RSA® Authentication Manager 8.0
管理者ガイド

商標について

RSA、RSA のロゴ、EMC2、EMC は、EMC Corporation の登録商標または商標です。その他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。RSA の商標の最新のリストについては、。**http://japan.emc.com/legal/emc-corporation-trademarks.htm#rsa** を参照してください

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMC が著作権を保有しており、ライセンス契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、ライセンス契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本ライセンス契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。
本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

本製品は RSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、製品 DVD の Third-Party Licenses フォルダをご参照ください。

暗号技術に関するご注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

免責事項

本書に記載されている EMC ソフトウェアを使用、複製、および配布するには、適切なソフトウェア・ライセンスが必要です。

EMC Corporation は、この資料に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。EMC Corporation は、本文書に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示の保証はいたしません。

Copyright © 1994-2013 EMC Corporation. All rights reserved.（不許複製・禁無断転載）
2013 年 3 月

目次

はじめに 15
本書について 15
RSA Authentication Manager 8.0 マニュアル 15
関連ドキュメント 16
サポートとサービス 16
カスタマー サポートにご連絡される前に 17

第 1 章：RSA Authentication Manager 概要 19
RSA Authentication Manager の概要 19
多要素認証 19
RSA Authentication Manager の主要なコンポーネント 20
プライマリ インスタンス 20
レプリカ インスタンス 21
アイデンティティ ソース 21
RSA 認証エージェント 22
Web ベース リソースのリスク ベース認証 22
RSA RADIUS の概要 23
Web Tier 23
Self-Service 24
ロードバランサ 25
RSA SecurID 認証の概要 25
RSA SecurID 認証プロセス 26
RSA SecurID トークン 26
SecurID 認証における RSA Authentication Manager の役割 29
On-Demand 認証 30
On-Demand 認証ユーザー ログオンの例 30
リスクベース認証 31
リスク ベース認証による、パスワード盗難時のデータ損失の防止 31
リスク ベース認証のしくみ 32

第 2 章：RSA Authentication Manager の管理の準備 33
Security Console 33
Security Console へのログオン 34
Security Console のカスタマイズ 34
Security Console の保護 38
Security Console の認証方式の構成 38
アイデンティティ ソース 39
LDAP ディレクトリのデータ 40
内部データベースのデータ 40
セキュリティ ドメインの概要 41
ユーザーの編成と管理 41
ポリシーの適用 42
管理者の権限適用範囲 42

セキュリティ ドメインとポリシー 43
セキュリティ ドメインの追加 44
デフォルトセキュリティ ドメイン マッピング 46
DNS（ドメイン ネーム システム）の更新計画 47
管理者ロールの概要 47
管理者ロールのタイプ 47
管理者ロールの割り当て 48
管理者ロールのコンポーネント 49
事前定義の管理者ロール 54
管理者ロールの設定 60
管理者ロールの権限適用範囲と権限 62
管理者ロールの追加 64
管理者ロールの割り当て 65
管理者の利用可能な権限の表示 66

第 3 章：認証エージェントの導入 69
RSA 認証エージェント 69
認証エージェントのタイプ 69
RSA Authentication Agent の取得 69
認証エージェントの導入 70
Authentication Manager 構成ファイルの生成 71
認証エージェントの追加 72
暗号化用のノード シークレット 75
ノード シークレットの手動送付 75
ノード シークレットの管理 76
Node Secret Load ユーティリティによるノード シークレットの更新 77
エージェントの自動登録 78
エージェントの自動登録を許可する 79
RSA Authentication Manager サーバ証明書のダウンロード 79
認証リクエスト用のコンタクト リスト 80
自動コンタクト リスト 80
手動コンタクト リスト 81

第 4 章：認証ポリシーの構成 83
ポリシー 83
トークン ポリシー 84
トークン ポリシー設定 85
トークン ポリシーの追加 90
オフライン認証ポリシー 92
オフライン認証ポリシーの設定 93
オフライン認証ポリシーの追加 94
パスワード ポリシー 96
パスワード ポリシー設定 97
パスワード ポリシーの追加 100

ロックアウト ポリシー 101
ロックアウト ポリシー設定 102
ロックアウト ポリシーの追加 103
セルフ サービス トラブルシューティング ポリシー 103
セルフ サービス トラブルシューティング ポリシー設定 105
セルフ サービス トラブルシューティング ポリシーの追加 106
リスク ベース認証ポリシー 107
RBA（リスク ベース認証）ポリシー設定 107
リスク ベース認証ポリシーの追加 108
リスク ベース認証メッセージ ポリシー 110
リスク ベース認証メッセージ ポリシー設定 111
リスク ベース認証メッセージ ポリシーの追加 111

