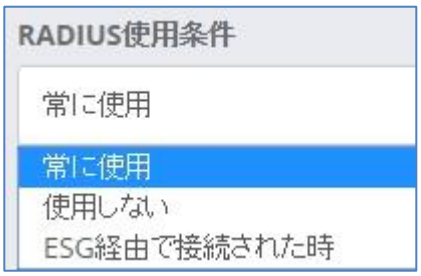
それ以外の場合、「ドメイン\ユーザ」が使用され、検証の警告が表示されます。

RADIUS 送信ユーザドメイン - RADIUS サーバに 完全修飾ユーザ名を使用する場合は、「はい」に設定します。 この属性を「いいえ」に設定すると、ユーザ名のみが送信されます((ドメイン\ユーザ のサフィックス部分、または ユーザ@ドメイン のプレフィックス部分)。この属性を「はい」に設定すると、完全修飾ユーザ名が送信されます。ユーザ名が完全装飾ユーザ名でない場合、RadiusDefaultDomain を指定していれば、それがサフィックスとして追加されます(ユーザ@ドメイン)。

RADIUS 認証方法 - RADIUS システムで使用する認証方法を選択します。指定した文字列が、認証の第一段階で「password」として RADIUS サーバに送信されます。

- **パスワード** - ネットワーク・パスワード
- **パスコード** – パスコード
- **パスワードおよびパスコード** – ネットワーク・パスワードとパスコードを連結した値
- **パスコード及びパスワード** – パスコードとネットワーク・パスワードを連結した値

RADIUS 使用条件 - エンドユーザに RADIUS の使用を要求する条件を選択します。



- 常に使用 - 常に RADIUS が使用されます
- 使用しない - RADIUS は使用されません
- ESG 経由で接続された時 - Ericom Secure Gateway(ESG) 経由でユーザが接続した場合、RADIUS が有効化されます。
- クライアント IP 属性の送信 - クライアントの IP アドレスを特定した属性の RADIUS サーバへ送信します。

ログの設定

各 Connect グリッド・コンポーネントのログ・レベルを設定します。

役割

Ericom Connect の管理者の役割は、このセクションで定義されています。

プライマリ・パネルには、以下の 2 つの機能があります:

- 「Admin の役割を作成」- 事前定義した権限を持つ新しい役割を作成します。
- 「Admin の役割を削除」- 選択した役割を削除します。

新しい役割を作成するには、「Admin の役割を作成」をクリックします。 表示される作成ダイアログに、新しい役割名と説明を入力します。

新しい役割の作成後、その役割を選択して「詳細」パネルでプロパティ設定します。

- 「プロパティ」- 名前と説明を設定します。
- 権限 - 役割の管理コンソール権限を設定します。 ラベル(クロステナント)の付いたすべてのプロパティは、グローバルに適用されます。
- ユーザ/グループ - 役割のメンバーとなるユーザ（複数可)とグループ(複数可)を設定します。

2.10 テナント

このセクションには、追加の構成の設定が含まれています。 1 つまたは複数のテナントを作成すると、「セカンダリ設定」が「テナント設定」に変わります。

デフォルト： 要件

このセクションでは、テナント・レベルで「要件」タブのデフォルトを設定します。同じ設定を同様にグループまたはリソース・レベルで定義できます。

デフォルト： 詳細タブ

このセクションでは、テナント・レベルで「詳細」タブのデフォルトを設定します。 同じ設定を同様にグループまたはリソース・レベルで定義できます。

設定：テナント設定

このセクションでは、様々なテナント・レベルの詳細と設定の構成を行います。例えば、「テナント名」や「「マイ デスクトップ」用の Active Directory 属性」などがあります。

設定：RADIUS

このセクションでは、テナントの RADIUS 設定を構成します。

役割

このセクションでは、テナントの管理者の役割を設定します。

2.11 詳細タブの設定

詳細タブには、様々な機能の設定パラメータが含まれています このセクションでは、いくつかの設定例が示されています。

サードパーティ・ソリューションの有効化

すべてのサードパーティのリダイレクト・ソリューションを有効にするには、「リダイレクトされるサードパーティのアドオン」に移動し、「*」を入力します。 アドオンには、Uniprint、Net2Printer、Tricerat などの数多くの RDP ベースのソリューションが含まれています。

Uniprint、Net2Printer や Tricerat などのサードパーティの印刷ソリューションは、「プリンタのリダイレクトモード」を無効としている場合でもリダイレクトされますので注意してください。 これらのソリューションは、上記の「リダイレクトされるサードパーティのアドオン」設定を使用して構成します。 「プリンタのリダイレクトモード」は、RDP ベースのビルトイン印刷および Blaze 汎用プリンタ のみに適用されます。

キーボード・ロケールの自動切り替え

この機能は日本語環境でサポートしておりません。

Ericom Connect と AccessServer 7.6.1 には、入力に基づいた入力ロケールの自動切り替え(AccessNow セッション内部)が追加されました。文字を入力すると、Ericom AccessServer によりその文字が特定の言語に関連するものであるかがチェックされます。そうである場合、それに応じてキーボードを変更して設定するよう RDP セッションにメッセージが送信されます。ユニコードおよびスキャンコードの入力の両方がサポートされています。 この機能は、互いに大きく異なる言語での使用に最適です(例: 英語とヘブライ語。一方は左から右への言語であり、他方は右から左への言語)。

この機能は、デフォルトでは無効になっています。設定は Ericom Connect 管理コンソールを使用して実行します。 この機能を有効化するには、以下を実行します：

- Ericom Connect 管理コンソールを開き、「詳細」タブのインプット構成 | キーボード言語の判別」へ移動します。
- この機能を有効化するための任意の設定文字列を入力します。

この設定の構文は、以下のとおりです:

keyboard detect languages:s:キーボード ID,開始-終了,開始-終了, ... ; キーボード ID,開始-終了,開始-終了

「開始-終了」の範囲内でキーボード入力が受信される場合は常に、対応する「キーボード ID」を設定する必要があります(キーボード ID

はリモート・オペレーティング・システム上の設定オプションである必要があります)。

例:

keyboard detect languages:s:0x04090409,41-5A,61-7A;0xf03d040d,5BE-5F4

キーボード ID: 0x04090409 = 英語(米国)。41-5A、文字「A-Z」および「61-7A」は、「a-z」です。

キーボード ID: 0xf03d040d = ヘブライ語。5BE-5F4 は次の文字列です: ヘブライ語の句読点 Maqaf - ヘブライ語の句読点 Gershayim。これには、すべてのヘブライ語の文字が含まれます(ヘブライ語の文字用のユニコードと HTML については次を参照してください: https://en.wikipedia.org/wiki/Unicode_and_HTML_for_the_Hebrew_alphabet)
文字の範囲は 16 進数であり、値はユニコード文字の範囲です。

サーバ側でキーボードを手動で変更する場合、クライアント上で言語が再度変更されるまで同期対象外となります。

この機能が正常に動作するには、RDP セッションの現在のユーザ向けに、該当する言語がインストールされている必要があります。 言語によっては、複数のバリエーションが存在します(例: 英語)。

AccessServer のインストール・ディレクトリに、 **LangControl.exe** という名前のプログラムが存在します。現在のユーザ向けにインストールされているすべてのキーボードの一覧を表示するには、**LangControl /list** を実行します。

言語が切り替えられると、新しい言語の最初の入力文字を検出・処理するために 500 ミリ秒のわずかな遅延が発生します。

2.12 正規表現の使用

Ericom Connect の管理者コンソールでは、検索機能での正規表現(regex)の使用がサポートされています。 これには、以下の領域が含まれています:

- 公開 | リソース
- 公開 | グループ
- システム | ホスト
- システム | グループ
- サービス
- ユーザ
- Active Directory の検索
- レポート

使用法:

* (アスタリスク) – 0 個以上の文字に一致します

? - 1 文字のみと一致します

^ - 文字列の先頭と一致します

$ - 文字列の末尾と一致します

% - 1 つのリテラル文字と一致します

大文字小文字を区別しません

部分文字列と一致します(デフォルト)

例: データベースに以下の文字列が存在する場合:

Michael Greenberg
James Lui
Eyal Golan

以下の文字列が一致します(実際の入力では「」記号を省略します):

- 「Greenberg」は 1 番目と一致します
- 「^g」は何とも一致しません
- 「g$」は 1 番目と一致します
- 「g」は 1 番目と 3 番目に一致します
- 「l g」は 1 番目と 3 番目に一致します
- 「l??」は 1 番目、2 番目、3 番目に一致します
- 「l??^」は 2 番目と一致します

3 エンドユーザ・ガイド

Ericom Connect では、様々なオペレーティング・システムやデバイスからのアクセスがサポートされています。 サポートされるデバイスは次のとおりです:

- HTML5 Web ブラウザが搭載されたすべてのデバイス(Access Now インターフェースを使用)
- Windows(7、8.1、2008R2、2012R2 以上)
- Apple Mac OSX 10.10 以上 (Intel のみ)
- ほとんどの Apple iOS デバイス (iPad、iPhone と iPod touch)
- ほとんどの Android デバイス
- Google Chromebook/Chromebox (AccessNow インターフェースを使用)

アプリケーションまたはデスクトップの表示には、以下の 2 つの方法があります:

- ネイティブ・クライアント - エンドユーザのオペレーティング・システムでネイティブに動作するアプリケーションを使用します。 ネイティブ・クライアントは、標準的な RDP の機能をサポートします。
- HTML5 インターフェース - 起動したアプリケーションおよびデスクトップは、Web ブラウザ内に常時されます。エンドユーザのデバイスにダウンロードするものは必要ありません。 印刷やファイル転送などの

機能は、ブラウザ・ベースとなり、ネイティブ RDP クライアントとは異なる動作をします。

エンドユーザは、以下のようなポータルの 1 つを使用してサインインし、割り当てられたアプリケーションとデスクトップを表示することができます。

- AccessPortal - 公開アプリケーションやデスクトップを起動する Web ベースのインターフェース。AccessNow HTML5 プロコトルを使用します。 AccessNow プロトコルはポート 8080 を介して通信します。
- AccessPad - 公開アプリケーションやデスクトップを起動するネイティブ・アプリケーション。RDP または Blaze プロコトルのいずれかを使用します。Blaze プロトコルを使用した場合、通信はポート 8080 を介して行われます。RDP プロトコルを使用すると、通信はポート 3389 を介して行われます。
- AccessToGo - 公開アプリケーションやデスクトップを起動する iOS と Android 向けのモバイル・クライアント。RDP または Blaze プロコトルのいずれかを使用します。Blaze プロトコルを使用した場合、通信はポート 8080 を介して行われます。RDP プロトコルを使用すると、通信はポート 3389 を介して行われます。

この 3 つすべての接続方法は、こちらの URL のページに説明が記載してあります。

https://<EUWS サーバアドレス>:8011/EricomXml/index.html または

http://< EUWS サーバアドレス>:8033/EricomXml/index.html

3.1 AccessPortal(Web)

3.1.1 使用方法

AccessPortal は Ericom Connect のインストールに含まれています。AccessPortal(EUWS) のインストール完了後、ユーザは以下のいずれかの AccessPortal URL を利用します:

HTTPS(信頼された証明書が必要です): https://<サーバアドレス>:8011
HTTP (非セキュア): http://<サーバアドレス>:8033

ESG: https://<ESG アドレス>:<ESG ポート>

ユーザの資格情報のフィールドが含まれたサインイン・プロンプトが表示されます。

ユーザ・インターフェース言語やキーボード・ロケールの選択などの追加設定や 「バージョン」情報にアクセスするには、設定ボタンをクリックします。

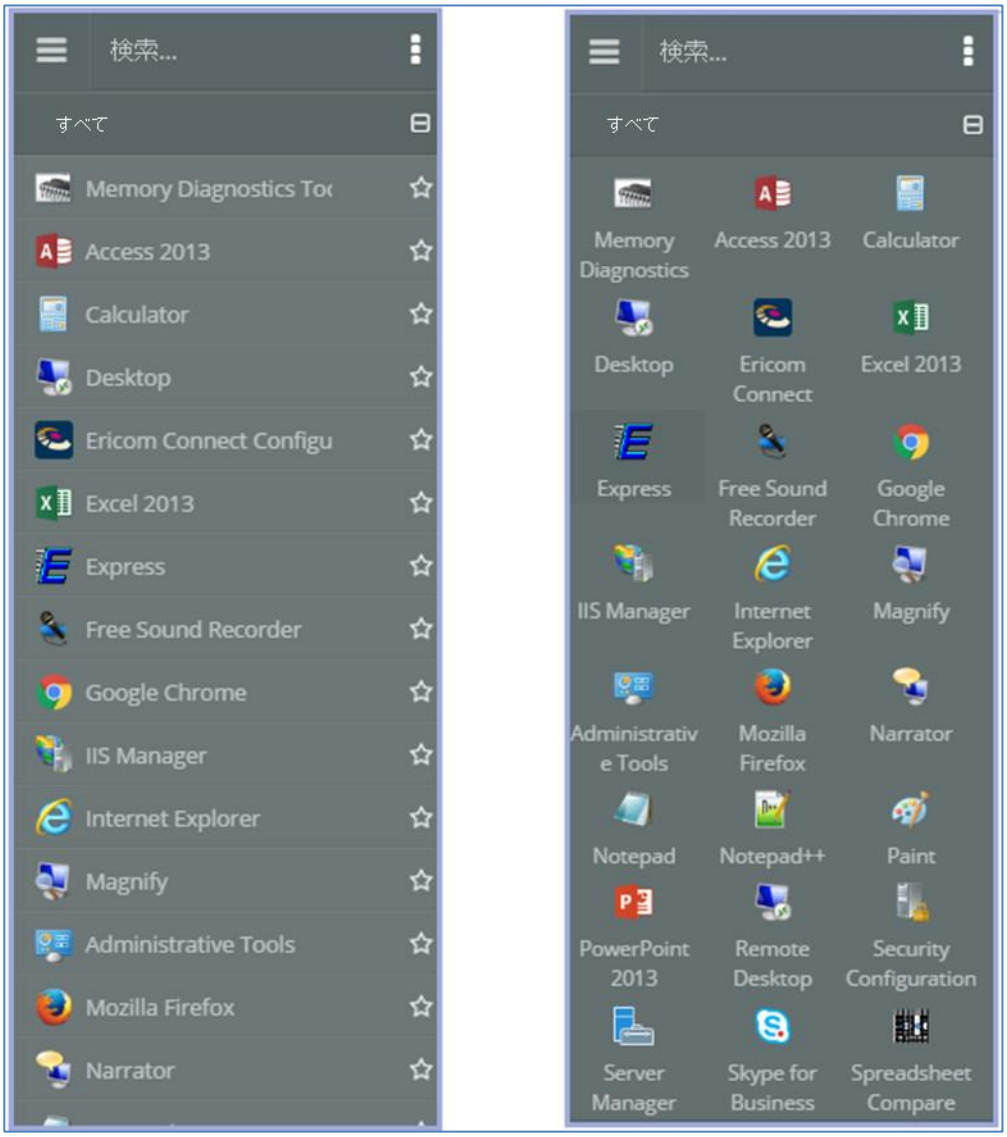
最初の画面には、以下のオプションが表示されます:

「言語(Language)」オプションを選択すると、以下の画面が表示され、そこでインターフェース言語およびキーボード・ロケールを選択することができます。「キーボードロケール(Keyboard Locale)」を選択して、ユーザがセッションで使用するキーボードの言語を選択することができます。 7.6.1 以降では、言語とキーボード・ロケールの設定はブラウザごとにデバイス上にローカル保存されます。 これらの設定をエンドユーザ側で設定すると、Ericom Connect サーバ側のデフォルトが上書きされます。

「バージョン(About)」オプションを選択すると、以下の画面が表示されます。バージョン情報と便利なリンクが含まれています。

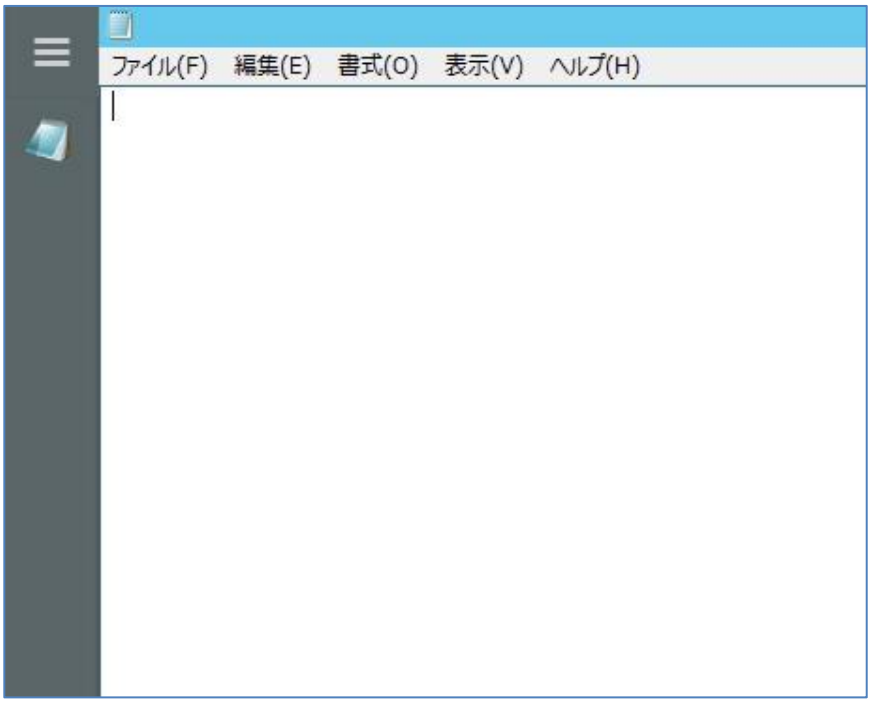
ログインに成功すると、割り当てられたアプリケーションやデスクトップが AccessPortal のメニュー・バーに一覧表示されます。割り当てられたリソースは、以下の 2 つのビューで表示される場合があり

ます: 一覧表示およびグリッド表示(ビューを変更するには、下部の AccessPortal メニュー・バーのセクションに移動します。)



リソースを起動するには、アイコンをクリックまたはタップします。AccessNow HTML5 インターフェースを使用してアプリケーションやデスクトップが起動し、AccessPortal バーは自動的に左に最小化

されます。AccessPortal バー上にアクティブなリソースが表示されます。



AccessPortal バーを表示するには、メニュー・ボタンをクリックまたはタップします:

ユーザのアプリケーション・セットに変更が行われた場合、変更を確認するためにはブラウザを更新します。場合により、ログオフしてから再度 AccessPortal へログインする必要があります。

3.1.2 AccessPortal メニュー・バー

AccessPortal メニュー・バーには、以下のような機能があります:

3.1.2.1 **ファンクション・バー**

ファンクション・バーには、以下のオプションがあります: メニュー・ボタン、検索、コンテキスト・メニュー

メニュー・ボタン - AccessPortal メニュー・バーの表示・非表示を操作するための半透明の移動可能なボタン。

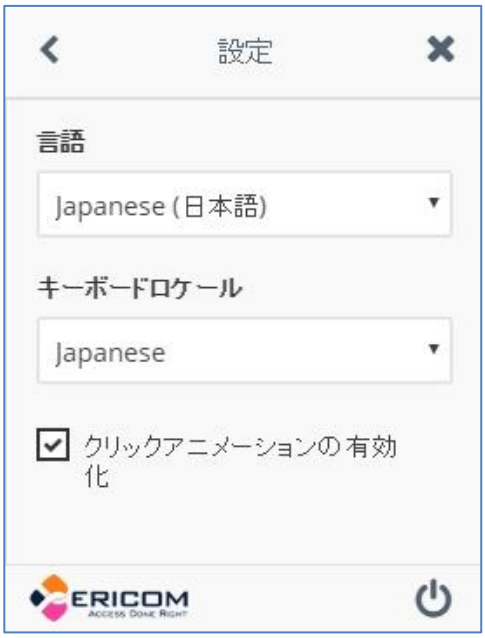
AccessPortal 検索 - 公開リソースの検索用の文字列を入力します。

「アプリケーション」一覧は、自動的にフィルタリングされます。すべてのフォルダが表示されます。これらは検索の文字列でフィルタリングされていません。

コンテキスト・メニュー - アイコンをクリックすると、以下のオプションが表示されます:

グリッドビュー/リストビュー- 一覧とグリッドの表示を切り替えることができます。

設定 - ログイン画面の「設定」オプションと同様、言語、キーボード・ロケールおよび追加のクリック・アニメメーション設定(タッチ・デバイスのみ対象)に関連する設定を変更することができます。

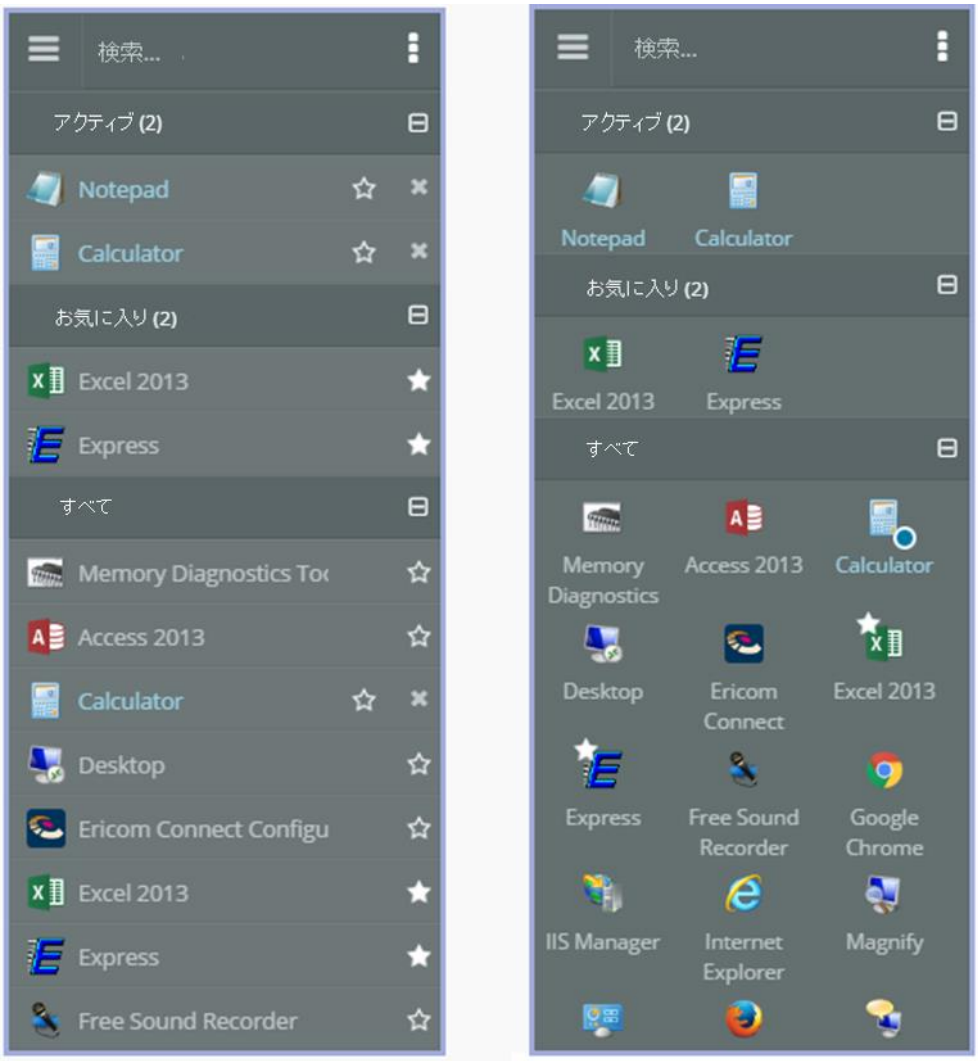


左上の矢印を使用して、前の画面に戻るか、右上の「X」を押してコンテキスト・メニューを完全に閉じることができます。

バージョン(About) – この画面には、現在のバージョン、現在ログインしているユーザ、接続中のーサーバおよび追加の便利なリンクが表示されます。

3.1.2.2 **リソース・エリア**

このエリアには、次の 3 つのセクションがあります: アクティブ、お気に入り、すべて。



アクティブ - すべてのアクティブなアプリケーションとデスクトップを表示します。 アクティブ・セッションが存在する場合のみ表示されます。リソース名は追加の識別として青色で表示され、グリッド表示でも色つきの丸で表示されます。

お気に入り - すべてのお気に入りのアプリケーションとデスクトップを表示します。 お気に入りのセッションが存在する場合のみ表示されます。リソースには、白い星のマークが付いています。

すべて - 使用可能なすべてのアプリケーションやデスクトップを表示します。

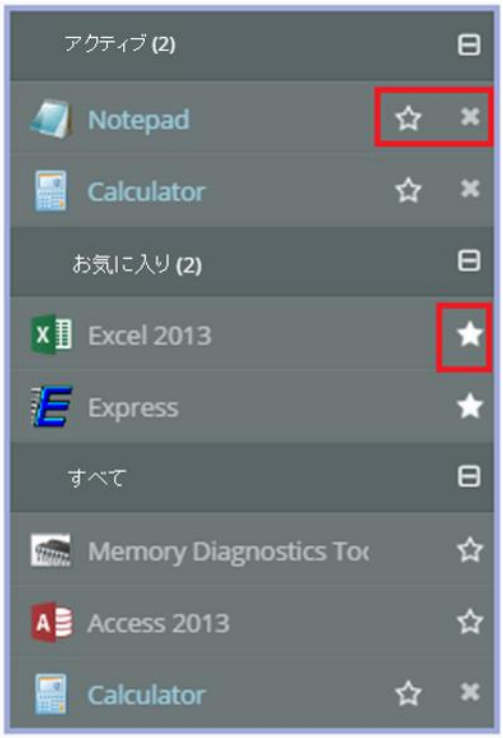
各セクションは、展開または折りたたむことができます。

3.1.2.3 **使用可能な操作**

リストビューでは、割り当てられたリソースについて、以下の操作を使用できます:

お気に入りの追加/削除 – 星のアイコンとして表示されます。使いやすくするために、アプリケーションやデスクトップをお気に入りとして登録することができます。リソースをお気に入りとして登録すると、自動的に「お気に入り」セクションに表示されます。

閉じる – 「X」アイコンとして表示されます。アクティブなセッションを切断します。そのセッションは、自動的に「アクティブ」セッションから削除されます。



グリッドビューでは、これらのアクションはリソース・アイコンにカーソルを合わせると表示される小さなメニューから使用できます。

3.1.3 複数タブの使用

AccessPortal では、ユーザが再度ログインすることなく、複数のタブでセッションを使用できます。 いずれかの AccessPortal タブからログアウトすると、関連するすべてのタブもログアウトします。この設計は、高レベルのセキュリティを維持するためのものです。 新し

いタブで同一のユーザ・セッションを使用して AccessPortal を開くには、次のいずれかの方法を使用します:

- ブラウザの「複製」機能(Chrome のみ)
  既存のタブを右クリックし、「タブを複製」を選択します。 既存のユーザ・セッションを使用して新しいタブが起動されます。

- AccessPortal の URL をコピー & ペーストします

AccessPortal の URL(例: https://<サーバアドレス>)を新しいブラウザ・タブへコピー & ペーストすると、既存のユーザ・セッションを使用した新しい AccessPortal セッションが起動されます。

3.1.4 RDP の推奨設定

AccessPortal の最適な使用のために、ユーザごとに複数のセッションを許可する RDP ポリシーを設定してください。 これにより、各アプリケーションにより同一のセッションが共有されるのではなく、各セッションを使用して起動されるようになります。

サーバのローカル・ポリシーでこの設定を行うには、「gpedit.msc」を起動して以下を設定します: r

セッションコンピュータの構成 | 管理用テンプレート | Windows コンポーネント | リモートデスクトップサービス | リモートデスクトップセッションホスト | 接続 |

ユーザリモートデスクトップサービスユーザに対してリモードデスクトップサービスセッションを 1 つに制限する　無効

これは、次のようにシステムのレジストリで設定することもできます:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fSingleSessionPerUser　REG_DWORD　0x00000000 r

設定後、「**gpupdate /force**」を実行します。

3.2 AccessPad(ネイティブ)

AccessPad は、Windows、Mac と Linux で利用可能なネイティブ・クライアント・アプリケーションです。 AccessPad から起動した公開アプリケーションは、リモート・アプリケーションとローカル・デスクトップが完全に統合されたシームレスなウィンドウとして表示されます。

AccessPad では、Microsoft Seamless と Ericom True Seamless Windows の両方の機能がサポートされ、Connect 管理コンソールを使用して一元的にモードの設定を行うことができます。 Microsoft Seamless 機能は、その機能がネイティブでサポートされる Microsoft のワークステーション用オペレーティング・システム上でのみ使用可能です。

3.2.1 ダウンロード場所

インストーラは Ericom の Web サイトから入手できます。

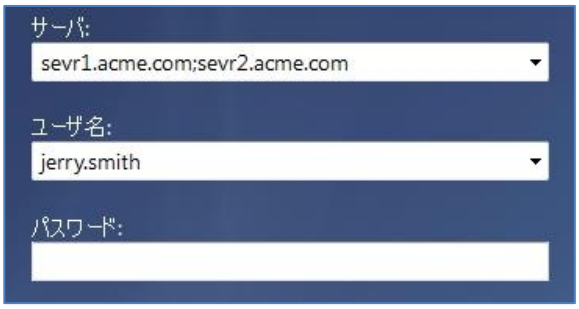
- Windows AccessPad x64 (Windows 7 以降):
  http://www.ericom.com/demos/EricomAccessPadClient64.msi
- Windows AccessPad 32 ビット (x86 Windows 7 以降):
  http://www.ericom.com/demos/EricomAccessPadClient.msi

3.2.2 使用方法

- AccessPad を起動します。
- AccessPad は、スタンドアロン・クライアントとして起動できます。 Mac 用 PKG インストーラと Windows 用の MSI インストーラがあります。
- サインイン・プロンプトが表示されます。 Ericom Connect サーバのアドレスに接続するように AccessPad を設定します。

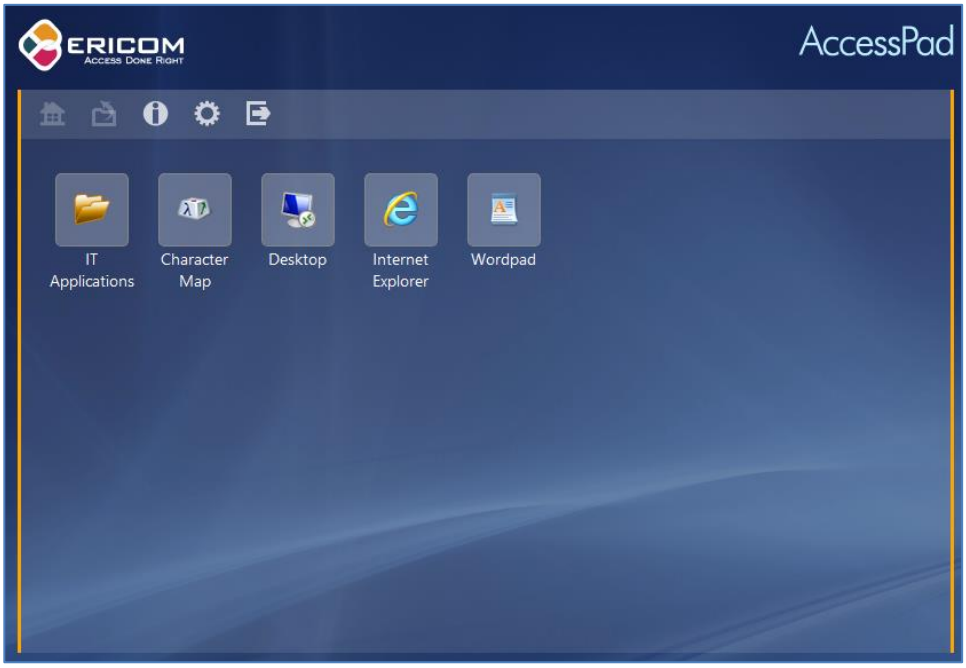
- ポートが 443 以外の場合、明示的に指定します(例: 192.168.1.1:8011)。

- 複数のサーバ・アドレス値をセミコロン区切りのリストとして入力できます。 例: 「sevr1.acme.com; sevr2.acme.com」



- 二要素認証の機能を有効化している場合には、このマニュアルの「二要素認証」のセクションを参照してください。

- サインインすると、利用可能な接続が AccessPad に表示されます。



- 接続を起動するには、目的の接続をクリックまたはタップします。
- AccessPad を終了すると、**すべて**の接続が切断されます。
- ユーザのアプリケーション・セットに変更を加えた場合、変更を確認するには、ログオフしてから再度 AccessPad にログインする必要があります。

3.2.3 AccessPad メニュー・バー

AccessPad のメニュー・バーには、以下の様な便利な機能が含まれています:

ホーム - メインの一覧へ戻ります

親フォルダ(アップ) - 親フォルダの一覧に戻ります

概要情報 - バージョン番号、インストール・フォルダ、Ericom Connect サーバ・アドレス、現在ログインしているユーザ名が表示されます。

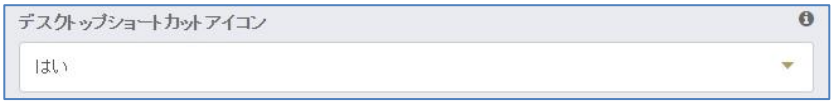
設定 - AccessPad のユーザ側の設定を行います

ログオフ - ログオフします

3.2.4 ローカル・デスクトップ・アイコン

AccessPad では、公開リソースのデスクトップ・ショートカット/アイコンの作成を有効化できます。

デスクトップ・アイコンの有効化は、「公開」|「リソース」｜「基本」タブ内で行います。 リソースのデスクトップ・アイコンを有効化するには、設定を「はい」に変更し、「保存」を押します。

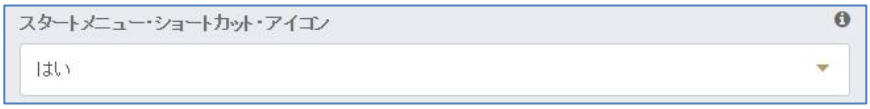


いずれかのデスクトップ・アイコンを有効化した状態でユーザが AccessPad を使用してログインすると、最小化された状態で AccessPad が起動し、デスクトップ・アイコンの有効化が行われたリソースがデスクトップに表示されます。

フォルダはアイコンとして表示されないため、フォルダが重要な場合は、各リソースのラベルに次のフォーマットを使用します: <フォルダ名>.<アプリケーション名>.

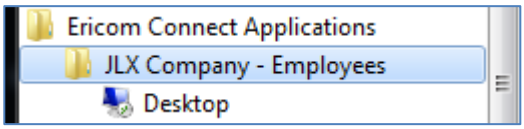
3.2.5 ローカルのスタート・メニュー・アイコン

AccessPad for Windows では、公開リソースのスタート・メニュー・ショートカット/アイコンの作成を有効化することができます。スタート・メニュー・アイコンの有効化は、「公開」|「リソース」｜「基本」タブ内で行います。 リソースのアイコンを有効化するには、設定を「はい」に変更し、「保存」を押します。



スタート・メニュー・アイコンを有効化した状態でユーザが AccessPad を使用してログインすると、AccessPad は最小化された状態で起動し、スタート・メニュー・アイコンの有効化が行われたリソースがデスクトップに表示されます。

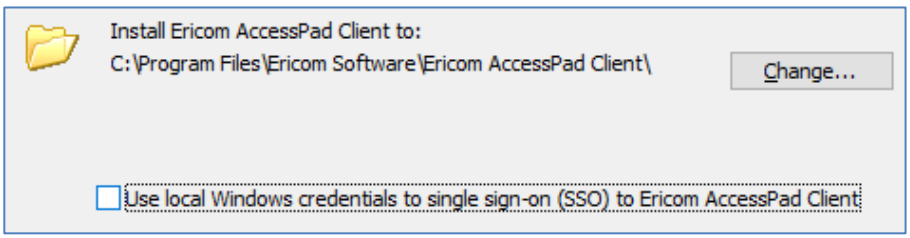
Ericom Connect Applications という名前のルート・フォルダを使用して、スタート・メニューにアイコンが表示されます。 各 Ericom Connect 環境には、次のフォーマットを使用したフォルダがそれぞれに存在します: 「組織名 - テナント名」 組織名の値が空の場合、テナント名のみが表示されます。



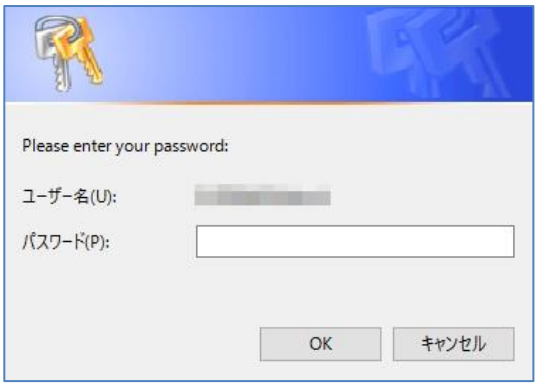
3.2.6 ローカル Windows からの SSO

AccessPad for Windows では、AccessPad へのシングル・サインオン(SSO)に ローカル Windows 資格認証を使用できます。 SSO を有

効にするには、インストール中に「User local Windows credentials...」チェックボックスをオンにします。



SSO 機能を有効にするには、AccessPad のインストール後に再起動が必要です。 再起動を行わない場合、初回の AccessPad の起動でパスワードを入力が必要になります。



RADIUS を有効化している場合、SSO は継続して動作し、接続プロセスで 2 番目の要素のダイアログが表示されます。

セッションでデスクトップ・アイコンが有効化されている場合、ログインが成功すると AccessPad は最小化された状態で起動します。

注意: サーバのアドレスが無効または存在しない場合、SSO 機能は停止します。 AccessPad MSI でサーバ・アドレスを事前設定することで、シームレスな接続が提供可能になります。 初回の接続の成功後、今後の使用のためにサーバ・アドレスをキャッシュすることもできます。

3.2.7 AccessPad Uniprint バンドル (Windows)

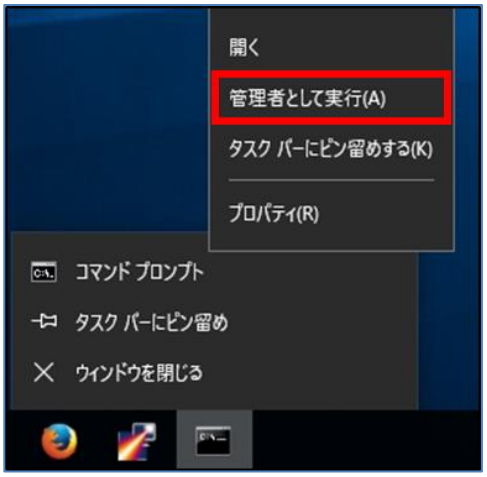
Uniprint クライアントがバンドルされた AccessPad MSI インストーラをダウンロードして入手できます。 このインストーラを使用すると、Uniprint クライアントがインストールされ、以前インストールした Uniprint クライアントが上書きされます。

バンドルされている AccessPad をアンインストールする場合、Uniprint クライアントもアンインストールされます。 バンドルされた AccessPad MSI には以下の 2 つのバージョンがあります:

- 32 ビット OS 用: EricomAccessPadClientExtended.msi
- 64 ビット OS 用: EricomAccessPadClientExtended64.msi

「管理者」権限(推奨)を使用して バンドルされた AccessPad MSI をインストールする場合、Uniprint は「C:\Program Files\UniPrint Client」にインストールされ、システムのすべてのユーザが利用可能になります。

コマンド管理者としてインストールするには、「管理者」としてコマンド・プロンプトを使用します



次を実行します: msiexec /i <AccessPad インストーラ>

管理者以外のユーザとしてインストーラを使用した場合、Uniprint は「C:\Users\<ログイン・ ユーザ>\AppData\Roaming」にインストールされ、現在のユーザのみが利用可能になります。

3.2.8 AccessPad Uniprint バンドル (Mac)

AccessPad と Uniprint クライアントがバンドルされたパッケージ・インストーラをダウンロードできます。このインストーラを使用すると、Uniprint クライアントがインストールされ、以前インストールした Uniprint クライアントが上書きされます。Mac OSX 10.8 以降と互換性があります。

Mac 用の Uniprint を使用するには、ユーザ・セッションでクリップボードのリダイレクトを有効化する必要があります。 詳細な説明については、Uniprint Mac クライアント管理者ガイドの「Uniprint Management Console Settings」セクションを参照してください (Uniprint の Web サイトからダウンロード可能です)。

3.2.9 AccessPad (Linux)

インストールの前提条件は以下のとおりです:

- Ubuntu 14.04 LTS
- MMX 対応の CPU
- 以下の依存関係:

sudo apt-get install libqt5x11extras5

sudo apt-get install libqt5printsupport5

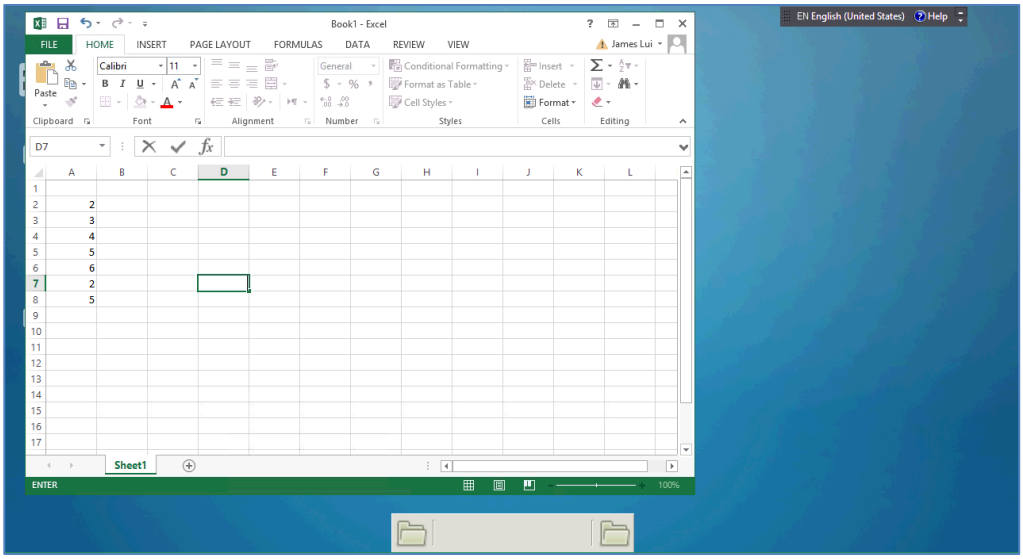
sudo apt-get install libqt5serialport5

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-accesspad_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-accesspad/
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 for Linux 7.6.1 は、64 ビット・クライアントの起動バージョンです。 以下は、このリリースにおける既知の制限の一部です。これらは、使用されているウィンドウ・マネージャによって異なります。

- フルスクリーン・モード中、セッションを「復元」すると、最大化・最小化の機能が動作しなくなります。 ウィンドウ・サイズを調整するには、アプリケーションを再起動してください。
- Blaze セッションを最小化すると、復元できなくなる場合があります。 アプリケーションを閉じ、再起動してセッションに再接続してください。
- フルスクリーン・モードを終了すると、新たなウィンドウが画面の上部隅にロックされる場合があります。
- シームレス・アプリケーションのウィンドウのドラッグがスムーズに動作しない場合があります。 ウィンドウのドラッグが完了するまで、黒色の空白エリアが表示さます。

- 低解像度ディスプレイに高解像度セッションを表示する際、セッションに白色の枠が表示される場合があります。

3.3 AccessToGo Connect (モバイル)

3.3.1 ダウンロードできる場所

次の 2 つのバージョンの AccessToGo で Ericom Connect がサポートされています: ユニバーサル AccessToGo アプリおよび AccessToGo Connect アプリ。 AccessToGo Connect は Ericom Connect ユーザ専用です。

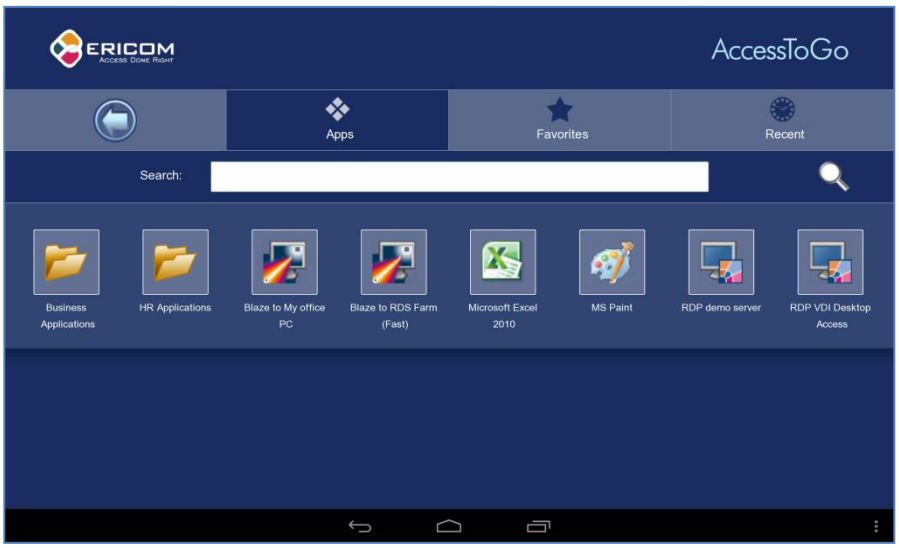
- Android AccessToGo Connect: Google Play または Amazon Android アプリストアで Ericom Connect を検索します。
- Apple iOS AccessToGo Connect: iOS App Store で Ericom Connect を検索します。

3.3.2 使用方法

AccessToGo を使用して、Ericom Connect 接続ブローカでホストされているアプリケーションやデスクトップへ接続できます。 Ericom Connect で AccessToGo を使用する手順は以下のとおりです:

- エンドユーザ・デバイス(例: iPad)に AccessToGo をインストールします。
- Ericom Connect サーバのアドレスに接続するよう AccessToGo を設定します。 ポート 8011 または 443 以外を使用する場合、明示的に指定します(例: 192.168.1.1:4343)。

- 接続がリモートで行われる場合、ファイアウォール/ルータの外部アドレスとポートを使用します。Ericom Connect サーバへの受信接続をポート転送するルールが設定されている必要があります。
- リモート接続用に Ericom Secure Gateway を使用している場合、その外部アドレスとポートを指定します(Ericom Connect の内部アドレスではなく)。 Secure Gateway は Ericom Connect 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)。
- ユーザがサインインすると、割り当てられたすべてのリソースが表示されます。



- 目的のリソースをタップして接続を開始します。

3.4 シングル・サインオン(SSO)のオプション

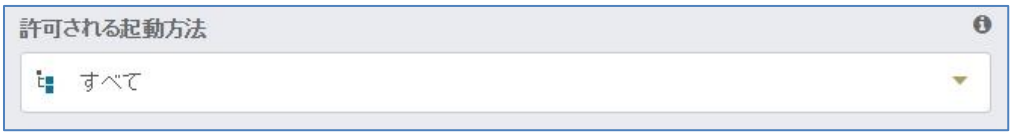
3.4.1 直接起動用の SSO インターフェース

Ericom Connect には、外部の Web サイトからリソースを起動するためのシングル・サインオン(SSO)インターフェースが含まれています。この機能により、AccessNow インターフェースを使用してアプリケーションやデスクトップを直接起動できます。

Connect にパラメータを渡すためのランディング・ページを設定する方法のデモとして、サンプルの SSO ページが次のリンク先で提供されています:
https://host.addr.com:8011/ericomxml/accesssso/ansso.htm
End User Web Service(EUWS) の呼び出しにより SSO が実行された場合:

- Blaze 設定パラメータは、Cookie または URL パラメータの形式でユーザのブラウザに戻されます。
- AccessNow Start ページへの URL が、指定したリソースで起動されます。
- エンドユーザに対し 1 つのグループのみが公開されている場合、グループ名をパラメータとして指定する必要はありません。
- Connect CLI コマンド「EncryptSsoPassword」により生成した暗号化パスワードを使用するには、SSO ページの「Encrypted」設定を確認してください。 POST SSO を実行する場合、値「**EncryptedPassword**」を渡し、 に設定します。

- アプリケーションとグループのエンコードされた ID がサポートされています。 ただし、アプリケーションの「許可される起動方法」が「標準」または「すべて」に設定されていることを確認してください。



- エンコードされた ID を使用した設定例:
-

End User Web Server	localhost:8033
Username	hpuser
Password	••••••••
Application (Name/ID)	d84dbac3-83d9-4612-8119-aa1bb5d6dbc9
Group (Optional:Name/ID)	a330d879-5ac6-46fe-84ab-97b604936f41

3.4.1.1 **要件**

AccessServer には、信頼された証明書の設定が必要です。 Access Server Configuration Tool | Security タブ | に移動し、サーバ上の信頼された証明書の拇印を入力します。 変更を適用するために、Access Server を再起動します。

3.4.1.2 **Cookie を使用した起動**

EUWS を呼び出すと、接続が呼び出されます。その接続では、Blaze 構成パラメータが直接 AccessNow start.html に Cookie で渡されます。

3.4.1.3 URL パラメータを使用した起動

EUWS を呼び出すと、Blaze 構成パラメータを含む URL に基づいて接続が呼び出されます。

URL の例:

https://servername/EricomXML/AccessNow/start.html?autostart=true&settingsURL=/EricomXML/GetAccessNowSettings.aspx?connectionSettingsId=a90b8b0d-0267-49a5-be73-6c88a5abed46_____user01_bf59952c-8f2b-4c24-a579-407705c22119

3.4.2 キオスク端末での SSO ページ

Ericom Connect 7.5.1 以降には、AccessNow インターフェースを使用して直接アプリケーション/デスクトップを起動するためのシングル・サインオン(SSO)ページが含まれています。 このページは、アプリケーション名、フォルダ名、フルスクリーン・モードを事前設定できます。

アプリケーションが最上位に存在し、ユーザのアプリケーション一覧の他の場所に存在しない場合のみ、「グループ」値がオプションとなることに注意してください。 アプリケーションが複数のグループに存在する場合、そのうち 1 つが最上位に存在する場合でも、「グループ」値を定義する必要があります。

次の例の URL を使用して この SSO ページにアクセスできます。

https://host.addr.com:8011/ericomxml/accesssso/ANSSO_LaunchApp.htm

このページは、キオスク端末や Chromebook で使用する際に、アプリケーションやデスクトップをフルスクリーン・モードで直接起動するのに役立ちます。

アプリケーション、フォルダ、フルスクリーン・モードを指定するには、htm ファイルを編集し、次の各変数を見つけます:

「application」、「group」、「fullScreen」。 ファイルの記載に従って各変数を設定します。

このファイルは、EndUserWebService 上の次の場所にあります:

C:\Program Files\Ericom Software\Ericom Connect Client Web Service\WebServer\AccessSso

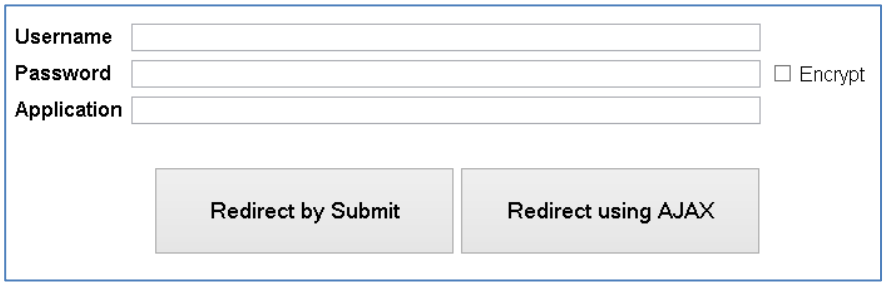
編集した設定ファイルをすべての EndUserWebService サーバにレプリケートしてください。Ericom Connect のバージョン 7.2 と 7.3 に互換性があります。

3.4.3 AccessPortal 用 SSO インターフェース

Ericom Connect には、外部の Web サイトから AccessPortal を起動する、シングル・サインオン(SSO)インターフェースが含まれています。 この機能により、SSO を介して資格情報を使用し、AccessPortal を起動します。

Connect AccessPortal にパラメータを渡すためのランディング・ページ設定方法のデモとして、サンプルの SSO ページが次のリンク先で提供されています:

https://your-host.ericom.local:8011/ericomxml/accesssso/accessportalsso.htm



以下のパラメータが SSO インターフェースに渡されます:

- このリソースへの POST: **/EricomXML/AccessPortalSso.aspx**
- Username(ユーザ名)
- Password(パスワード)
- Application(アプリケーション)
- Connect CLI コマンド「EncryptSsoPassword」により生成した暗号化パスワードを使用するには、SSO ページの「Encrypted」設定を確認してください。 POST SSO を実行する場合、値「EncryptedPassword」を渡し、yes に設定します。

詳細については、「accessportalsso.htm」ページのソースを参照してください。

3.5 エンコードされた AccessPad アイコンの配置

Ericom Connect と AccessPad 7.5.2 以降では、独自のエンコードされた AccessPad ショートカットを手動で作成することができます。 これにより、AccessPad へのユーザのログインを必要とせずに、事前に作成したショートカットを配置することができます。

公開済みのアプリケーションとグループ用に、エンコードされた ID を作成します。 アプリケーションが複数のグループに割り当てられている可能性があるため、このグループ値が必要とされます。

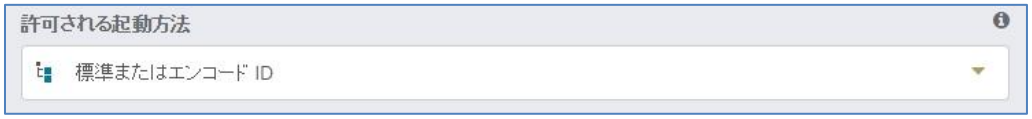
ConnectCLI GenerateEncodedConnectionID <アプリケーション名 | アプリケーション固有 ID > <グループ名 | グループ固有 ID>

アプリケーション名およびグループ名は大文字小文字が区別されることに注意してください。

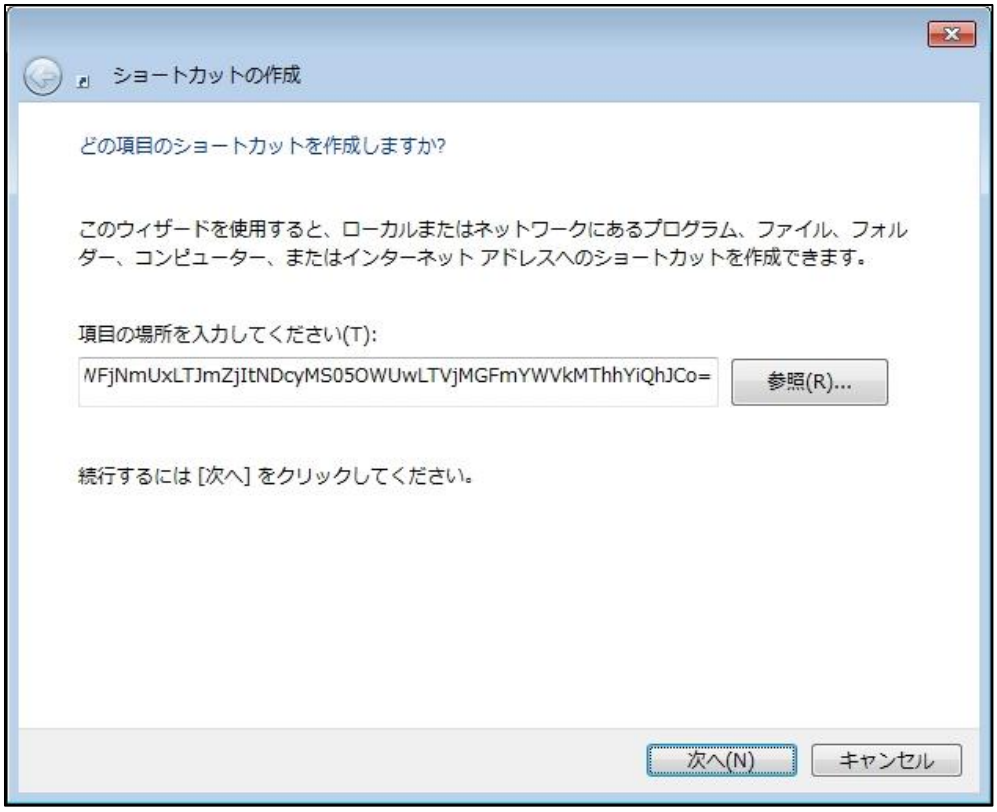
これにより、エンコードされた接続 ID が生成されます。この ID を AccessPad アプリケーションの起動用ショートカットで使用します。

```
C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>connectcli Ge
nerateEncodedConnectionID d84dbac3-83d9-4612-8119-aa1bb5d6dbc9 a330d879-5ac6-46f
e-84ab-97b604936f41
Connect Admin User: vis
Password: **********
Before encoding: d84dbac3-83d9-4612-8119-aa1bb5d6dbc9$!$*a330d879-5ac6-46fe-84ab
-97b604936f41$!$*
Invoke as
  <Path to AccessPad installation>\Blaze.exe -accesspad /encodedConnectionId=v1/
ZDg0ZGJhYzMtODNkOS00NjEyLTgxMTktYWExYmI1ZDZkYmM5JCEkKmEzMzBkODc5LTVhYzYtNDZmZS04
NGFiLTk3YjYwNDkzNmY0MSQhJCo=
```

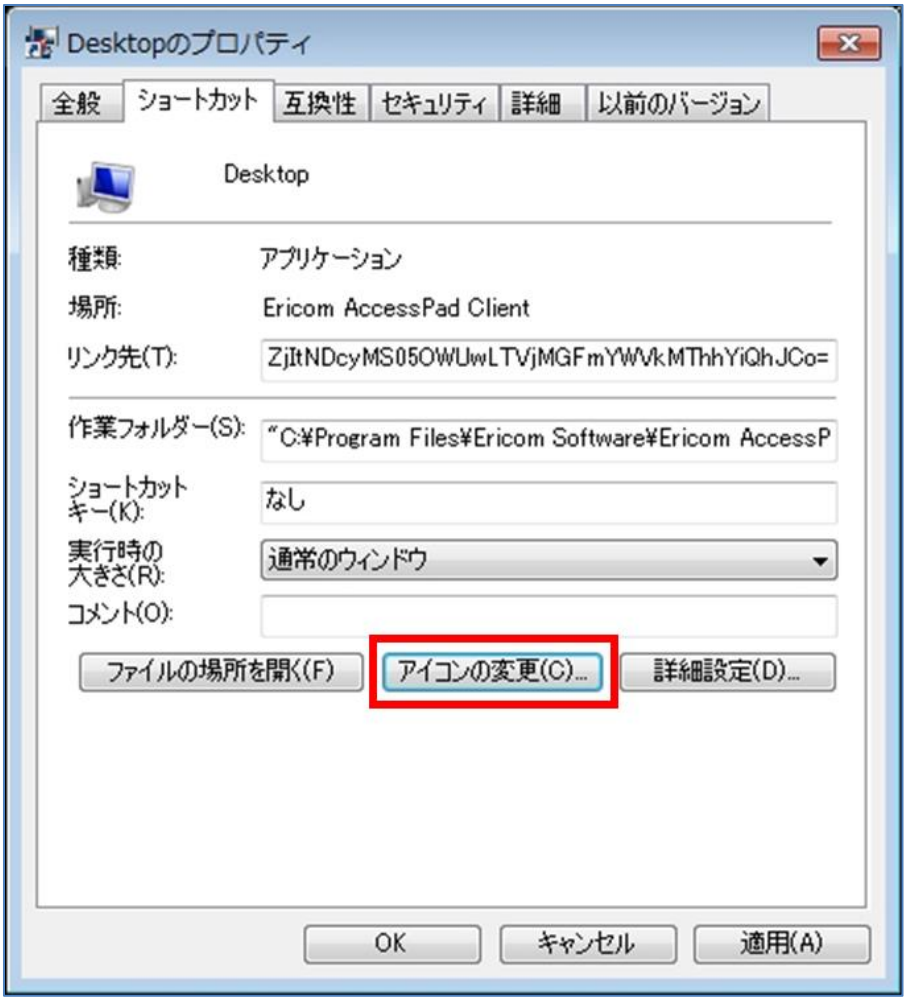
エンコードされた値をショートカットで使用する際には、「設定 | デフォルト | 要件 | 許可される起動方法」で「エンコード ID」の使用が許可されていることを確認してください。



AccessPad へのパスとエンコード ID を使用して新しいショートカットを作成します。 以下は、Windows の「新しいショートカットの作成」での例です。



目的のアプリケーション・アイコンと使用し、目的の場所(例: デスクトップ、スタートメニューなど)にアプリケーションを配置するようショートカットを設定します。

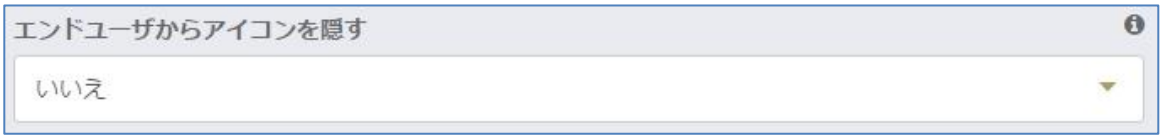


初回の AccessPad の起動では、Ericom Connect サーバのアドレスの手動入力が必要であることに注意してください。 一度アドレスを入力して使用すると、今後の使用のためにキャッシュされます。 さらに、「エンドユーザ・ポイントのカスタマイズ」に記載の手順を使用して、アドレスを事前設定できます。

既知の動作

「エンコードされた ID のみ」を使用するよう設定したアプリケーション(および関連するグループ)は、「デスクトップ・アイコン」また

は「スタートメニュー」を有効化することができません。 さらに、「エンドユーザからアイコンを隠す」を有効化する必要があります。



3.6 Web サイトからのアプリケーションの起動

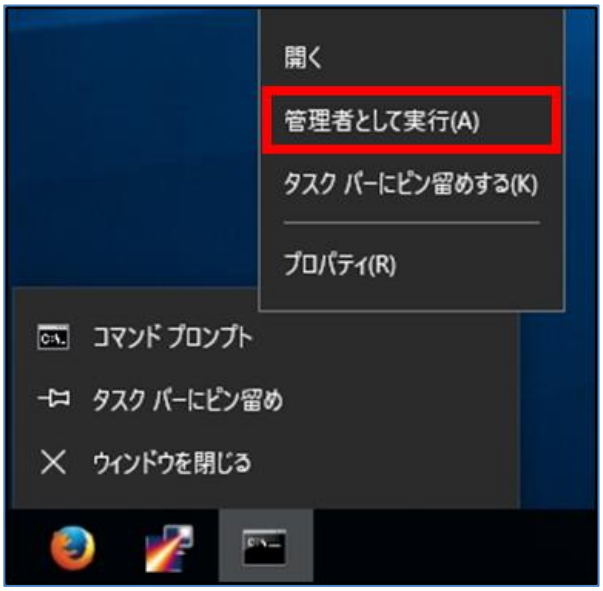
公開済みのアプリケーションとデスクトップは、URI(Uniform Resource Identifier)を使用して、AccessPad 経由で起動することができます。 デフォルトの UR は、「estp」ですが、カスタマイズが可能です。 この機能を使用すると、構成済みのパラメータを使用して公開済みアプリケーションを起動できる独自の URL を公開できます。 この機能には以下のような使用例があります:

- 公開済みの Web ブラウザを起動し、構成済みの Web サイト URL を起動するセキュアな URL リンクの公開
- ターミナル・サーバの仮想 Excel を使用して開く Excel ドキュメントの公開
- 事前定義した設定ファイルを使用したターミナル・エミュレーターの起動

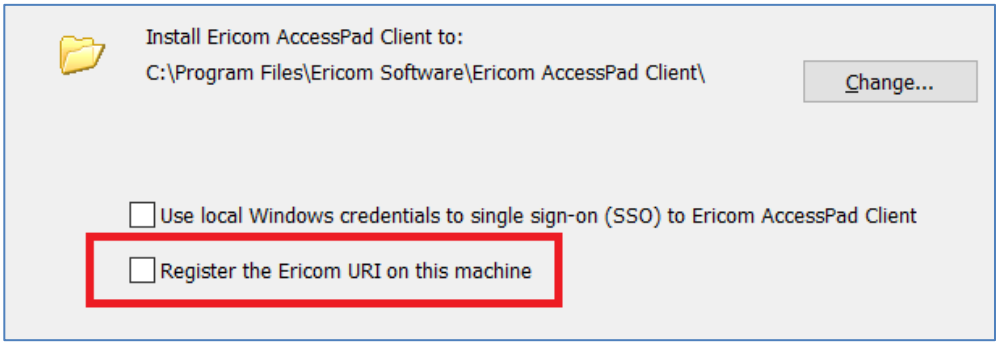
この機能には Windows ホスト・オペレーティング・システムが必要です。この機能は AccessPad 7.5.2 以降のバージョンでサポートされています(AccessPortal および AccessToGo には対応していません)。

3.6.1 インストール

URI 登録は、AccessPad Windows インストーラのオプション機能です。 この機能を使用するには、「管理者」権限を使用してコマンド・プロンプトから MSI を起動する必要があります。 「管理者」権限でコマンド・プロンプトを起動するには、アイコンを右クリックし、「管理者として実行」を選択します。



インストール中、構成オプションのプロンプトが表示されます。 この機能を有効化するには、「Register the Ericom URI on this machine (Ericom URI をこのマシンに登録)」をチェックします。



3.6.2 エンコードされた URL を作成する

Ericom Connect と AccessPad 7.5.2 以降では、エンコードされた AccessPad URI を作成できます。 これにより、管理者は、ローカルにインストールした AccessPad を使用して公開アプリケーションを起動する指示をウェブサイトに配置することが可能になります。 エンコードされた URI は、アプリケーションとグループを BASE64 の文字列にエンコードします。

まず、公開済みのアプリケーションとグループ用に、エンコードされた URI を作成します。 アプリケーションが複数のグループに割り当てられている可能性があるため、このグループ値が必要とされます。

ConnectCLI GenerateEncodedUri <アプリケーション名 | アプリケーション固有 ID> <グループ名 | グループ固有 ID>

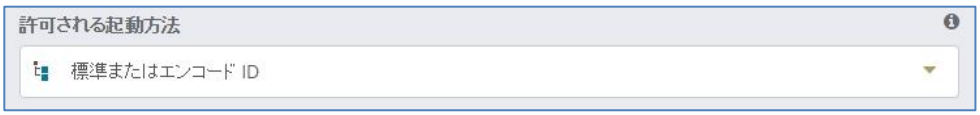
アプリケーション名およびグループ名は**大文字小文字が区別される**ことに注意してください。

名前ではなく ID を使用することは、推測が困難になるため、一般的にセキュアな方法となります。 ID は時間経過によって変更されることがありません。「名前」は管理者によって変更され、以前エンコードされた URL が使用不可能となる可能性があるため、ID はより信頼性のあるものとなります。

これにより、エンコードされた接続 URI が生成されます。この URI を AccessPad アプリケーションを起動するための Web ページに使用します。

```
C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>connectcli Ge
nerateEncodedUri ?
Connect Admin User: vis
Password: ************
Too few arguments

C:\Program Files\Ericom Software\Ericom Connect Configuration Tool>connectcli Ge
nerateEncodedUri d84dbac3-83d9-4612-8119-aa1bb5d6dbc9 a330d879-5ac6-46fe-84ab-97
b604936f41
Connect Admin User: visitor
Password: ************
Before encoding: d84dbac3-83d9-4612-8119-aa1bb5d6dbc9$!$*a330d879-5ac6-46fe-84ab
-97b604936f41$!$*
estp://accesspad/v1/ZDg0ZGJhYzMtODNkOS00NjEyLTgxMTktYWExYmI1ZDZkYmM5JCEkKmEzMzBk
ODc5LTVhYzYtNDZmZS04NGFiLTk3YjYwNDkzNmY0MSQhJCo=
```

エンコードされた値をショートカットで使用する際には、「設定 | デフォルト | 要件 | 許可される起動方法」で「エンコード ID」の使用が許可されていることを確認してください。



URL の生成後、目的の Web ページにこれを埋め込みます。 URL を使用した HTML コードのサンプル:

**<A href="estp://accesspad/v1/NDg4NTMwYTUtZDI0Zi00ZGMyLWE1OTEtNTM3YTc0ZTQ1ZTgyJCEkKjYwN2FlYmQxLTRkNzktNDE1MS04NzM1LWYwYWRlMDU5NWE5MyQhJCo=">Browser ESTP Encoded</A>
**

初回の AccessPad の起動では、Ericom Connect サーバのアドレスの手動入力が必要であることに注意してください 一度アドレスを入力して使用すると、今後の使用のためにキャッシュされます。 さらに、「エンドユーザ・ポイントのカスタマイズ」に記載の手順を使用して、アドレスを事前設定できます。

3.6.3 カスタム URI を作成する

デフォルトの Ericom URI は「estp」です。 対象のシステムに新しいレジストリ・エントリを追加することで、カスタム URI を作成できます 新しい URI レジストリ・キーを作成するには、デフォルトの estp キーを変更し、目的の URI を入力します(estp の文字列を置換します)。

```
[HKEY_CLASSES_ROOT\estp]
@="\"URL:Ericom Protocol\""
"URL Protocol"="\"\""

[HKEY_CLASSES_ROOT\estp\DefaultIcon]
@="Blaze.exe,1"

[HKEY_CLASSES_ROOT\estp\Shell]

[HKEY_CLASSES_ROOT\estp\Shell\Open]

[HKEY_CLASSES_ROOT\estp\Shell\Open\Command]
@="\"C:\\Program Files\\Ericom Software\\Ericom AccessPad
Client\\Blaze.exe\" \"-accesspad\" \"%1\""
```

3.6.4 URI を使用するためのホスト Web ページを構成する

Ericom URI は、Web ページから起動します。 Ericom より、URL を構成する方法例のページが提供されています(EncodedShortcut.html)

URL リダイレクションを使用する各ページに、次の 2 つの Javascript ファイルが必要です: jquery-2.2.3.min.js および EricomLaunch.js

この 3 つのファイルのご要望は、Ericom テクニカル・サポートまでお問い合わせください。

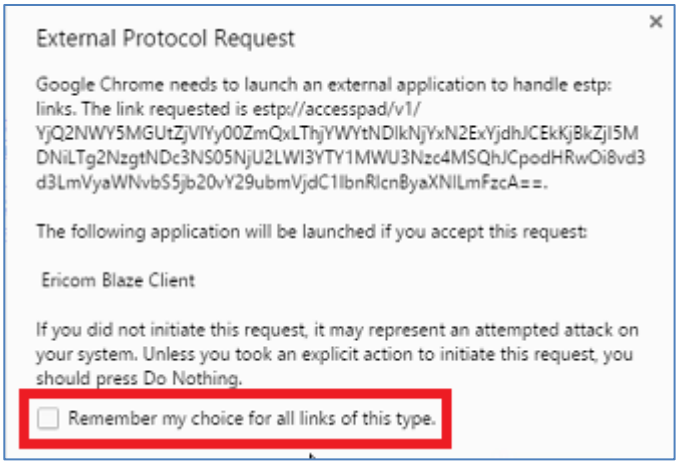
以下に沿って EricomLaunch.js を構成します:

- App：名前または ID。(ID は、リソースの「基本」タブ内にあります)
- Group：空白、名前または ID。(ID は、グループの「基本」タブ内にあります)
- URI：構成済み URI の値(デフォルト = estp)

構成のサンプルについては、「4.15 Windows RDS でのセキュアなブラウジング」のセクションを参照してください。

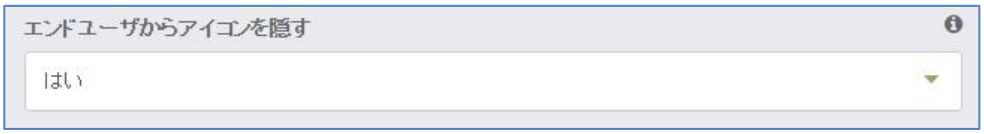
3.6.5 ブラウザの警告メッセージ

一部のブラウザでは、Web サイトから AccessPad のようなローカル・アプリケーションを起動する際に、警告メッセージが表示されます。 今後このメッセージを非表示とするには、「Remember my choice for all links of this type(このようなリンクの設定をすべて保存する)」を選択します。



3.6.6 既知の動作

「エンコードされた ID のみ」を使用するよう設定したアプリケーション(および関連するグループ)は、「デスクトップ・アイコン」または「スタートメニュー・アイコン」を有効化することができません。さらに、「エンドユーザからアイコンを隠す」(Hide icon from end-user)を有効化する必要があります。



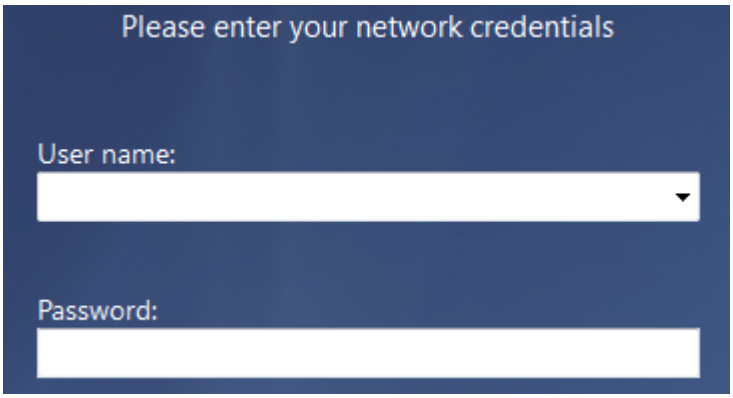
3.7 エンドユーザ・ポイントのカスタマイズ

このセクションでは、環境をカスタマイズするために様々なエンドユーザ・タッチポイントを設定する方法を説明します。 カスタマイズは Ericom のテクニカル・サポートの対象ではなく、Ericom のエンジニアはオリジナル・ファイルの問題に限りトラブルシューティングを提供することにご留意ください。 変更を行う前に、**すべてのオリジナル・ファイルをバックアップ**してください。

3.7.1 AccessPad の事前構成アドレス

- AccessPad exe には、事前設定およびサーバ・アドレスの非表示を行うためのサーバ・パラメータを使用できます。
- パラメータには、次のフォーマットを使用します:
  "-accesspad /server=<サーバ名>"
- 例:

- セミコロンで区切ることで、複数のアドレスを使用できます。
  例:「-accesspad /server=servr1.acme.com;servr2.acme.com」
- 事前設定したアドレス値を使用する場合、サーバ・アドレス入力用の GUI の項目は非表示になります。



3.7.2 AccessPad SSO と URI コマンド・ライン

AccessPad SSO と URI の機能は、インストーラのコマンド・ラインで標準 MSI パラメータを使用することで有効化できます。

SSO と URL の両方を有効にするには、次のコマンドを使用します:

- EricomAccessPadClient64.msi **ESSO=1 URI1=1**

SSO 機能のみを有効化するには、以下のいずれかを使用します:

- EricomAccessPadClient64.msi ESSO=1
- EricomAccessPadClient64.msi ESSO=1 URI1=""

URI 機能のみを有効化するには、以下のいずれかを使用します:

- EricomAccessPadClient64.msi URI1=1
- EricomAccessPadClient64.msi ESSO="" URI1=1

3.7.3 独自の AccessPad 設定のパッケージ化

- 「msi2xml/xml2msi」などのツールを使用して、独自の AccessPad 設定の再配布可能な MSI パッケージを作成できます。
- MSI を編集可能な XML に展開するには、次を実行します:
  msi2xml.exe -b streams -c files EricomAccessPadClient64.msi
- 「 EricomAccessPadClient64.xml」ファイルを開き、15458 行目に移動し、「SHORTCUT_PARAMS」をアドレス・パラメータで置き換えます。

```
15458    <td>-accesspad /server=connectaddress.acme.com</td>
```

- XML を MSI に再パッケージ化するには、次を実行します:
  xml2msi -m EricomAccessPadClient64.xml

3.7.4 AccessPortal

- AccessPortal の画像は、エンドユーザ Web サーバ 上の次の場所にあります: C:\Program Files\Ericom Software\Ericom Connect Client Web Service\WebServer\AccessPortal\img
- 「background-neuronal.jpg」などの任意のファイルに変更を加えることで、外観のカスタマイズが可能です。

3.7.5 RADIUS マルチファクターのプロンプト

- Ericom Connect サーバ上で、次の場所へ移動します:

  C:\Program Files\Ericom Software\Ericom Connect Configuration Tool
- 次のファイルを編集します:

  Csi4MessageDescriptorsTranslatable.xml
- 288 行目を編集し、パスコードフィールド・ラベル(最大 36 文字)を以下のように変更します:

  <TranslatableMessage id="Passcode">**Enter Passcode or authentication key**</TranslatableMessage>

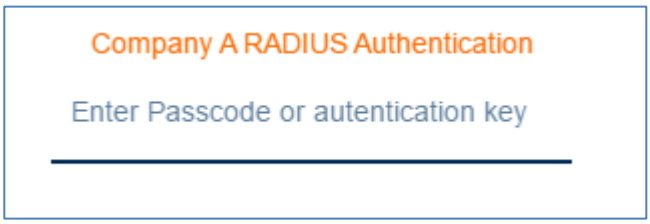
- 290 行目を編集し、説明テキスト(最大 36 文字)を以下のように変更します:

  <TranslatableMessage id="RadiusAuthentication">**Company A RADIUS Authentication**</TranslatableMessage>

- コマンド・プロンプトから以下の CLI コマンドを実行し(同じディレクトリから)、変更を読み込みます: **ConnectCLI ImportLanguageFiles "C:\Program Files\Ericom Software\Ericom Connect Configuration Tool"**

- 次回ユーザが AccessPortal、AccessPad、AccessToGo (Connect Mobile App)でログインすると、変更内容を利用できるようになります。

AccessPortal の結果:

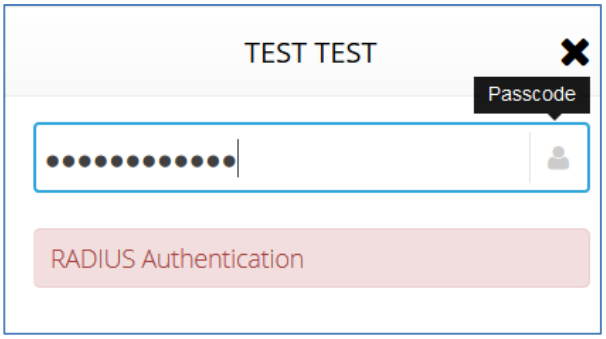


AccessPad の結果:

AccessPortal のプロンプトには、タイトルに追加のテキストが存在します。 デフォルトのテキスト「RADIUS Login」を変更するには、以下の手順を実行します:

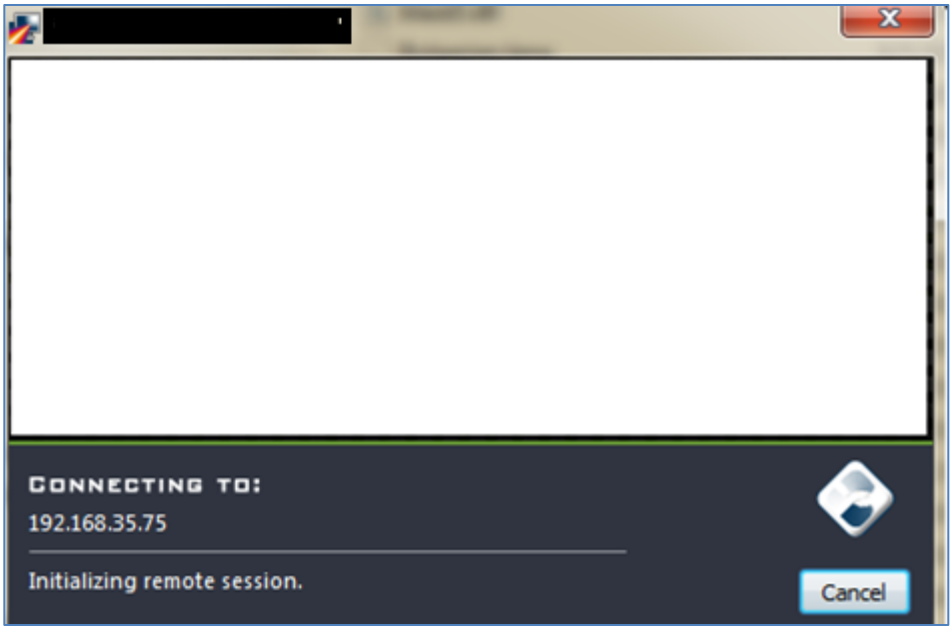
- C:\Program Files\Ericom Software\Ericom Connect Client Web Service\WebServer\AccessPortal\templates へ移動します
- テキスト・エディタで Open radius-form.htm を開きます
- 次の行を編集します: {{ 'TEST TEST' | translate }}

変更を確認するために、ブラウザ・キャッシュのクリアが必要となる場合があります。



3.7.6 独自の AccessPad ログイン・バナー画像

このカスタマイズは、Ericom プロフェッショナル・サービスを通して利用可能です。 AccessPad のログイン・バナーに独自のロゴを設定することができます。 独自のスプラッシュ画面を有効化するには、Ericom に PN ファイルを依頼します。 PN ファイルを受け取った後、「splash.png」という名前の PNG 画像を作成します。 画像の解像度は 462x194 である必要があります。 PN ファイルには、バナーのタイトルを変更するため独自のラベルを含めることも可能です。 以下の例では、黒いエリアは独自のラベルを表し、白いエリアは splash.png ファイルで設定されたイメージを表しています。



PN ファイルおよび内部に含まれる PNG ファイルと AccessPad MSI を再バンドルすることで、独自の MSI を作成することができます。

3.8 パスワードの変更

ユーザが Ericom Access のポイントにログインし、パスワードの変更が必要な場合、プロンプトが表示されます。

継続するには、現在のパスワードを正しく入力し、一致する新しいパスワードを 2 箇所に入力する必要があります。 変更と認証が成功すると、公開リソースのページが表示されます。

パスワード変更ダイアログで元のパスワードの入力に失敗すると、次のエラー・メッセージが表示されます: 「古いパスワードが間違っています」

古いパスワードが間違っています。

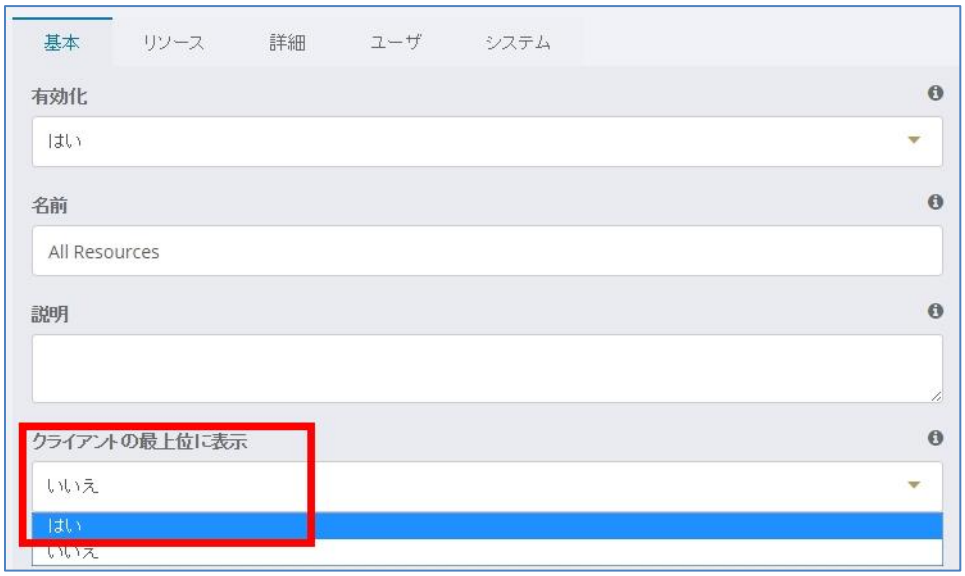
「古い」パスワードの再入力が可能です。操作をキャンセルするには、AccessPad を閉じます。

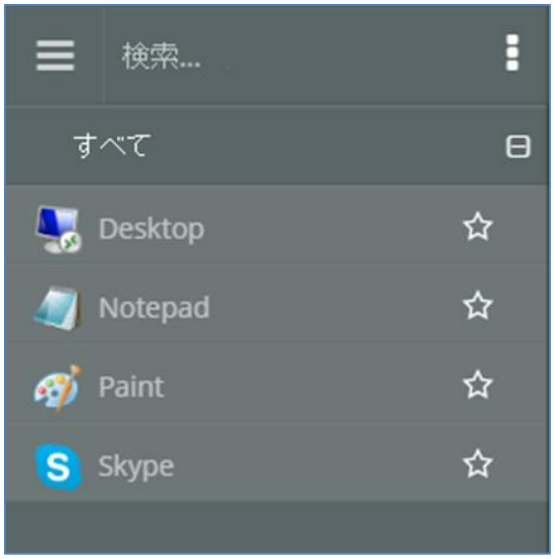
ユーザが入力した新しいパスワードがセキュリティ・ポリシーを満たしていない場合、次のようなエラー・メッセージが表示されます: 「パスワードはパスワードポリシー要件に一致していません。パスワード長の制限 ...履歴の要件を確認してください」

3.9 フォルダの構造

ユーザ向けの公開グループが 1 つだけ存在する場合、グループのすべてのコンテンツはルート「最上位」に表示されます。 ユーザが 2 つ以上のグループのメンバーである場合、各グループのコンテンツはフォルダとして表示されます。

管理コンソール内のグループの「基本」設定に移動して、すべてのグループのコンテンツを最上位(フラット化した状態)に表示できます。 設定「クライアントの最上位に表示」を「はい」に設定します。





設定が「いいえ」の場合、各グループのコンテンツはフォルダとして表示されます。

4 展開ガイド

Ericom Connect を展開するための計画プロセスの中で、以下の項目を検討してください:

- どのユーザが Ericom Connect リソースへのアクセス権を持つ必要がありますか?
- すべてのユーザに同じようなニーズがありますか? または、個別のアクセス・ニーズを持つユーザのグループがありますか?
- その環境にプライベート・ネットワークの外部からアクセスするユーザが存在しますか?
- 担当者と彼らグループ内での変更は、アクセス・ポリシーにどのような影響を与えるでしょうか?
- どのような種類のアプリケーションが公開されますか?