第 5 章：LDAP ディレクトリの統合 113
アイデンティティ ソース 113
LDAP ディレクトリのデータ 113
内部データベースのデータ 114
アイデンティティ ソース データ フロー 114
アイデンティティ ソースのプロパティ 116
アイデンティティ ソース範囲 121
グローバル カタログでない Active Directory アイデンティティ ソース 123
Active Directory グローバル カタログ アイデンティティ ソース 124
Active Directory 接続タイムアウトの構成 127
LDAP ディレクトリをアイデンティティ ソースとして統合 127
アイデンティティ ソースの追加 129
アイデンティティ ソースとシステムのリンク 130
LDAP ディレクトリ アイデンティティ ソースの検証 131
フェイルオーバー サーバ 132
通信パスの保護 133
アイデンティティ ソース SSL 証明書 134
Active Directory のパスワード ポリシー 136
カスタム属性マッピング 136
アイデンティティ ソース ユーザー属性 137
一意識別子の属性 138
ユーザー アカウントの有効状態の属性 139

第 6 章：ユーザーの管理 141
一般的なユーザー管理タスク 141
内部データベースへのユーザーの追加 141
ユーザー ステータス 144
ユーザー アカウントの無効化 144
ユーザー アカウントの有効化 145
セキュリティ ドメインによるユーザーの編成 145
セキュリティ ドメイン間でのユーザーの移動 146
ユーザー ID の重複 146

ユーザー認証 147
ユーザー認証設定の管理 147
ログオン エイリアス 149
ユーザーのロック解除 149
不正なパスコード カウント 150
セキュリティ クエスチョンの管理 150
セキュリティ クエスチョンの要件の設定 151
カスタムのセキュリティ クエスチョン 151
セキュリティ クエスチョン ファイルの変更 152
エマージェンシー オンライン認証 153
ワン タイム トークンコードのセットの割り当て 154
一時固定トークンコードの割り当て 156
エマージェンシー オフライン認証 157
オフライン エマージェンシー アクセス トークンコードの提供 158
オフライン エマージェンシー パスコードの提供 159
RSA SecurID PIN 160
On-Demand 認証の初期 PIN の設定 161
ユーザーの On-Demand 認証 PIN のクリア 161
RSA SecurID PIN のクリア 163
RSA SecurID 800 トークンの PIN ロック解除キーの取得 163
PIN ロック解除キーのインポート 164
ユーザー グループ 165
ユーザー グループの編成 165
ユーザー グループの特徴 165
ユーザー グループの作成 166
内部ユーザー グループ 167
ユーザー グループの追加 168
ユーザー グループへのユーザーの追加 169
認証エージェントによるユーザー アクセスの制御 170
ユーザー アクセスを制御するための制限付きエージェントの構成 170
ユーザー グループに対するアクセス時間制限 172
Active Directory グループによる制限付きエージェントへのアクセス 174
制限付きエージェントで認証が許可されたユーザー グループの表示 175
LDAP ディレクトリ内のユーザー データ 175
ユーザーが解決不可能になる仕組み 175
ユーザー グループが解決不可能になる仕組み 176
解決不可能なユーザーの手動クリーンアップ 176
解決不可能なユーザーの手動クリーンアップ 177
解決不可能なユーザーおよびユーザー グループのスケジュール クリーンアップ 179
クリーンアップ ジョブのスケジュール 180
LDAP ディレクトリ内でのユーザーの移動 183
LDAP ディレクトリ内のユーザーの変更 186
LDAP ディレクトリ内のグループ メンバーシップの変更 187

第 7 章：RSA Authentication Manager の管理 189
システム管理の委任 189
スーパー管理者 189
Operations Console 管理者 189
システム管理者アカウント 190
Authentication Manager 管理者アカウント 190
アプライアンス オペレーティング システム アカウント 191
スーパー管理者の追加 192
Operations Console 管理者の追加 193
Operations Console 193
Operations Console へのログオン 194
セッション有効期間の制限 194
セッション有効期間の制限のタイプ 195
セッション有効期間の設定の編集 196
アイデンティティ ソース プロパティの更新 197
システムからのアイデンティティ ソースのリンク解除 197
アイデンティティ ソースの編集 198
アイデンティティ ソースとシステムのリンク 199
LDAP ディレクトリ アイデンティティ ソースの検証 200
SSL 証明書の管理 200
コンソール証明書 201
コンソール証明書の置換 201
Operations Console による証明書署名リクエストの生成 202
コンソール証明書のインポート 204
新しい SSL コンソール証明書のアクティブ化 205
有効期限の切れたコンソール証明書の置換 206
ライセンス 207
ライセンスのインストール 208
インストール済みライセンスの表示 209