このような質問は、リソースの公開の方法や、リソースを「公開」と「システム」のグループに編成する方法を定義するのに役立ちます。

4.1 データ・モデルの理解

4.1.1 継承階層

「詳細」や「要件」タブなどの Ericom Connect の設定は、複数のレベルで定義できます。 階層レベルを定義する優先順位は以下のとおりです:

- ハードコードされた(ビルトインの)デフォルト - 優先順位: 最低
- システム定義のデフォルト (グローバル・レベル)
- アプリケーションとデスクトップ (リソース・レベル)
- 「公開」グループ (グループ・レベル)
- ユーザ (Active Directory とグループ・ポリシー) - 優先順位: 最高

より上位のレベルで変更されるまで、下位レベルの設定が継承されます。

上位レベルで定義された設定は、下位レベルに反映されません。 例えば、アプリケーション・レベルで「接続バー」が「いいえ」に設定されている場合、優先順位が低いために「グループ」では表示されません。

公開グループがアプリケーションよりも高い優先順位を持つ理由は、公開グループには詳細な設定が含まれているためです。例えば、アプリケーションのインスタンスは、異なる構成が含まれる複数のグループのメンバーである場合があります。

4.1.2 システム・オブジェクト

システム・オブジェクトには、システム全体にグローバル・レベルで定義されているプロパティがあります(例: 「詳細」設定と「要件」)。これは、管理コンソールにあるナビゲーション・パネルの「設定」オプションで設定されています。

4.1.3 グループ・オブジェクト

グループ・オブジェクトには、類似した属性を持つオブジェクトのグループが含まれています(例: 同じ部署の従業員)。 これにより、類似したエンティティを分類することや見つけ出すことが容易になります。Connect には、次の 2 つのタイプのグループがあります: 「公開」グループと「システム」グループ。

4.1.3.1 公開グループ

「公開」グループには、次が含まれています: ユーザの割り当て、リソース、「詳細」タブの設定、「システム」要件、リンクされた「システム」グループ。

リソースが「公開」グループに属している場合、グループから一部またはすべてのプロパティを継承します。リソース・オブジェクトで明示的に定義されていないすべてのプロパティは、グループから取得されます。

設定がグループ・レベルで明示的に定義されていない場合、グループのユーザはシステム・オブジェクトからデフォルトの設定を継承します。

4.1.3.2 システム・グループ

「公開」グループと同様、「システム」グループには、そこに含むシステム(サーバまたはワークステーション)を定義するための値が含まれています。「システム」グループを使用して類似したシステムをグループ化して、「公開」グループへ割り当てることができます。 例えば、デスクトップ接続に割り当てられる「システム」グループにワークステーションを割り当てます。ユーザがそれぞれのデスクトップ接続を選択すると、定義済みのバインド要件に基づいて 1 つのワークステーションが割り当てられます。

4.1.3.3 グループの無効化

グループ・オブジェクトを無効化または削除すると、システムで無効になり、すべての設定と要件は接続に適用されなくなります。

4.1.4 リソース・オブジェクト

アプリケーションとデスクトップは、リソースとみなされます。 詳細設定とバインド「要件」は、各リソースで定義できます。
リソース・オブジェクトには、アプリケーション名、リダイレクト機能、接続動作などの起動パラメータを定義するプロパティが含まれています。 Ericom Connect では、次の 3 つの異なるタイプのホストがサポートされています: リモート・デスクトップ・サーバ(ターミナル・サーバ)、物理ワークステーション、仮想デスクトップ。

リソースにアクセスするには、リソースが「公開」グループ・オブジェクトに割り当てられている必要があります。このグループ・オブジェクトが接続の所有者になります。1 つのリソースを複数の「公開」グループに割り当てることが可能です。

4.1.5 ユーザ・オブジェクト

ユーザ・オブジェクトには次が含まれています: Active Directory で定義された資格情報、属性、グループ・メンバーシップ、ポリシー情報。Ericom Connect にはこのデータへの完全な可視性があり、認証、リソースの割り当て、セッション・プロパティの定義のためにデータが使用されます(例: ユーザのオフィス・ワークステーションの場所を決定するなど)。

Connect 内では、設定をユーザ・オブジェクトに直接割り当てることはできません。 すべての設定は、ユーザの Active Directory オブジェクトで定義され、それらがユーザのセッション最も高い優先順位を与えられます。

4.2 バインド要件の理解

ビルトインのリソース・バインド・アルゴリズムにより、接続リクエストに一連のルールが適用され、リソースの起動方法が決定されます。

ルールでは以下がチェックされます:

- 定義されたホストの制限があるかどうか
- 既存の切断されたセッションに再接続するかどうか

- セッションを共有するべき既存のアクティブ・セッションがあるかどうか
- 「要件」タブで定義されたしきい値に基づいた新しいセッションのための有効なシステムかどうか

リソースのリクエストは、上記の基準を満たす**最初**のシステムへ接続されます。

4.2.1 AD を経由してデスクトップとユーザをバインドする

デフォルトでは、既にサインインしているデスクトップへの接続を試行する際、すでにサインインしているユーザによる試行であっても、接続は失敗します。 この動作は、セキュリティ上の理由のためです。

Connect には、「後続」のデスクトップ・セッションを可能にするために、構成されたユーザのみがデスクトップに接続できるよう割り当てする機能が含まれています。 この機能の使用には、対象のデスクトップのアドレスが Active Directory で利用可能であることが必要です。機能の設定は、管理 GUI または コマンド・ラインを使用して行います。

GUI を使用した方法: LDAP 属性の割り当て

「Active Directory 属性アドレス」でユーザアドレスを含む AD 属性を入力すると、デスクトップ・リソースの宛先アドレスを Active Directory から取得することができます。

この設定を行うには、まずデスクトップ・アドレス(複数可)を含む Active Directory 属性を設定します。

- 「設定」|「テナント設定」または「セカンダリ設定」に移動し、「「マイ デスクトップ」用の Active Directory の 属性」設定で、ユーザのワークステーション(ターゲット)アドレスを含むすべての Active Directory 属性を入力します。

- 次に、デスクトップ・コネクションの「基本」タブ | 「Active Directory 属性アドレス」で属性値を入力します。

複数のデスクトップ接続がある場合、各コネクションにより 1 つの「属性アドレス」が使用されますが、すべての属性値が「Active Directory 属性」設定に含まれている必要があります。

- デスクトップ対象のユーザの「起動分析」を使用し、接続が正しく目的のデスクトップに設定されていることを確認します。

4.2.2 デスクトップからのシームレス・アプリケーション

管理コンソールを使用してアプリケーションを公開します。 次に、アプリケーションの「要件」タブを開き、プロパティ「ワークステーション OS でのアプリの起動を許可」を有効にします。 ユーザがこのアプリケーションを選択すると、Connect は、利用可能な(現在どのユーザもサインインしていない)ワークステーションを使用して公開アプリケーションを起動します。

4.2.3 切断のステータス

RemoteAgent およびコンポーネント・サービスには、次の 2 つの切断ステータスがあります: 「永久に切断」と「一時的に切断」

サーバ/コンポーネントは以下の方法でこれらの状態になります:

- 一般的な構成ツールから: Disconnect or Prepare for cloning(複製用の切断または準備)
- RemoteAgent 構成ツールから: Disconnect or Prepare for cloning(複製用の切断または準備)
- サーバ/コンポーネントがアンインストールされた場合。
- ConnectCLI 経由でサーバ/コンポーネントをその状態とした場合

4.2.4 公開グループをポータル・タイプにバインドする

SetConnectionRule コマンドを使用して、公開グループを特定のポータル・タイプと ESG モードに割り当てることができます。

例えば、AccessPad クライアント・タイプに「ap」という名前の公開グループを割り当てるには、次のコマンドを実行します:

connectcli setconnectionrule ap * PortalType==’AccessPad’

ユーザが AccessPad を使用してログインすると、AccessPad とすべてのタイプ('*'）にバインドされているグループのみが表示されます。

全コマンドの詳細:

使用法: ConnectCLI SetConnectionRule { リソースのグループ名または ID } { バインドするグループ名または ID | * } formula

1 つのリソース・グループ内で 1 つまたは複数のバインディング・グループ用の接続ルールを設定します。式の例

true　常に有効化

false　常に無効化

ViaEsg　ESG へ接続している時

ViaEsg==false　ESG へ接続していない時

PortalType!='AccessPortal'　AccessPortal への接続時

PortalType=='AccessPortal' && ViaEsg　ESG と AccessPortal を経由して接続している時

有効なポータル・タイプ(大文字と小文字を区別): AccessPortal、AccessPad、AccessToGo、AccessNowSso、AccessPortalSso、*

演算子: && || (..) == !=

変数(大文字と小文字を区別): ViaEsg, PortalType

リテラル(大文字と小文字を区別): true, false, 'string value'

```
/adminUser <string>     []
/adminPassword <string> []
/tenant <string>        [rootURL]
/gridName <string>      [EricomConnect]
/locators <string>      [10.0.0.12:4174]
/[no]techSupport        [False]
```

より詳細な情報は、テクニカル・サポートまでお問い合わせください。

このコマンドの既知の動作:

- PortalType は、コマンドを実行する際に公開グループに割り当てられているすべてのユーザ/グループに適用されます。 このコマンドの後に追加されたユーザやグループには、PortalType が継承されず、デフォルトの「*」が使用されます。 公開グループのすべてのメンバーに Portal Type を適用するには、Connect CLI コマンドを実行します。
- PortalType ラベルは大文字と小文字が区別されます。 AccessPad は「AccessPad」として入力する必要があります。 「Accesspad」と入力すると、公開グループが無効なポータルに割り当てられます。 この失敗を修復するには、公開グループを「*」PortalType にもう一度割り当てます。

4.2.5 ESG 階層

ユーザの接続に使用される ESG アドレスの決定には、3 つのレベルが使用されます。 階層の順序は次のとおりです:

- システム・グループ・レベル
- システム全体のデフォルト
- ユーザ・アクセスのアドレス

例えば、システム全体のデフォルトのアドレスが aaa.company.com であり、システム・グループ・レベルのアドレスが bbb.company.com である場合、bbb.company.com が使用されます。

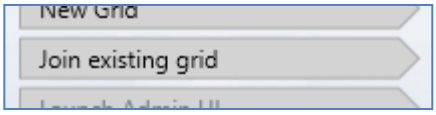
ユーザ・アクセスのアドレスは、他の 2 つの値が空白である場合のみ使用されます。

4.3 ビジネス・ロジック・サービスの理解

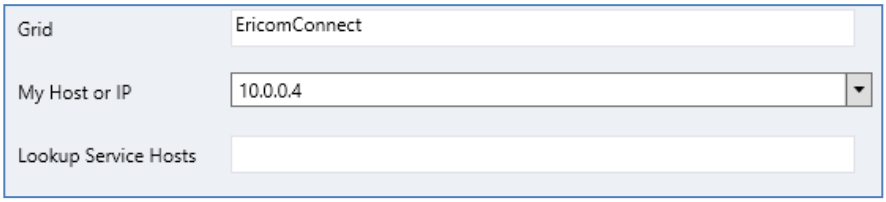
Ericom Connect サービスの高可用性を維持するために、グリッドに Connect Business Logic(BL) コンポーネント・サーバを追加し、冗長性を持たせることができます。 サーバに障害が発生した場合、他のサーバのいずれかがサーバの停止をカバーできます。

4.3.1 Connect BL サーバ

高可用性のために Connect BL サーバを追加するには、Connect をインストールし、Ericom Configuration Tool を使用してサーバを「existing grid」(既存グリッド)に「Join(参加)」します。



プロンプトが表示されたら、新しいサーバが接続するグリッド名を入力します。



4.3.2 データ・パーティション

データ・パーティションには、データの素集合が保持されています。全体として、すべてのパーティションですべてのデータが保持されています。 オブジェクトがパーティションに加わると、そこに恒久的に存在し続けます。 システムの起動後にパーティション数を変更するには、RemoteAgent を含む接続されたすべての Ericom グリッド・コンポーネントを再起動する必要があります。 そのため、後の大規模な再構成変更を避けるために、インストール時にパーティション数を適切に決定することが重要です。パーティション数を変更した場合、すべての Ericom Connect グリッド・コンポーネントを再起動する必要があります。

パーティション内のデータは、インスタンスとしてすべてのマシンに分散されます。 各インスタンスには、パーティション内のデータの完全なコピーが保持されます。 インスタンスをプライマリとすると、他のすべてのものはバックアップ・インスタンスとなります プライマリ・インスタンスに障害が発生すると、バックアップ・インスタン

スの 1 つがプライマリとなります。 データのコピー数は、インスタンス数と等しくなります。

バックアップ数は、インスタンス数から 1 を引いた数となります。システムにより、プライマリ・インスタンスからバックアップ・インスタンスへのレプリケートが自動的に行われます。 バックアップ数は、インスタンスから 1 を引いた数となります(バックアップ数 = インスタンス数 -1)。

バックアップ数を変更した場合、Ericom Connect Business Logic Controller サービスのみを再起動する必要があります。

Grid Storage Container(GSC)は、単一インスタンス(プライマリまたはバックアップ・インスタンス)を保持するプロセスです。 各マシンには、任意の数のコンテナを持たせることができます。

GSC の必要数を決定するための式は次のようになります:GSC 必要数 = パーティション数 x (1 + バックアップ数) + 1(ミラー用)。

デフォルト(バージョン 7.5.1 より)では、単一マシンの展開は バックアップ 0 の 1 つのパーティションとなります。 1 x (0 + 1) + 1 = 2

ミラーは、データベースへの書き込みを担当します。

グリッド・ステータスの定義

- Intact - 健全で、すべてが利用可能です
- Compromised - すべてのプライマリが利用可能ですが、一部またはすべてのバックアップが利用不可能です

- Dameged - 一部またはすべてのプライマリが利用不可能で、BL サービスが自動的に再起動します

4.3.3 データの分散

利用可能なシステム数に基づいて複数の構成の組み合わせがあります。まず、ユーザ数を均等にパーティションに割ります。

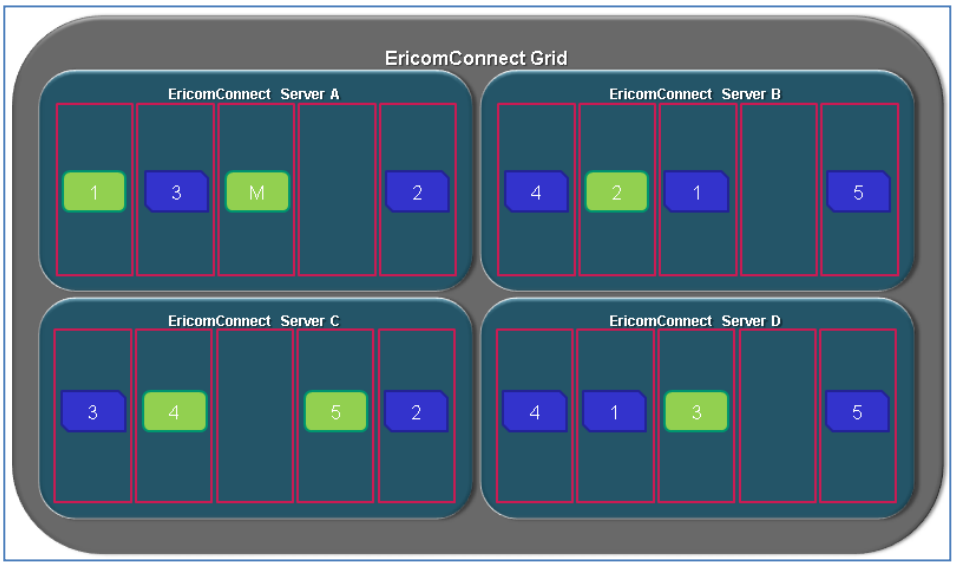
例えば、30,000 ユーザが存在する場合、組み合わせは次の通りになります:

それぞれが 1 つのパーティションを持つ 4 つのシステム (7,500 ユーザ/パーティション)

それぞれが 2 つのパーティションを持つ 2 つのシステム

4 つのパーティションを持つ 1 つのシステム

下図は、4 つの BL コンポーネント・サーバのグリッドのパーティションにデータがどのように保存されているかをサンプルとして図解したものです:



4.3.4 高可用性の実装

高可用性は、システムに単一障害点が存在しないことを保証するものです。単一のサーバまたはコンポーネントに障害が発生しても、システムが正常に動作し続けることを意味します。 グリッドを複数のサーバで実行することにより、高可用性を実現できます。グリッドは、レプリケートし、データを共有することが可能で、各サーバのメモリに渡り処理を行います。これにより、ソリューションに高い拡張性を追加し、単一障害点を防ぐことができます。

データ・グリッドには、ユーザ、ホスト・マシン、公開リソース、アクティブ・セッション、サーバ・ステータスについてのすべてのデータが含まれています。Ericom Connect により、データの整合性とコンポーネントの整合性の両方が管理されます。

4.3.4.1 データの整合性

データの整合性は、コンポーネントに障害が発生した場合でも、オペレーティング・システムに必要なすべてのデータが利用可能なことを保証するものです。グリッド・サービスは、サーバのメモリ(RAM)で実行されます。サービスの内部には、データのコンテナが含まれています。各コンテナには、システムの全体的なデータのインスタンスが保持されています。 グリッド上で管理されている各データには、少なくとも 2 つのコピーが存在します。これにより、データの整合性と高可用性が保証されます。Ericom Connect のインフラストラクチャを設計する際、データ整合性に関連した以下の事項を検討してください:

- 各データ・インスタンスは、どのくらいの数のコピーを維持する必要がありますか?
- 各グリッド(BL)マシン上に、どのくらいのコンテナをホストしますか?
- どのような方法で、各マシンのコンテナに渡ってデータを分散しますか?

概念実証(Proof of Concept)環境または小規模な本番稼働システムでは、単一サーバ上でグリッドを動作させることができます。各データ・インスタンスの少なくいとも 2 つのコピーが維持されますが、単一サーバは単一障害点となります。

2 台のサーバ構成では、各パーティションの 1 つのインスタンスは、それぞれのサーバで維持される必要があります。いずれかのサーバに障害が発生した場合、データ整合性はそのまま維持されます。

4.3.4.2 コンポーネントの整合性

Ericom Connect コンポーネントはモジュール式であり、コンポーネント・レベルの高可用性を提供するように設計することが可能です。各 Ericom Connect コンポーネントは、グリッドのクライアントです。コンポーネントはグリッドから設定情報を受け取り、グリッドとリアルタイムで通信しステータスの送受信と情報の更新を行います。 グリッドには各コンポーネントとそのステータスが認識されます。例えば、End User Web Service(EUWS)が応答しなかった場合、以降グリッドはそのサ

ービスへリクエストを送信しなくなり、利用可能な他の EUWS コンポーネントにリクエストをルーティングするようになります。

ベスト・プラクティスとしては、各 Ericom グリッド・コンポーネントに少なくとも 2 つのインスタンスを維持するようにします。複数のコンポーネントがアクティブ/アクティブ構成で動作することで、ファイルオーバー中のダウンタイムの心配がありません。 Ericom Connect では、システム内のグリッド・コンポーネント数は無制限にサポートされています。新しいコンポーネントの登録は迅速かつ容易に行うことができます。コンポーネントをインストールしてグリッドに接続するだけです。このプロセス全体は通常数分以内で完了します。

4.3.5 2 台のサーバ構成(例)

GSC の必要数を決定するための式は次のようになります: GSC 必要数 = パーティション数 x (1 + バックアップ数) + 1(ミラー用)。

小規模な展開(5,000 ユーザ未満)には、1 つのみパーティションが必要なため、次のコマンドを使用します:

ConnectCLI SetGridParameters 1 1 2 1

より規模の大きい展開 (5,000 ~ 10,000) には、次のコマンドを使用して 2 つのパーティションを割り当てます:

ConnectCLI SetGridParameters 2 1 3 1

次の構成は、高可用性に適して**いません**:

ConnectCLI SetGridParameters 2 1 3 2

システム設定データを保存するためにバックアップが必要です。バックアップを 2 つにすることをお勧めします。

構成後、構成を検証するために ConnectCLI GridInfo を実行し、**設定を反映するためにすべてのグリッド Controller サーバを再起動します**(バックアップ値のみがデフォルトのグリッド・パラメータ「１０２１」から変更されます)。

サーバがダウンした場合、BL サービスに欠陥が生じていること、およびミラーが失われていること(ミラーがダウンしているサーバにホストされている場合)が、自動的にグリッドに検知されます。

```
EricomConnectBusinessLogic Compromised; Partitions=2; Backups=1; MaxInstancesPerMachine=1
EricomConnectMirrorService Broken; Partitions=1; Backups=0; MaxInstancesPerMachine=0
```

ダッシュボードのシステムヘルスにも、グリッド・ステータスが「障害(Compromised)」であることが表示されます。

数分以内に、ミラーが運用サーバへ移されます。

```
EricomConnectBusinessLogic Compromised; Partitions=2; Backups=1; MaxInstancesPerMachine=1
EricomConnectMirrorService Intact; Partitions=1; Backups=0; MaxInstancesPerMachine=0
```

グリッドを「Intact」の状態にリストアするには、破損したサーバを復旧します。 即時にリカバリを実行できない場合は、可用性を高めるために 3 番目のサーバを追加することを検討してください。

4.3.6 複数パーティション・コピーの構成

2 台のサーバがダウンしても問題ないように Ericom Connect を構成するには、最低 3 台のサーバが必要です。 3 つのうち 2 つがダウンした場合、システムは「Compromised」状態になります。

2 台のサーバがダウンしてもシステムを「Intact」状態を維持できるように Ericom Connect を設定するには、4 台のサーバが必要です。

4 つのパーティションと 2 つパーティションを持つ 4 台のサーバを構成するには次を実行します:

ConnectCLI SetGrid parameters 4 2 3 1

(これにより、2 台のサーバがダウンしても問題ないようになります)

ConnectCLI SetGrid parameters 4 2 5 1

(これにより、グリッドの起動を維持するための 2 台のサーバ用として十分な 5 つのパーティションが設定され、3 つのサーバがダウンしても問題ないようになります)

次の構成は、高可用性に適していません:

ConnectCLI SetGridParameters 3 2 4 3

1 台のサーバがデータ・セット全体(パーティション + バックアップ)を保持する可能性があるため、この構成が正しく動作するには、3 台すべてのサーバがオンラインである必要があります。

4.4 Connect での Active Directory の使用法

Connect は、認証のために 1 つまたは複数の Active Directory を使用するように構成されています。

項目「ActiveDirectoryInfo」では、単一の Active Directory ドメインの構成情報が参照されています。項目「ActiveDirectorySet」では、1 つまたは複数の ActiveDirectoryInfo オブジェクトを含むコレクションが参照されています。

Connect の構成情報には、以下の 2 つの独立した ActiveDirectorySets が含まれています。

- AdminSet：Connect 管理者の検証に使用される ActiveDirectorySet です。
- EndUserSet：エンドユーザの検証に使用される ActiveDirectorySet です。

Connect では、ドメイン間の信頼関係がサポートされていません。 これは次のことを意味します: ドメイン A が ドメイン B を信頼し、ドメイン B がドメイン C を信頼している場合、3 つすべてのドメインのユーザを含めるためには、3 つすべてのドメインを EndUserSet に追加する必要があります。

Connect では、ドメインで明示的に設定された UPN をすべてのユーザに与えることが必要になります。 これはすべての最新の Active Directory におけるデフォルトの動作ですが、古いオペレーティング・システムから移行したディレクトリでは設定されていない可能性があります。

4.4.1 認証プロセス

Connect の認証プロセスは以下のように動作します:

- ユーザ名が管理者またはエンドユーザにより入力されたとします:
- 入力されたユーザ名にドメインが含まれていない場合(例: Michael@test.com または Test\Michael ではなく、Michael が入力された場合)、ActiveDirectorySet の設定からデフォルトのサフィックス(またはプレフィックス)が使用されます。
- ActiveDirectorySet 内のどのドメインに対して検証するかが決定されます。

- ドメインでユーザが見つかるかどうか検証されます。
- 資格情報が検証されます。
- 検証が失敗した場合、エラー・メッセージが返されます(無効な資格情報、パスワード有効期限切れなど)。
- 検証が成功すると、ドメインからユーザの情報が取得されます。

4.4.2 認証の詳細

ユーザ名の補完: ユーザ名にドメインが含まれていない場合、セットのデフォルトのドメインからデフォルトのサフィックス(またはプレフィックス)が取得されます。セット内で、ドメインの 1 つがデフォルトとして設定されています。 この目的のために、デフォルト・ドメインにはサフィックス/プレフィックスが設定されています。

- 複数のドメインで同一の UPN サフィックスを使用することが可能です。
- ドメインで UPN サフィックスを適切に公開しないことが可能です。 このようなサフィックスは、「非標準 UPN サフィックス」として知られています。

各ドメインに、既知の UPN サフィックスの一覧が関連付けられています。 この一覧により、自動的に「標準 UPN サフィックス」が決定されます。 複数のドメインを使用する場合、非標準 UPN サフィックスを追加する必要があります。

検証対象となるドメインは、以下のように決定されます:

- セットに単一のドメインが存在する場合、そのドメインが使用されます。
- 複数のドメインが存在する場合:
- user@domain または domain\user からの UPN サフィックスが、セット内のドメイン名と一致する場合、そのドメインが使用されます。
- UPN サフィックスがドメインの標準 UPN サフィックスと一致する場合、そのドメインが使用されます。同じサフィックスを持つ複数のドメインの場合、動作は指定されません。
- UPN サフィックスが、ドメインに構成済みの非標準サフィックスと一致する場合、そのドメインが使用されます。

4.4.3 最初の ActiveDirectorySets の作成

インストール時に、以下のようにエンドユーザと管理者用の Active Directory が作成されます:

- 「初期管理者ユーザ」が user@upnsuffix として提供されている場合。
- 「upnsuffix」が Active Directory ドメイン名である場合、そのドメインが追加され、デフォルトのサフィックスが「@upnsuffix」に設定されます。
- 「upnsuffix」が Active Directory ドメイン名ではなく、現在のマシンが登録されている Active Directory で user@upnsuffix が検出可能な場合、マシンのドメインが追加され、デフォルトのサフィックスが「@upnsuffix」に設定されます。

- 「初期管理者ユーザ」が domain\user として提供された場合
- 「ドメイン」が Active Directory ドメインである場合、そのドメインが追加され、デフォルトのプレフィックスは「domain\」に設定されます。

初期管理者ユーザの「upnsuffix」がドメイン名か現在のマシンのドメインのどちらでもない場合、そのユーザを初期管理者として設定することはできません。 後でその追加を行うことができます。

エンドユーザと管理者の Active Directory セットの両方で同様の初期設定が使用されます。

4.4.4 複数の Active Directory の使用

Ericom Connect で使用するために複数の Active Directory を設定する場合、すべてのドメインにアクセスするのに十分な権限を持った資格情報がグリッド・サービスにより使用されることを確認してください。

例:

Ericom Connect が 信頼されていない「abc.local」上にインストールされています。

管理者は、次のコマンド・ラインを使用してドメインを追加します: ConnectCLI ActiveDirectories add test.local

エラーは返されませんでした。しかし、管理者が「test.local」からユーザを追加しようとした際にエラーが返されました: Unable to add domain ‘test.local’（ドメイン「test.local」を追加できません）

これは、グリッドサービスがドメイン「test.local」へアクセスできない資格情報を使用しているために発生します。

4.4.5 Active Directory ConnectCLI の使用法

ConnectCli ActiveDirectories を使用して、追加と変更のコマンドを実行することで、すべてのアクティブ・ディレクトリ情報を設定することができます。 これらのコマンドは、綿密なテストを実行するためにも使用できます。

「add」(追加)と「modify」(変更)コマンドは、同じセットのパラメータと引数を使用できます。 システムに登録されていない Active Directory には、「add」コマンドを使用します。

使用法: ConnectCli ActiveDirectories [オプション]* add | modify ドメイン名 [テスト・ユーザ [テスト・パスワード]]

例：

- ConnectCli activeDirectories add test.local testuser@test.local passwordForTestUser
  - testuser@test.local が認証可能であることをテストした後、Active Directory に test.local を追加します
- ConnectCli activeDirectories /default modify test.local
  - test.local をデフォルトの Active Directory に設定します
- ConnectCli activeDirectories /adUser domainAdmin@test.local test.local **testuser@test.local** passwordForTestUser
  - testuser@test.local が認証可能であることを検証した後、Active Directory に test.local を追加します

    - ユーザ domainAdmin@test.local がすべての Active Directory 操作に使用されます。
- ConnectCli activeDirectories /simulate modify test.local **testuser@test.local** passwordForTestUser
    - 現在 test.local に構成されている設定を使用して、ユーザ testuser@test.local が認証可能であるかを検証します
- ConnectCli activeDirectories /simulate add test.local **testuser@test.local** passwordForTestUser
    - 登録されていない Active Directory の test.local を使用して、ユーザ testuser@test.local が認証可能であるかを検証します

testuser を指定する場合、そのテスト・ユーザ用の情報がアクセス可能であること、およびそのユーザが認証可能であることが、Ericom Connect によって検証されます。 パスワードなしでユーザ名を指定した場合、プロンプトが表示されます。

/noconfirm を指定している場合を除き、変更を適用する前に確認が必要です。

「add」コマンドを使用すると、指定した設定で Active Directory が作成されます。 「modify」コマンドを使用すると、コマンド・ラインで指定したすべての設定により、現在の値が置き換えられます。

ConnectCLI ActiveDirectories のオプション	**説明**
/adUser <文字列>	Active Directory に接続する際に使用するユーザ。指定しない場合、Controller サービスで使用されている資格情報を

	使用して Active Directory の操作が実行されます。
/adPassword <文字列>	Active Directory ユーザのパスワード。コマンド・ライン上で/ adUser の指定があり、/ adPassword の指定がない場合、パスワードのプロンプトが表示されます。
/adDefaultSuffix <文字列>	Active Directory のデフォルトのサフィックス(@domainname のデフォルト)。 これには、任意の UPN サフィックスを使用できます。@upnsuffix または domain\ の形式である必要があります。
/[no]default	これがデフォルトの Active Directory に設定されます。テナントに複数の Active Directory がある場合、ログイン時に UPN サフィックスが指定されなかった時にこれが使用されます。
/contextOptions <コンテキストオプション>	使用する Active Directory のネゴシエーション・コンテキストのオプション(複数可)。 デフォルトは、Negotiate です。一部の状況(例: Microsoft 以外の LDAP)では、SimpleBind を使用する必要があります。カンマ区切りのリスト

	(例: Negotiate, SimpleBind)を使用できます。使用できるオプションは以下のとおりです: Negotiate, SimpleBind, SecureSocketLayer, Signing, Sealing, ServerBind。
/nonStandardUpnSuffixes <文字列[,...]>	この Active Directory 向けに想定する UPN サフィックスのカンマ区切りのリスト。 通常、Ericom Connect では、Ericom Connect 自体 の UPN サフィックスを使用して Active Directory が照会されます。 一部のケースでは、Ericom Connect により正しいリストを決定することができません。その場合、このオプションを使用する必要があります。例えば、/adUser が情報を取得するために必要なアクセス権を持っていない場合、または UPN サフィックスが Active Directory の構成パーティション内に適切に記録されていない場合。これは、複数の Active Dirctory を設定している場合のみ関連があることに注意してください。
/testOnly	Active Directory のみをテストします。変更を保存しないでください。(/testOnly)

/noconfirm	アクションを実行する前に確認を要求しません。
/adminUser <文字列>	Ericom Connect の管理者ユーザ。指定しない場合、プロンプトが表示されます。
/adminPassword <文字列>	Ericom Connect の管理者パスワード。指定しない場合、プロンプトが表示されます。
/tenant <文字列>	更新するテナント。指定しない場合、ルート・テナントが使用されます。
/techSupport	テクニカル・サポートに詳細な情報を提供します。

コマンドを実行する際にユーザ・アカウントの AD の詳細を表示する

出力例:

ConnectCli activeDirectories /testOnly modify corp.acme.com user@corp.acme.com passwordForTestUser

特定の AD パラメータとともに、ユーザの詳細が返されます。

Domain Information for corp.acme.com
MinPasswordLength = 7
MaxPasswordAgeDays = 42
LockoutThreshold = 0
UpnSuffixes =

Information about user@corp.acme.com

GetStdLoginName: user@corp.acme.com
PrincipalName: user@corp.acme.com
SamAccountNamee: user
Name: user
AccountExpirationDate:
CannotChangePassword True
Last password set: 6/23/2016 3:24:32 PM
Enabled: True
Is Locked out: False
Account Lockout Time:
Bad Logon Count: 0
Pre-authentication analysis for user@corp.acme.com
Password never expires
Authentication succeeded
Member of: Domain Users, Users
Active directory configuration is OK

(20160831,20161027)

Active DIrectory ドメインに関する情報を取得するには、次を使用します:

- ConnectCLI GetDomainInfo domainName

Active Directory からユーザの情報を取得するには、次を使用します:

- ConnectCLI UserActiveDirectoryInfo username

ユーザの資格情報を確認するには(Connect で使用するのと同じ方法で)、次を使用します:

- ConnectCLI CheckUserCredentials

ユーザが初期管理者アカウントとして使用可能かどうかを確認するには、次を使用します:

- ConnectCLI CheckInitialUser

4.4.6 ネストされた AD グループのサポート

Ericom Connect では、ネストされた AD グループがサポートされています。 グループ B がグループ C のメンバーであり、グループ C にアプリケーション D へのアクセス権が与えられている場合、そのユーザはアプリケーション D へのアクセス権を持つことになります。

4.4.7 要件と既知の問題

要件

初期ユーザは、次のいずれかの形式である必要があります:
user@domain (domain は Active Directory ドメイン) または
user@upnsuffix (UPN サフィックスはマシンのドメインに存在するもの)

複数のドメインを使用する場合、現在のマシンが登録されているドメインに非標準 UPN サフィックスが存在する必要があります。

既知の問題

Active Directory からの情報にアクセスするための権限が不十分な場合、Connnect により ログインの失敗が誤って診断される可能性があります。 例えば、「パスワードを変更する必要があります」の代わりに、「アカウントが無効です」というエラーがユーザに表示される場合があります。 この問題は、「ConnectCLI

UserActiveDirectoryInfo」を実行してアカウントが無効になっているかを確認することで検出できます。 Connect サービスは通常「local service account」として実行されます。 このアカウントに十分な権限が与えられていない場合、以下のオプションを検討する必要があります:

- ドメインの完全な読み取りアクセスを許可するように Active Directory の権限を変更する
- サービスに別の資格情報を使用する
- Active Directory にアクセスする際に使用する資格情報を設定する

4.5 アップグレードと再展開

Ericom グリッド・コンポーネントとサービスの一部には、相互互換性がありません。 新しいバージョンへアップグレードする場合(例: 7.2 から 7.3)、以下の順序で Ericom コンポーネント(例: ESG, EUWS など)のアップグレードを実行します:

- Ericom Business Logic
- エッジサービス: ESG, AWS, EUWS など
- RemoteAgent
- 最後に、エンドユーザの AccessPad クライアント

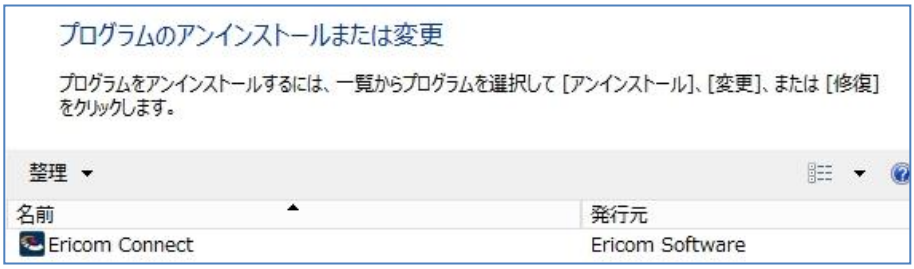
4.5.1 アンインストール手順

Ericom の展開に関連する以下のデータを収集します:

- Grid Name (グリッド名)

- Ericom Connect SQL データベースのユーザ・アカウント
- Ericom Connect SQL データベースのパスワード
- Ericom Connect の管理者ユーザ(任意のマスター管理者)

Winsows のアンインストール機能を使用して Ericom Connect をアンインストールします。

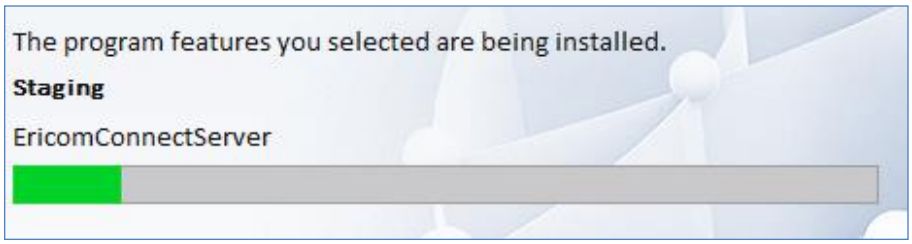


削除プロセス中に「Preserve existing configuration」チェックボックスが表示されたらそれを選択し、「Remove」ボタンをクリックします。 これにより、今後の使用のためにサーバ上の展開情報が保存されます。 この手順は、バージョン 7.0 では必要ありません。

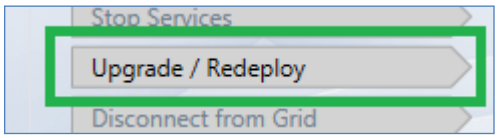
「アンインストール」後にロールバックが必要となる場合に備え、**SQL データベース**と次のフォルダ(隠しフォルダ)**C:\ProgramData\EricomConnect** をバックアップします。

4.5.2 再展開の手順

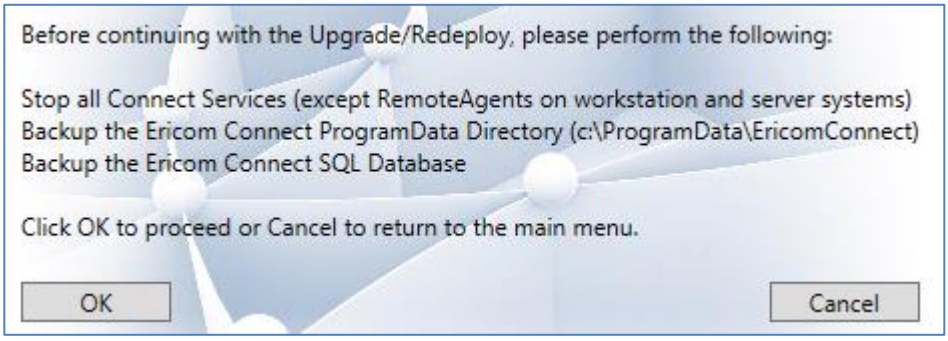
Ericom Connect を同じサーバにインストールする場合、メモリ内の以前のファイルがすべて消去されたことを確実にするために、アップグレードの前に再起動することをお勧めします。



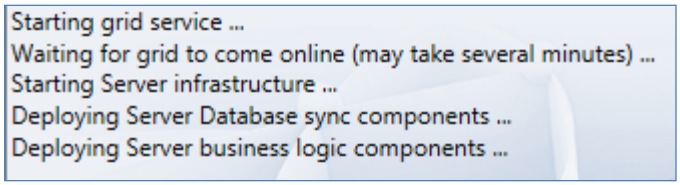
インストールの最後で、自動的に Configuration Tool が起動します。「**Upgrade /Redeploy**」を選択します。



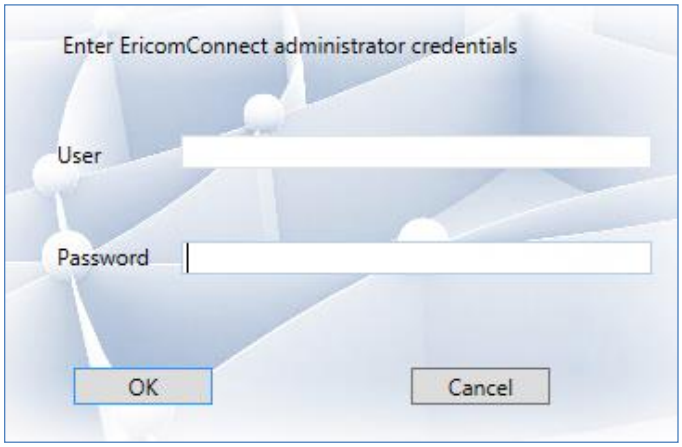
続行する前に、c:\ProgramData\EricomConnect フォルダと SQL データベースをバックアップするようにメッセージが表示されます。 これは、必要な場合にロールバックを実行するために強く推奨されています。



「OK」をクリックして続行すると、 Ericom Connect の再展開が開始されます。



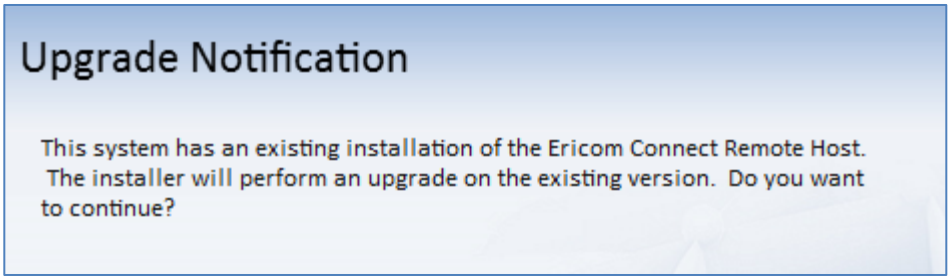
初期化プロセス中に、初期管理者の資格情報を要求するプロンプトが表示される場合があります(通常は以前のバージョンからアップグレードする場合)。 続行するには有効な資格情報を入力します。



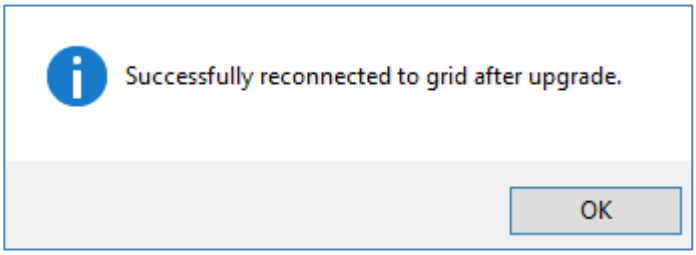
元の環境に 2 つ以上の Ericom Connect サーバが存在する場合、グリッドのパラメータはアップグレード後にデフォルトに戻ります。 この動作について警告メッセージが表示されます。 すべての独自のグリッドのパラメータを再適用する必要があります。

4.5.3 RemoteAgent のアップグレード

バージョンのアップグレードの最後の手順として、RemoteAgent をアップグレードします。 バージョン 7.3 より、既存の RemoteAgent をインストールしたままで RemoteAgent をアップグレードすることが可能になりました。 以前のバージョンが存在する場合、インストーラによりアップグレードの通知が表示されます。



RemoteAgent のアップグレードが成功すると、成功のメセージが表示されます。 この時点で、アプリケーションやデスクトップは Ericom Connect で使用可能な状態になっています。



新しい RemoteAgent は、以前のバージョンの Ericom Connect サーバと互換性がありません(例: 7.5 RemoteAgent は 7.3 Ericom Connect では動作しません)。ただし、新しい Ericom Connect サーバは、現行バージョンの RemoteAgent と旧バージョンの RemoteAgent の併用に対応しています。 これは、RemoteAgent のアップグレード移行時の下位互換性を提供するためです。

4.5.4 SQL DB からの再展開

元のグリッドのパラメータが保存されている場合、既存の SQL データベースからグリッドを展開できます。

- ライセンスの有効性を維持するために、グリッドの名前は元のグリッドと一致する必要があります(グリッド名はライセンス・ファイルの必須項目です)。

- **最初に作成した**管理者ユーザのドメインにアクセスできる必要があります(既存の SQL DB を新しいドメインに再展開することはできません)。
- Ericom Connect データベースの資格情報は既知である必要はありません(ただし、データベースにアクセスするために SQL Server 内で適切な資格情報が要求されます)。 元の資格情報を持つことで、データベースの構成を効率的に行うことができます。
- データベースが異なるサーバへ移動されている場合、元の資格情報が有効でない場合があります。 このシナリオでは、新しいセット資格情報を作成し、データベースへアタッチします。
- SQL データベース名が必要です(データベースの詳細を取得するには SQL Management Studio を使用します)。
- LUS 値は元のものと一致する必要はありません。

4.5.5 以前のバージョンへのロールバック

以前のバージョンにロールバックするには、以下の手順を実行します:

- 現在のバージョンをアンインストールします
- 以前の SQL データベースをリストアします
- ProgramData フォルダをリストアします(オプションとして、ローカル構成情報をリストアします。手動で入力することもできます)
- 以前のバージョンの Ericom Connect をインストールします
- 「Upgrade /Redeploy」を実行します

- グリッド名、データベース名、データベース・ユーザ、および LUS アドレスが正しいことを確認します 必要に応じて任意のパラメータを設定します
- 以前のバージョンの展開を続行します

4.6 マルチテナント機能

Ericom Connect では、マルチテナントがサポートされています。 Ericom Connect アプリケーションの 1 つのインスタンスが、複数ユーザに提供するためのプライベート・コンテナに細分されます。 マルチテナント機能の利点は以下のとおりです:

- 多くのバラバラなサイロをインストールするのではなく、1 つのスケーラブルなインストールを活用します。
- 複数顧客をサポートする 1 つのインストールにより、インストール、設定、保守にかかるオーバーヘッドが削減されます。
- 各テナントのリソース(ユーザ、グループ、ターミナル・サーバなど)は、他のテナントから保護されています。
- 各顧客は専用のアクセス URL を受け取ります。

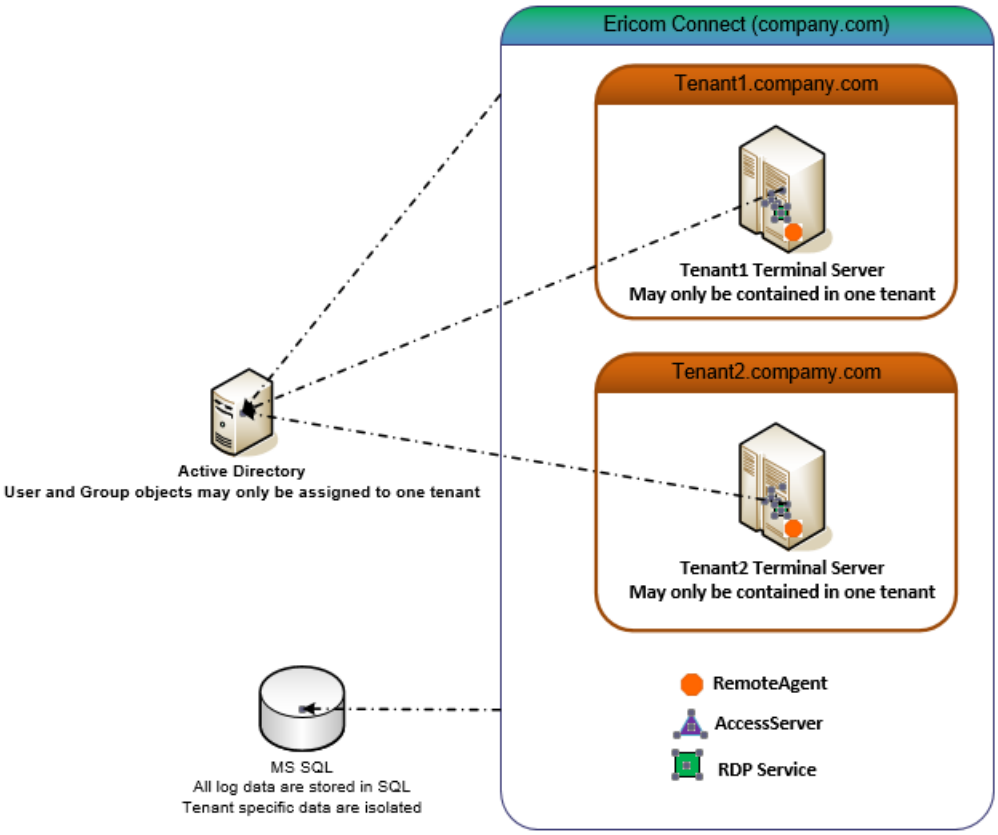
以下はマルチテナントの使用例の一部です:

- 各顧客が自らのユーザ、設定、リソースを管理できる Daas(Desktop as a Service)プラットフォームを、クラウドに展開する。
- ベンダー業者用に、内部ネットワークとリソースから分離されたテナントを展開する。

- クリティカルなアプリケーションを非クリティカルなアプリケーションから分離する。 クリティカルなアプリケーションをホストするテナントに、より高度なセキュリティ要件(例: 二要素認証)を追加する。

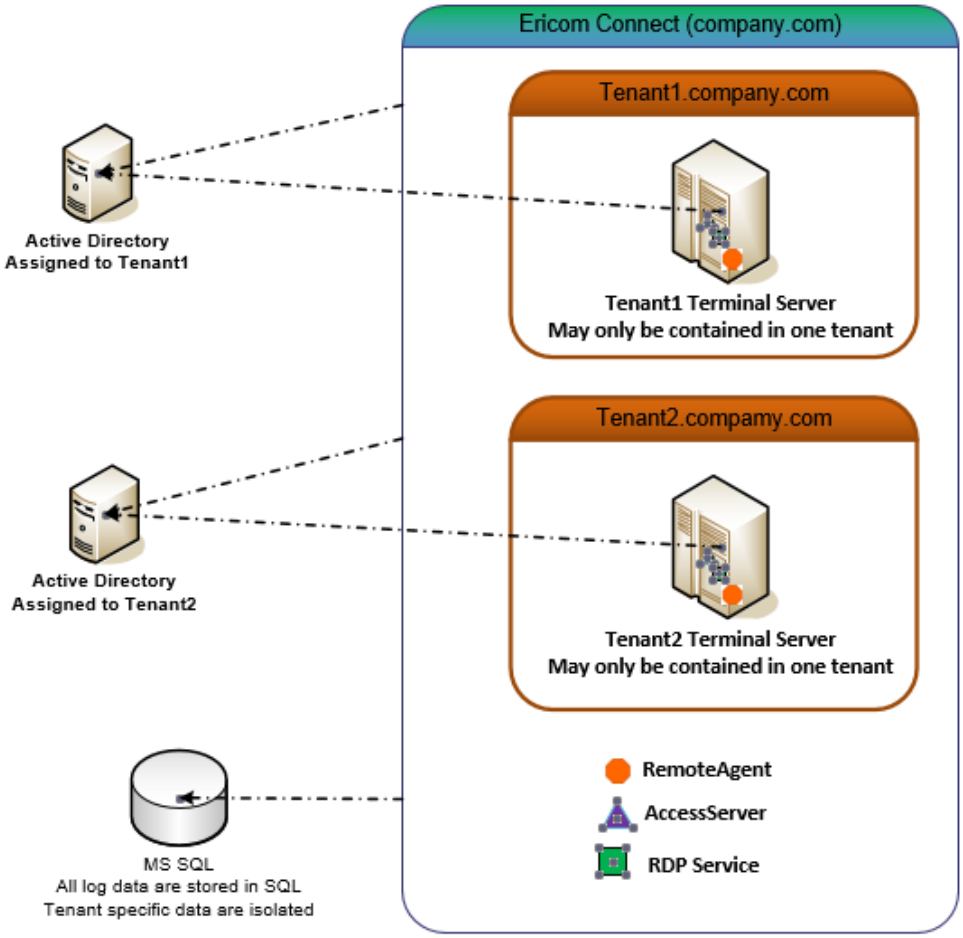
4.6.1 共有 Active Directory モデル

複数テナントで 1 つの Active Directory を共有できます。 厳密なリソース保護を確実にするため、Ericom Connect ではテナントにつき 1 ユーザ が許可されています。



4.6.2 専用 Active Directory モデル

Ericom Connect では、複数の Active Directory の使用がサポートされています。 この機能により、各テナントが独自の Active Directory を持つソリューションを実装できます。



テナントに特定の Active Directory を割り当てる CLI コマンドは次のとおりです:

ConnectCLI ActiveDirectories /tenant TenantA add company1.com

4.6.3 マルチテナント機能のベスト・プラクティス

- テナントの使用を計画している場合、ルートのテナントを空のままにしておきます。 テナントのアーキテクチャを設計し、ユーザ、サーバ、ワークステーションおよびアクティブ・ディレクトリをそれぞれのテナントに割り当てます。
- テナントへの接続元となる URL と URL プレフィックスが一致する必要があります。 接続を確立するために、DNS の構成が必要となる場合があります。 ホスト・ファイルの設定をローカル・テストに使用します。
- ルート・テナントは、「rooturl」のラベルがついています。 これにより、その IP にマップされた未設定のアドレスを使用して、ルート・テナントのログイン・ページを閲覧できます。 ユーザの資格情報を使用したページはセキュリティで保護されていますが、ルート・テナントを特定のアドレスの下に隠すことをお勧めします。 ただし、これを実施する場合、そのアドレスを書き留めておいてください。そのアドレスが不明になると、ルート・テナントへのアクセスができなくなります。 このアドレスは、管理者のログインのために、DNS またはホスト・ファイル構成からもアクセス可能である必要があります。
- ユーザがログインすると、テナントへ割り当てられた状態になります。 テナントにログインすると、ユーザは恒久的にマップされます。

- 特定の委任された管理者要素は「クロステナント」です。これらを割り当てる場合は注意してください。 通常は、ルート管理者のみにこれらへのアクセス権が必要です。
- 通常は、ルート・テナントのプレフィックスを変更する必要はありません。ただし、ルート・テナント用の特定の値を定義することで、ユーザがそのテナントへ誤ってログインする可能性を最小限にできます(特定の値を非公開とした場合)。

4.6.4 テナントの作成

Ericom マルチテナント機能は、ConnectCLI を介して管理されます。
使用可能なすべてのオプションを参照するには、次を実行します: ConnectCLI tenant /?
新しいテナントを作成するには、次を実行します: ConnectCLI tenant /**TenantUrlPrefix acme add company1**
このコマンドにより、一意の識別子「**company1**」とプレフィックス「**acme**」を持った新しいテナントが作成されます。

このプレフィックスは管理コンソールへのログインに使用され、テナントの URL プレフィックスとして使用されます(例: **acme**.serviceprovider.com)。

構成済みのすべてのテナントを一覧表示するには、次を実行します: ConnectCLI tenant list

4.6.5 テナントの管理

テナントを管理するには、 Ericom 管理コンソールのログイン・ページに移動します。 テナントが作成されている場合、テナント・フィ

ールドが表示されます。 テナント用に設定したプレフィックスを入力します。これがテナントの URL プレフィックスとなります(例: **acme**.serviceprovider.com)。

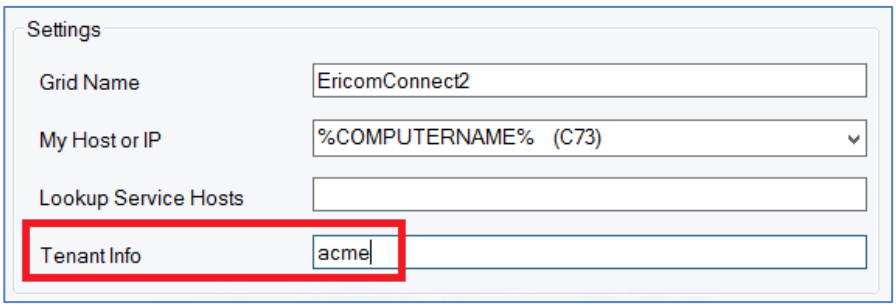
ルート・システム管理者グループが自動的にテナント管理者として割り当てられます。

テナント管理者の割り当てを行うためにログインする際は、ルート・アカウントを使用します。 テナントの「管理者の役割」セクションに移動し、テナント管理者の割り当てと管理を行います。

注意: 同一のブラウザを使用して同時に複数のテナントの管理を行わないでください。 異なるテナントの管理を行うには、シークレット・モードまたは違う種類のブラウザを使用してください。

4.6.6 テナントにホストを追加する

テナントの値が RemoteAgent で設定される場合(例: 「テナント情報」に「Acme」を入力し、「Connect to Grid」を選択)、ホスト(例: ターミナル・サーバ) はテナントに関連付けられています。



RemoteAgent の接続を一度行うと、ホストとテナントの関連付けは永続的となります。

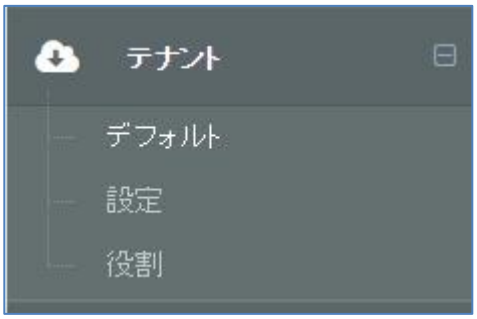
テナントを消去すると、関連付けられたすべての「孤立した」ホストは、再構成するまで使用不可能になります。 孤立したホストをConnect に接続しようとした場合、「テナントを見つけることが出来ません(Cannot find tenant)」というエラーが発生します。

新しいテナントが同じ名前で再作成されたとしても、再構成されるまで、ホストは機能しません。

RemoteAgent を再構成するには、グリッドから切断し、新しい「テナント情報」を入力した後、グリッドに再接続します。

4.6.7 テナント設定

テナント固有の設定は、「テナント設定 | テナント設定」の下の管理コンソールで構成します。



テナントの URL プレフィックスを FQDN URL として定義できます(例: xyz.abc.com)

4.6.8 ESG の設定

Ericom Secure Gateway(ESG)は、テナント固有ではありません。Ericom Connect の展開において構成された任意の ESG を介して、

すべてのテナントのユーザがログイン可能です。 異なるテナント用に ESG を展開するには、複数のシナリオがあります。

オプション 1:

すべての ESG 用に、同一のワイルドカード証明書(例: *.provider.com)を使用する

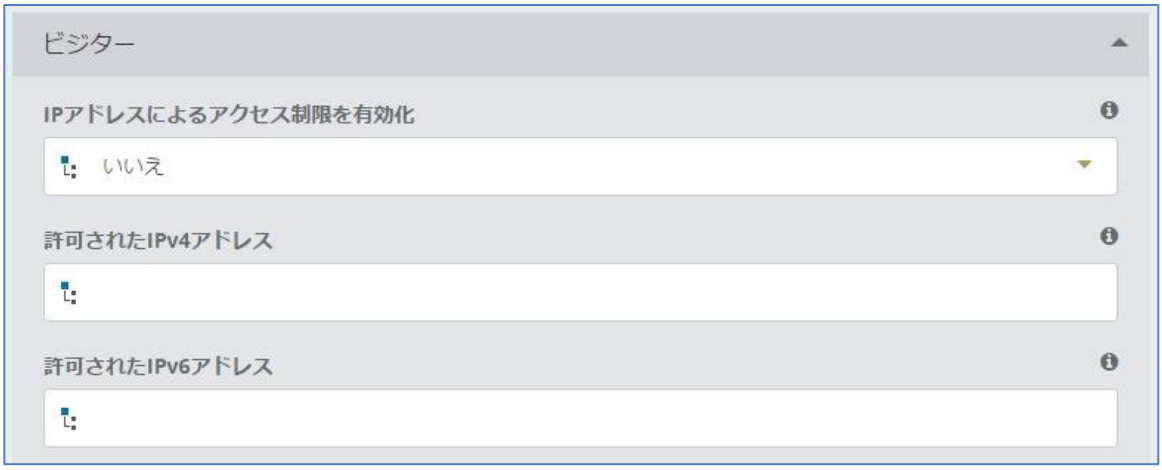
- すべてのテナントにわたり、1 つのワイルドカード証明書を使用することができます。
- アクセスレベルのセキュリティは、テナントの公開グループにそれぞれの「ESG ホスト・アドレス」を設定することで提供されます。 例えば、company2.provider.com のユーザは、「ESG ホスト・アドレス」を company1.provider.com に制限した公開グループからはリソースを起動できません。
- 認証レベルのセキュリティは、テナントにそれぞれの Active Directory を割り当てることで提供されます。

オプション 2:

特定の ESG をテナントに割り当て、専用の証明書を使用する。

- 管理コンソールを使用して、割り当てられた ESG システムに専用の証明書を設定します(「サービス | ESG サービス」に移動し、目的の ESG サーバをクリックします。「設定タブ」をクリックし、「証明書の設定方法」および「証明書の設定値」を設定します)。

- 専用の名前を割り当てます。例: 構成済みの ESG の手前のロード・バランサに users.company1.com を割り当てます。
- 「company1」のユーザには、その専用のアドレスを使用するよう指示します。
- アクセスレベルのセキュリティは、テナントの公開グループにそれぞれの「ESG ホスト・アドレス」を設定することで提供されます。 例えば、company2.provider.com のユーザは、「ESG ホスト・アドレス」を users.company1.com に制限したすべての公開グループからリソースを起動できません。
- 認証レベルのセキュリティは、テナントにそれぞれの Active Directory を割り当てることで提供されます。
- ESG の「設定 | ビジター」セクションから、ホワイトリスト・セキュリティ(エンドユーザの IP アドレスが分かる場合)を構成できます:



4.7 Ericom Analytics

Ericom には、ビジネス・インテリジェンス用のデータのビジュアル化機能が統合されています。 このアドオンには、Microsoft IIS が必要とされ、通常は Ericom Connect 管理 Web サービスと共にインストールされます。Ericom Analytics インストーラは、次で示される Ericom Connect 管理 Web サービスのフォルダにあります:

C:\Program Files\Ericom Software\Ericom Connect Admin Web Service\Ericom Analytics.msi

Ericom Analytics パッケージをインストールするには、MSI を起動します。インストール中、Analytics パッケージで使用するために Ericom Connect データベースのパラメータが自動的に設定されます。

Ericom Analytics パッケージのインストールが完了すると、IIS が有効になり、システム上で構成されます。 IIS によりポート 8057 がリッスンされます。リモート・システムからのアクセスを可能とするために、ローカル・ファイアウォール上でこのポートを手動開放する必要があります。Ericom Analytics のビジュアル化データにアクセスするために、以下の様なスタンドアロンの URL を使用できます:

https://<<サーバアドレス>>:8057/Dash.aspx#/EricomConnect/Dashboard

この URL は Ericom Connect が自動的に構成します: 「設定」|「設定」|「システム設定」タブ|「Analytics Url パス」

「Analytics」をクリックすると、ビルトインのビジュアル化機能が表示されます。 「Analytics」オプションを選択した場合、一部のブラウザではビジュアル化されたデータが新しいブラウザ・タブに表示されます。

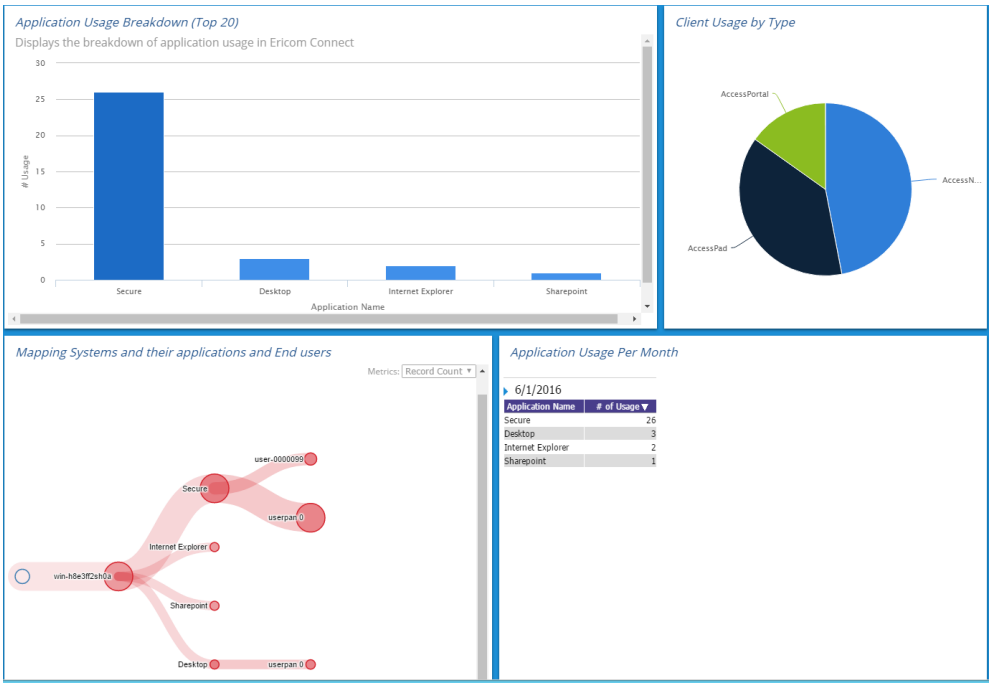
4.7.1 ビルトインのビジュアル化機能

以下の様なビルトインのレポート・ビジュアル化機能が提供されています:

- アプリケーションの使用状況の内訳(トップ 20) (Application Usage Breakdown (Top 20)) - この棒グラフでは、使用されたトップ 20 のアプリケーションと、各アプリケーションが使用された時間が表示されます。
- タイプ別のクライアント使用状況(Client Usage By Type) - この円グラフでは、エンドユーザの起動タイプの内訳が表示されます。次のタイプが含まれます: AccessPortal、AccessPad、AccessToGo、AccessNowSSO、および AccessPortalSSO。
- システムとアプリケーションのエンドユーザへのマッピング- このツリー・グラフでは、過去にエンドユーザが使用した公開アプ

リケーションをホストしているシステムが示されます。このビジュアル化では、システムの視点から過去の使用状況を追跡することができます。 Ericom Connect で使用された各システムがツリーによって示されます。 過去に使用されていないシステムは表示されません。 システムをクリックすると、そのシステム上で使用されたすべての公開アプリケーションが表示されます。 過去に起動されていないアプリケーションは表示されません。 アプリケーションをクリックすると、システム上でそのアプリケーションを起動したことがあるユーザが表示されます。 そのシステムを使用したことがないユーザは表示されません。

- 月ごとのアプリケーション使用状況(Application Usage per Month) - このレポートでは、各公開アプリケーション/デスクトップが使用された回数が月別に表示されます。



カスタマイズされたビジュアル化機能を Ericom プロフェッショナル・サービス経由でリクエストできます。 詳細については、Ericom の営業担当者にお問い合わせください。

4.7.2 インストールのトラブルシューティング

Analytics パッケージのインストールに失敗した場合、次のコマンド・ラインを使用してパッケージを再度起動してください:

msiexec /i <MSI のパス> /L*v < Log.log のパス>

分析のために、このログ・ファイルを Ericom Customer Advocacy に送信してください。

4.8 RemoteAgent の展開を自動化する

以下のスクリプトを使用して、Ericom Connect RemoteAgent を自動的に展開し、リモート・デスクトップ・サーバを起動できます(スクリプトと EricomConnectRemoteHost_x64.exe が同じフォルダ/場所に存在する必要があります):

- start /wait EricomConnectRemoteHost_x64.exe /LAUNCH_CONFIG_TOOL=false /silent
- "C:\Program Files\Ericom Software\Ericom Connect Remote Agent Client\RemoteAgentConfigTool_4_5.exe" connect /GridName **(既存のグリッド名を使用)** /myIP **(グリッドで表示されるシステムのアドレス)** /LookupService **(1 つまたは複数のカンマ区切りのアドレス)**
- 以下のサンプルのコマンドでは、**EricomConnect** という名前のグリッドに接続します。その際、**%computername%** 変数の使用、検索ホストの特定、テナント **xyz** への接続を行います: C:\Program

Files\Ericom Software\Ericom Connect Remote Agent Client>RemoteAgentConfigTool_4_5.exe connect /gridName EricomConnect /myIP %computername% /lookupServiceHosts 10.0.2.76 /tenantinfo xyz

- システムには複数の環境変数が存在する可能性があるため、myIP 設定用に環境変数を使用して IP アドレスを指定することはできません。

RemoteAgentConfigTool のコマンド・ライン・オプションの一覧は以下のとおりです:

```
Usage: RemoteAgentConfigurationTool command [options]*

Commands
  connect            [<connectOptions>] [/logFile<logFile>] [/interactive]
  disconnect         [/permanent] [/logFile<logFile>] [/interactive]
  upgrade            [/logFile <logFile>] [/interactive]
  prepareForCloning  [/logFile <logFile>] [/interactive]
  ui

Connect options:
  /gridName <gridName>              Grid Name.
  /myIP <hostOrIP>                  HostName or IP to register as.
  /lookupServiceHosts <hosts>       Comma separated List of Lookup Service Hosts, separated with comma (,).
  /tenantInfo <tenantInfo>          Tenant association information.

Others options
  /logFile <logFile>                Log file name (not used by 'ui'). Default is 'ConnectInstall.log' in the working directory.
  /interactive                      Show final status message in a pop-up window for connect, disconnect and upgrade.
  /permanent                        Make the 'disconnect' permanent.
```

以下のコマンドを使用してアップグレードを実行できます:

- インストーラのアップグレードと現在のグリッドへの接続を含む、エンドツーエンドのアップグレード:

  <RemoteAgent EXE> LAUNCH_CONFIG_TOOL=True

- グリッドに接続せずに、RemoteAgent をアップグレード:

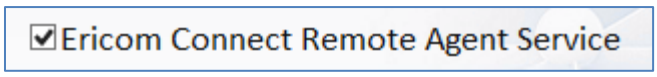
  <RemoteAgent EXE> LAUNCH_CONFIG_TOOL=False RemoteAgentConfigTool_4_5.exe upgrade

- グリッドに接続せずに、RemoteAgent をサイレント・アップグレード: **<RemoteAgent EXE> /silent LAUNCH_CONFIG_TOOL=False RemoteAgentConfigTool_4_5.exe upgrade**

4.9 RemoteAgent(Win) を使用してサーバを複製する

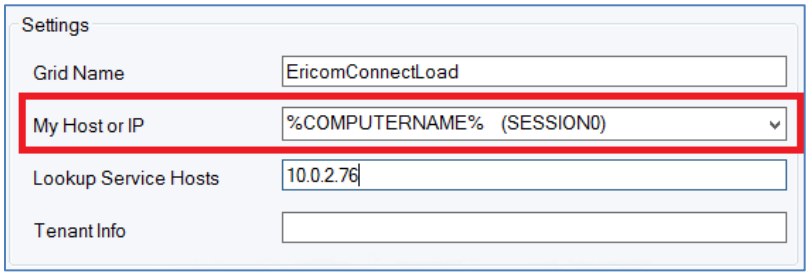
今後の展開用に複製されるように設計されているシステム上に、RemoteAgent を構成できます。 以下の手順に従って、既存システムを複製する準備を行います。

Ericom Connect インストーラまたは RemoteAgent インストーラを使用して、RemoteAgent をインストールします。 どちらのインストーラにも、「複製の準備」のためのオプションがあります。 各セッション・ホストには、RemoteAgent のみをインストールします:



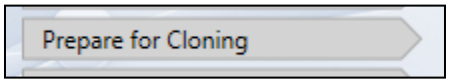
グリッド名と「Lookup Service Hosts」(通常は最初の Business Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します)を入力し、RemoteAgent をグリッドに接続します。

「My Host or IP」値の環境変数を選択します。 IP アドレスまたは DNS 名を使用しないでください。それらを使用すると、Sysprep 後に生成されたすべての新しいマシンでは 同一の Ericom Connect へのアドレスが表示されてしまいます(コンピュータ名を解決のために作動する DNS が必要になります)。



そのセッション・ホスト上でエンドユーザにより使用されるすべてのアプリケーションのインストールと設定を行います。

マシンのイメージ化の準備が完了したら、Configuration Tool を実行し、「Repare for Cloning(複製の準備) 」を選択します。



複製の準備では、以下の 3 つが実行されます:

- サービスの停止
- 「c:\ProgramData\EricomConnect」ディレクトリの削除
- Ericom Connect を起動した際に作成されたすべての証明書の削除

システムの Sysprep を実行すると、自動的にシャットダウンされます。シャットダウンが成功すると、システムは複製の準備が完了した状態になります。

4.10 LUS 設定 - マルチキャストが無効化されている場合

マルチキャストが利用できない場合は、最初の Connect マシンをインストールする前に以下の事項を決定する必要があります:

- どのサーバを「Lookup Service Hosts」(LUS)とするかを決定します。2 つにすることをお勧めします。
- これらは、「Business Logic Server」が実行されるマシンであることが必要です。

- コントローラ・システムに静的 IP アドレスを割り当てます。
- LUS マシンの数は冗長性に影響します。すべての LUS マシンがダウンすると、システムが動作しなくなります。 マルチキャスト環境では、Ericom Grid により自動的に冗長性が管理されます。
- (最初のサーバを含む)それぞれの Conect インストールにおいて、「Lookup service host」入力フィールドに適切な IP を**カンマ区切りリスト**として入力します(これらは静的 IP であることに注意してください)。 これには RemoteAgent マシンが含まれています。

LUS マシンのリストを変更するには:

- 各マシンをグリッドから切断します
- 「Join Existing Grid」を選択すると、すべての既存の設定値が入力されます。LUS リストへの正しいアドレスの入力のみが必要になります。
- グリッドへ再接続すると、新たな LUS の値が反映された状態になります。
- 代わりに、設定ファイル **C:\Program Files\Ericom Software\Ericom Connect Data Grid\NET v4.0\Config\Settings.xml** を手動で編集し、次の値を変更する方法もあります(アドレス例を実際の値に置換してください):
  <XapNet.HostName>**192.168.0.1,192.168.0.2**</XapNet.HostName>
- 静的アドレスが使用されるため、以下が false に設定されていることを確認してください:
  <XapNet.Multicast.Enabled>**false**</XapNet.Multicast.Enabled>
- XML ファイルを編集した場合、Business Logic サーバのサービスを再起動してください。

4.11 LUS 設定 – 混合モード

混合モード設定とは、マルチキャストが有効化されたネットワーク上にプライマリ・グリッド・コンポーネント(Business Logic サーバ)が存在し、マルチキャストの対象外である他のサブネット上にリモート・システム(RemoteAgent)が存在するものです。

このような環境では、プライマリ・サブネットのすべてのグリッド・コンポーネントは、LUS 設定を必要としません。 最初にオンラインになる 2 つの Business Logic サーバが、LUS サービスとして自動的に指定されます。

プライマリ以外のサブネット内のグリッド・コンポーネントは、2 つの LUS(静的)アドレスを設定する必要があります。 ベスト・プラクティスとして、すべてのグリッド・コンポーネントで明示的に LUS アドレスを設定し、環境全体で一貫性を持たせるようにしてください。

4.12 ワークステーション OS でのアプリケーションの展開

Ericom Connect では、Windows ワークステーションのオペレーティング・システムからアプリケーションを公開することができます。 ワークステーション OS 上でアプリケーションを公開する場合、エンドユーザのセッションにはアプリケーションのみが表示され、デスクトップ要素(例: スタート・メニュー)は表示されません。 ワークステーション OS からアプリケーションを公開するには、以下を実行します:

- Ericom Connect 管理コンソールを開き、「設定」| 「デフォルト」に移動します: 要件
- 「ワークステーション OS でアプリの起動を許可」(Allow App Launch on Workstation OS)の設定を「はい」(Yes)にします(この設定は、すべての公開アプリケーションに適用されます)。 これは、公開アプリケーションのレベルでも設定が可能です。
- ワークステーション OS からアプリケーションを公開するには、「セカンダリ設定」または「テナント設定」に移動し、「ワークステーション OS からの公開を許可」(Allow Publish From Workstation OS)を「はい」(Yes)に設定します。
- (RDS とワークステーションを使用する環境への推奨) すべてのリモート・デスクトップ・サーバから分離させるために、ワークステーションから構成されるシステム・グループを作成します。
- 公開グループを作成し、ワークステーションが含まれるシステム・グループに関連付けます。

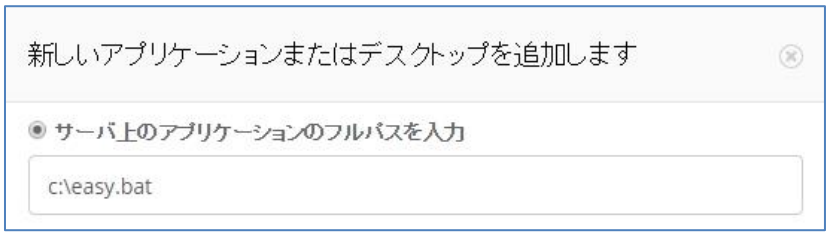
目的のアプリケーションを(ワークステーションから)公開し、ワークステーションのシステム・グループにマップされている公開グループに関連付けます。

4.13 .BAT バッチファイルの公開

アプリケーションの追加機能を使用して、バッチファイル（.BAT 形式）を公開できます。ファイルを正常に公開するために、そのファイルがいずれかの RDS サーバ上に存在することを確認してください。

「アプリケーション追加」をクリックし、「サーバ上のアプリケーションのフルパスを入力」を選択します。

バッチファイルのパスを入力します。



アプリケーションを追加する既存の公開グループ(オプション)を選択して、「追加」ボタンをクリックします。

4.14 Linux 前提条件の設定

このセクションでは、Ericom Connect で Ubuntu 14.04.3 Linux システムを使用するための、手動構成の手順の概要を説明します。**(Linux 環境はサポートしておりません)**

4.14.1 Ubuntu のアップグレードとアップデート

Ubuntu **14.04.3** をお勧めします。

次を使用してバージョンを確認します: **lsb_release –a**

```
ubuntu@:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.3 LTS
Release:        14.04
Codename:       trusty
ubuntu@:~$
```

14.04.2 から 14.04.3 にアップグレードするには、最初にすべてのアップデートをインストールします。

sudo apt-get update

QT ライブラリの依存関係をインストールします: **sudo apt-get install qt5-default**

4.14.2 Linux Ericom RDX のインストール

Ericom から、Ericom RDX という名称の X ウィンドウ向けの RDP コンポーネントが提供されています。 このパッケージにより、印刷やオーディオのリダイレクトなどの強化された機能が提供されます。

まず、以下の前提条件をインストールします:

sudo apt-get install cups
sudo apt-get install cups-filters
sudo apt-get install cups-daemon
sudo apt-get install socat

次に、Ericom パッケージをインストールします:

sudo dpkg -i ericom-x11rdp.deb
sudo dpkg -i ericom-xrdp.deb

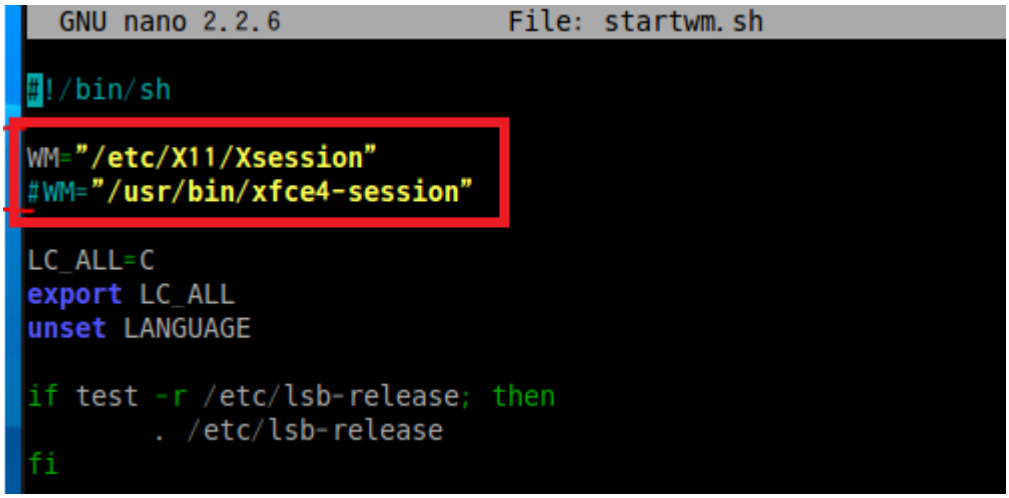
ネイティブ RDP 印刷リダイレクトを使用する場合、Linux からソフトウェア・ベースのプリンタへの印刷は使用できないことに注意してください。例: Microsoft OneNote および Microsoft XPS ドキュメン

ト ライター。 このようなプリンタへ印刷するには、ユニバーサル印刷を使用してください。

4.14.3 XFCE4 のインストール

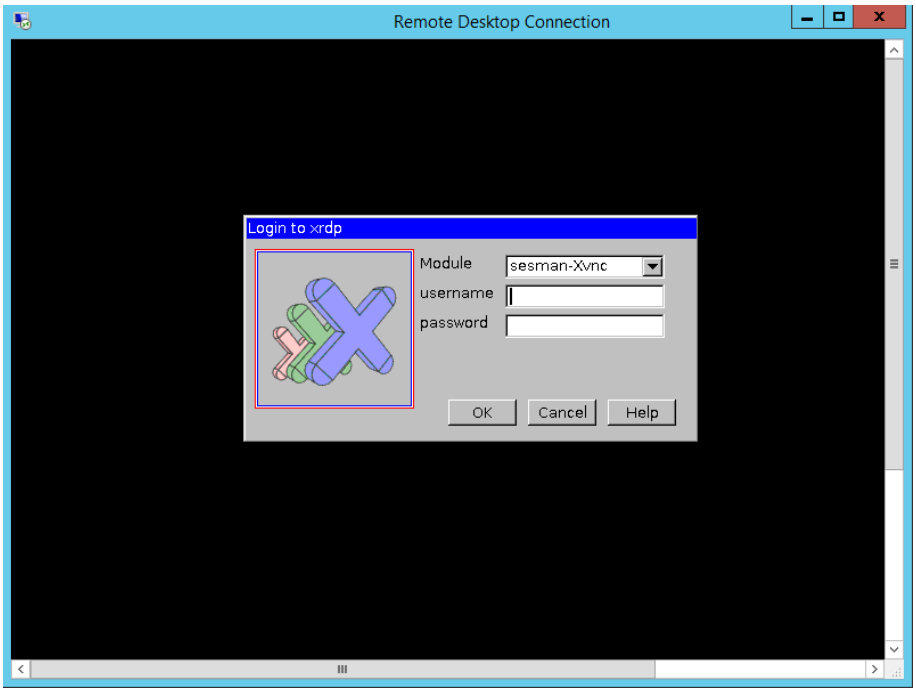
- XFCE4 をインストールします: sudo apt-get install -y xfce4
- XFCE4 をデフォルトとして設定します: **echo >~/.xsession**
- **/etc/xrdp/startwm.sh** を編集し、セッションのデフォルトのアプリケーションを変更します
- セッション開始時に ウィンドウ・マネージャ(またはアプリケーション)が起動するように設定します。 これを実行する方法は複数ある場合がありますが、目的は「**/etc/**X11/Xsession」を「/usr/bin/xfce4-session」で置き換えることです。

以下は、「xfce4-session」を追加する例です:



```
    if [ -r /etc/X11/Xsession ]; then
  # . /etc/X11/Xsession
  xfce4-session
      exit 0
    fi
```

- 行の先頭に「#」を入力し、デフォルトのウィンドウ・マネージャを無効化します。
- アクティブなウィンドウ・マネージャとして **xfce4-session** を入力します。
- オプション: 起動するブラウザを追加します(例: firefox)
- XRDP を再起動します: **sudo /etc/init.d/xrdp restart**
- mstsc.exe などの RDP クライアント を使用して、XRDP がアクセス可能な状態であることを確認します。



4.14.4 ActiveDirectory サポート(Likewise)を追加する

Likewise を使用して、Ubuntu Linux に Active Directory 対応を構成できます。 この構成により、Linux セッションへのログインに ActiveDirectory の認証された資格情報を使用することで、シングル・サインオン機能を実現できます。

必要なパッケージをインストールする前に、Linux システムがインターネットに接続され、パブリック DNS ネーム・サーバ が構成済みであることを確認します。

まず、必要な likewise パッケージをダウンロードします:

- **sudo wget** http://de.archive.ubuntu.com/ubuntu/pool/main/l/likewise-open/likewise-open_6.1.0.406-0ubuntu5.1_amd64.deb
- **sudo wget** http://de.archive.ubuntu.com/ubuntu/pool/main/libg/libglade2/libglade2-0_2.6.4-2_amd64.deb
- **sudo wget** http://de.archive.ubuntu.com/ubuntu/pool/universe/l/likewise-open/likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb

ダウンロードしたパッケージをインストールします:

- **sudo dpkg -i likewise-open_6.1.0.406-0ubuntu5.1_amd64.deb**
- **sudo dpkg -i libglade2-0_2.6.4-2_amd64.deb**
- **sudo dpkg -i likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb**

Likewise GUI を使用して Linux を Active Directory に追加します (nano エディターが必要です)。

- ターミナル・ウィンドウを開き、次を実行します: **sudo nano /etc/nsswitch.conf**
- 次の行を見つけます **hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4**
- 上記の行を次のように変更します **hosts: files dns [NOTFOUND=return]**

ネットワークを再起動します: **sudo /etc/init.d/networking restart**

ドメインに参加します: **sudo domainjoin-gui (or sudo domainjoin-cli)**

Active Directory ユーザを使用して Ubuntu 14.04 上の GUI ログオンを実行するには:

「/usr/share/lightdm/lightdm.conf.d/」にある 「50-ubuntu.conf」ファイルを編集し、以下の行を追加します:

- allow-guest=false
- greeter-show-manual-login=true

最後に、システムを再起動します。 再起動後、ログオン画面で「ログイン」を選択し、適切な構文を使用して Active Directory ユーザの資格情報を入力します:

- abc.com\domain_user_name

または

- domain_user_name@ericom.local

4.14.5 ActiveDirectory サポート(Pbis)を追加する

- **sudo wget http://download.beyondtrust.com/PBISO/8.0.1/linux.deb.x64/pbis-open-8.0.1.2029.linux.x86_64.deb.sh**
- **sudo chmod +x pbis-open-8.0.1.2029.linux.x86_64.deb.sh**
- **sudo ./pbis-open-8.0.1.2029.linux.x86_64.deb.sh**

ターミナルから以下を設定します:

cd /opt/pbis/bin/
sudo domainjoin-cli join --disable ssh $domainname $domainaccount

例: sudo domainjoin-cli --disable ssh abc.com admin@abc.com

パスワードを要求された場合、適切な資格情報を入力し、完了後に「成功」プロンプトが表示されます。

参考資料: https://community.spiceworks.com/how_to/80336-join-ubuntu-14-04lts-to-a-windows-domain-using-pbis-open

ドメイン・プレフィックスを定義するには、次を使用します:

sudo ./opt/pbis/bin/config UserDomainPrefix <domain-name>

デフォルトのドメインを使用するには、次を使用します:

sudo ./opt/pbis/bin/config AssumeDefaultDomain true

4.14.6 DNS の構成

Linux システムから Active Directory の接続に問題が発生している場合、その Active Directory システムが DNS ネーム・サーバ・リストの最上部にあるかを確認します。

DNS ネーム・サーバを追加するには:

cd /etc/network/interfaces.d に移動します

ネットワーク・アダプタ・ファイルを編集します: **sudo nano eth0.cfg**

dns-nameservers 10.0.1.1 を追加します(実際の DNS アドレスを入力してください)

ネットワークを再起動します: **sudo /etc/init.d/networking restart**

使用されているネーム・サーバを確認します: **cat /etc/resolv.conf**

```
ubuntu@:~$  cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.0.2
nameserver 10.0.2.76
nameserver 8.8.8.8
```

4.15 Linux アプリケーションとデスクトップの展開

Ericom Connect 7.5 以降では、Ubuntu ベースの Linux システムへの接続がサポートされています。 Linux は、デスクトップとアプリケーションを実行するための理想的な低コストのオペレーティング・システムです。
以下の説明は、Linux の基本的な知識を前提としています(例: ファイルの編集など)。 前提条件をインストールするために Linux シェル へアクセスできるよう、 PowerTerm InterConnect などの SSH アプリケーションの知識も必要とされます。

4.15.1 前提条件

- Ubuntu 14.04.3 x64
- Ericom RDX Linux xRDP
- Windows デスクトップ環境 (XFCE4 など)
- QT ライブラリ依存関係パッケージ
- Linux システムの Root(su) アクセス

- AccessPad 7.5.0 以上
- 接続先となる Ericom Connect RemoteAgent Web サービス

前提条件をインストールするには、「4.13 Linux 前提条件の設定」の章に記載されている説明に従ってください。

前提条件の準備完了後、Ericom RemoteAgent for Linux のインストールを開始します。

4.15.2 Ericom RemoteAgent for Linux のインストール

Ericom Connect グリッドが存在し、アクセス可能であることを確認した後、Ericom RemoteAgent for Linux のプロセスを開始してください。 前提条件の準備完了後、Ericom RemoteAgent for Linux のインストールを開始します。

- ターミナル・ウィンドウから su モードに入ります: **sudo su** (Ericom RemoteAgent for Linux をインストールするために、この操作が必要です)
- インストーラはコマンド・ラインから起動する必要があります。デスクトップからファイルをダブルクリックする操作ではインストールすることができません。
- Ericom RemoteAgent for Linux のインストール:

  dpkg –i ericom-connect-remote-host_x64.deb

- これにより、「**/opt/ericom/:**」にフォルダがインストールされます
  - ericom-access-server
  - ericom-connect-remote-agent-client

- インストーラのログ・ファイルは次の場所にあります: /var/log/ericom/install
- ログ・ファイルは次の場所にあります: /var/log/ericom/
- サービスは次の場所にあります: /etc/init.d
- 識別子ファイルは次の場所にあります: ~/.local/share/applications/ericom-connect-remote-agent
- 「service」を使用してアクション・コマンドを実行します。例: **ericom-connect-remote-agent service start**

注意:

- su アクセスなしでインストールを起動した場合、次のエラーが表示されます: 「dpkg: エラー: 要求された操作にはスーパーユーザの権限が必要です」

xrdp が存在しない状態でインストールを起動した場合、次のエラーが表示されます: 「エラー: このインストールを続行するには xrdp パッケージが必要です。(Error: xrdp package is required for this installation to continue.)」

4.15.3 AccessServer for Linux

Ericom AccessServer for Linux は、RemoteAgent と共にインストールされ、インストール後に自動的に起動します。

手動で Ericom AccessServer を起動するには、次を実行します:
sudo service ericom-access-server start
AccessServer を再起動する際、通信の同期を維持するために RemoteAgent も同様に再起動してください。

4.15.4 Ericom RemoteAgent for Linux の実行と構成

Ericom RemoteAgent for Linux を実行するコマンドには、以下の形式を使用します(注意: http ではなく、**https** を使用してください):

sudo service ericom-connect-remote-agent connect -server-url https://<RAWSaddress>:8044 [-host-name RemoteAgentAddress] [-tenant-info TenantInfo]

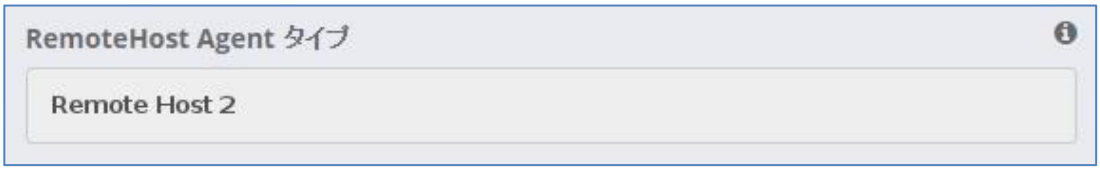
上記の内容について:

- **RAWSaddress** は、RemoteAgent Web サービスを実行しているシステムの IP アドレスです - 通常は Ericom Connect サーバです。
- **RemoteAgentAddress** (省略可能)は、RemoteAgent を実行しているシステムの IP アドレスです。
- **TenantInfo** (省略可能)は、この RemoteAgent の割り当て先とする必要のあるテナントの名前です。

例えば:

sudo service./ericom-connect-remote-agent connect -server-url https://10.0.2.76:8044 -host-name 10.0.2.184 –tenantInfo myTenantId

- ここまでの手順で、Linux RemoteAgent が管理コンソールに登録されます。 Linux RemoteAgent は タイプ *2* の RemoteAgent であり、次から確認できます 「システム | ホスト | 設定」



4.15.5 Linux RemoteAgent アクション・コマンド

Linux RemoteAgent を Ericom Connect から切断するには、次を実行します:

sudo service ericom-connect-remote-agent disconnect

Linux RemoteAgent のバージョンを確認するには、次を実行します:

sudo service ericom-connect-remote-agent version

Linux RemoteAgent のステータスを確認するには、次を実行します:

sudo service ericom-connect-remote-agent status

Linux RemoteAgent を起動するには、次を実行します:

sudo service ericom-connect-remote-agent start

Linux RemoteAgent を停止するには、次を実行します:

sudo service ericom-connect-remote-agent stop

Linux RemoteAgent を再起動するには、次を実行します:

sudo service ericom-connect-remote-agent restart

すべての RDP セッションの一覧表示(セッション・ステータス、ローカル・ユーザ名、セッション ID、プロセス ID、セッション経過時間、セッション切断経過時間)するには、次を実行します:

sudo service ericom-connect-remote-agent list-sessions

システムと AccessServer の情報を確認するには、次を実行します:

sudo service ericom-connect-remote-agent system-info

グリッドから取得された Linux RemoteAgent 設定を確認するには、次を実行します:

sudo service ericom-connect-remote-agent grid-settings

Linux RemoteAgent サービスの使用状況を確認するには、次を実行します:

sudo service ericom-connect-remote-agent

高いログ・レベルで Linux RemoteAgent を実行するには、以下を使用します:

sudo service ericom-connect-remote-agent start -log-debug-level <目的のレベル> | 使用可能なオプション: Debug, Verbose

4.15.6 Linux デスクトップを公開する

Linux リソースは、「デスクトップ」セッションとして公開されます。「公開」に移動し、「デスクトップ追加」を選択します。

Linux デスクトップの公開グループへの関連付けを行った後、目的の Linux システムを含むシステム・グループにその公開グループを割り当てます。

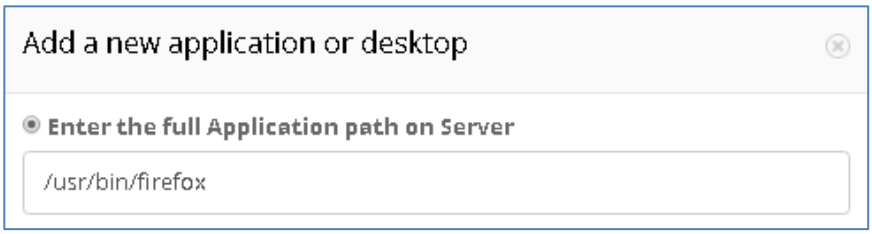
Ericom Connect に Windows と Linux 両方のシステムを使用する場合、エンドユーザの混乱の可能性をさけるために、同じタイプのオペレーティング・システム用にシステム・グループを別に作成することを強くお勧めします。

4.15.7 Linux アプリケーションを公開する

7.6.1 以降では、ネイティブ Linux アプリケーションの公開が利用可能です。 以下の最新のコンポーネントが必要です: Ericom RDX、Ericom Connect、Ericom AccessServer、および AccessPad(すべてのコンポーネントは同一バージョンである必要があります)。

Linux アプリケーションを公開するには、以下を実行します:

- 管理コンソールを使用して、「公開 | リソース | アプリケーションの追加」に移動します。
- アプリケーションの完全なパスを Unix 形式で入力します(例: **/usr/bin/firefox**)



- デフォルトのアイコンが使用されます。 これは、**ConnectCLI SetIcon** コマンドを使用して変更できます。

- ユーザがアプリケーションを起動すると、そのアプリケーションを含むホスト・システムが Ericom Connect によって自動的に選択されます。
- すべてのアクティブ・アプリケーションを終了した場合、ユーザのセッションはログオフされます。

4.15.8 Linux でのセッション共有

後続の Linux アプリケーションを起動すると、既存のアクティブな Linux セッション内にアプリケーションが起動する場合があります。

Linux アプリケーションでのセッション共有を有効化するには、以下を実行します:

- Ericom Connect 管理コンソールで、公開アプリケーションの「要件」タブに移動し、「接続共有を使用」の設定を「はい」に変更し、「保存」ボタンをクリックします。
- セッション共有には、Ericom Linux RemoteAgent が必要です。デフォルトでは、エージェントは opt/ericom/ericom-connect-remote-agent/ericom-remote-session-agent にインストールされています。 Linux アプリケーションを起動すると、プログラムと引数がエンコードされます(base64)。
- Linux でのセッション共有のパフォーマンスを向上するには、「システム | ホスト | 設定(歯車アイコン) | サービスの Keep Alive 間隔 (秒)」を「30」から「3」に変更し、「保存」をクリックします(Windows には適用できません)。

- 「ログオン名のフォーマット」が次のいずれかに設定されていることを確認します: AsLoggedIn、UserPrincipalName、DownLevelLogonName、または OmitDomain

4.15.9 アプリケーションとしての Linux デスクトップ

Linux デスクトップをアプリケーション(設定されたアプリケーションのみを起動し、デスクトップ・マネージャを表示しないデスクトップ)として公開するには、以下を実行します:

- Linux アプリケーションは、本質的には特定のアプリケーション(例: Firefox)を起動する Linux セッションです。 目的のアプリケーションをシステムの次の場所で指定します: **/etc/xrdp/startwm.sh**
- 目的のアプリケーションのみを起動する すべての Linux システムを含んだシステム・グループを作成し、それに応じたグループの名前をつけます。例: 「Linux Firefox システム」
- 「公開」に移動し、「デスクトップ追加」を選択します。