第 8 章：Web Tier 導入環境の管理 211
Web Tier 導入環境の管理 211
Web Tier の構成の編集 211
Web Tier サーバの IP アドレスの変更 212
ロードバランサと仮想ホストの更新 213
Web Tier バージョンの確認 214
Web Tier の更新 215
Windows での Web Tier のアンインストール 215
Linux での Web Tier のアンインストール 216
Web Tier サービスの管理 217
Windows での RSA Web Tier Bootstrapper Server の管理 217
Linux での RSA Web Tier Bootstrapper Server の管理 218
デフォルトの RSA 仮想ホスト証明書の置換 219
認証局証明書ファイル 219
デフォルトの仮想ホスト証明書の置換 220

Web Tier の CSR（証明書署名リクエスト）の生成 220
署名済み仮想ホスト証明書のインポート 221
仮想ホスト証明書のアクティブ化 222
Web Tier 上の Self-Service Console のログアウト エラー 223

第 9 章：RSA SecurID トークンの導入と管理 225
RSA SecurID トークン 225
RSA SecurID トークンの導入 226
トークン レコード ファイルのインポート 226
新しいセキュリティ ドメインへのトークン レコードの移動 227
ユーザーへのトークンの割り当て 228
ソフトウェア トークン プロファイル 229
ソフトウェア トークン プロファイルの追加 232
ハードウェア トークンの配布 234
ファイル ベースの配布を使用した複数のソフトウェア トークンの配布 234
ファイル ベースの配布を使用した単一のソフトウェア トークンの配布 236
動的シード配布（CT-KIP）を使用した複数のソフトウェア トークンの配布 238
動的シード配布を使用した単一のソフトウェア トークンの配布 240
CTF（Compressed Token Format）を使用した複数のソフトウェア トークンの配布 242
CTF（Compressed Token Format）を使用した単一のソフトウェア トークンの配布 244
RSA SecurID トークンの管理 245
トークンの有効化または無効化 246
トークンの有効化 246
トークンの無効化 247
トークンの削除 247
トークンの編集 248
トークンの紛失、盗難、破損、有効期限切れに関するユーザー支援 248
交換用トークンの割り当て 249
トークンの再同期 249
導入環境間でのユーザーとトークンのエクスポートおよびインポート 250
エクスポートおよびインポートによる認証への影響 250
エクスポートおよびインポートによるアイデンティティ ソースへの影響 250
エクスポートおよびインポートによるユーザーへの影響 252
暗号化キーのダウンロード 254
トークンのエクスポート 254
別の導入環境からのトークンのインポート 256
トークンを割り当てられたユーザーのエクスポート 257
トークンを割り当てられたユーザーのインポート 259

第 10 章：On-Demand 認証の導入 263
On-Demand 認証 263
On-Demand 認証の計画 263
テキスト メッセージによる On-Demand トークンコード配信の構成 264
On-Demand トークンコードをテキスト メッセージで配信するための アイデンティティ属性定義 264
On-Demand トークンコードの配信のための HTTP プラグ インの構成 266
SMS HTTP プラグ イン構成パラメータ 270
メールによる On-Demand トークンコード配信の構成 271
SMTP メール サービスの構成 272
On-Demand トークンコードをメールで配信するための アイデンティティ属性定義 273
On-Demand トークンコードの配信のためのメールの構成 275
On-Demand 認証を使用するためのユーザーの構成 276
ユーザーの On-Demand 認証の有効化 276
On-Demand 認証用の PIN 278
ユーザーによる On-Demand 認証の初期 PIN の設定の有効化 278
On-Demand トークンコードの一時 PIN の設定 279
ユーザーによる電話番号およびメール アドレスの更新の有効化 279
認証エージェントまたは RADIUS クライアントでの On-Demand 認証 281
認証エージェントまたは RADIUS クライアントでの PIN 作成と On-Demand トークンコード 282
On-Demand トークンコードの制限 282

第 11 章：RSA セルフサービス 283
RSA セルフサービスの概要 283
Self-Service Console のユーザー操作 284
ユーザーアカウント登録 284
セルフ サービス ユーザーのアイデンティティ ソース 285
セルフサービスの構成 286
アイデンティティ ソースの選択によるアカウント登録の有効化 286
セルフ サービスのセキュリティ ドメインの選択 287
セルフ サービスのユーザー グループの選択 288
セルフ サービスのユーザー プロファイル構成 289
Self-Service Console の認証方式の設定 291
セルフサービス用のセキュリティ クエスチョン 291
セルフ サービス ユーザー アカウント変更のメール通知の構成 292
セルフ サービス用メール テンプレートの例 294
Self-Service Console のカスタマイズ 295
セルフサービス機能の有効化または無効化 295
Self-Service Console の Web ページのカスタマイズ 296
Self-Service Console ユーザー ヘルプのカスタマイズ 297