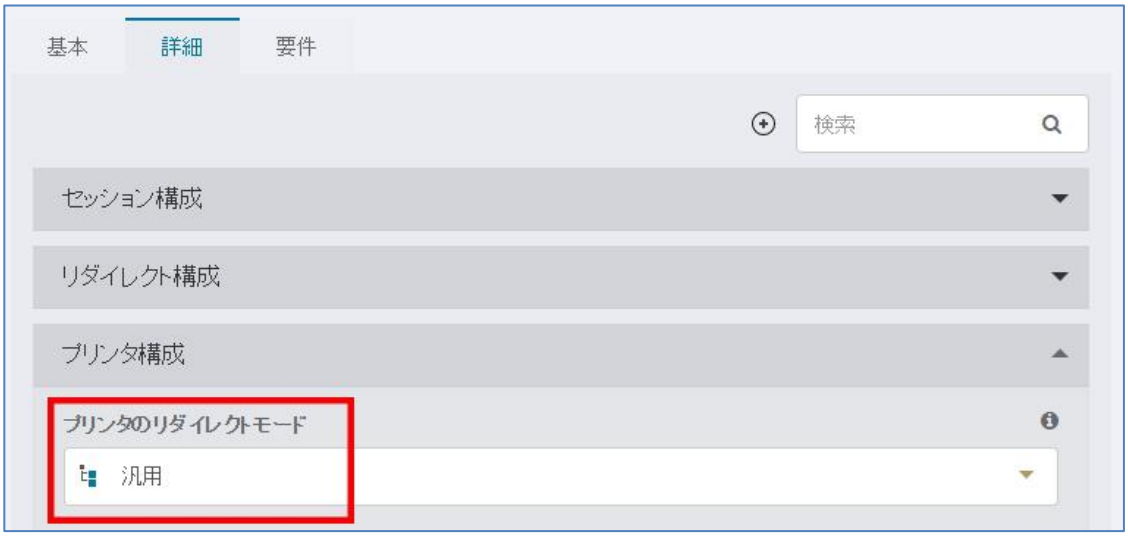
- デスクトップ・リソースの名前をアプリケーション名に変更します。例:「Linux Firefox」- これがエンドユーザに表示されます。
- アイコンを変更したい場合は、次の ConnectCLI コマンドを使用します: **ConnectCLI SetIcon**
- 「Linux Firefox」という名前の公開グループを作成し、アプリケーションをそのグループに割り当てます(「デスクトップ」タブの下にあります)。

  最後に、アプリケーションの公開グループにシステム・グループを関連付けます

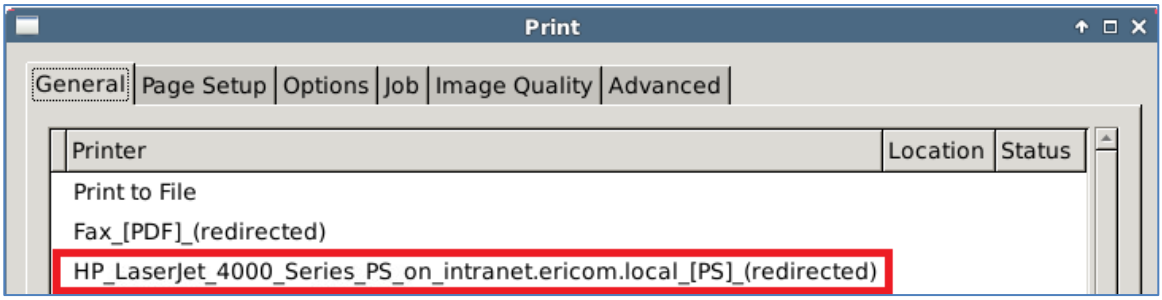
  「Linux Firefox」公開グループに割り当てられたユーザには、クライアント(例: AccessPortal)でこのリソースが表示されます。

4.15.10 Linux セッションでの印刷

Linux セッションでの印刷機能がサポートされています(Ericom RDX の機能の 1 つ)。 印刷を有効化するには、Ericom Connect 管理コンソールを使用して、「汎用」ベースの印刷リダイレクトを有効化します。 これは、「詳細タブ | プリンタのリダイレクトモード」で設定されています。



ユーザがログインすると、ローカル・プリンタが Linux セッションへリダイレクトされます。 PostScript 印刷が利用可能な場合、プリンタ名にラベル 「PS」が表示されます。



PostScript が利用可能でない場合、印刷ジョブをローカル・デバイス

へ送信するために PDF 変換が使用されます。この場合、プリンタ名にラベル「PDF」が表示されます。

4.15.11 Linux セッションでのオーディオ

Linux セッションでのオーディオのリダイレクトがサポートされています(Ericom RDX の機能の 1 つ)。 オーディオを有効化するには、Ericom Connect 管理コンソールを使用して、「詳細タブ | リダイレクト構成 | オーディオのリダイレクト」を有効化します。

4.15.12 Linux RemoteAgent をアンインストールする

サービスを停止します:

- sudo service ericom-connect-remote-agent stop
- sudo service ericom-access-server stop

次に、パッケージをアンインストールします:

sudo dpkg --purge ericom-connect-remote-host

4.15.13 AccessPortal の設定

Linux セッションへの接続には、手動の設定を AccessPortal で行う必要があります。

Ericom Connect エンド・ユーザ・ウェブサービスを実行しているシステム上で、次の場所に移動します:

C:\Program Files\Ericom Software\Ericom Connect Client Web Service\WebServer\AccessNow

「config.js」をテキスト・エディタで開きます。

「encryption: false」に対してのコメント「//」を削除します。

ファイルを保存すると、今後の AccessPortal セッションで Linux リソースへ接続できるようになります。

4.16 Windows RDS でのセキュアなブラウジング

セキュアな Web ブラウジングのソリューションとして Ericom Connect を構成することができます。 セキュアなブラウジングとは、エンドユーザのローカル・デバイスとブラウジング環境を隔離することを意味します。 ブラウジングのアクティビティは、DMZ などのセキュアな場所で稼働するサーバ上で実施されます。 このアーキテクチャには、以下のようなセキュリティ上の利点があります:

- マルウェアやランサムウェアなどの悪意のある攻撃をネットワークの境界で隔離、ブロックし、ローカル・ネットワークへの侵入を防止します

- パスワードや Cookie などのユーザの機密情報はサンドボックス環境へ隔離され、使用後に消去されます

Ericom Connect では、Windows リモート・デスクトプ・サーバ(RDS)と Linux Ubuntu サーバの両方にセキュアなブラウジングを提供できます。機能は、バックエンドのオペレーティング・システムとブラウザにより異なります。

悪意のあるコードが内部ネットワークへ到達することを防ぐため、DMZ または ローカルのネットワークやコンピューティング・リソースから隔離されたテナント上にセッション・ホストを展開することをお勧めします。

4.16.1 Windows RDS サーバの構成

Windows でのセキュアなブラウザの構成には、目的のブラウザの公開およびブラウザ・セッション用のパラメータの指定(例: キオスク・モード)を行います。RDS システムへブラウザをインストールした後、そのブラウザを Ericom Connect で公開します。

4.16.2 Web サイト・アクセス用にブラウザを公開する

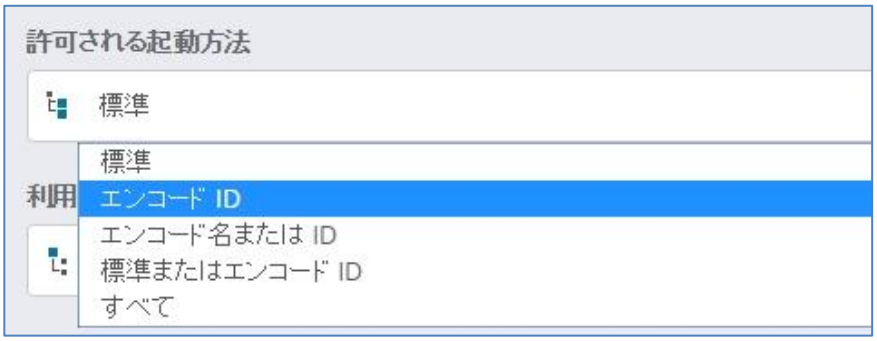
Ericom Connect では、任意の Web ページに埋め込み可能な URL を使用して、ブラウザ・セッションを起動するための革新的な方法が提供されています。ユーザが URL をクリックすると、AccessPad と公開済みのブラウザが起動し、構成済みの Web サイトが自動的に開きます。これは、セキュアなブラウザ環境(例: DMZ でブラウザを実行

する RDS サーバ)で隔離する必要のあるインターネット・リンクを公開する際に特に便利です。

セキュアなブラウジングのために特別に使用する Web ブラウザを公開する方法は以下のとおりです:

- (LNK ファイルではなく)完全なパスを使用してブラウザを公開します
- **${param1}** を使用して、パラメータの使用を指定します
- 公開済みのブラウザは一般的な目的で使用するものではない(URI から渡すパラメータを必要とする)ため、アイコンをエンドユーザに対し非表示にします。

- 「要件」タブに移動し、「許可される起動方法」がアプリケーションの参照方法と一致していることを確認します。方法は、「リソース名」または「エンコード ID」を使用します。 例えば、ConnectCLI コマンドまたは Javascript を使用して生成したエンコード済みの値には、「エンコード ID」を許可する必要があります。



4.16.3 EricomLaunch.js ファイルの構成

URI を使用する場所に EricomLaunch.js ファイルを配置します。公開済みのブラウザ、そのブラウザがメンバーとなっているグループおよび URI に、名前または一意の ID を設定します。

// 起動するアプリケーションの名前または ID

var app = "**Secure Browser**";

// アプリケーションの含まれるグループの名前または ID 空白文字列を使用可能です。

// その場合、ユーザにとっての一意の存在がサーバにより検索されます。

var group = "**DMZ**";

// これはデフォルトで使用される URI です。 異なる URI を使用する場合、この行を変更してください。

var uri = "**estp**";

4.16.4 Web ページへの URI の追加

ID への参照を Web ページに追加します。 例:

<A id="ERICOM" href="http://www.ericom.com<>">http://www.ericom.com</A>

比較として、ローカルで起動される標準的な URL は次のとおりです:

Ericom

ConnectCLI GenerateEncodedUri コマンドにより生成される静的なエンコード済み URL は、「id=ERICOM」タグを使用せずに入力することもできます。例:

**<A href="estp://accesspad/v1/NDg4NTMwYTUtZDI0Zi00ZGMyLWE1OTEtNTM3YTc0ZTQ1ZTgyJCEkKjYwN2FlYmQxLTRkNzktNDE1MS04NzM1LWYwYWRlMDU5NWE5MyQhJCo=">Secure webpage</A>
**

4.16.5 AccessPad URI の使用方法のサンプル HTML:

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Ericom Sample URI Launch Page</title>
</head>
<body>
<h2>Dynamic entry of website URL into secure browser defined in EricomLaunch.js</h2>
<A id="ERICOM" href="http://www.ericom.com/connect-enterprise.asp">http://www.ericom.com/connect-enterprise.asp</A> <br>
<!-- 下記により、id="ERICOM" を持つ要素のすべての href が置換されます -->
<script type="text/javascript" src="./jquery-2.2.3.min.js"></script>
<script type="text/javascript" src="./EricomLaunch.js"></script>
<h2>Static URL to launch AccessPad with website already encoded</h2>
```

<A
href="estp://accesspad/v1/ZGU3MzdmMzMtNjQwMi00YmNlLWFkMGEtYzBkYTk3MzFjZDdjJCEkKjc4NDE3Y2NhLWMwYWQtNDE2Yi04ZjEzLTM4MzllMDQxZmViZCQhJCo=">ESTP Encoded URL to pre-configure website/A>

</body>
</html>

4.17 Linux Ubuntu でのセキュアなブラウジング

オペレーティング・システムとして Linux を使用するには、まず Ericom Connect に Linux Ubuntu 14.04 サーバを展開する手順に従います。 Linux システムを実行後、Web ブラウザをインストールします(例: Chrome をインストールするには、sudo apt-get-install chromium-browser を実行します)。

ブラウザのインストール後、『Linux アプリケーションを公開する』の説明に従ってそれを公開します。ブラウザは、パラメータ付きで公開できます。例えば、キオスク・モードで最大化された状態で起動し、URL www.ericom.com を開くには、以下のように設定します:

chromium-browser --start-maximized --kiosk "http://www.ericom.com"

キオスク・モードでは、タブやアドレスバー、設定ボタンなどの一部のブラウザ要素が非表示となることに注意してください。ブラウザの「終了」ボタンが利用できなくなるため、セッションの切断時にオペレーティング・システムによりユーザが自動的にログオフされるようにしてください。

4.18 ロード・バランサ Ping ポイント

Ericom Connect では、ping ベースの健全性モニタリングを使用したロード・バランサがサポートされています。ロード・バランサを以下のいずれか 1 つのポートに誘導します:

- EUWS HTTPS:
  https://サーバアドレス:8011/ericomxml/ping
- EUWS HTTP:
  https://サーバアドレス:8033/ericomxml/ping
- ESG
  https://ESG サーバアドレス:443/ping

4.19 ESG 経由での管理者ページの公開

```
ConnectCLI EsgConfig common
ExternalWebServer$UrlServicePointsFilter="<UrlServicePointsFilter>
<UrlFilter> <UrlPathRegExp>^/Admin</UrlPathRegExp>
<UrlServicePoints>https://<local-admin-
address>:8022/</UrlServicePoints> </UrlFilter> </UrlServicePointsFilter>"
```

4.20 Qualys のグレードを A に向上する

Qualys (https://www.ssllabs.com/) は、リモート・アクセスページのセキュリティを評価するためのオンライン・ツールを提供しています。 以下は、 **Windows 2012 R2** サーバ上の Ericom Connect ESG をセキュリティ保護し、高いグレードを達成するための手順です:

- 証明機関から信頼された証明書を使用します

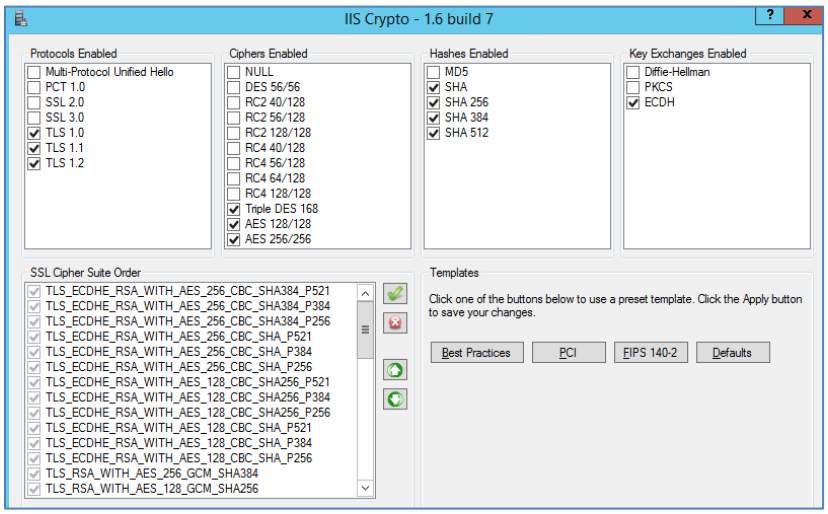
- MITM の脆弱性を除くために、サーバ上での非セキュアな再ネゴシエーションを無効にします(http://support2.microsoft.com/kb/980436/en-us)。 これには、レジストリ設定で次を実行します: 以下のレジストリ・キーを作成し、両方を 「0」(ゼロ)に設定します。

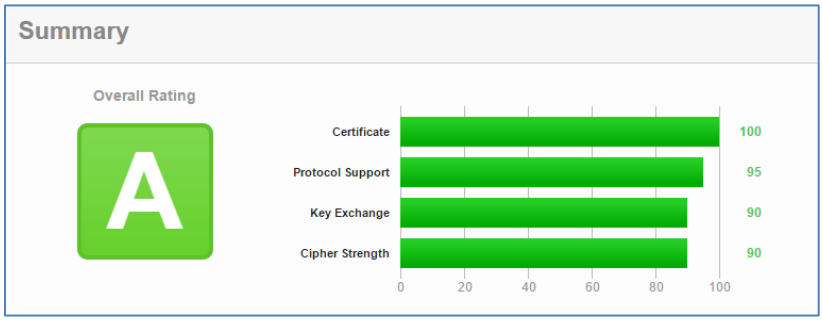
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\AllowInsecureRenegoClients
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\AllowInsecureRenegoServers

- 以下のレジストリ・キーを「0」(ゼロ:無効化)に設定することで、Ericom Secure Gatwway(ESG) サーバ上の RC4 を無効にします。「この設定を展開したサーバでは、RC4 の使用が必要とされているクライアントにサービスを提供できなくなる」ということに注意してください。

  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128] | "Enabled"=dword:00000000
  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128] | "Enabled"=dword:00000000
  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128] | "Enabled"=dword:00000000
  - ESG 上で上記の設定を行った後、ESG アドレスの Qualys のグレード は「A」の範囲に入ります。

- 「A」グレードを達成できるよう ESG を設定するための無料ツール(IIS Crypto)が利用可能です。以下は、「A」グレードと評価される構成(Windows 2012 R2 サーバ上)の例です。スクリーンショットは 2015 年 10 月 5 日に作成されたものです:





注:Windows 2008 R2 サーバでは、この手順では「B」グレードと評価されます。

4.21 ワークステーションでのセッション・フォロー

Ericom Connect 7.3 より、ユーザがワークステーションへの接続を既存のセッション(例: ロックされた状態)で試みた場合、ユーザは自動的にそ

のワークステーションに再接続されます。 他のユーザがそのワークステーションにログオンした場合、オペレーティング・システムの警告メッセージが表示されます(ここではオペレーティング・システムの標準ルールが適用されます)。 ルール「ワークステーションの OS で条件を無視」はデフォルトで「はい」に設定されているため、ワークステーション・ベースの接続にはバインド条件が無視されます。

Ericom Connect 7.2 とそれ以前のバージョンでは、「マイデスクトップ」ワークステーション(LDAP)属性が設定されている場合のみ、ユーザは既存セッションに再接続することができました。(「マイデスクトップ」を使用しない場合、1 台のワークステーション上で許可されるのは 1 つのセッションでした)

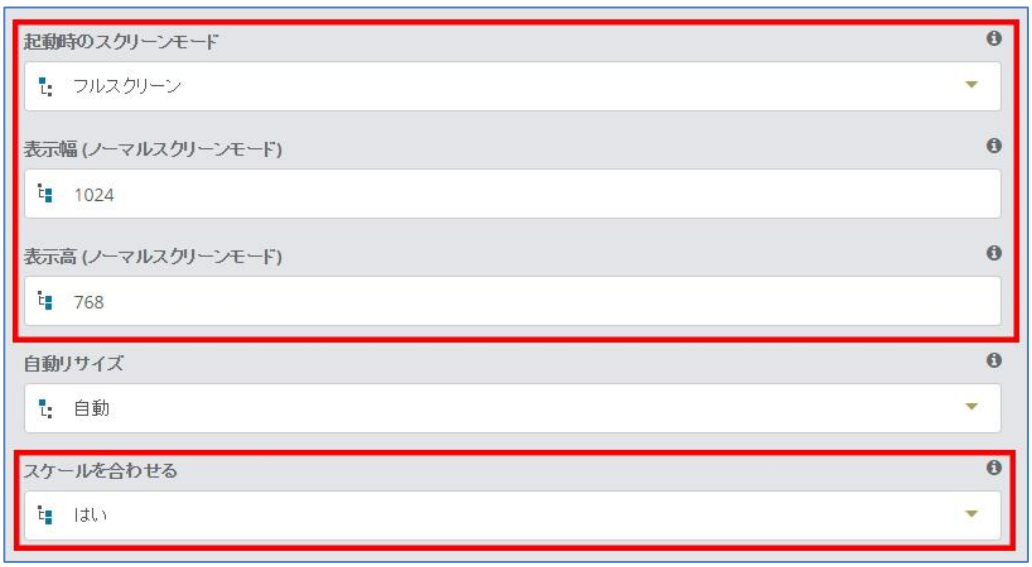
4.22 セッション・ホスト機能を構成する

4.22.1 AccessNow 用の Scale-to-Fit 機能を使用する

一部のアプリケーションでは、固定の解像度が要求され、その解像度がエンドユーザのブラウザや Chromebook で利用可能な解像度を超える場合があります。Ericom Connect には、Scale-toFit 機能(スケールを合わせる)が含まれ、AccessNow セッションを実行しているブラウザで利用可能な表示域にフィットするようアプリケーションの自動的な拡大縮小を行うことが可能です。

Scale-to-Fit を設定するには、「起動時のスクリーンモード」を「フルスクリーン」に設定します。「表示幅」と「表示高」に必要な解像

度を設定します。「スケールを合わせる」で「はい」をクリックして有効にします。



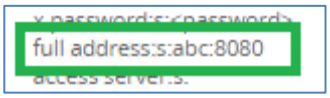
アクティブ・セッション中、ブラウザをリサイズすると、新しいサイズにフィットするようアプリケーションの拡大縮小が行われます。

4.22.2 構成済みのカスタム・ホスト名を使用する

Ericom Connect では、ユーザ接続用のリモート・ホストを識別する際に、リモート・ホストの「完全修飾ドメイン名」が使用されます。一部のネットワークでは、「ホスト名」または「IP アドレス」のみが要求されます。 ネットワーク内で接続先のアドレスが渡される方法(例:ESG の接続先となるホスト・アドレスの決定) を設定するには、「システム」|「登録済み」に移動し、「共通」(歯車) アイコンと「設定」タブをクリックします。 アドレス値が渡される方法の定義には、次の 2 つのオプションがあります:

- 「 RemoteHost 接続に使用するアドレス」から目的の値を選択する
- 「カスタムアドレス(オプションポート)」に値を入力する - この値は最も高い優先順位が与えられ、「RemoteHost 接続に使用するアドレス」の値はこの値により上書きされます。

設定を行ったシステムに対して起動分析を実行し、正しい値が使用されているか確認してください。



4.22.3 TsAgent による切断したセッションのログオフ

以下の設定は、デスクトップとシームレス・アプリケーション・モードに関連するものです。

- 「切断されたセッションをログオフ」 (デフォルト:「いいえ」)
- 「ログオフ遅延(秒)」 (デフォルト:3 秒)

4.22.4 「ログオフ」遅延秒数を使用する

リモート・デスクトップ・セッションを明示的にログオフするには、リモート・デスクトップの「スタート メニュー」の「サインアウト」機能を使用します。この機能が選択されると、セッションは直ちにログオフされます。

特定のアプリケーションのみが実行されるセッションであるリモート・シームレス・アプリケーション・セッションでは、この方法でログオフすることができません。代わりに、これらのセッションでは、

表示されるウィンドウがなくなった時に自動的にログオフされます。例えば、すべてのアプリケーションを閉じた時です。

読み込み中など、一部のケースでは、通常操作中の短い時間にアプリケーションから何も表示されない場合があります。このようなセッションが途中でログオフされるのを防ぐため、自動ログオフを遅延させます。この遅延中に新しいウィンドウが作成されるか既存のウィンドウが表示された場合、ログオフはキャンセルされ、セッションはアクティブな状態で保たれます。

デフォルトの遅延時間は、構成により異なります:

- マイクロソフト シームレス (デフォルトのモード) を使用する AccessPad では 30 秒です。
- Ericom True Seamless を使用する AccessPad では 300 秒です。
- AccessNow と AccessToGo では 3 秒です。

セッションの作成から 30 秒間は、そのセッションは終了されません。

上記の 300/30/3 秒の遅延時間は、Ericom Connect「ログオフ遅延 (秒)」(「詳細」タブの下)を使用して調整できます。この設定で指定した値は、すべての種類のクライアントに使用されます。セッション作成からの 30 秒間の遅延は変更できないことに注意してください。

AccessPad で長い遅延が使用されているのは、クライアントにより追加アプリケーション用に既存セッションの再利用が可能なためです。このことは、ログオフの遅延の間に新しいアプリケーションが起動された場合、そのアプリケーション用に新しいセッションを作成するの

ではなく、既存のセッションを再利用できることを意味します。AccessNow と AccessToGo では、セッション共有は使用できません。

4.22.5 TsAgent によるログオフ

以下のシナリオでは、TsAgent によりセッションのログオフが実行されます。

- デスクトップまたはシームレス・モードを使用中に、セッションが切断され、かつ 「切断されたセッションをログオフ(Logoff Disconnected Sessions) 」が「はい(Yes)」の場合。 次のケースでは、「ログオフ遅延(秒)(Logoff Delay(sec))」が無視されることに注意してください。
- Microsoft シームレス・モードを使用中に、セッションが切断され、かつアクティブ・ウィンドウが存在しない場合。
- Ericom シームレス・モードを使用中に、セッションが切断され、かつ 「ログオフ遅延(秒)(Logoff Delay(sec))」タイマーが期限切れとなった場合。 「ログオフ遅延(秒)(Logoff Delay(sec))」タイマーは、最後のウィンドウが閉じられた時に開始されます。

4.22.6 TSagent VBS のスクリプト

PowerTerm TSagent では、特定の RDP セッションのイベント間に .vbs スクリプトを実行する機能がサポートされています。 この機能により、アプリケーションが起動時やセッションの接続または接続解除時に特定のコマンドを実行する機能のレイヤーを追加することが可能です。

すべてのセッションの Startup 後のログイン・スクリプト (_login)

_login.vbs という名前のファイルを作成し、TSagent がインストールされている *scripts* 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 セッションが *Startup* フォルダを処理した後に実行されます。

すべてのセッションの Startup 前のログイン・スクリプト(__login)

__login.vbs という名前のファイルを作成し、TSagent がインストールされている *scripts* 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 セッションが Startup フォルダを処理する前に実行されます。

既存セッションへの接続時スクリプト(_connect)

_connect.vbs という名前のファイルを作成し、TSagent がインストールされている *scripts* 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。

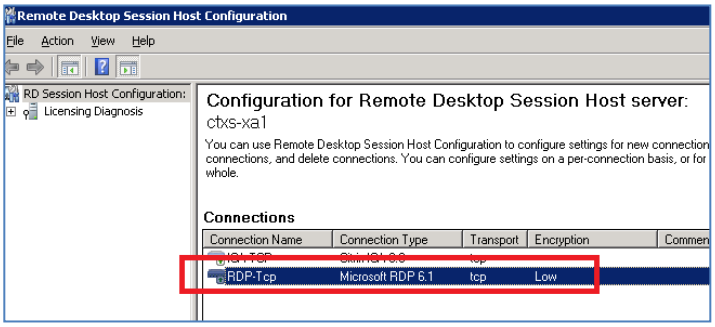
セッション切断時スクリプト (_disconnect)

_disconnect.vbs という名前のファイルを作成し、TSagent がインストールされている *scripts* 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 セッションの接続解除時に実行されます。

4.22.7 XenApp サーバからの公開

既存の Citrix XenApp サーバを、Ericom ターミナル・サーバ・ファーム(ターミナル・ サーバまたは RDS サーバ)として使用できます。RDP 着信接続を許可するために、2 つの設定変更を XenApp サーバに追加する必要があります。 以下の情報は Citrix の Web サイトから改変したものであり、違うバージョンの Citrix Presentation Server または XenApp では、情報が異なる場合があります。 Web サイトのリンク:http://support.citrix.com/article/CTX124745

4.22.7.1 XenApp サーバで RDP を有効にします(例: Windows Server 2008 R2)

- 「リモート デスクトップ セッション ホストの構成」を開きます
- 「新規接続の作成」を選択します
- 「接続プロコトル」に RDP を選択します。
- 

- 「次へ」をクリックし、設定を完了します。 追加の RDP 設定を実行するには、プロコトルの「プロパティ」に移動します。

4.22.7.2 アプリケーションとデスクトップ・アクセスの許可

Citrix XenApp サーバでは、ユーザが RDP 経由で直接アプリケーションを起動できなくなります。 この制約は、ターミナル・サーバとして使用する Citrix XenApp(6.0)で以下の手順を実行することにより、取り除くことができます。

Changing the Default Unfiltered User Policy Settings for ICA in the DSC

To change the default unfiltered User policy settings for ICA in the DSC, complete the following procedure:

1. Select **Policies**.
2. Activate the **User** tab (you notice the default unfiltered policy).
3. To access the default policy settings, activate the **Settings** tab in the lower pane.
4. Click **ICA** on the Categories window.

Allowing Non-administrative Users to Connect to the Server Desktop

To allow non-administrative users to connect to the server desktop, complete the following procedure:

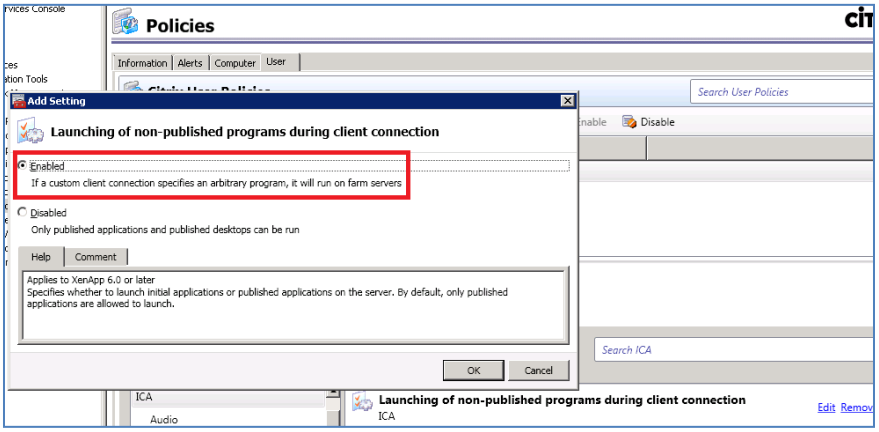
1. Click the **Add** link for starting the Desktop.
2. Select **Allowed**.
3. Click **OK**.

Allowing Non-administrative Users to Start Any Application during Client Connection

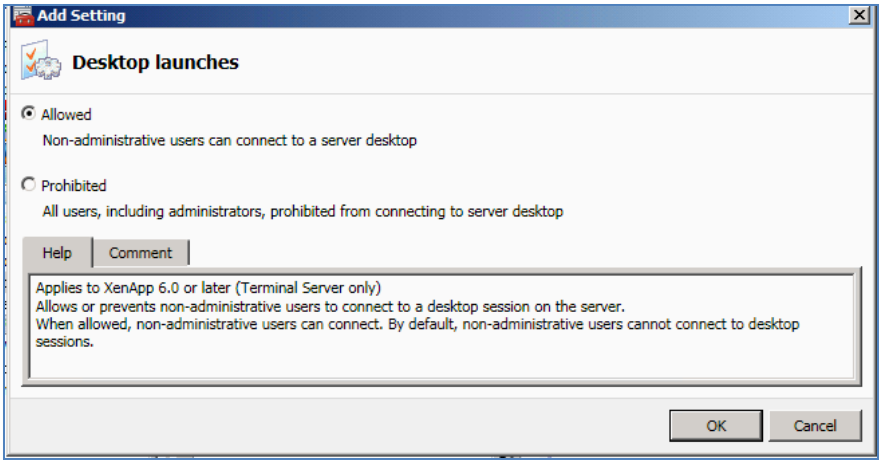
To allow non-administrative users to start any application during client connection, complete the following procedure:

1. Click the **Add** link for starting the non-published programs during client connection.
2. Select **Enabled**.
3. Click **OK**.

「Launching of non-published programs during client connection」ルールを「Enable」にします。



「Desktop launches」ルールを「Allowed」にします。



4.22.8 RDSH 上の App-V クライアントの公開

対象の OSD ファイルをパラメータとして sftrun.exe を公開することで、Microsoft App-V パッケージを Ericom Connect で公開することができます。

例

.OSD ファイルの SOFTPKG NAME と VERSION。NAME と VERSION は大文字と小文字が区別されます:

- PATH\sftrun.exe **"Default App-V Application 1.0" [%*]**

ローカル・ドライブまたは.OSD ファイルへマップされたドライブ:

- PATH\sftrun.exe "**C:\App-V\DefaultApp.osd" [%*]**

.OSD ファイルの汎用命名規則 (UNC)パス:

- PATH\sftrun.exe **"\\SERVER NAME\SHARE NAME\DefaultApp.osd" [%*]**

.OSD ファイルの HTTP パス:

- PATH\sftrun.exe **"http://SERVER NAME/SHARE NAME/DefaultApp.osd" [%*]**

4.22.9 セッション共有

ターミナル・サーバのリソース使用を効率化するために、複数のシームレス・アプリケーションで同一の RDP セッションを共有できます。セッションを共有すると、複数のシームレス・アプリケーションを実行するために複数回サインインする必要がなくなります。 サインイン・プロセスは、最も多くリソースを消費するターミナルサービスの操作の 1 つです。「セッション共有」はデフォルトで有効化されているため、このプロセスは可能な限り削減されます。

「セッション共有」が有効な場合、最初に起動したアプリケーションのプロパティ(色深度など)が使用されます。 後続のアプリケーションには、独自の設定に関わらず、最初のアプリケーションのプロパティが使用されます。 リソースのセッションが常に設定通り起動されるようにするには、「セッション共有」を無効にします。

Ericom Connect 管理コンソールでは、セッション内のすべてのプロセスが同一のステータスを持ちます。 セッションのプロセスが終了する際、Ericom Connect には認識されません。

セッション共有の使用を改善するには:

- すべてのターミナル・サーバに同じアプリケーションをインストールする必要があります。これにより、既にアクティブなターミナル・サーバに、追加で起動するアプリケーションが存在している状態になります。

- ターミナル・サーバへのサインインには、同一の形式で指定された同一の資格情報(ユーザ名とドメイン)を使用する必要があります。Ericom Connect 資格情報を使用するよう設定した公開アプリケーションでは、これは自動的に行われます。

5 エコシステムガイド

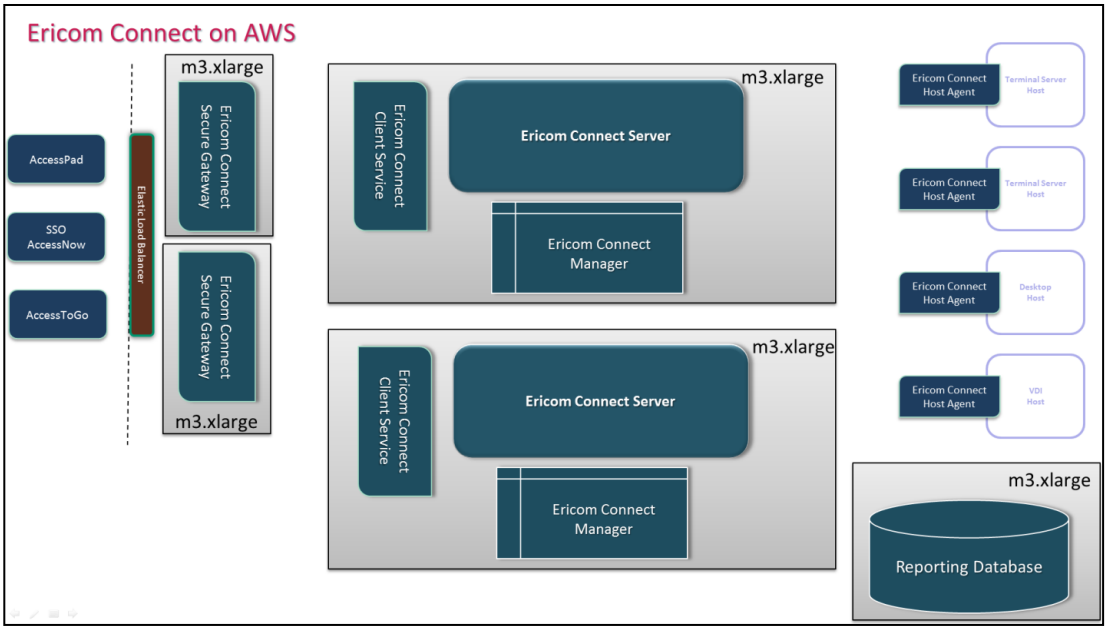
5.1 Amazon AWS での展開

5.1.1 概要

セッション・ホスト・ベースのアプリケーションとデスクトップ・セッションを管理するために、Ericom Connect を Amazon AWS EC2 上に展開可能です。 Ericom Connect のクラウドでの使用には、以下のような利点があります:

- 設備投資から定量課金型の変動費への移行
- インフラストラクチャの弾力性 - 必要に応じて拡張
- 迅速なグローバル展開 - 高速にスケール
- まだまだ沢山あります。

次の図では、Amazon AWS 上 の Ericom Connect 7 のリファレンス・アーキテクチャが示されています。



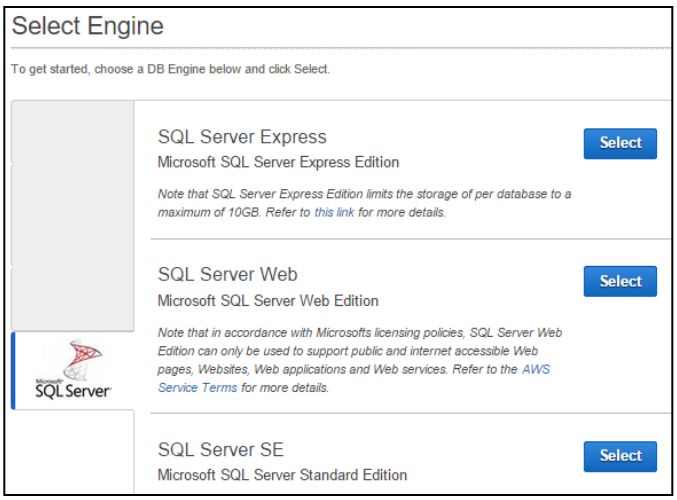
要件

Ericom Connect サーバ用に、AWS EC2 **m3.xlarge** インスタンスをお勧めします。

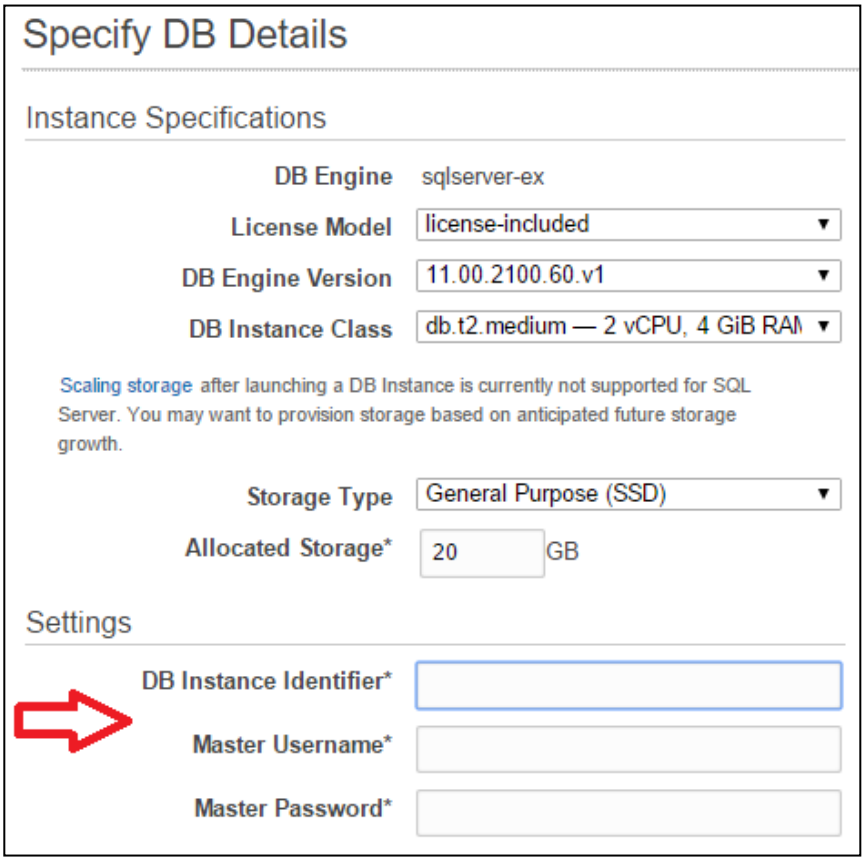
SQL サーバを同一マシンにホストする場合、100 GB のストレージを確保することをお勧めします。

5.1.2 AWS RDS SQL データベースを使用する

Ericom Connect は、AWS でホストされている MS SQL 互換データベースと互換性があります。 新しい RDS データベースを追加する場合、互換 SQL エンジンから選択します:



データベース・エンジンのパラメータを設定します。 識別子、ユーザ名、パスワードを定義します。 この情報はグリッド設定のために必要になりますので注意してください。



「Pubkicly Available」エンドポイントを使用している場合、セキュリティ・グループを介して SQL ポート(1433) が利用可能であることを確認してください。

Security Groups	default (active)
Publicly Accessible	Yes

セキュリティ・グループで、SQL ポートの着信ルールを定義します。

Edit inbound rules

Type	Protocol	Port Range
MS SQL	TCP	1433

SQL インスタンスへの DNS アドレスはデフォルトで提供されていることに注意してください(例: connecttestdb.cozfmi2xxroy.us-east-1.rds.amazonaws.com:1433) データベース・インスタンスへの IP を、Ericom Connect グリッド設定にも使用できます(IP アドレスを取得するには、DNS アドレスに ping します)。

5.1.3 AWS RDS Microsoft SQL を使用する

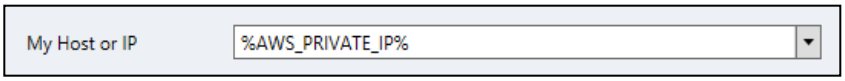
Ericom Connect では、AWS RDS MSSQL がサポートされています。AWS SQL を使用するよう Ericom Connect を設定するには、Ericom Conenct の設定で「Admin User(管理者ユーザ)」と「Server User(サーバユーザ)」の両方に SQL 管理者アカウントを使用します。

接続が完了すると、Ericom Connect により SQL データベース・サーバ内に新しいデータベースが作成されます。

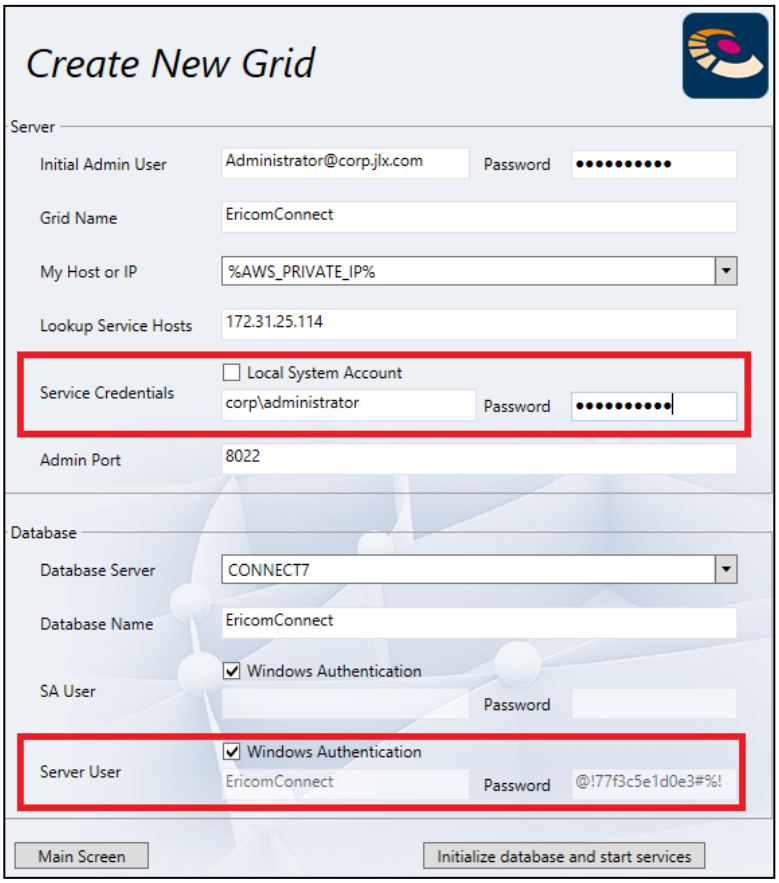
注意: MS SQL の着信ポート(1433)が Ericom Connect サーバに対し利用可能となっていることを確認してください。 この設定を、関連する AWS セキュリティ・グループで行います。

5.1.4 Business Logic マシンのインストール

EC2 インスタンスに Ericom Connect をインストールします。 最初のサーバのインストール中に「**New Grid**」を選択します。 Host IP が AWS PI であることを確認します。



SQL へのアクセス権を持つサービス・アカウントを使用して、「Server Service Credentials」を定義します。



すべての追加のグリッド・マシンでは、「**Join existing grid**」を選択し、最初のマシンのインストールで使用したグリッド名を指定します。 「Lookup Service Hosts」を入力します(通常は最初の Business

Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します)。

このサービス向けの将来のマシン作成のために、2 台目のマシンを使用し、そのマシンが既存のグリッドに参加するよう構成できます。

5.1.5 RDS ターミナル・サーバの設定

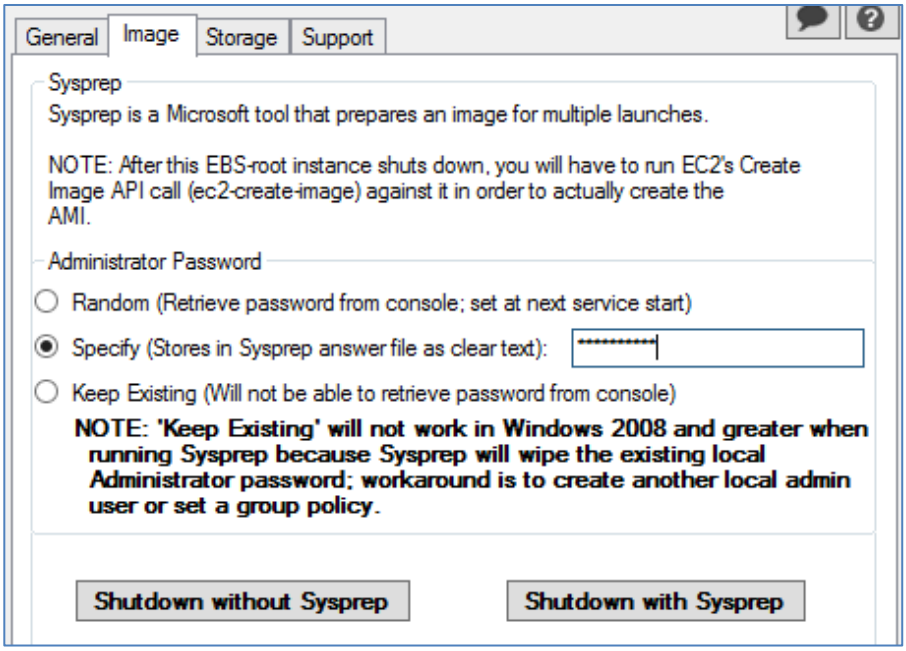
以下のセクションに記載されている手順に従ってください:

RemoteAgent を使用してサーバを複製する

Windows の Sysprep コマンドは使用しないでください。

EC2ConfigService 設定の使用

このツールを使用して、Sysprep パラメータと管理者パスワードを設定します。 「Shudown with Sysprep」をクリックし、Sysprep の操作を開始します。



詳細については、こちらの AWS Web サイトを参照してください:

http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ami-create-standard.html#sysprep-gui-procedure

上記の Web サイトの手順では、新しいインスタンスのドメインへの追加は行われません。 AWS XML 応答ファイルでこれを実行する方法があります(例:UnattendedJoin)。

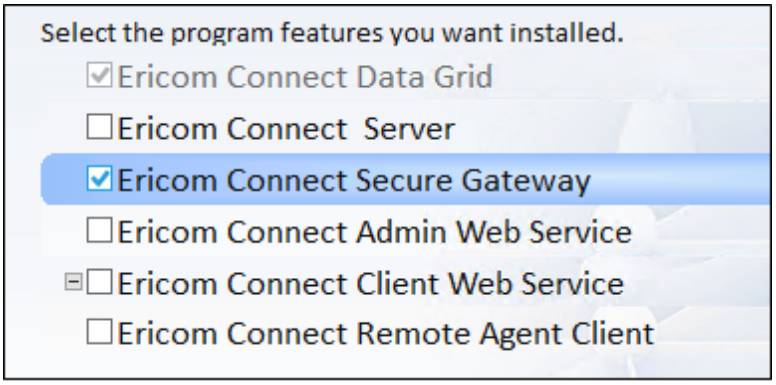
システムのシャットダウン後、今後の展開のための AMI の作成にそれが使用されます。

5.1.6 Ericom Secure Gateway のインストール

Ericom Secure Gateway(ESG) 専用のインスタンスを作成します。

Connect をインストールし、「Custom」を選択します。

「Ericom Connect Secure Gateway」を選択します:



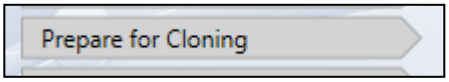
インストールの完了後、Configuration Tool で次を選択します:

Join existing grid(既存グリッドへの参加)

グリッド名と「Lookup Service Hosts」を設定します(通常は最初の Business Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します。

- Elastic Load Balancer を複数の ESG の負荷分散に使用する場合、そのロード・バランサと一致する署名された証明書 をインストールします。
- Connect で ESG 名を設定します(ConnectCLI SystemConfig EsgHostAddress=%ELB_NAME%:443)
- ポート 443 以外を使用する場合、ポートを設定します (ConnectCLI EsgConfig common Network$SecuredPort=%EC_ESG_PORT%)
- 証明書を設定します(ConnectCLI ConfigureCertificates FindByThumbPrint xyz)

マシンのイメージ化の準備が完了したら、構成ツールを実行し、「Prepare for Cloning(複製の準備)」を選択します。



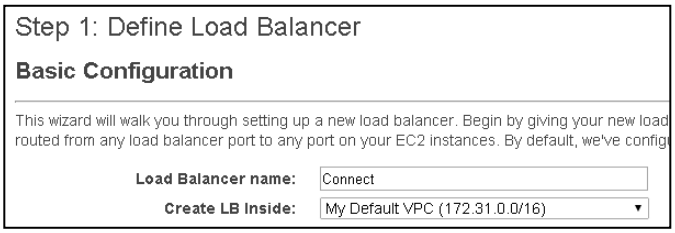
システムの Sysprep を実行すると、自動的にシャットダウンされます。

このシステムは、今後の ESG 展開用の AMI の作成に使用できます。

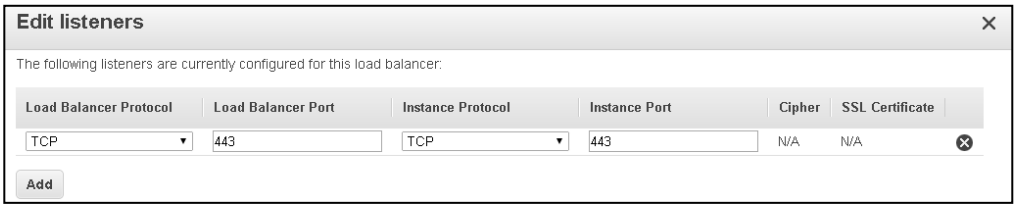
5.1.7 ELB と DNS の設定

ESG 間の負荷分散を行うための ELB を作成するには、EC2 Admin Console を使用します。

- Load Balancers -> Create Load Balancer に移動します
- ELB の名前を入力します:



- Configure Health Check に移動します
- Ping protocol: 「HTTPS」を選択し、Port「443」を指定します
- Path:「/ping」を指定します
- Security Group を割り当てます
- グループを作成します: TCP 443
- リスナーを追加します



- インスタンスを追加します
- ESG マシンを指すように ELB を設定します

5.1.8 Ericom Connect AMI の準備

Amazon Machine Images(AMI) を使用して、他のイメージの生成元となるベース・マシンの準備を行います。 Ericom Connect AMI には以下が含まれている必要があります:

- 最新の Windows Update
- インストール済みの署名された証明書

AMI を使用して、ESG とセッション・ホストを展開できます。 この時点では、Business Logic サーバの展開に AMI を使用しないでください。 AMI は、イベントの自動スケールにも使用できます。

5.2 Microsoft Azure Cloud での展開

5.2.1 概要

セッション・ホスト・ベースのアプリケーションとデスクトップ・セッションを管理するために、Microsoft Azure Cloud(サービス・マネージャまたはリソース・マネージャ)上に Ericom Connect を展開でき

ます。 このドキュメントは、(クラシック)サービス・マネージャに基づいています。Ericom Connect のクラウドでの使用には、以下のような利点があります:

- 設備投資から定量課金型の変動費への移行
- インフラストラクチャの弾力性 - 必要に応じて拡張
- 迅速なグローバル展開 - 高速にスケール
- 他にも沢山の利点があります。

5.2.2 要件

Ericom Connect サーバには、Azure A3 インスタンス(4 コア、7GB)の使用をお勧めします。

Windows オペレーティング・システム上に SQL が必要です。 バージョン 7.3 以降では、Azure Cloud SQL がサポートされています。

SQL サーバを同一マシンにホストする場合、100 GB のストレージを確保することをお勧めします。

5.2.3 Business Logic マシンのインストール

VM インスタンスに Ericom Connect をインストールします。 最初のサーバのインストール中に「New Grid」を選択します。 ホスト IP が正しいアドレスであることを確認します。

SQL へのアクセス権を持つサービス・アカウントを使用して、「Server Service Credentials」を定義します。

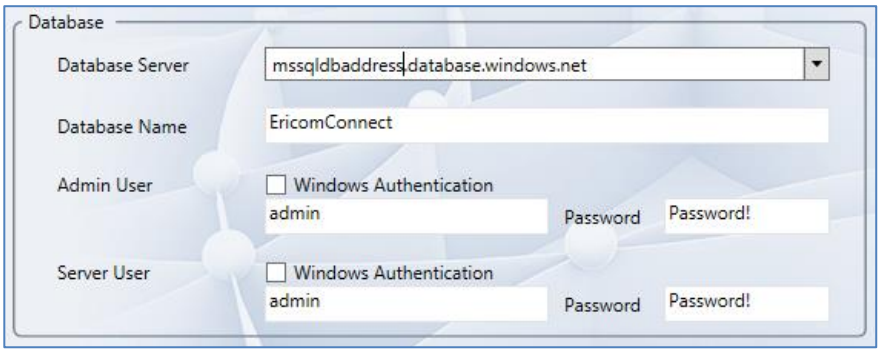
すべての追加のグリッド・マシンでは、「Join existing grid」を選択し、最初のマシンのインストールで使用したグリッド名を指定します。

「Lookup Service Hosts」を入力します(通常は最初の Business Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します)。

このサービス向けの将来のマシン作成のために、2 台目のマシンを使用し、そのマシンが既存のグリッドに参加するよう構成できます。

5.2.4 Microsoft Azure SQL の使用

Ericom Connect では、Azure Cloud での Microsoft SQL がサポートされています。 Azure SQL を使用するよう Ericom Connect を設定するには、Ericom Conenct の設定で「Admin User(管理者ユーザ)」と「Server User(サーバユーザ)」の両方に SQL 管理者アカウントを使用します。



接続が完了すると、Ericom Connect により Azure データベース・サーバ内に新しいデータベースが作成されます。

注意: MS SQL の着信ポート(1433)が Ericom Connect サーバに対し利用可能となっていることを確認してください。 関連するエンドポイントの設定でこれを設定します。

5.2.5 RDS ターミナル・サーバの設定

Ericom Connect インストーラまたは RemoteAgent インストーラのいずれかを使用して、RemoteAgent をインストールします。 どちらのインストーラにも、「複製の準備」のためのオプションがあります。各セッション・ホストには、RemoteAgent のみをインストールします:

☑Ericom Connect Remote Agent Service

グリッド名と「Lookup Service Hosts」(通常は最初の Business Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します)を入力し、RemoteAgent をグリッドに接続します。

今後の展開用に VM のイメージを作成するには、以下のセクションに含まれる手順に従ってください: **RemoteAgent を使用してサーバを複製する**

Windows の Sysprep コマンドは使用しないでください。 Sysprep で使用するためにイメージをキャプチャする方法については、次のリンクに記載されている手順に従ってください:

https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-capture-image-windows-server/

5.2.6 Ericom Secure Gateway

Ericom Secure Gateway(ESG) 専用のインスタンスを作成します。Connect をインストールし、「Custom」を選択します。

「Ericom Connect Secure Gateway」を選択します:

☑Ericom Connect Secure Gateway

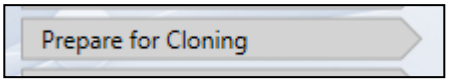
インストールの完了後、Configuration Tool で次を選択します:

Join existing grid (既存グリッドへの参加)

グリッド名と「Lookup Service Hosts」を設定します(通常は最初の Business Logic サーバが Lookup Service Hosts であるため、そのアドレスを使用します。

- Elastic Load Balancer を複数の ESG の負荷分散に使用する場合、そのロード・バランサと一致する署名された証明書 をインストールします。
- Connect で ESG 名を設定します(ConnectCLI SystemConfig EsgHostAddress=%ELB_NAME%:443)
- ポート 443 以外を使用する場合、ポートを設定します (ConnectCLI EsgConfig common Network$SecuredPort=%EC_ESG_PORT%)
- 証明書を設定します(ConnectCLI ConfigureCertificates FindByThumbPrint xyz)

マシンのイメージ化の準備が完了したら、Configuration tool(構成ツール)を実行し、「Prepare for Cloning (複製の準備)」を選択します。



システムの Sysprep を実行すると、自動的にシャットダウンされます。

このマシンは、今後の ESG 展開用の AMI の作成に使用できます。Sysprep を使用した新しいマシンの起動が完了するまでには 5 分から 20 分 かかることがある点に注意してください。

5.2.7 エンドポイントの設定

ポート(443)を許可する ESG マシンのエンドポイントを追加します。

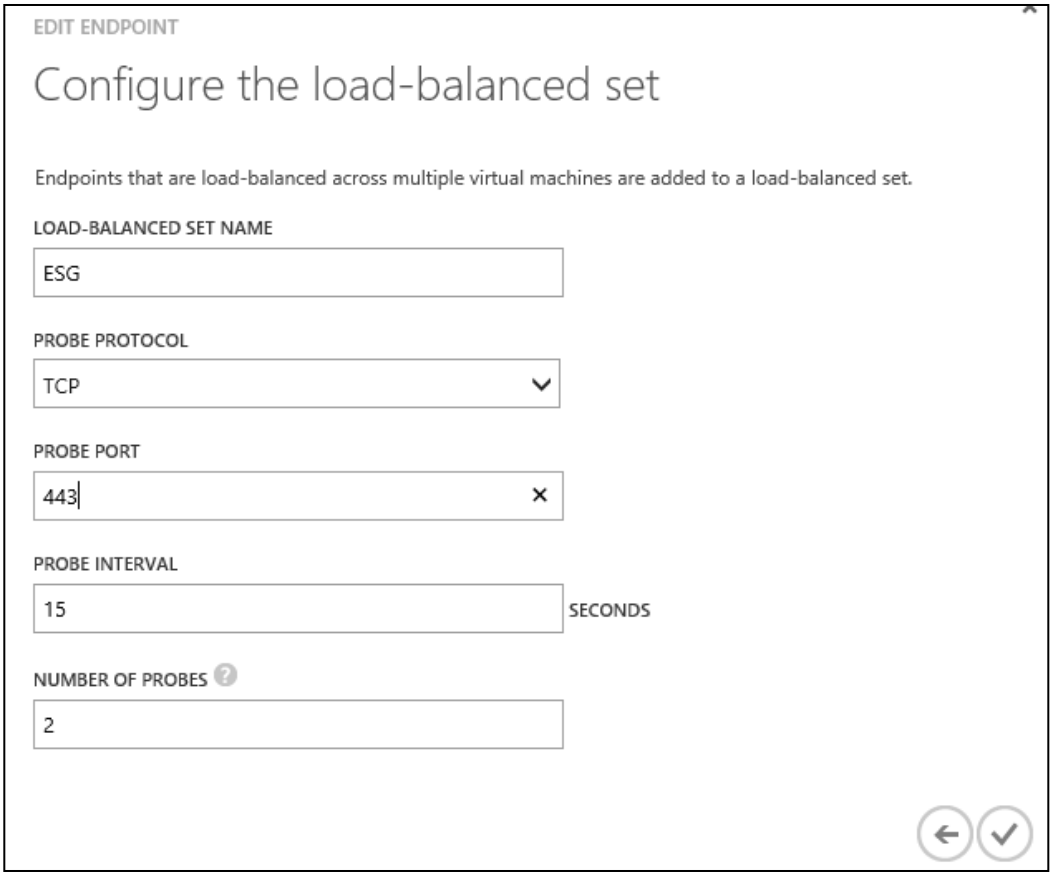
NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
Ericom	TCP	443	443
PowerShell	TCP	54037	5986
Remote Desktop	TCP	55961	3389

5.2.8 負荷分散の設定

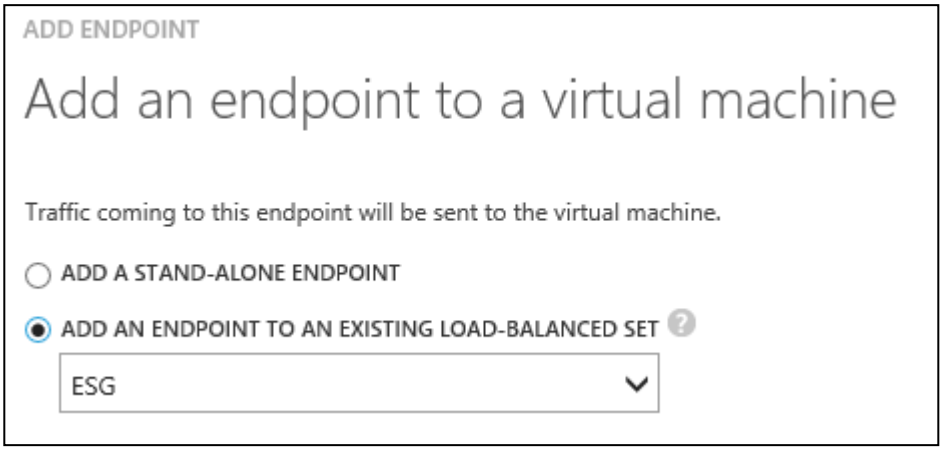
ESG ポートのエンドポイントを定義する際、「CREATE A LOAD-BALANCED SET」を選択します。 これにより、ラウンドロビン方式の負荷分散ソリューションが作成されます。

☑ CREATE A LOAD-BALANCED SET

セット名を定義します:



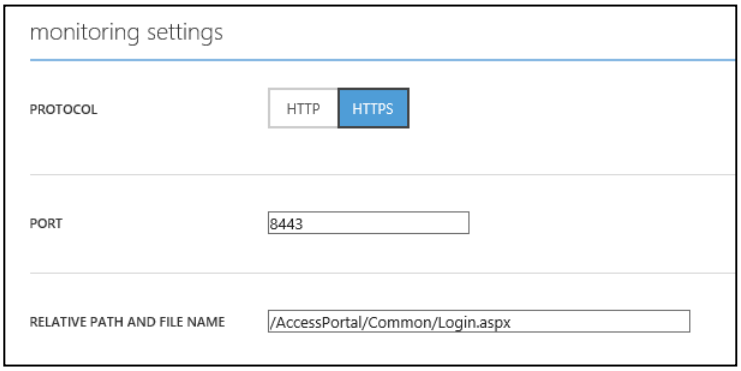
ESG を追加する場合、このセットを使用するようにエンドポイントを設定します。



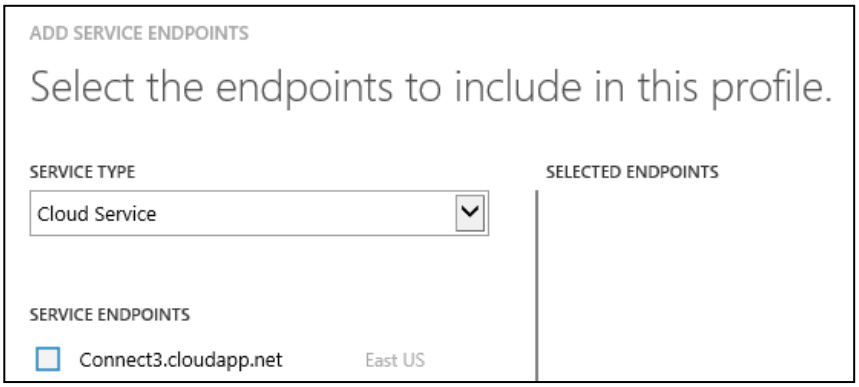
5.2.9 Traffic Manager の設定

異なるリージョンの複数 Connect 環境間の負荷分散をおこなうために Traffic Manager を作成するには、Azure Admin Console を使用します。 各 Connect システムが実行されている Azure クラウド・サービスにそれぞれの環境が関連付けられます。 Traffic Manager は、複数の環境の中から最も近い Connect 環境にユーザを誘導するのに役立ちます。 このことにより以下が実現されます: トラフィックの分散に「パフォーマンス」を使用する場合の最高なパフォーマンス。「ラウンドロビン」を選択した場合の均等な負荷分散。「フェイルオーバー」を選択した場合の高可用性。

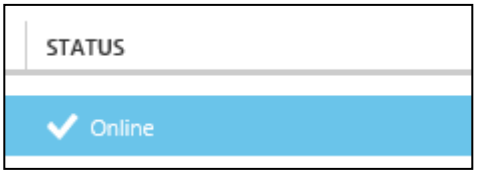
- Traffic Manager の名前を入力します。
- モニタ設定の構成
- Ping protocol: HTTPS を「HTTPS」 を選択し、Port 「443」を指定します(以下の例で使用されている「8443」はカスタム・ポートです)
- Path: 「/AccessPortal/Common/Login.aspx」を指定します



- ESG を選択して、エンドポイントを設定します。



- Traffic Manager が ESG にリーチできることを確認してください。



- Traffic Manager のアドレスを使用して、ロード・バランサへ接続します(ポート 443 以外を使用する場合は、ポート値を指定します)
- ユーザがログインし、アプリケーションへ接続すると、ESG の(プロキシではなく)実際の外部エンドポイントを通してリソースが起動されます。

5.2.10 高可用性と負荷分散の構成

複数リージョンに渡る Connect サービスを提供するには、Load Balanced Sets と Traffic Manager の組み合わせを使用します。 1 つの環境での高可用性を提供するために Load Balanced Sets を使用した上で、複数の Connect 環境に渡る 高可用性を提供するために Traffic Manager を使用します。

5.2.11 Ericom Connect イメージの準備

Azure を使用して、今後の使用のために Ericom システムをキャプチャします。 イメージをキャプチャする前に、以下の事項がシステムに適用されているかを確認してください:

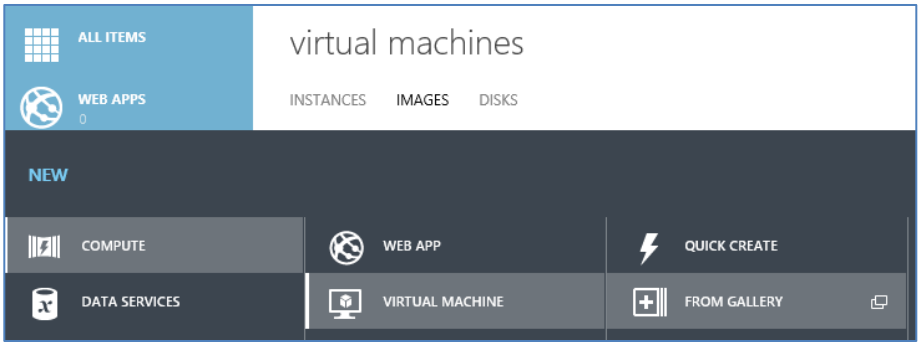
- 最新の Windows Update
- インストール済みの署名された証明書

イメージを使用して、ESG とセッション・ホストを展開できます。この時点では、Business Logic サーバの展開にイメージを使用しないでください。

Azure でイメージをキャプチャする方法については、こちらのリンクの手順に従ってください: http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-capture-image-windows-server/

5.2.12 イメージからの作成

VM をイメージとして保存した後、「ギャラリー」内のイメージを使用して新しいマシンを作成します。 新しいマシンの準備ができると、Sysprep によりシステムが初期化されます。 Ericom Connect コンポーネントはすでにイメージ上にインストールされているため、新しく作成したサーバは初期化後にグリッドに追加されます。



5.2.13 ホストへの遅いログインの解決

セッション・ホストの AMI では、イメージにユーザ・プロファイルが含まれていません。 そのため、AMI を使用してセッション・ホストを展開する場合、すべてのユーザのログインは初回のログインとなり、予想以上に長い時間がかかることがあります。 この遅れにより、Microsoft シームレス(Connect でのデフォルトの設定)を使用する公開アプリケーションが切断される場合があります。 この問題は、Ericom Seamless を使用することで回避できます。

5.3 RSA SecureID RADIUS 二要素認証

5.3.1 RSA RADIUS の設定

Ericom Connect 管理コンソールにログオンし、「RADIUS」タブを開きます。

「**RADIUS 有効化**」を「**はい**」に設定し、RSA 認証マネージャ・サーバの設定を構成します。

- サーバ・アドレスを入力します。

- サービス記述を入力します。
- 共有シークレットを入力します。
- 認証方法を**パスコード**に設定します。
- 認証ポートを 1812 または 1645(デフォルト)に設定します。

5.3.2 エージェント・ホスト設定

Ericom Connect と RSA 認証マネージャ間の通信を確立するために、エージェント・ホスト・レコードを RSA 認証マネージャ・データベースに追加する必要があります。エージェント・ホスト・レコードには Ericom Connect を識別する機能があり、通信と暗号化についての情報が含まれています。

認証エージェントを追加する際には、エージェント・タイプを「Radius クライアント」に設定します。 Ericom Connect では RADIUS を経由して RSA 認証マネージャが行われるため、エージェント・ホスト・レコードに対応する RADIUS クライアントを RSA 認証マネージャ内に作成する必要があります。RADIUS クライアントは、RSA セキュリティ・コンソールを使用して管理されます。

RADIUS クライアントを作成するには、以下の情報が必要です:

- ホスト名
- ネットワーク・インターフェースの IP アドレス
- RADIUS シークレット

(vf020715)

5.4 SecurEnvoy RADIUS 二要素認証

5.4.1 SecurEnvoy RADIUS の設定

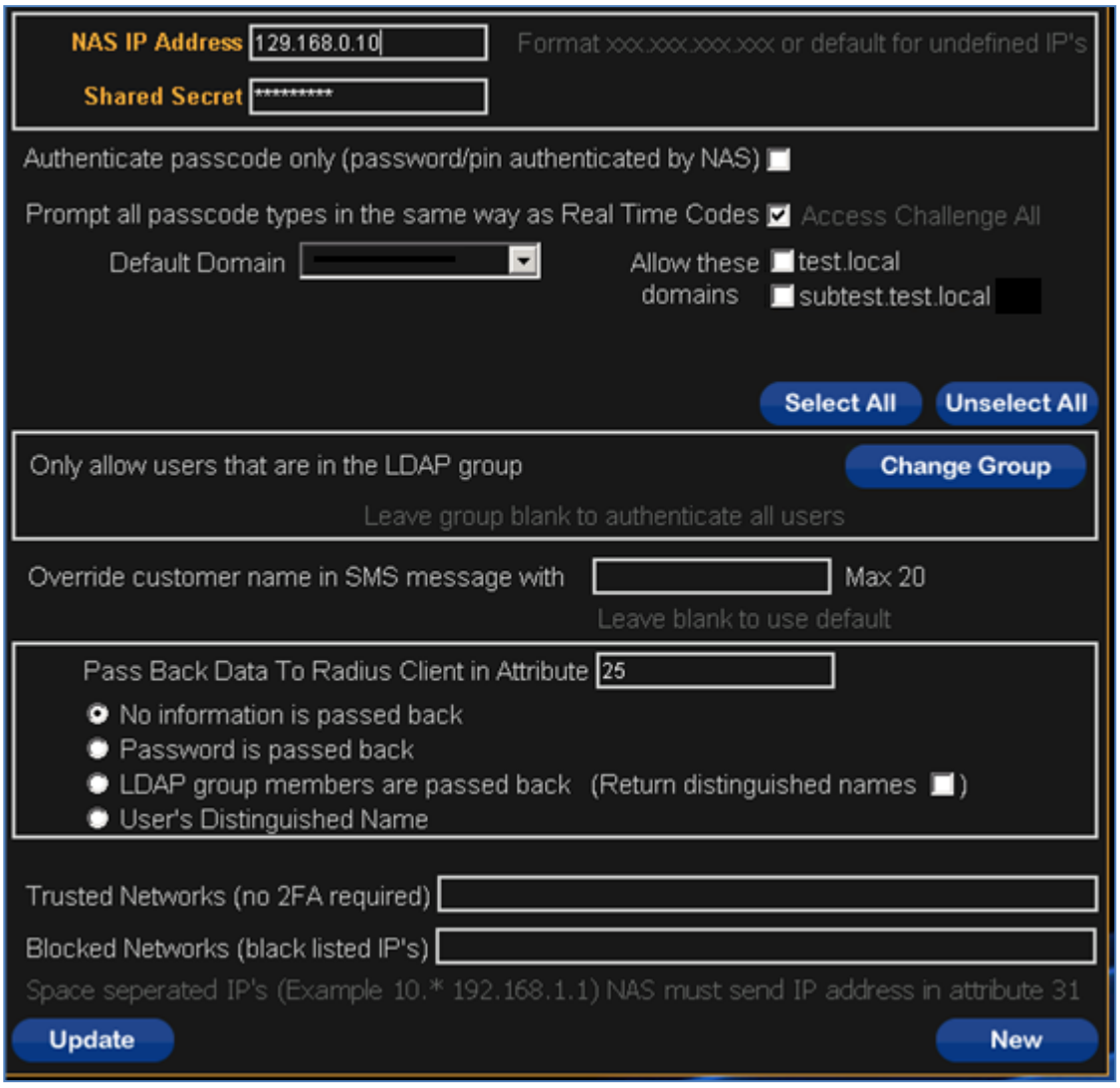
- Ericom Connect 管理コンソールにログオンし、「RADIUS」タブを開きます。
- 「RADIUS 有効化」を「はい」に設定し、RADIUS サーバ設定を構成します。

- 「サーバアドレス」を入力します
- 認証ポート値を確認します。
- 「サービス記述」を入力します。 このテキストは、Connect Access クライアントに表示されます。
- 「共有シークレット」を入力します。
- 必要な認証方法を選択します。

5.4.2 エージェント・ホスト設定

Ericom Connect と SecurEnvoy 管理サーバ間の通信を可能にするために、NAS クライアントを SecurEnvoy 管理データベースに追加する必要があります。NAS レコードで Connect サーバの識別が行われ、2 つのシステム間の接続が可能になります。

NSA クライアントを作成するために以下の情報が必要です:

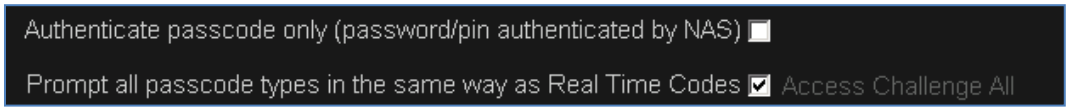


- NAS の IP アドレスを入力します。
- 共有シークレットを入力します。
- 必要なオプションを選択します。

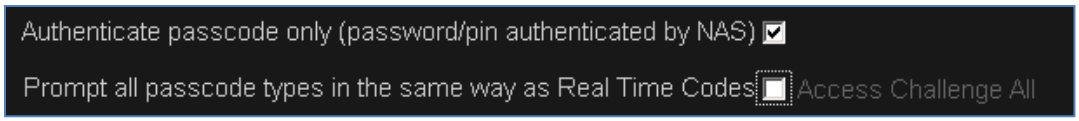
5.4.2.1 **設定オプション**

SecurEnvoy は、複数の方法で Connect に設定できます。 どの場合でもエンドユーザ・エクスペリエンスは同じです。 Ericom クライアントが SecurEnvoy にデータを送信する方法に違いが存在します。

認証サーバ・モードを使用するには 「パスワード/PIN」、SecurEnvoy を次のように設定します:

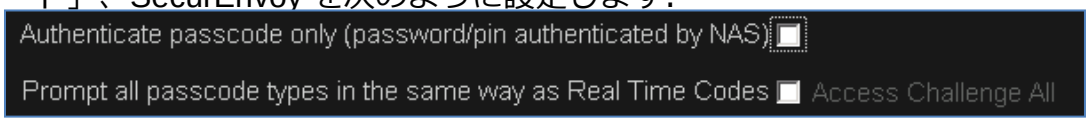


認証サーバ・モードを使用するには 「パスコード」、SecurEnvoy を次のように設定します:



このモードでは、ユーザ名とパスワードは Connect により確認され、パスコードのみが SecurEnvoy に確認されます。

認証サーバ・モードを使用するには 「パスワード/PIN + パスコード」、SecurEnvoy を次のように設定します:



5.5 Duo RADIUS 二要素認証

5.5.1 Duo RADIUS の設定

- Ericom Connect 管理コンソールにログオンし、「RADIUS」タブを開きます。
- 「RADIUS を有効化」を「はい」に設定し、RADIUS サーバ設定が Duo 認証プロキシを指定するように構成します。
- 「サーバ・アドレス」を入力します
- 認証ポート値を確認します。
- 「サービス記述」を入力します。 このテキストは、Connect Access クライアントに表示されます。
- 「共有シークレット」を入力します。
- 認証方法を設定します。「パスコード」に設定します(これは各環境の Duo 認証プロキシモードにより異なります)。

5.5.2 DUO プロキシの構成

Ericom Connect により Active Directory 認証が処理されるため、DUO では DUO パスコードの認証のみが必要です。 authproxy.cfg ファイルにて、「duo only client」として DUO を構成します。

ファイル構成のサンプル:

```
[duo_only_client]
[radius_server_duo_only]
ikey=DJ9DHWX3WQCQ9OJW4RTC
skey=im7Ra4DFEbSW85Iei1JcxQQmP31ddEiYhNab0uwR
api_host=api-18906ea1.duosecurity.com
radius_ip_1=enter-ericom-server-address
radius_secret_1=YourPass123
failmode=safe
client=duo_only_client
port=1812
```

第二要素のプロンプトでは、3 つのオプションが使用可能です:

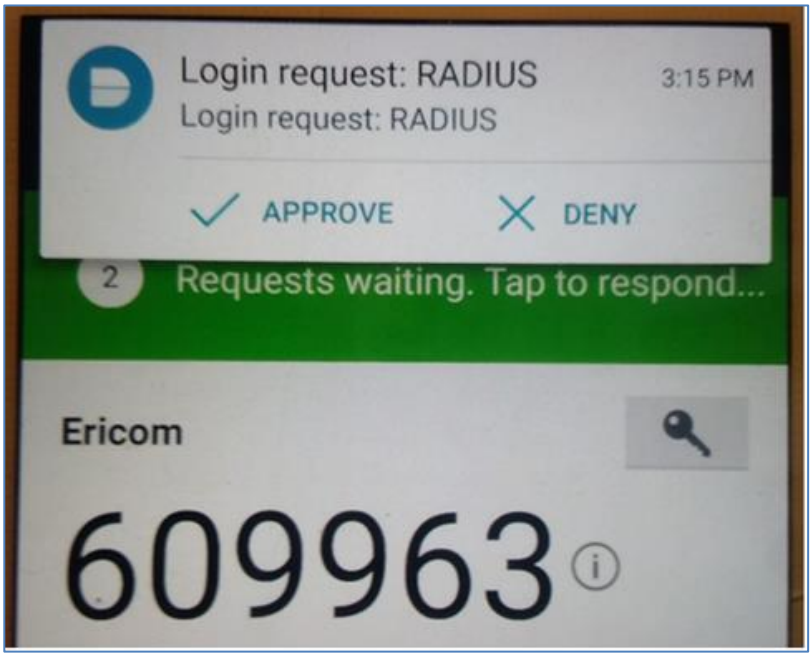
- DUO アプリのパスコードのみを使用して認証のパスコードを入力する。
- 値「push」を入力して、ユーザの登録済みデバイスにプッシュ通知を送信する。
- 値「phone1」を入力して、ユーザの登録済みの電話機を呼び出す。 認証を完了するには、ユーザが呼び出しに応答し、指示に従う必要があります。

現在、SMS 認証はサポートされていません。

5.5.3 エンドユーザ・アクセス

AccessPortal、AccessPad または AccessToGo からログインしてください。 DUO を有効化している場合、DUO パスコードの入力を求めるプロンプトが表示されます。DUO アプリ上に表示されるパスコードを入力します。

データが受信されると、ユーザのデバイスへプッシュ通知が送信されます。



Ericom にログインするには、「APPROVE」をタップします。

認証を確認するには、DUO ダッシュボードを参照します。

Timestamp	User	Application	Event	Result	Access Device	Second Factor
3:16 PM		RADIUS	Authentication	Access Granted User approved	0.0.0.0	Duo Push

5.6 AccessPortal での OneLogin SSO

AccessPortal SSO は、OneLogin のフォームをベースにした SSO と互換性があります。 フォームベースの認証は、保存されたパスワードを取得して、アプリケーションのログイン・ページへの挿入、フォームへの入力、ユーザのログインを実行するサインイン方法です。この方法は、

SAML を採用していないアプリケーションや API インターフェースを持たないアプリケーションで SSO アクセスを使用するために役立ちます。

OneLogin では、アカウント・パスワード(OneLogin 自体のアカウントへのログインに使用するパスワード)に加え、SAML または OAth 認証がサポートされていないアプリケーション用のパスワードも管理されます。ソルト OneLogin のアカウント・パスワードは、ソルト(salt)付きハッシュを使用して保管されます。アプリケーションのパスワードは、強力な対称鍵暗号化アルゴリズムを使用して暗号化されます。 OneLogin と Ericom Connect 間の SSO で正常に機能するために、Active Directory のユーザが使用されます。 このため、OneLogin AD Connector を使用して、AD と OneLogin のアカウント情報を同期する必要があります。

OneLogin のフォームベースのアプリケーションでは、ユーザが OneLogin ブラウザ拡張をインストールすることが必要になります。(20160831)

5.6.1 システム構成

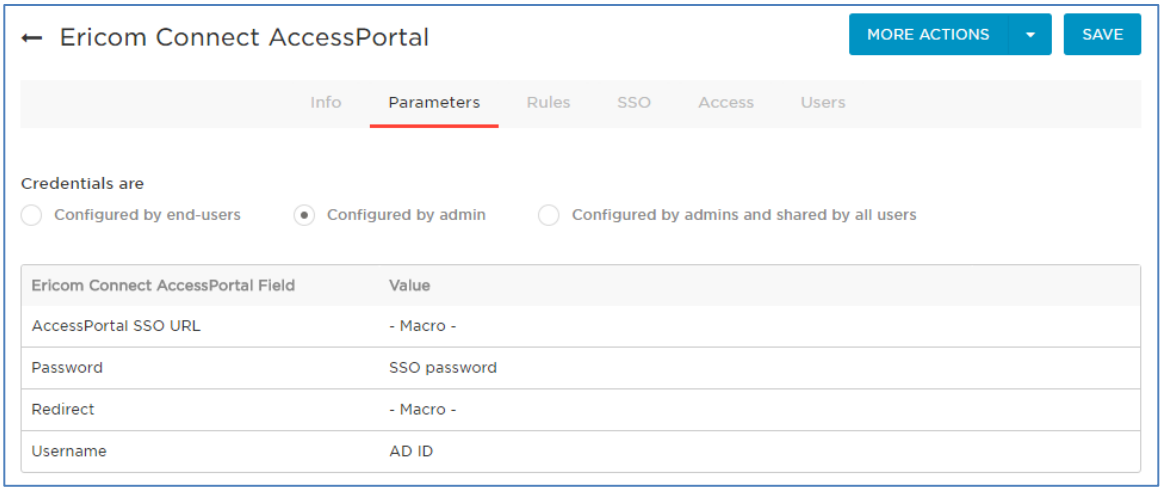
設定を開始するには、OneLogin ポータルで Ericom Connect AccessPortal コネクターを検索します。

新しいコネクターに名前を付け、「保存」をクリックします。

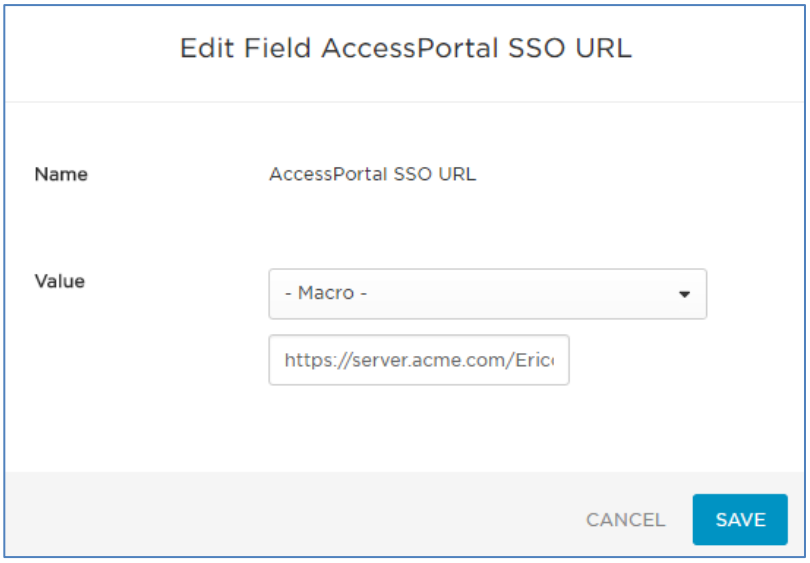
これで、パラメータ設定ページが使用可能になります。

次のオプションを選択します: **Configured by admin**

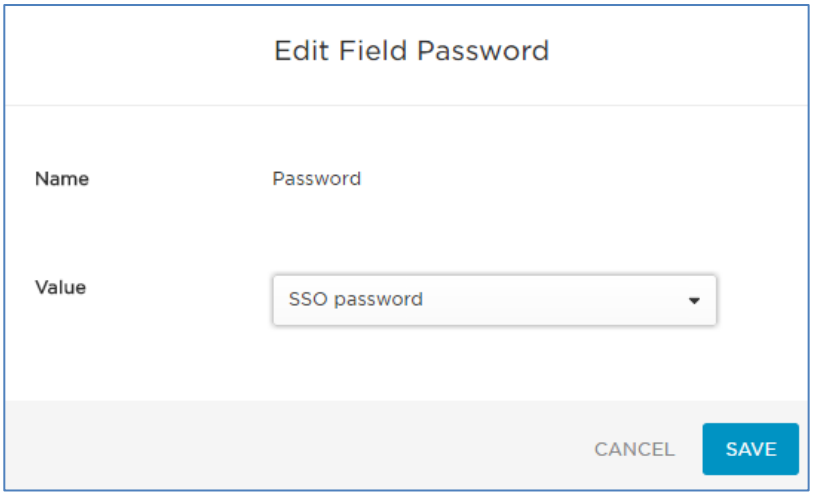
4 つの設定を構成する必要があります。



- 「AccessPortal SSO URL 」をクリックし、「マクロ」を選択します。
- AccessPortal SSO のアドレスを入力し、「保存」をクリックします。



- 「パスワード」をクリックし、「SSO パスワード」を選択し、「保存」をクリックします。



- 「リダイレクト」をクリックし、「マクロ」を選択します。「true」を入力し、「保存」をクリックします。
- 「ユーザ名」をクリックし、AD ユーザの ID(例: AD ID)を示すユーザ名の変数を選択します。その後、「保存」をクリックします。

アプリケーションの作成が完了すると、目的のユーザへの割り当てが行われ、使用できるようになります。

5.7 Juniper SSL VPN を使用した展開

Ericom Secure Gateway と SSL VPN を組み合わせて使用することで、2 重ファイアウォール環境用のセキュアなアクセス・ソリューションを実現できます。 このセクションでは、参照用として ファームウェア 8.0 を実行する Juniper SA SSL VPN が使用されています。

Juniper と共に動作するように Ericom Connect を設定するには、次の 2 つの Web リソース・プロファイルが必要です:

- Juniper ポータルから Ericom AccessPortal への SSO 用のプロファイル。 このプロファイルは、ユーザのブックマークに表示されます。
- ESG 経由での AccessPortal への接続を許可するリバース・プロキシで、書き換えを無効にしたもの。

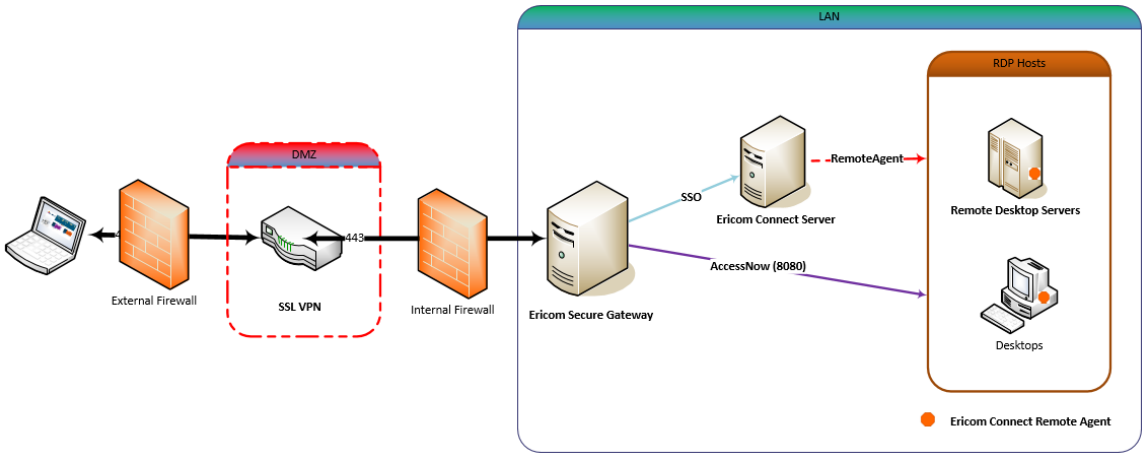
Juniper から公開アプリケーションへの接続プロセスは以下のようになります:

- ユーザが Juniper にログインし、AccessPortal ブックマークを選択します。
- Juniper により、ESG 経由で AccessPortal SSO への POST が実行されます。
- Connect SSO によりブラウザ Cookie が設定され、リバース・プロキシ経由で AccessPortal のスタート・ページへブラウザがリダイレクトされます。
- AccessPortal ページは、ESG 経由で EUWS により提供されます。 リバース・プロキシが使用されるため、ページの書き換えは発生しません。

ユーザにより、起動するアプリケーションが選択された場合:

- ESG とリバース・プロキシを経由して、EUWS に起動要求が送信されます。
- リバース・プロキシ経由で 起動ファイルから ESG が参照されます (ESG ホスト・アドレス で適切なアドレスが指定されます)。

- リバース・プロキシを介して、AccessPortal により AccessNow セッションが起動されます。
- セッションを確立するために、AccessNow によりリバース・プロキシと ESG を経由して ターゲットの AccessServer に WebSoket が作成されます。



5.7.1 リバース・プロキシの構成

リバース・プロキシにより、書き換えルールを使用せず AccessPortal にアクセスすることが可能になります。 リバース・プロキシを使用するには、追加の仮想ホストを使用する必要があります。

この実装例では、以下の設定が使用されています:

Juniper アドレス: https://juniper.acme.com

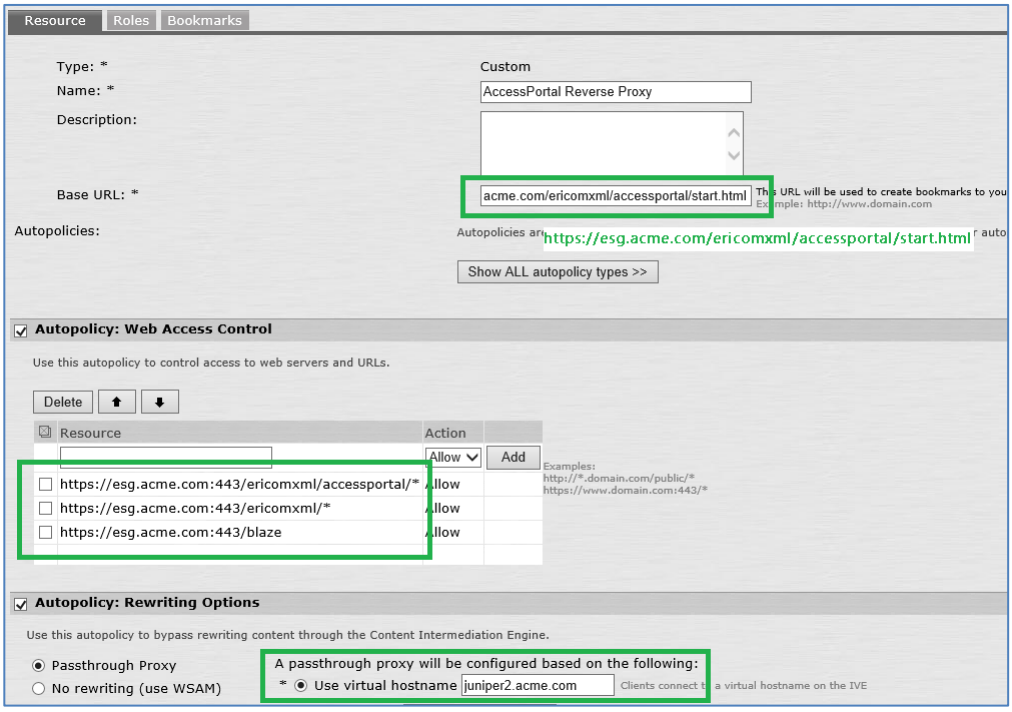
仮想ホスト・アドレス: juniper2.acme.com

ESG アドレス: ESG.acme.com:443

「juniper2.acme.com」が「juniper.acme.com」のエイリアスとなる DNS エントリを作成します

Ericom Connect で、ESG ホスト・アドレスは「juniper2.acme.com:443」用である必要があります。

以下を例として新しい Web リソースを作成します(ユーザはこのブックマークをクリックしないでください):



5.7.2 SSO の設定

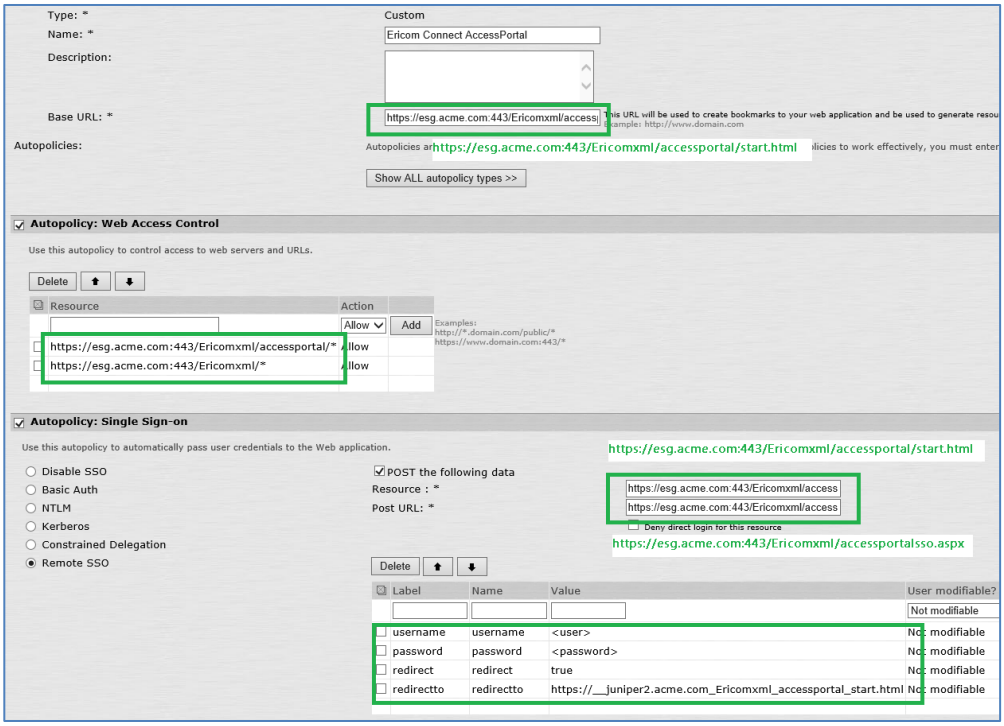
この実装例では、以下の設定が使用されています:

Juniper アドレス: https://juniper.acme.com

仮想ホスト・アドレス: juniper2.acme.com

ESG アドレス: ESG.acme.com:443

以下を例として新しい Web リソースを作成します(このブックマークは、ユーザが今後使用するものとなります)



POST の「RedirectTo」の値は、次の値である必要があります:

「https://juniper2.acme.com/EricomXml/accessportal/start.html」

ただし:すべての「/」は「_」により置換されるため、正しい値は次のようになります:

「https:__juniper2.acme.com_EricomXml_accessportal_start.html」

これが、SSO が完了した後にブラウザがリダイレクトされる AccessPortal スタート・ページとなります。「_」により書き換えが防止されます。

5.8 F5 SSL VPN での展開

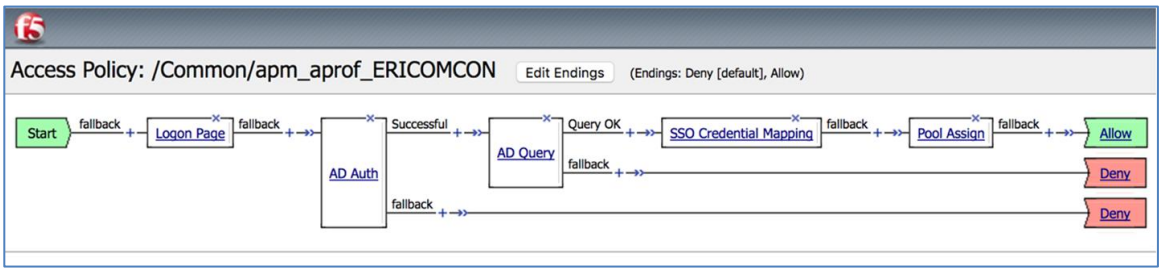
Ericom Secure Gateway と SSL VPN を組み合わせて使用することで、2 重ファイアウォール DMZ 環境用のセキュアなアクセス・ソリューション

を実現できます。 このセクションでは、バージョン 12.1.1 を実行する F5 BIG-IP SSL VPN が参照用として使用しています。 バージョン 11.4 以降の F5 HTTP プロファイルでは、Websocket アップグレード・ヘッダーがサポートされています。

(13022017JL)

5.8.1 オプション 1: リバース・プロキシ

リバース・プロキシにより、書き換えルールを使用せず Ericom Connect の AccessPortal にアクセスすることが可能になります。 Ericom Connect インフラストラクチャに使用される内部ホスト名(例: Ericomcon.acme.com)は、アプリケーションの「公開された」外部 DNS 名と一致する必要があります。 Ericomcon.acme.com は、内部ネットワーク上の内部 IP (Ericom Connect Gateway サーバを指すもの)に解決する必要があります。同一のホスト名が、外部ネットワークの別のパブリック IP(AMP プロファイルを持つ F5 VS を指す物)に解決します。



アクセス・プロファイル:

```
apm profile access apm_aprof_ERICOMCON {
accept-languages { en }
access-policy apm_aprof_ERICOMCON
app-service none
customization-group apm_aprof_ERICOMCON_logout
```

```
default-language en
domain-cookie none
domain-mode single-domain
eps-group apm_aprof_ERICOMCON_eps
errormap-group apm_aprof_ERICOMCON_errormap
exchange-profile none
framework-installation-group
apm_aprof_ERICOMCON_frameworkinstallation
general-ui-group apm_aprof_ERICOMCON_general_ui
generation 6
generation-action noop
httponly-cookie false
log-settings {
 default-log-setting
}
logout
```

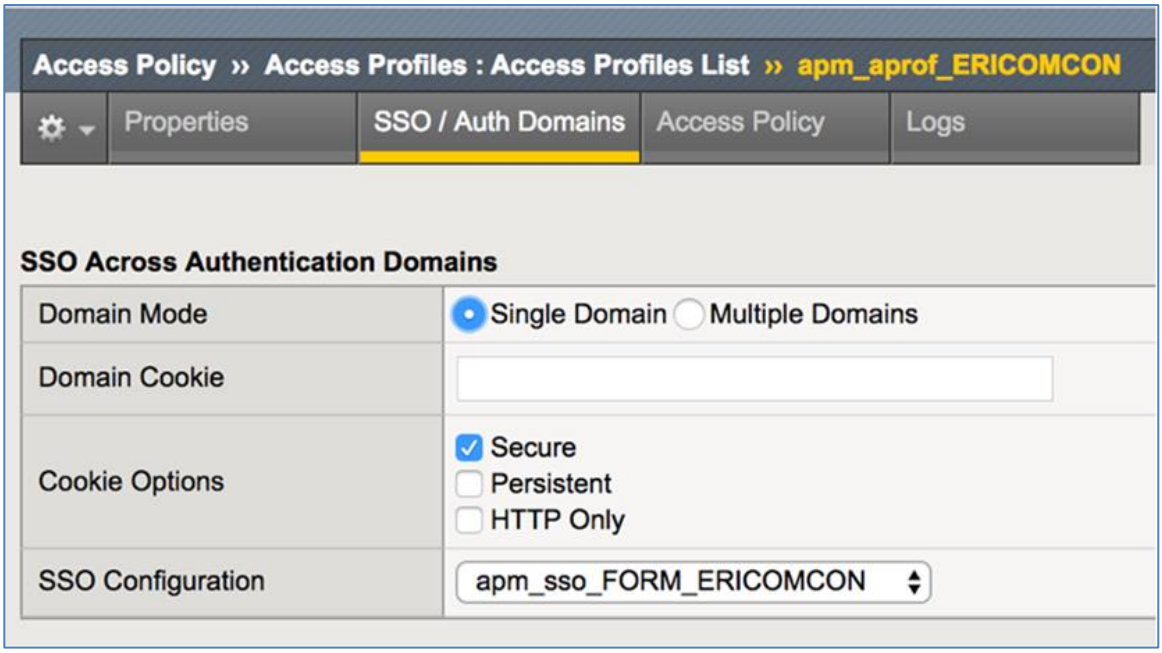
Virtual Server Configuration for ERICOMCON

```
ltm virtual virt_ERICOMCON {
destination <F5_external_address>:https
ip-protocol tcp
mask 255.255.255.255
profiles {
apm_aprof_ERICOMCON { }
clientssl {
context clientside
}
http { }
rba { }
serverssl {
context serverside
}
tcp-lan-optimized { }
```

```
websso { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
vlan_VIRTS_115
}
vlans-enabled
vs-index 44
}
```

SSO の設定

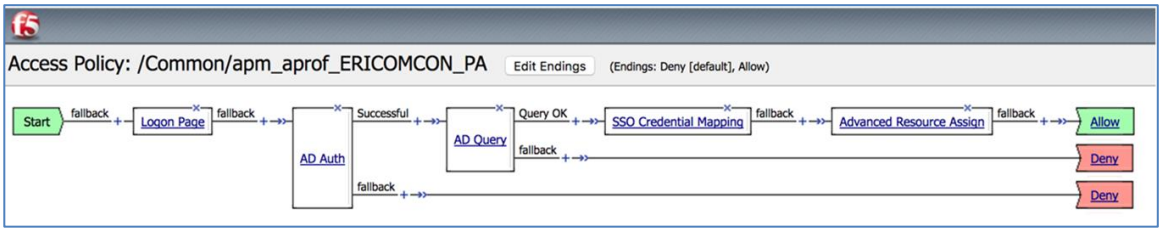
以下のスクリーンショットの例のように、アクセス・ポリシーの「SSO/Auth ドメイン」セクションから SSO ポリシーを設定します:



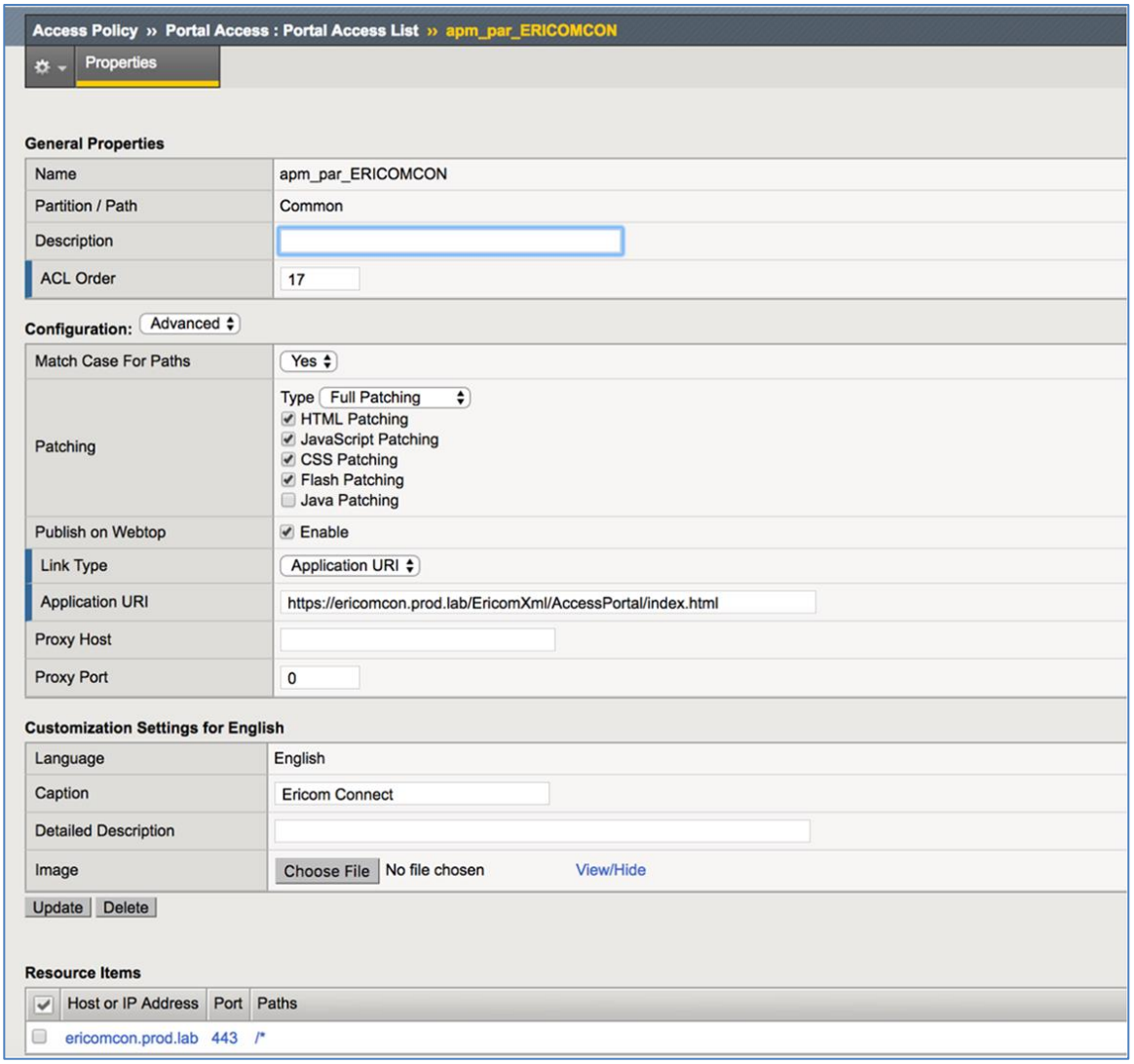
5.8.2 オプション 2: リライタ

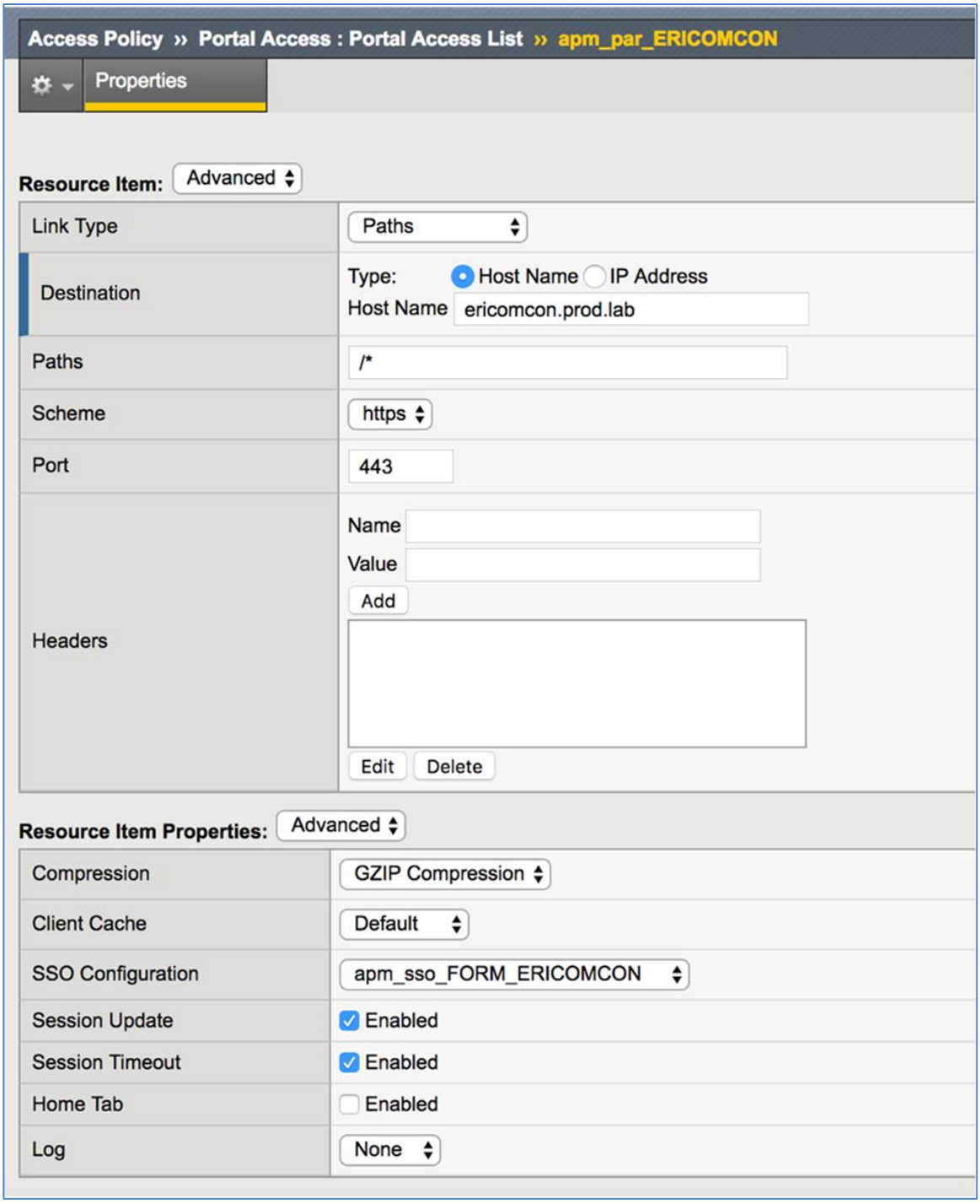
F5 の別の設定オプションは、リライタを使用する方法です。 ビルトインのリライタを使用する場合、F5 APM モジュールによりユーザ認証が行われます。オプションとして Ericom Connect サーバへの SSO を行い、必要に応じてアプリケーション・トラフィック(Websocket コールを含む)を書き換えできます。 F5 により、Webtop(アイコン付きのポータル)上のポータル・アクセス・リソースを使用してリンクが書き換え(非表示化)られます。 このオプションには、この章で後述する iRule の設定が必要です。

Ericom Connect で使用する内部ホスト名(例: ericomcon.prod.lab)は、アプリケーション用の「公開された」外部 DNS 名とは異なります。



アクセス・プロファイル:


Access Policy » Portal Access : Portal Access List » apm_par_ERICOMCON
Properties
General Properties
Name
apm_par_ERICOMCON
Partition / Path
Common
Description
ACL Order
17
Configuration: Advanced
Match Case For Paths
Yes
Patching
Type Full Patching
HTML Patching
JavaScript Patching
CSS Patching
Flash Patching
Java Patching
Publish on Webtop
Enable
Link Type
Application URI
Application URI
https://ericomcon.prod.lab/EricomXml/AccessPortal/index.html
Proxy Host
Proxy Port
0
Customization Settings for English
Language
English
Caption
Ericom Connect
Detailed Description
Image
Choose File
No file chosen
View/Hide
Update
Delete
Resource Items
Host or IP Address
Port
Paths
ericomcon.prod.lab
443
/*



Virtual Server Configuration for ERICOMCON_PA

ltm virtual virt_ERICOMCON_PA {

```
destination <F5_external_address>::https
ip-protocol tcp
mask 255.255.255.255
profiles {
apm_aprof_ERICOMCON_PA { }
apm_seccon_PORTAL {
context clientside
}
clientssl {
context clientside
}
http { }
ppp { }
rba { }
rewrite-portal { }
serverssl {
context serverside
}
tcp-lan-optimized { }
websso { }
}
rules {
irule_APM_ERICOMCON
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
vlan_VIRTS_115
}
```

```
vlans-enabled
vs-index 44
}
Connectivity / rewrite-portal profiles: Use Default
Required iRule configuration:
when HTTP_REQUEST {
set tmm_apm_rewrite_request 0
}

when REWRITE_REQUEST_DONE {
set tmm_apm_rewrite_request 1
if { [HTTP::header exists Upgrade] && \
[string tolower [HTTP::header Upgrade]] contains "websocket" } {
# 元のヘッダーをバックエンドアドレスで置換
HTTP::header replace Origin "https://[HTTP::host]"
# リライト・プラグインを無効化。無効化しない場合はリクエスト停止します
REWRITE::disable
}
}

when HTTP_RESPONSE {
if { !$tmm_apm_rewrite_request } { return }

set tmm_apm_chunked 0
if { [HTTP::header Content-Type] contains "javascript" } {
if { [HTTP::header Transfer-Encoding] == "chunked" } {
set tmm_apm_chunked 1
} elseif { [HTTP::header Content-Length] == 0 } {
return
}
HTTP::collect 1
```

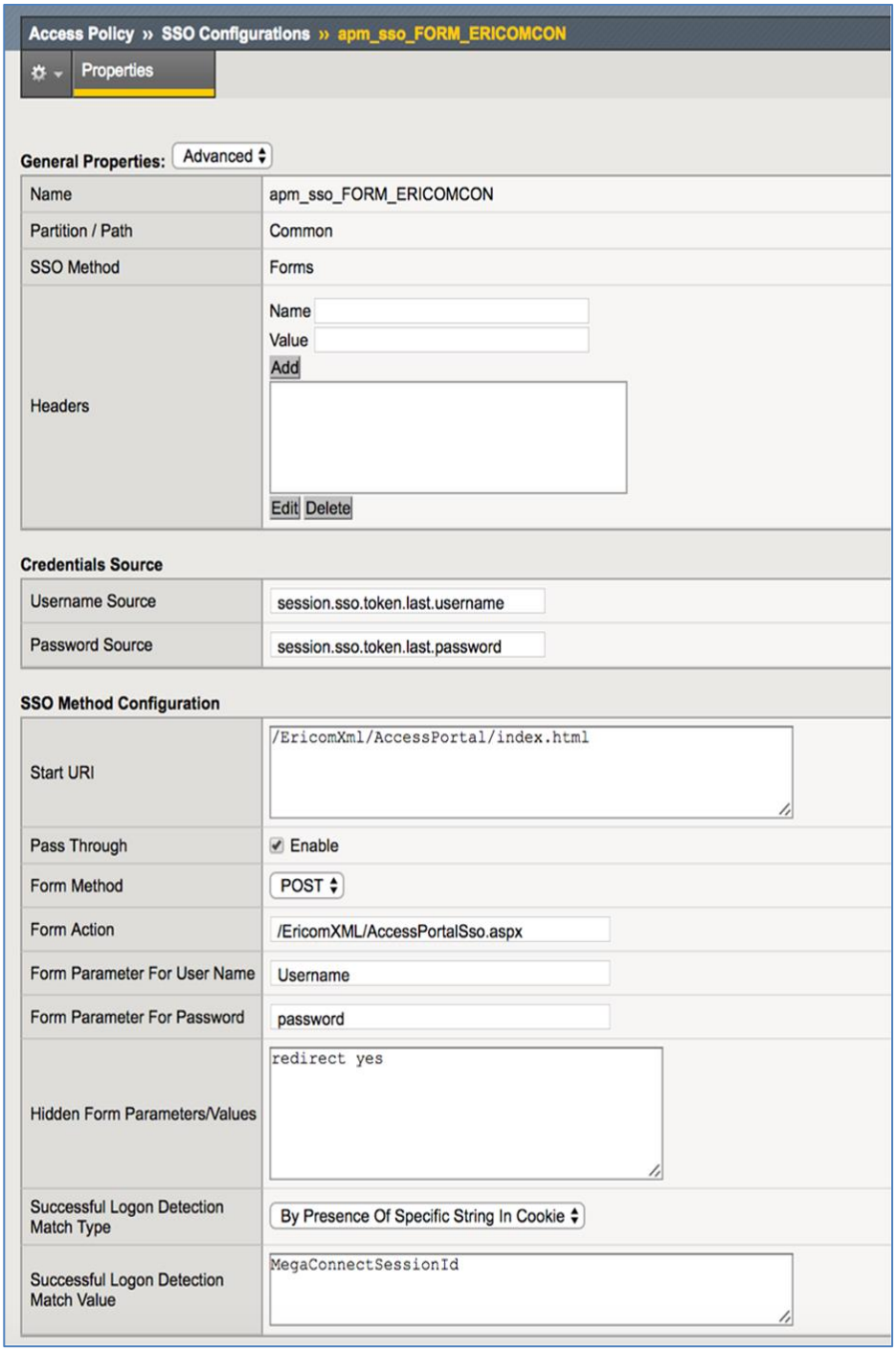
```
}
}

when HTTP_RESPONSE_DATA {
if { !$tmm_apm_rewrite_request } { return }

set tmm_apm_patch {
function wsWrapper(F5_orig) {
var wrapper = function WebSocket() {
if (typeof(arguments[0]) === 'string') {
arguments[0] = F5_WrapURL(
arguments[0].replace(/^ws/,'http'))
.replace(/^http/,'ws');
}
var socket = new F5_orig(arguments[0], arguments[1]);
socket.constructor = wrapper;
return socket;
};
if (Object.setPrototypeOf) {
Object.setPrototypeOf(wrapper, F5_orig);
} else { // IE10
Object.keys(F5_orig).forEach(function (key) {
wrapper[key] = F5_orig[key];
});
}
wrapper.F5_original = F5_orig;
wrapper.prototype = F5_orig.prototype;
wrapper.toString = function toString() { return F5_orig.toString();};
return wrapper;
};
if ((typeof(window.MozWebSocket) !== 'undefined') &&
!window.MozWebSocket.F5_original) {
window.MozWebSocket = wsWrapper(window.MozWebSocket)
```

```
}
if ((typeof(window.WebSocket) !== 'undefined') &&
!window.WebSocket.F5_original) {
window.WebSocket = wsWrapper(window.WebSocket)
}
}

if { $tmm_apm_chunked } {
set tmm_apm_patch "[format %x [string length
$tmm_apm_patch]]\r\n$tmm_apm_patch"
}

HTTP::payload replace 0 0 $tmm_apm_patch
HTTP::release
}

when HTTP_RESPONSE_RELEASE {
if { [HTTP::header exists Content-Security-Policy] } {
HTTP::header replace Content-Security-Policy \
[string map {"data:" "data: blob:"} [HTTP::header Content-Security-
Policy]]
}
}
```

5.8.3 SSO の設定

SSO を使用する場合、SSO ポリシーをアクセス・ポリシー内に設定してください(設定方法により場所が異なります。使用している方法のスクリーンショットを参照してください)。

以下の画像は、Ericom Connect インターフェース用に F5 SSO ポリシーを作成する方法の例を示しています:


Access Policy » SSO Configurations » apm_sso_FORM_ERICOMCON
Properties
General Properties: Advanced
Name
apm_sso_FORM_ERICOMCON
Partition / Path
Common
SSO Method
Forms
Headers
Name
Value
Add
Edit Delete
Credentials Source
Username Source
session.sso.token.last.username
Password Source
session.sso.token.last.password
SSO Method Configuration
Start URI
/EricomXml/AccessPortal/index.html
Pass Through
Enable
Form Method
POST
Form Action
/EricomXML/AccessPortalSso.aspx
Form Parameter For User Name
Username
Form Parameter For Password
password
Hidden Form Parameters/Values
redirect yes
Successful Logon Detection Match Type
By Presence Of Specific String In Cookie
Successful Logon Detection Match Value
MegaConnectSessionId

6 サポート・ガイド

6.1 Ericom Connect に関する法律上の注意事項

このドキュメントの所有権は Ericom Software に属し、明示的かつ適切に認められた **Ericom Connect** のユーザを支援することのみを目的としています。 この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。ソフトウェアおよびドキュメントは、契約の条件に従う場合または法令により許可される場合のみに限り、使用または複製できます。

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。誤りを見つけた場合、書面にてご報告ください。

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。

このドキュメントでは、第三者からのコンテンツ、製品、サービスを利用することがあります。Ericom Software およびその関連会社は、第三者のコンテンツ、製品、サービスに関していかなる責任を負わず、すべての保証を一切認めません。Ericom Software およびその関連会社は、第三者のコンテンツ、製品、サービスの使用により生じたいかなる損失、費用または損害に責任を負いません。

Ericom と PowerTerm は、Ericom Software の登録商標です。Ericom Connect, Ericom Blaze、Ericom AccessNow、Ericom AccessToGo、PowerTerm WebConnect 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。

Copyright © [2016], Ericom Software.All rights reserved.
EC_AdminMan20160406

6.2 用語集

AccessNow	公開されたアプリケーションやデスクトップへのアクセスに使用される HTML5 ベースの技術。ホスト側に「AccessServer」が必要です。
AccessPad	Windows と Mac 用のネイティブ・クライアント
AccessPortal	エンドユーザが割り当てられたリソースへアクセスするための Web ベースサインイン・ポイント。 起動したアプリケーションとデスクトップでは AccessNow HTML5 インターフェース が使用されます。
AccessToGo	iOS と Android で利用可能なネイティブ・モバイル・アプリ
管理コンソール	Ericom Connect の監視、設定、管理を行うための Web ベースの管理インターフェース。
AWS (管理 Web サービス)	ユーザが、Ericom Connect を管理するための Web ベースの管理コンソールを参照するのを可能にします。
EC (Ericom Connect)	任意のデバイス・場所のユーザと企業のアプリケーションおよびデスクトップを接続する、エンタープライズ・クラスの接続ブローカ。
EC BL (Ericom Connect Business Logic サービス)	コントローラ・サービスとも呼ばれる、ビジネ

	ス・ロジックとインメモリ・データーベースを含むメイン・サービス。
Ericom Connect Configuration Tool	Connect のインストール後に自動的に起動される Windows ベースのアプリケーション。Ericom グリッドとデータベースの初期設定の構成に使用します。
ESG (Ericom Secure Gateway)	ファイアウォールの外部からの安全なリモート・アクセスを可能にする SSL ベースの高性能ゲートウェイ。
EUWS (エンドユーザ Web サービス)	クライアント Web サービスとも呼ばれます。Ericom クライアントと Web ポータルを Ericom Connect に接続することを可能にします。
グリッド	すべての Connect 関連サービスを管理するための基盤となるグリッド・ベースのプラットフォーム。 各グリッド・メンバーには、データベースのデータへのアクセス権が与えられます。
グループ - 公開	「公開グループ」により、公開されたアプリケーションとデスクトップおよびそのプロパティが管理されます。
グループ - システム	「システム・グループ」により、類似するプロパティを持つシステムのコレクションが管理されます。 公開グループで関連付けられたアプリケーションをどのシステムから起動するかを指定する

	ために、システム・グループが公開グループに割り当てられます。
RDP	リモート・デスクトップ・プロコトル(Remote Desktop Protocol)。 このプロコトルは、キーボード、マウス、およびデータ表示のために、AccessNow と Blaze のプロコトルで使用されています。 登録されたサーバとワークステーション上でこのプロコトルが利用可能である必要があります。
RAWS (RemoteAgent Web サービス)	タイプ 2 の Remote Agent を管理するための Ericom Connect RemoteAgent Web サービス。 グリッドの一部である RemoteAgent は、タイプ 1 として分類され、Web サービスを使用しません。
リモート・エージェント (RemoteAgent)	登録されたリモート・サーバ(TS/RDS)とワークステーションを管理・監視するための Connect Agent。 ホストの健全性とアクティビティに関する Ericom Connect データを提供します。 新しい RemoteAgent は、以前のバージョンの Ericom Connect サーバと互換性がありません(例: 7.5 RemoteAgent は 7.3 Ericom Connect では動作しません)。
SQL データベース	レポートと分析用の履歴データを格納するための Microsoft SQL データベース。また、Ericom

	Connect の起動と再起動時に使用される構成データも格納します。
セッション・ホスト	セッション・ホストの役割が有効化された Windows 2008 以上のサーバ。 Ericom Connect ではこの役割のみが有効化されていることが必要であり、他の Microsoft RDS コンポーネント(例: TSGateway)は必要ありません。
SSO	シングル・サインオン(Single Sign On)
ターミナル・サーバ / リモート・デスクトップ・サーバ	複数のユーザからの RDP リクエストを受信することができるオペレーティング・システム。 通常は、Windows 2003、2008、2008 R2、2012 です。

6.3 リリース・ノート

6.3.1 Ericom Connect v7.6.1

[リリース日(GA)]

2017 年 2 月

[Ericom Connect 機能]

Linux での URL リダイレクト**(Linux 環境はサポートしておりません)**

Linux でのアプリケーションの公開**(Linux 環境はサポートしておりません)**

Linux セッションでのセッション共有**(Linux 環境はサポートしておりません)**

AccessPortal キーボードのロケールをデバイス上にローカル保存

英語以外の文字でのパスとパラメータの公開

ユーザ・セッションでのキーボード言語の自動検出と切り替え

管理ツール: F11 の実行スコープの新しい設定

管理ツール: キーボード検出言語の新しい設定

管理ツール: 新しい Blaze 設定と「True Lossless」モードのオプション

CLI(EndUserSessions)コマンドでユーザ向けのポータルとセッションの一覧を表示

RDP (19702) により、プログラムのフィールド長さを 256 文字に設定

未使用の RemoteAgent サービス(LB/RB)をデフォルトで無効化 (19995)

RADIUS の「接続が失われました」のバグを解決(解決済み: CA0000030979、CA0000031435)

解決された CA の問題: CA0000029922、CA0000031271、CA0000032348

解決された AccessPortal CA の問題: CA0000021667、CA0000031612

[AccessNow]

AccessNow セッションでのキーボード言語の自動検出と切り替え(解決済み: CA0000027367)

AccessNow 印刷エンジンのアップデート(解決済み: CA0000027126)

サービス・クラッシュに関連するバグの解決(解決済み: CA0000031844、CA0000032064)

解決された CA の問題: CA0000030558、CA0000027262、CA0000031844、CA0000032645

[AccessPad/Blaze]

Ubuntu 14.04 用の新しい Linux x64 バージョン

「True Lossless」モードの機能を追加

フルスクリーンの接続バーの高さを 3 ピクセル拡張

解決された CA の問題: CA0000010088、CA0000001106、CA0000029266

CA0000029267、CA0000027817

[AccessToGo]

新しいデフォルト: マルチタッチ・モードを有効化

新しいデフォルト: 向きを変更する際のフルスクリーンのリサイズを有効化

キーボードを非表示にした時の余分なスペースを解決 (CA0000022001)

解決された CA の問題: CA0000027842、CA0000029228、CA0000008976、CA0000031158、CA0000032211

6.3.2 Ericom Connect v7.6.0

[リリース日(HF)]

7.6.0.15799

2017 年 2 月

Chrome 56 で動作するよう AccessPorta の HTTP モードを修正

[リリース日(GA)]

7.6.0.12954

2016 年 10 月

[Ericom Connect 機能]

新しい AccessPortal ユーザ・エクスペリエンス

新しい管理コンソールのユーザ・エクスペリエンス

Windows 2016 リモート・セッション・ホスト(RDSH) との互換性

Windows 2016 SQL Server との互換性

セッション・シャドウイング

セッションのログオフ、切断およびリセット

管理コンソールでの RDP エクスペリエンスの設定

事前作成された空の SQL データベースの使用をサポート

RADIUS - 属性を使用した「Send Client IP」を追加

RADIUS – 「<domain>\」または「@<domain>」を受け入れるようデフォルト・ドメインを変更

2008R2 の展開から SP1 の要件を削除

Ericom RDX Linux xRDP

Linux セッションでの印刷とオーディオのサポートを追加

新しいダッシュボード要素: データベースの使用状況、RemoteAgent のステータス(Windows、Linux)

AccessPortal で項目をお気に入りとして保存することが可能

特定の日付以前のデータベース・データを消去するための CLI

クライアント・タイプに基づいて公開グループを設定するための CLI(SetConnectionRule)

デスクトップ・セッションのタイトル・ラベルを変更するための CLI

サポートを目的として dbgmon の詳細を表示するための CLI

.BAT ファイルの公開

AccessNow セッションで CTRL+P をブロックするための管理者設定

レポート: 「ユーザ | リモートセッション」で起動中のすべてのアプリケーションを表示

クライアント名の保存(Preserve Client Name)を自動化し、システム設定から削除

RDP_WithExplorer 機能のサポート

各コンポーネントで生成されたすべての**自己署名証明書**に **SHA256RSA** を使用

AccessPortal と管理 Web ページの IE 10 のサポートの廃止(マイクロソフトによる MSIE10 のサポートが終了したため)

Linux 環境はサポートしておりません

以下の CA 解決の追加: CA0000027476, CA0000009580,

CA0000011254, CA0000012806, CA0000013556, CA0000014653, CA0000014731, CA0000017781, CA0000018073, CA0000018444, CA0000018861, CA0000018915, CA0000019440, CA0000019480, CA0000019828, CA0000019872, CA0000019919, CA0000020173, CA0000020240, CA0000020733, CA0000021667, CA0000021738, CA0000022059, CA0000022295, CA0000022442, CA0000023090, CA0000023124, CA0000023397, CA0000023457, CA0000023497, CA0000023554, CA0000024676, CA0000025372, CA0000025412, CA0000025509, CA0000025574, CA0000025998, CA0000026201, CA0000026963, CA0000027124, CA0000027203, CA0000027312, CA0000027534, CA0000027543, CA0000027749, CA0000027866, CA0000028394, CA0000028564, CA0000028840, CA0000029061,

[AccessPad 機能]

Mac 版をバージョン 7.6 にアップデート

Mac 版のアクセラレーション・モードでの NLA のサポート

Windows 版でのテキストと画像のコピー/ペーストの改善

[AccessToGo の機能]

[AccessToGo の機能]

Android 6.0 との互換性

7.6 以降では、デフォルトでマルチタッチ・モードを有効化

[AccessNow]
外観と使い勝手のアップデート

タッチ対応デバイス向けのクリック・アニメーション

セッション内のコピー・ペーストでテキストの書式を保持(16584)

6.3.3 Ericom Connect v7.5.2

[リリース日]

2016 年 5 月

[Ericom Connect 機能]
公開アプリケーションとグループが一意の ID を持つ

アプリケーションの起動にエンコードされた ID と名前を必要とする新しいセキュリティ・オプション

プロ・エディションでも起動分析が利用可能

「Preserve ClientName」メソッドの追加、オプションの「“CC#」メソッド

ConnectCli resourceDefinitions の追加

AccessPortal のバグを解決 - パスワードに特殊文字を使用可能

Linux 環境はサポートしておりません

[AccessPad 機能]

URI 機能を使用した Windows AccessPad の起動

Windows AccessPad の事前設定可能なショートカット

estp URL を登録するためのオプションをインストーラに追加

6.3.4 Ericom Connect v7.5.1

[リリース日]

2016 年 3 月

[Ericom Connect 機能]

Ericom Connect Linux セッションのサポート**(Linux 環境はサポートしておりません。)**

AccessServer for Linux (管理対象モードのみ) **(Linux 環境はサポートしておりません。)**

RemoteAgent for Linux (タイプ 2)**(Linux 環境はサポートしておりません。)**

タイプ 2 RemoteAgent 用の新しい RemoteAgent Web サービス

データのビジュアル化とビジネス・インテリジェンス用の Ericom Analytics (エンタープライズ)

データベースをバックアップ/復元するための CLI コマンド

すべてのコンポーネントの証明書をデフォルトにリセットするための CLI コマンド

アプリケーション・リストの最上位レベルに公開フォルダのコンテンツを表示可能 (AccessPortal、 AccessPad、AccessToGo)

ナビゲーション・パネルのコンテンツをより操作しやすいように並び替え

グリッドの新しいデフォルトパラメータ: 1、0、2 (以前は 2 1 5)

3 つの新しい「ログイン名形式」: 資格情報の省略(AccessPad 7.5 以上が必要)、ドメインの省略およびカスタム。

事前定義パラメータを受け取る、追加の SSO ページ: アプリケーション名、フォルダ名、フルスクリーン・モード

エンタープライズ・ライセンスで許可されるテナント数のデフォルトを 10 から 1,000 へ増加

EndUserSessionReportingView に新しいパラメータを追加

登録済みシステムのカスタム・アドレスとポートを指定する機能を追加

固定タイムゾーンの処理(11740)

Win2008R2 への Ericom Connect のインストール

AccessPortal にキーボード・ロケール設定オプションを追加

以下の CA 解決の追加: CA0000016532、CA0000016607、CA0000017772、CA0000018188、CA0000018930、CA0000019240、CA0000016384、CA0000013377、CA0000017013、CA0000018568、

CA0000019072、CA0000020912(2016 年 3 月に 8522 へコメントを追加)

[AccessNow 機能]

AccessNow ツールバー内の ALT+Tab ボタン

固定解像度を必要とするアプリケーション用の「Scale to FIt」の適用

Chrome とローカル・デバイス(Windows)間の直接コピー/ペースト

デフォルトの最小解像度を 768 x 600 に変更

以下の CA 解決の追加: CA0000011389、CA0000016173、CA0000016352、CA0000009575、CA0000009580、CA0000011463、CA0000014455、CA0000017781、CA0000018715、CA0000018812、CA0000001109、CA0000008917、CA0000009640、CA0000016102、CA0000017701、CA0000019039

[AccessPad/Blaze]

AccessPad スタート メニューのショートカット・アイコン

AccessPad 署名付き構成ファイルのサポート

以下の CA 解決の追加: CA0000018720、CA0000009603、CA0000017172

6.3.5 Ericom Connect v7.3.0

[リリース日]

2015 年 10 月

[管理機能]

マルチテナント

カスタマイズ可能な管理者の役割委任管理

ESG に、ローカル・サーバを使用するオプションを追加

ESG に、割り当てられたシステム・グループのみに接続するオプションを追加

ESG 接続のみに RADIUS を有効にする新しいオプションを追加

RADIUS のテナント対応

Configuration Analyzer ユーティリティを個別ダウンロードとして利用可能

インラインで RemoteAgent を 7.2 から 7.3 にアップグレードすることが可能に

新しいオプションの追加(例:「失敗したログイン」)

RemoteAgent に Windows 2008 32 ビットのサポートを追加(9347)

新しいクライアント「Access」ページを追加

Configuration Tool のクライアント・リンクを新しい「Access ページ」に移動(9006)

管理コンソールでの .lnk ファイルの公開

Microsoft Azure SQL のサポート(AWS RDS MS SQL に追加)

グリッド・コンポーネントと RemoteAgent 用の新しい切断の状態

AD 検索フィールドを 50 文字をサポートするように拡張(9209)

Secure Active Directory の資格情報を使用してグリッドを初期化する新機能

RemoteAgent が正式に Windows 10 に対応

グリッドからの切断時に RemoteAgent の情報を消去するオプション

修正されたバグ:

機能マトリックスの定義を満たすよう Ericom Connect Pro をアップデート (9472)

セッションの切断後に自動的に AccessPortal メニュー・バーを表示(9649)

ユーザビリティ向上のためにデフォルトのバインド値を更新(9007)

「パスワードを変更する必要があります」設定に関連する認証の修正(9002)

Active Directory 検索結果でのフル・ネーム表示(9211)

ESG 設定の順番の改善(8982)

「アプリとデスクトップ | プロパティ | 詳細」に「リダイレクト構成」セクションを追加(6543)

[AccessNow 機能]

タッチパッド・マウス

Chrome からローカルへの直接コピー

グループ・ポリシーを有効化した NLA のサポート

[AccessPad 機能]

AccessPad Windows でのデスクトップ・ショートカット/アイコンのサポート

AccessPad Windows でのローカル Windows OS からの SSO のサポート

AccessPad Windows x64 が利用可能に

AccessPad での NLA/TLS のサポート(アクセラレーション・モード中)

Mac AccessPad に Uniprint クライアントをバンドル(9620)

6.3.6 Ericom Connect v7.2.0

[リリース日]

2015 年 8 月

[管理機能]

Windows AccessPad でのサーバ・アドレスの受け入れ

Windows AccessPad MSI をサーバ・アドレスで事前定義可能

Windows AccessPad が Windows 10 に対応

Windows と Mac 用 AccessPad で Uniprint 互換対応

Amazon AWS SWL Cloud Database のサポート

修正されたバグ:

9007 - デフォルトのバインド値の更新

8978 - (AN) アプリケーション・モードでの CTRL+ALT+DEL を非表示化

8026 - RemoteAgent の再起動後に「マイ コンピュータ」の機能を維持

8750 - (AP) ウェルカム・ダイアログを非表示にするためのチェックボックスを追加

7442 - (AN) リストにあるキーボードを Auto-sense でアクティブにしない

7460 - (AN) オートキーボード用の 2 回のクリックを通知する iOS 上のメッセージを表示

7888 - (AN) ツールバーがメニュー・バーの下に隠される問題を解決

6860 - (AP) 画面の小さいデバイスでのデスクトップ・セッションでの問題を解決

7356 - (AP) Juniper との互換性を追加

ダイアログ 7431 - (AP) MSIE 11 での「ブラウザがサポートされていません」ダイアログの問題を解決

7884 - (AP) メニュー・ボタンが消える問題を解決

7984 - (AP) モニタのパフォーマンスを向上

8464 - (AP) 新しい PIN コードの問題を解決

8276 - (AP) 言語入力の問題を解決

8162 - (AP) Firefox での空のスクリーンの問題を解決

8028 - (AP) 最後のアプリケーションから切断した場合にリストを表示

8029 - (AP) マウスのバック・ボタンでセッションを切断しない

6.3.7 Ericom Connect v7.1.0

[リリース日]

2015 年 6 月

[管理機能]

管理コンソールの多言語サポート - 8 言語を追加

ビルトインの Configuration Analyzer

公開アイコンを変更するための ConnectCLI コマンド

追加のライセンス詳細が表示されるようアップデートされたシステム・ヘルス・ウィジット

アップグレード/再展開機能

SSO で暗号化パスワードを使用するオプション

テスト用の AccessPortal HTTP インターフェース

[エンドユーザ機能]

新しく改良された AccessPortal インターフェース

AccessNow 7.1 アップデート

AccessPortal URL は、7.0 での 「<サーバアドレス>/AccessPortal」から 「<サーバアドレス>/EricomXML/」に変更

[要件]

AccessPortal には IIS が必要なくなりました

RemoteAgent は Windows 10 上でテストを実施しました

AccessPad と AccessPortal は Windows 10 上でテストを実施しました

6.3.8 Ericom Connect v7.0.2

[リリース日]

2015 年 4 月

[メンテナンス・パッチ]

AccessNow のサイズ変更バグを修正

6.3.9 Ericom Connect v7.0.1

[リリース日]

2015 年 3 月 31 日

[管理機能]

管理コンソールに RADIUS を追加

管理コンソールの設定に、システム・レベルの設定を追加

ユーザ・リスト、登録済みシステム、Connect サービス用の新しいフィルタリング機能

一部のツールチップのテキストを強化

スタンドアロンの RemoteAgent での LUS のサポート

バグ修正

新機能について更新されたドキュメント

[セキュリティ機能]

強化された XTEA 暗号化

6.3.10 Ericom Connect v7.0.0

[リリース日]

2015 年 3 月 15 日

[管理機能]

Web ベースの管理コンソール

ヘルス・ステータス・ウィジェット

リソース起動分析

包括的なレポート機能

ConnectCLI コマンド・ライン・インターフェース

[エンドユーザ機能]

AccessNow v7.0 HTML5 インターフェース

AccessToGo v7.0 モバイル・クライアント

AccessToGo Connect v7.0 モバイル・クライアント

AccessToGo Sector v7.0 モバイル・クライアント

AccessPad Windows 3.4、AccessPad Mac 3.1 ネイティブ・クライアント

ダイレクト・シングル・サインオン・インターフェース

AccessPortal ログイン・ポータル

[セキュリティ機能]

HTTPS 互換性

リモート・アクセス用の Ericom Secure Gateway の搭載

RADIUS 2 要素認証方法のサポート

サードパーティの信頼された証明書のサポート

[インフラストラクチャ機能]

PoC と本番環境のインストーラ・オプション

高可用性のためのビルトインされた Ericom グリッド

[要件]

Microsoft Active Directory

Microsoft SQL または SQL Express 2012

Microsoft IIS 8 以上

Ericom Connect グリッド・コンポーネント用の Windows 2012R2

ターミナル・サーバとリモート・デスクトップ・サーバには Windows 2008 以上をお勧めします

ワークステーション・アクセス(物理・仮想デスクトップ)には Windows 7 以上をお勧めします

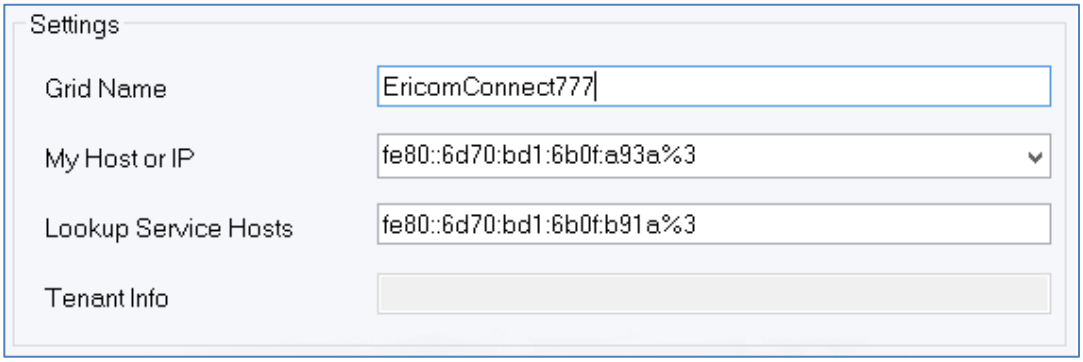
6.4 サーバ・サイドの FAQ

6.4.1 Ericom Connect のインストール用にサーバを検証する

Configuration Analyzer を Ericom Connect Configuration Tool とは別に起動することができます。 これは、Ericom Connect をインストールする時間と労力をかける前に、Ericom Connect で使用するサーバを検証するのに役立ちます。

6.4.2 IPv6 マシンをグリッドに参加させる

IPv6 を使用しているマシンをグリッドに参加させるには、「Lookup Service Hosts」フィールドに IPv6 アドレスを入力します。 IPv6 以外のアドレスが使用されている場合、エラーが表示されます。



6.4.3 ホストの IP アドレスの変更

ホストの IP アドレスを変更した場合、RemoteAgent をグリッドに接続することができなくなり、Configuration Tool 以下のエラーが表示されます:

Updating configuration files ... done.

Searching for grid EricomConnect ...
*** Cannot find EricomConnect ***

これを解決するには、RemoteAgent の Configuration Tool を起動し、「%COMPUTERNAME%」を使用します(システムに 2 つ以上の IP アドレスが存在する場合、この変数により正しい IP アドレスへ誘導されることを確認してください)

6.4.4 最初の Connect 管理者を割り当てることができない

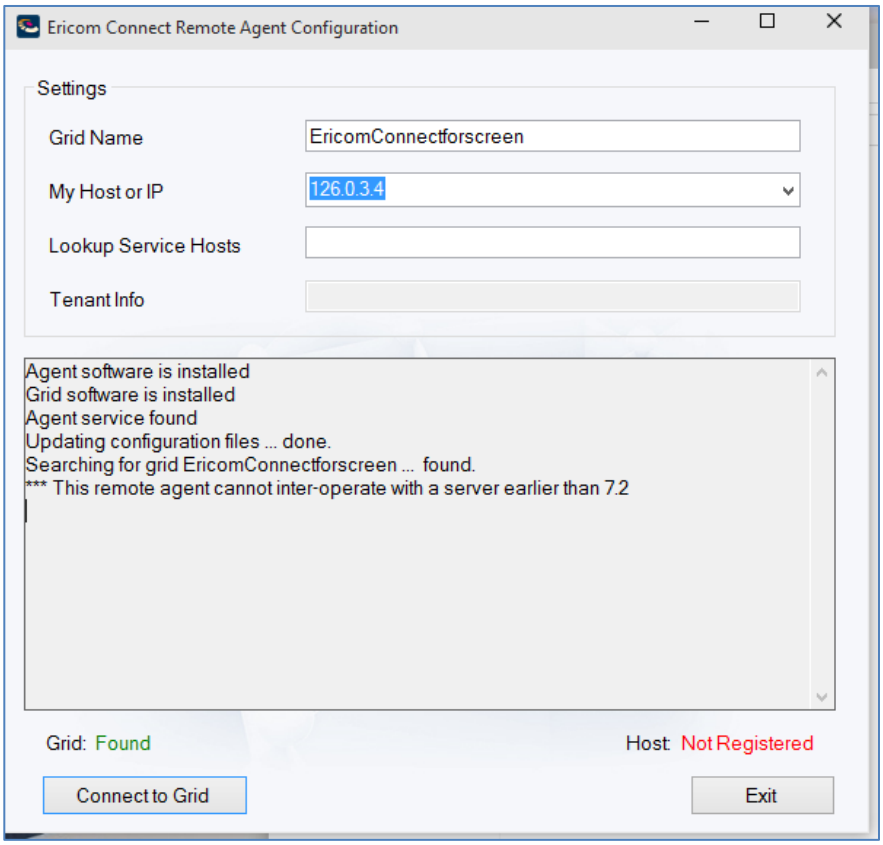
ドメイン管理者ユーザには、ユーザ・ログオン名とドメイン名が定義されない場合があります。 「Active Directory ユーザとコンピュータ」に移動し、目的の管理者ユーザの「アカウント」タブ内のすべての項目が定義されていることを確認してください。 例:

6.4.5 グリッド・コンポーネントに同じバージョンを使用する

Ericom Connect コンポーネントは、同じバージョン内で動作するよう設計されています。 古いバージョンの RemoteAgent を 新しいバージョンの グリッドに接続できる場合がありますが、同じバージョンとなるようにすべてのグリッド・コンポーネントをアップグレードしてください(例:EUWS)。 グリッド・コンポーネントが一致しない場合、「パラメータのカウントの不一致」のエラーが表示されます。

6.4.6 古いバージョンのグリッドとの互換性がない RemoteAgent

新しいバージョンの RemoteAgent で 古いバージョンのグリッドに接続を試みた場合、初期化プロセスでエラーが表示されます。



RemoteAgent をグリッド・コンポーネントと同じバージョンにアップデートしてください。

6.4.7 SQL での Windows 認証

SQL アクセスに Windows 認証を使用する場合、明示的に Ericom Connect 管理者ユーザを管理者グループに追加することが必要です。さらに、Ericom Connect システムが登録されているドメインに、その管理者ユーザが登録されている必要があります。

6.4.8 ビルトイン証明書の復元

ESG、管理 Web サービス、およびエンドユーザ Web サービス用の元の自己署名証明書を復元するには、Ericom Connect サーバで次のコマンドを実行します:

ConnectCLI ConfigureCertificates FindByExtension 1.2.840.113556.1.8000.2554.57748.52896.21682.18417.45066.8514989.679433.1

6.4.9 AccessPortal HTTP ポイントの無効化

「接続サービス」|「エンドユーザ Web サービス」に移動します

「HTTP 有効化」を「いいえ」に設定します。

この変更後に EUWS サービスを再起動します (7.1)

HTTP を使用することにより、接続のトラブルシューティング中の SSL エラーを回避できます。

6.4.10 AccessServer ポートの変更

AccessServer では、デフォルトで 8080 ポートを使用して通信が行われます。 このポート値は、次のレジストリから変更することができます:

[HKEY_LOCAL_MACHINE\SOFTWARE\Ericom Software\Access Server\CLIENT Side]\"Port"=

AccessServer にカスタム値を使用する場合、適用した変更が約 1 分で自動的に RemoteAgent に認識されます。 管理者に必要とされるサーバ・サイドの追加設定はありません。

6.5 サーバ・サイドの既知の動作

6.5.1 Database Server User は英語の名前である必要があります

「Database Server user name」は、英語である必要があります。 デフォルトでは、この値はグリッドと同じ文字列に設定されており、英語の文字列を使用して再入力する必要があります。 (Connect 7.0.x が対象です)

6.5.2 レポート: Access Server フィルタには RemoteAgent が必要です。

AccessServer ステータスには、RemoteAgent が必要です。 RemoteAgent サービスが「実行中」でない場合、AccessServer ステータスは無効となります。

6.5.3 クロス・ドメイン・グループはサポートされません

クロスドメイン・グループ・メンバーシップはサポートされていません。 例えば、あるドメインのユーザ/グループが別ドメインのグルー

プのメンバーである場合、別のドメインに割り当てられたリソースは、前述のユーザ/グループからアクセスすることができません。

6.5.4 レポートの結果における負の数

Ericom グリッドのすべてのマシンは、共通のタイム・ソースを使用して同期する必要があります。 マシンが同期されていない場合、レポートの時系列の結果に負の数が表示される場合があります。

6.5.5 信頼された証明書によるページの中断

システムにインストールされた信頼された証明書を Connect に使用する場合、その証明書は「エクスポート可能」としてシステムにインストールする必要があります。 証明書が適切にインストールされていない場合、各コンポーネントにアクセスすることができなくなります。 証明書が適切にインストールされたことを確認するには、HTTPS アクセス用の IIS でその証明書を設定します。 IIS で証明書が動作する場合、Connect でも同様に動作します。

6.5.6 EUWS グローバル証明書の問題

EUWS でのグローバル証明書の設定に関する既知の問題は次のとおりです:証明書をグローバル・レベルで設定した場合に、マシンの追加で問題が発生する可能性があり、新しいサーバに「Unable to function」というエラーが表示されます。

6.5.7 RemoteAgent が存在しない場合のセッション・リダイレクト

RDS ファームを使用する場合、ユーザがセッションを開始した際にセッションのリダイレクトが発生する場合があります。

例えば、ログインするユーザが他のホスト上に切断されたセッションを持つ場合です。リダイレクトが行われたターゲット・ホストに RemoteAgent がインストールされている場合、Connect 管理(ユーザ)コンソールにユーザの RDP セッション・データが正しく表示されます。

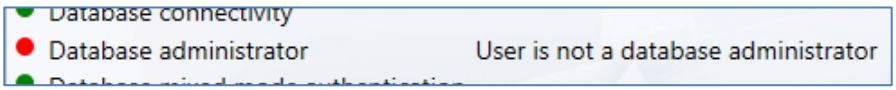
しかし、リダイレクトが行われたターゲット・ホストに RemoteAgent が存在しない場合、ユーザのセッション・データは空になります。 対応するレポートのエントリでは 最終的なホスト・アドレスは表示されませんが、元のリダイレクトが発生したホストは表示されます。 したがって、リダイレクト機能は適切に実行されるものの、レポートのデータには最終的なホスト・アドレスが反映されません。

このレポートの不一致を避けるには、可能な限りすべての宛先ホスト上に RemoteAgent をインストールすることをお勧めします。

6.5.8 Cloud DB での Configuration Analyzer のエラー

Amazon AWS SQL と Microsoft Azure SQL でのテストの際、Configuration Analyzer により「User is not a database administrator(ユーザがデータベース管理者ではありません)」というエラーが返されます。 Ericom Connect は適切な資格情報を使用して

SQL データベースと正常に通信できるようになるため、このエラーは無視します。



6.5.9 サービスの再起動後に管理者がオフラインとなる

Admin サーバ・サービスを再起動した後、そのサービス用の信頼された証明書がインストールされていない場合は、次のエラー・メッセージが表示されます:

ログイン・プロンプトを回復するには、Web ページを強制的に更新します。 今後この問題が発生するのを避けるには、Admin サービス用の信頼された証明書をインストールします。

6.5.10 RemoteAgent WMI エラー

RemoteAgent Configuration Tool により次のメッセージが表示される場合があります:

Unable to retrieve all the required information from WMI. Please see the documentation on how to proceed.(すべての必要な情報を WMI から取得することができません。 続行する方法については、マニュアルを参照してください)

このメッセージは、システム上で WMI リポジトリが破損している可能性を示しています。

詳細については、WMI Diagnosis Utility を実行してください:
https://www.microsoft.com/en-us/download/details.aspx?id=7684
RemoteAgent では、システム・レベルのイベント(例: CPU 使用率)を監視するために、WMI が使用されます。

6.5.11 セッションの ClientName の CC# とは

Ericom Connect 7.5.1 およびそれ以前のバージョンでは、RDP セッションの 「ClientName」の末尾に「CC#」という文字列が追加されていました。 この文字列は、追跡のためにセションを識別するために使用されます。 一部のアプリケーションでは、「ClientName」は「CC#」ラベルのない、ネイティブな状態を維持する必要があります。Ericom Connect 7.5.2 以降では、Ericom Connect サービス、AccessPad、RemoteAgent のバージョンが 7.5.2 以降であれば、「CC#」ラベルは必要なくなりました。バージョン 7.5.2 で「CC#」識別子の使用を無効化するには、「システム構成 | システム設定」に移動し、「RDP クライアント名を保持(Preserve RDP Client Name)」を「はい(Yes)」に設定します。

「RDP クライアント名を保持(Preserve RDP Client Name)」が有効化され、古いバージョンのクライアントが使用される場合、以前と同様「CC#」が「ClientName」に追加されます。

バージョン 7.6 以上では、CC# の存在は自動で設定され、手動設定は必要ありません。

6.5.12 ファームと NLA で IP アドレスを使用する

Ericom Connect を使用して、NLA を有効化したホストの RDS ファームからセッションを起動する場合 - FQDN ではなく静的 IP を使用するよう RemoteAgent が設定されます。

この動作は、DNS サーバによってファーム名がファームのホスト IP の 1 つへと名前解決されるために発生します。 名前解決された IP は、各 DNS 呼び出しごとに異なる場合があります。 ファーム名によって選択されたホストが、実際のサーバ・アドレス(AccessServer の接続先)と異なる場合、NLA 認証は失敗します。

6.5.13 IPv4 または IPv6 の使用(どちらか一方のみ)

グリッドのコンポーネントは、環境全体にわたって一貫したアドレスによって認識される必要があります。 システム上の同じ NIC を参照している場合であっても、IPv4 と IPv6 のアドレスを混合して一致させないでください。

また、環境全体にわたって変数 %COMPUTERNAME% のアクセス先が同じであることを確認してください。 例えば、Business Logic Controller サービスによって ESG gateway.acme.com を IPv6 アドレスに解決している一方で、ESG サーバによって 変数 %COMPUTERNAME% を IPv4 アドレスへと解決している場合、この 2 つのエントリは同期されず、Business Logic Controller によって ESG システムが認識されません。

6.5.14 ユニバーサル・アプリケーションを公開できない

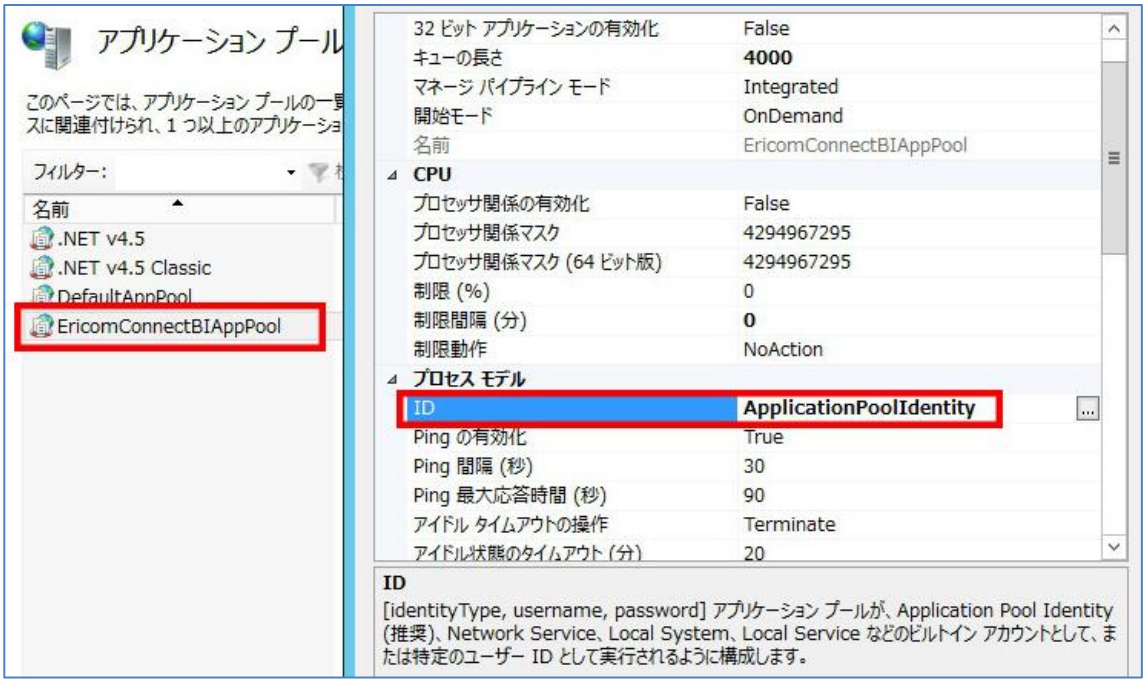
マイクロソフト・ユニバーサル(Metro としても知られています)は、公開することができません。 Microsoft Edge ブラウザは、このようなアプリケーションの一例です。

6.5.15 Ericom Analytics でデータベースを読み込むことができない

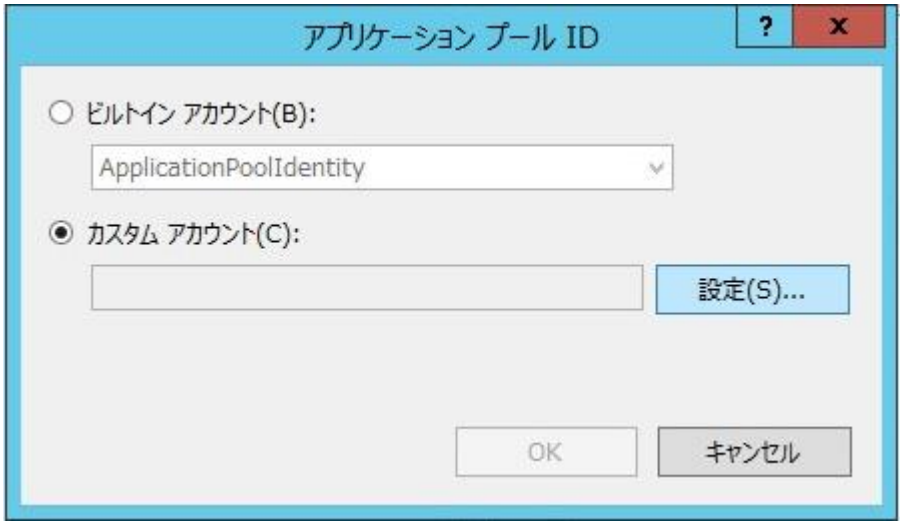
Ericom Analytics で Ericom データベースに接続できない場合は、IIS アプリケーション・プールがデータベースの読み込みが可能なアカウントで設定されていることを確認してください。 以下の手順を実行して、アカウントの確認・設定します

- Global.aspx (C:\Program Files\Ericom Software\Ericom Analytics) のデータベース接続文字列を確認・設定します。

  AdHocSettings.SqlServerConnectionString = @"server=<SQL サーバ>=<データベース名>;Trusted_Connection=SSPI;";
- IIS マネージャを起動し、「アプリケーション プール | EricomConnectBIAppPool」へ移動します。
- 「EricomConnectBIAppPool」を右クリックし、「詳細設定」を選択します。



- ID の「参照」ボタンをクリックします。
- カスタム アカウントをクリックし、Ericom Connect データベースにアクセスできるユーザの詳細を入力します。



- IIS をリセットします(iisreset.exe)

6.5.16 Windows 7 のセッション・シャドウイング

Windows 7 ホスト上でのセッション・シャドウイングを許可するには、以下の設定が構成されていることを確認します:

- ポート 445 上の 受信 TCP トラフィックを許可するよう、ホストのファイアウォールを設定します
- 以下のレジストリ・キーの値を「1」に設定します:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\AllowRemoteRPC

6.5.17 MS ユニバーサル/Metro アプリケーションの公開

マイクロソフト・ユニバーサル・アプリケーション(Metro として知られます)は、LINK または EXE ファイルとして公開することができません。 ユニバーサル・アプリケーションを公開するには、explorer.exe をアプリケーションとして公開し、AppUserModelId をアプリケーションのパラメータとして入力します。

explorer.exe shell:AppsFolder\Microsoft.WindowsReadingList_8wekyb3d8bbwe!Microsoft.WindowsReadingList

AppUserModelId およびそれを Windows でアプリケーション・ショートカットを作成するための詳細な方法については、インターネットで検索してください。

6.5.18 SQL データベースの資格情報を変更する

Ericom Connect データベースに使用されている資格情報を変更するには、以下を実行します:

- すべての Connect グリッド・サービスを停止します
- 各グリッド・マシン上で、次のファイルを編集します: c:\programdata\ericomconnect\dbconnection.xml
- ファイル構造は、以下のように表示されます:

```
<?xml version="1.0" encoding="utf-8"?>
<DatabaseConfiguration>
  <Server>.</Server>
  <Database>ConnectionBroker</Database>
  <User>ConnectUser</User>
  <!-- Replace EncryptedPassword by Password to change the password -->
  <EncryptedPassword>aslkajqoiwlqnas</EncryptedPassword>
  <Timeout>300</Timeout>
</DatabaseConfiguration>
```

- 新しいパスワード(例: abc123)を入力するには、「<EncryptedPassword>」 の行を「<Password>abc123</Password>」に置き換えます。
- 新しい XML があるマシンから、グリッド・サービスを再起動します。
- システムの起動後、「<Password>」の値を、「<EncryptedPassword>」に置き換えることができます。

6.5.19 最小パスワード長

Ericom Connect では、パスワードの長さが最低 3 文字必要です。 ユーザの Active Directory パスワードが 2 文字である場合、ポータル(e.g. AccessPad)にはログインできますが、アプリケーションを起動する際にエラーが発生します。

6.6 エンドユーザのトラブルシューティング

6.6.1 MSTSC/RDP を使用したテスト

Ericom クライアントは、新しいセッションを開始するために RDP の可用性に依存しています。 RDP にアクセスできない場合、Ericom クライアントを接続することができません。 接続の問題を Ericom に報告する前に、mstsc.exe を使用したアクセスがリモート・ホストで使用可能であることを確認してください。

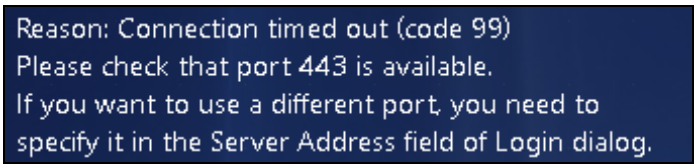
6.6.2 ポート接続の確認

ポートの可用性は、telnet.exe コマンド・ライン・ユーティリティを使用して確認できます。 コマンド・プロンプトで、サーバのアドレスを telnet し、確認するポートを指定します(例: telnet.exe server.ericom.com 443)。 応答が受信された場合、そのポートは telnet コマンドを実行しているシステムからアクセス可能です。 一部のオペレーティング・システムには telnet.exe が含まれていないことに注意してください。

応答が受信されない場合、Ericom Connect 環境がエンドユーザ・デバイスからアクセス可能であることを確認します。 一般的な問題は、リクエストされたポートをブロックしているファイアウォールが通信経路に存在していることです。

6.6.3 接続タイムアウト

エラー・メッセージ: Connection timed out (code 99) Please check that port 443 is available. If you want to use a different port, you need to specify it in the Server Address field of the Login dialog.(接続はタイムアウトしました(コード 99) ポート 443 が使用可能であることを確認してください) 別のポートを使用する場合は、ログイン・ダイアログのサーバ・アドレス・フィールドを指定する必要があります)



考えられる理由: Connect サーバがアクセスできない状態にあります。アドレスとポートの接続を確認してください。

6.6.4 AccessPortal の変更時のブラウザ・キャッシュのクリア

AccessPortal に関連する設定を変更する場合(例: EUWS ポートまたは ESG ポートの変更)、変更を反映するために、エンドユーザはブラウザ・キャッシュをクリアする必要があります。

6.6.5 IE で 検索テキストを選択できない

Microsoft IE または Edge で AccessPortal を使用する場合、検索フィールドに入力したテキストをマウスでハイライトすることができません。 これはブラウザの制約によるものです。

(7.1, 7.3)

6.6.6 Firefox 上の AccessPortal のスクロールが遅い

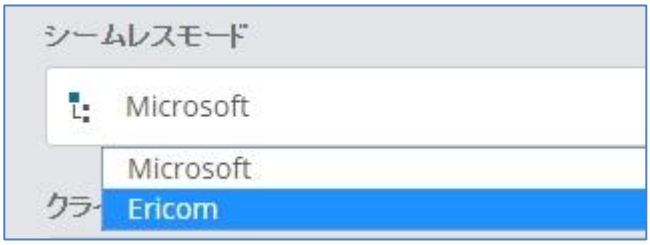
AccessPortal のアプリケーション・リストのスクロールが遅くなるという Firefox の既知の問題があります (https://github.com/cubiq/iscroll/issues/577)。 Firefox でのこの既知の動作を避けるには、別のブラウザを使用してください。

6.6.7 新規ユーザのログインが切断される

これは、セッション・ホストから起動するシームレス・アプリケーションに影響する既知の問題です。

負荷のかかったセッション・ホストにユーザが誘導された場合、新しいユーザ・プロファイルの作成にかかる時間がアイドル接続時間を超えることがあり、結果としてセッションが切断されます。 ユーザが再度シームレス・アプリケーションを起動すると、この時点ではユーザ・プロファイルがセッション・ホストに存在するため、セッションが正常に接続されます。

解決策は、「シームレスモード」を「Microsoft」から「Ericom」に変更することです。

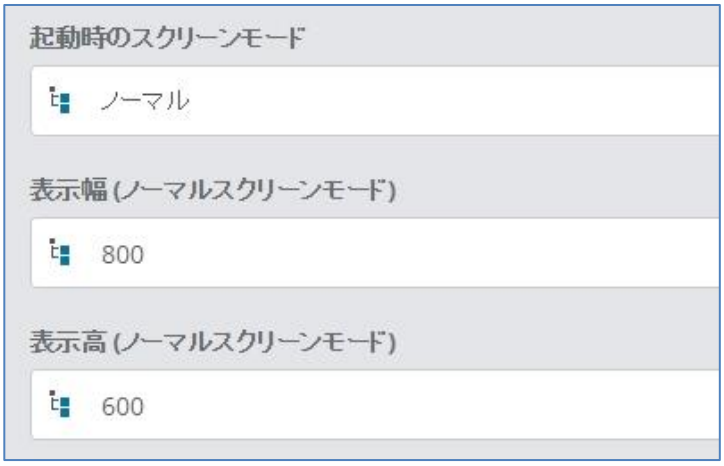


6.6.8 印刷アドオンでの印刷ができない

一部のサードパーティ製アドオン・ソリューション(Tricerat、Net2Printer など)では、プリンタ・クライアントのビット・レベルを AccessPad のビット・レベルと一致させる必要があります(32 bit の AccessPad では 32 ビットのプリンタ・クライアントを使用する必要があります) Uniprint を使用する際には例外があり、ビット・レベルはクライアントと一致する必要がありません。 結果として、AccessPad(32 bit) は、x64 OS 上の Uniprint x64 と共に動作可能です。

6.6.9 AccessNow タブレットの解像度が 800x600 に設定される

AccessNow では、幅 800 ピクセルと高さ 600 ピクセル以下の解像度のデバイスにおいて、 800x600 ピクセルの最小解像度が使用されます。 これらの値は、Ericom Connect 管理コンソールの「表示幅」と「表示高」のパラメータを設定することで変更できます。 この設定を行うには、「起動時のスクリーンモード」が「ノーマル」に設定されている必要があります。



6.6.10 Firefox 44 で音声が出力されない

Firefox バージョン 43 と 44 上の AccessNow では、オーディオ再生は機能しません。 バージョン 40 へ戻すか、バージョン 45 へアップグレードすることでこの問題は解決します(2016 年 3 月 1 日時点で、バージョン 45 はベータ版です)。

6.6.11 USB ドライブのリダイレクト

ダイナミック・ドライブ(例:セッション開始後にプラグインされる可能性のあるドライブ)をサポートするようセッションを設定するには、「Ericom Connect 管理コンソール」| 「詳細タブ」 | 「リダイレクトするドライブ」 に移動し、値「DynamicDrives」を入力します。

6.6.12 iOS 上の AccessNow は 1 つのファイルアップロードのみ

AccessNow の iOS ユーザは一度に 1 つのファイルしかアップロードできません。

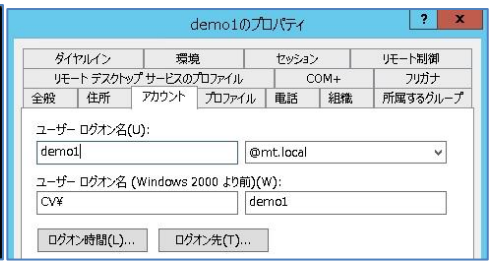
6.7 認証のトラブルシューティング

6.7.1 ログイン: ドメインの定義

Ericom Connect にサインインする Active Directory ユーザは、各ユーザ・アカウントの「プロパティ」でドメインが定義されている必要があります。定義されていない場合、サインインに失敗する可能性があります。 ドメインを設定するには、Active Directory でユーザの「プロパティ」画面を開き、「アカウント」タブを選択します。 「ユーザーログオン名」の隣に希望するドメインを選択します。

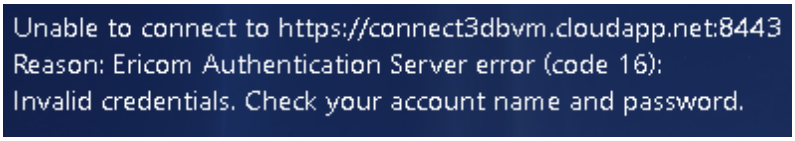
6.7.2 ログイン: ユーザ・ログオン名の定義

ユーザが Access コンポーネントの一部にアクセスできない場合、そのユーザ・アカウントの「ユーザー ログオン名」が定義されているかどうかを確認してください。 次の例では、「admin」ユーザはログインすることができません。 「demo1」ユーザは、アカウント・パラメータが適切に定義されているため、ログインが可能です。



6.7.3 認証サーバのエラー

エラー: Unable to connect to <アドレス> Ericom Authentication Server error (code 16): Invalid credentials. Check your account name and password.



考えられる理由:

- ユーザ名とパスワードを再度確認します。
- 正しいドメイン名が指定されていることを確認します。

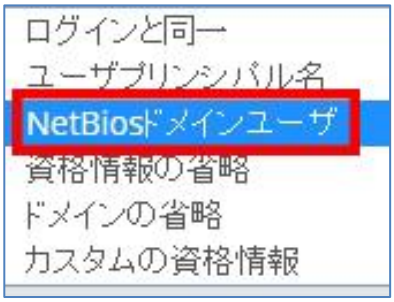
6.7.4 Windows 8/2012 でのログイン・フォーマットの問題

Windows 8.0 と 2012 (R2 以外)では、UPN フォーマットされたユーザ名「user@domain」の動作を妨げる、オペレーティング・システムのバグがあります。 NetBIOS 形式「domain\user」はサポートされています。 この問題は、8.1(Server 2012 R2) では修正されています。

この既知の問題への対策として、以下の 2 つの方法があります:

- Access クライアントのいずれかを使用して Connect にサインインする場合、 「user@domain」形式ではなく、NetBIOS 形式 (domain\user) を使用します。
- Connect 管理コンソールを使用して、システムまたはグループ・レベルの「詳細」タブに移動し、「ログイン名フォーマット」の設定を行います。 NetBIOS 形式を使用するには、「NetBios ドメ

インユーザ」を選択します。



6.7.5 SSL ネゴシエーションの失敗

Secure Gataway 経由で AccessNow を使用してアプリケーションまたはデスクトップへの接続を試みた場合、次のエラーが表示される場合があります: 「Gateway:SSL negotiation with host faile. (ゲートウェイ: ホストとの SSL ネゴシエーションに失敗しました)」

このエラーを解決するには、以下の手順を実行してください。

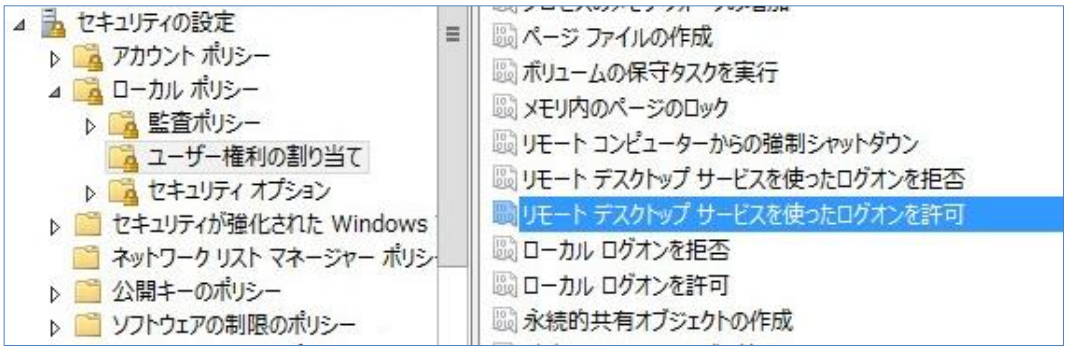
- AccessServer 管理コンソールを開きます
- 「General」タブで AccessServer サービスを停止します
- 「Security」タブに移動します
- 「Restore Default」ボタンをクリックします
- 「MMC」を開き、「証明書」のスナップインを開きます

- 「ローカルコンピューター」| 「個人」の下で、「Ericom Self Signed Certificate」を見つけ、それを削除します。
- AccessServer サービスを再起動すると、証明書が再作成されます。
- ESG を経由して接続を再試行します

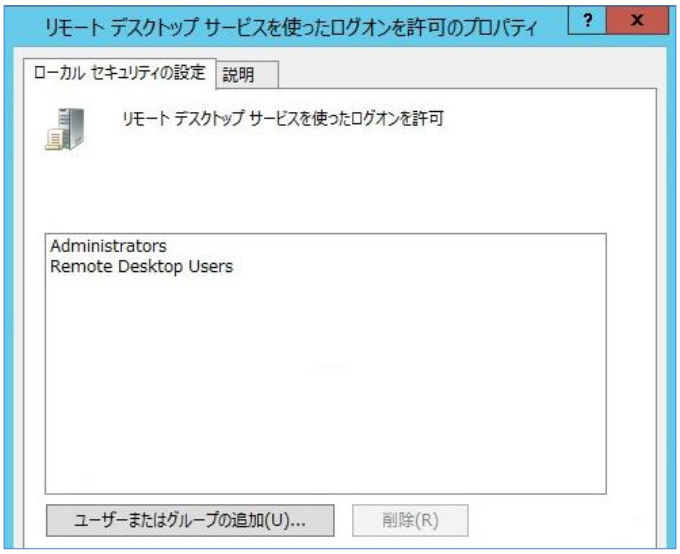
6.7.6 Windows 2012 での RDP アクセス許可の問題

Windows 2012 では、ユーザを Active Directory の「Remote Desktop Users」グループに追加するだけでは、システムへの RDP はユーザに許可されません。 ユーザ(またはユーザのグループ)には、ローカル・アクセスも必要とされます。 この設定を行うには:

- Windows 2012 サーバで「ローカル セキュリティ ポリシー」コンポーネントを開きます。
- 「ローカル ポリシー」を展開し、「ユーザー権利の割り当て」を選択します。ポリシーの一覧が表示されます。「リモート デスクトップ サービスを使ったログを許可」という名前のポリシーを右クリックし、「プロパティ」を選択します。



- 目的のユーザまたはグループをポリシーに追加します。



6.8 パラメータ値とエラーコード

6.8.1 パラメータの説明と値

	設定名	説明	デフォルト	値の範囲
管理 Web サーバ	サービスの Keep Alive 間隔 (秒)	グリッドとの Keep Alive の間隔	10	10-3600
	Connect Admin アイドルタイムアウト (秒)	「X 秒でログアウトします」という警告メッセージを表示するまでのアイドル時間	300	10-2678400

	Connect Admin アイドル警告(秒)	実際に管理者セッションをログオフするまでの「X 秒でログアウトします」という警告メッセージのカウントダウン時間	30	10-2678400
EUWS	エンドユーザポータルセッションの Keep Alive 間隔(秒)	エンドユーザのポータル・セッションとグリッドの Keep Alive	300	10-3600
	サービスの Keep Alive 間隔 (秒)	エンドユーザの Web サーバとグリッドの Keep Alive の間隔	10	10-3600
ESG	サービスポイント当たりの最大接続数	ESG とサービス・ポイント(サービス・ポイント = EUWS アドレス+ポート)の間で開くことのできる 最大同時 HTTP セッション数	32	2-最大

	リクエスト当たりの最大サービスポイント試行数	HTTP リクエストごとの、エラーを返すまでにリトライする EUWS の最大数	3	1-最大
	サービスの Keep Alive 間隔 (秒)	ESG サーバとグリッドの Keep Alive の間隔	10	10-3600
	新しい接続のタイムアウト(秒)	新しい RDP セッション用の認証トークンの有効期限	60	2-最大
	再接続タイムアウト(秒))	RDP セッション再接続用の認証トークンの有効期限	60	2-最大
	リダイレクトタイムアウト(秒)	RDP セッション・リダイレクト用の認証トークンの有効期限	60	2-最大
RemoteAgent	サンプリングレート(秒)	CUP とメモリ消費量のポーリングの間隔	1	1-最大
	最小サンプリングレ	CPU/メモリのサン	60	1-最大

	ート(秒)	プリングが変更された際にグリッドに通知するメッセージの最小間隔時間		
	AccessServer サンプリングレート	Access Server のステータスを確認する間隔	20	1-最大
	リソースサンプリング	CPU の変更を送信する前に収集する CUP とメモリ消費量のサンプルの最小数	30	1-最大
	通知しきい値(%)	更新をトリガするメモリまたは CUP の変更量(パーセンテージ)	25	0-100
	サービスの Keep Alive 間隔 (秒)	Remote Agent サーバとグリッドの Keep Alie の間隔	300	1-3600
	リソースサンプリングレートの確認(秒)	マシンでプログラムの追加または削除が行われたかを	300	10-最大

		検証する間隔		

6.8.2 エラーコードの定義

ログイン・エラー・メッセージ	考えられる理由:
ログインに失敗しました - 資格情報が無効です (Login Failed – Invalid Credentials)	ユーザ名および/またはパスワードが間違っています
ログインに失敗しました - ロックされています (Login Failed – Locked out)	そのユーザ・アカウントはロックされています。継続するには、アカウントのロックを解除します
ログインに失敗しました - Radius パスワードが拒否されました (Login Failed – Radius Password Rejected)	RADIUS 認証に入力した値が拒否されました。
ログインに失敗しました - Radius のアクセスが拒否されました (Login Failed – Radius Access Rejected)	RADIUS 認証へのアクセスが拒否されました。ユーザが登録されていることを確認してください。
ログインに失敗しました - ライセンスを取得することができません (Login Failed – Unable to obtain a license)	サーバ上のライセンス・エラーのためにログインが失敗しました。ライセンスが有効であることを確認してください。
ログインに失敗しました - 認証が拒否されました (Login Failed – Authentication Rejected)	一般的な認証エラーが発生しました。 このエラーの例としては、ユーザのパスワードの有効期限が切れているにも関わらず、

	パスワードの変更がユーザに許可されていない場合に発生します。詳細については、「ユーザ | 失敗したログイン(Users | Failed Logins Report)」 のレポート」を確認してください。
ログインに失敗しました - ログイン時にエラーが発生しました (Login Failed – An error occurred during login)	ログイン時に予期しないエラーが発生しました。サーバのエラー・レポートで、このエラーの完全な説明を確認してください。テクニカル・サポートまでお問い合わせください。
以前に別のテナントにログインしています (You have previously logged in to a different tenant)	このユーザは、以前に別のテナントにログインしたことがあり、このテナントにログインできない場合があります。 管理者が Connect CLI EndUserTenantReassign コマンドを使用して、割り当てられたテナントをリセットすることができます。
Your session is no longer valid. Please login again (セッションが有効ではありません。再度ログインしてください。)	クライアントのセッションが期限切れになっているため、ログオフして再度ログインする必要があります。

パスワードの通知	理由
パスワードの有効期限が切れています (Your password has expired)	パスワードの有効期限が切れているため、変更する必要があります。

ログインする前にパスワードを変更する必要があります (You must change your password before logging in)	このアカウントは、ログインの前にパスワードを変更する必要があります。
2 つのパスワードが一致しません (The two passwords do not match)	パスワードを変更する際に、2 つのパスワードが一致していません
古いパスワードが間違っています (The old password is not correct)	パスワードを変更する際に、入力した古いパスワードが間違っています
The password does not meet the password policy requirements.Check the minimum password length, password complexity and password history requirements (パスワードはパスワード・ポリシーの要件を満たしていません。パスワードの最短の長さ、パスワードの複雑性、およびパスワード履歴の要件を確認してください)	入力した新しいパスワードは、パスワードの要件を満たしていません。 パスワードについては、システム管理者に相談してください。

6.9 テクニカル・サポートのお問い合わせ先

オンライン・フォーラム

質問の投稿や他のユーザからのレビューや回答・反応を参照するには、Ericom のオンライン・コミュニティ・サイトを参照ください。

https://www.ericom.com/communities/forums

Email/お電話

Ericom の顧客支援部門宛に電子メールまたはお電話でテクニカル・サポートを依頼いただくには、有効な Ericom メンテンナス・サブスクリプションが必要です。 依頼を送信する際には、迅速な処理のために、以下の情報をご提供ください:

Webサイトでのケースのオープン：
http://www.ericom.com/Issues_Connect.asp

- エラー・メッセージの画像などを添付してください
- 発生した問題を再現するための手順を記載してください
- 影響を受けているユーザ数を記載してください: 1 ユーザ、一部、またはすべて
- エンドユーザのデバイスのオペレーティング・システムを記載してください(例: Android タブレット)
- Ericom Connect サーバのオペレーティング・システムを記載してください(例: Windows 2012 R2)
- ターミナル・サーバのオペレーティング・システムを記載してください(例: WIndows 2012 R2)
- 問題が発生した際、環境で何か変更を行ったものがあれば記載してください。

- ケースは電子メール(ca@ericom.com)でオープンすることが可能です。より迅速なサービスのために上記情報をすべて提供してください。
- 電話でのお問い合わせはお近くの Ericom オフィスまたはパートナーにご連絡ください。