プロビジョニングの概要 298
プロビジョニングの管理者ロール 298
Request Approver および Token Distributor の権限適用範囲 299
Request Approver および Token Distributor の権限 300
プロビジョニング リクエストのワークフロー 300
ワークフロー ポリシー 301
プロビジョニングの構成 302
プロビジョニングの有効化 302
デフォルトのワークフロー ポリシーの変更 302
セキュリティ ドメインへのワークフロー ポリシーの割り当て 303
ワークフロー定義の変更 303
プロビジョニング リクエストのためのメール通知の使用 305
プロビジョニングのワークフロー参加者へのメール通知の構成 305
セルフ サービス ユーザーのトークンの管理 306
セルフ サービス ユーザーのトークンの構成 307
ハードウェア トークンの送付先住所の構成 308
セルフ サービス トラブルシューティング 309
セルフ サービス トラブルシューティング ポリシーの追加 310

第 12 章：リスク ベース認証の導入 311
リスクベース認証 311
リスク ベース認証のデータ フロー 312
リスク ベース認証の導入に関する検討事項 314
リスク ベース認証のリスクエンジンに関する検討事項 316
最低保証レベル 316
最低保証レベルを決定するための推奨事項 317
リスク ベース認証に対するユーザーの行動パターンの影響 317
サイレント収集 319
リスク ベース認証の実装 319
リスク ベース認証のバックアップ認証方式 320
RSA Authentication Agent の取得 321
RBA 統合スクリプト テンプレートのインストール 322
リスク ベース認証用の認証エージェントの構成 322
リスク ベース認証の統合のテスト 324
認証テストのトラブルシューティング 325
ユーザーのリスク ベース認証の有効化 328
リスク ベース認証ポリシーのユーザー確認方法の有効化 329
ユーザーによるユーザー確認方法の構成方法 329
リスク ベース認証のデバイス設定 330
リスク ベース認証ポリシーのデバイス登録の構成 331
リスク ベース認証ポリシーのデバイス履歴の設定の構成 331
リスク ベース認証を使用する Web ベース アプリケーション向けの
カスタム ソリューション 332

第 13 章：RSA RADIUS の管理 333
RSA RADIUS の概要 333
RSA RADIUS 認証プロセス 333
RADIUS のネットワーク トポロジー 335
RADIUS サーバとクライアント間の通信 336
RSA RADIUS サーバの管理 338
RSA RADIUS 管理用の管理コンソール 338
RADIUS サーバの表示 339
RADIUS データ レプリケーション 339
システム生成 PIN を使用するための RSA RADIUS の構成 344
RADIUS サーバの再起動 345
RADIUS クライアント 347
RADIUS クライアントの追加 349
EAP-POTP 設定 351
RADIUS サーバ証明書の置換 352
信頼するルート証明書の追加 353
ユーザー アクセスの管理 354
RADIUS プロファイル 354
RADIUS プロファイルの追加 357
RADIUS プロファイル関連づけ 358
プロファイルの割り当ての例 361
デフォルトの RADIUS プロファイルの指定 362
RADIUS ユーザー属性 363
ユーザー属性の割り当ての例 364
カスタム RADIUS ユーザー属性定義の追加 364
RADIUS ユーザー属性のユーザーへの割り当て 366
アイデンティティ ソース属性への RADIUS ユーザー属性定義のマッピング 367
システム使用状況の監視と解析 367
RADIUS サーバの認証統計情報 368
RADIUS クライアントの統計情報 370
RADIUS サーバ ログ ファイル 374
RADIUS アカウンティング属性 377

第 14 章：ログとレポート 381
ログ メッセージの概要 381
ログのタイプ 381
ログ レベル 381
トラブルシューティング ファイルのダウンロード 382
リアルタイム監視 384
複数のアクティビティ モニタを使用したリアルタイム モニタリング 384
アクティビティ モニタでのメッセージ表示 385
レポート 386
管理者ロールごとの実行可能なレポート 386
スケジュール レポート ジョブ 390

カスタム レポート 390
レポートの追加 391
完了したレポート 392
サンプル レポート 392
アプライアンス ログのローテーション ポリシー 396
アプライアンス ログ設定の構成 397
ログ ファイルの使用 398
ログ アーカイブ 398
アーカイブされたログ ファイルの完全性の検証 399
ログ メッセージのローカルファイルへの保存 400
ローカル ログ ファイルの最大ログ ファイル数の設定 402
ローカル ログ ファイルの最大サイズの設定 403
ログ内のトークン シリアル番号のマスク 404
高度なログとトラブルシューティング 405
SNMP の概要 405
SNMP の構成 406
トラブルシューティング用のログ ファイル 409
トレース ログ 412
リアルタイム ログ監視用のリモート Syslog ホストの構成 412
重大システム イベントの通知の構成 413
重大システム イベントのタイプ 414

第 15 章：災害復旧 417
導入環境の問題のトラブルシューティング 417
プライマリ インスタンスまたはレプリカ インスタンスのデータを紛失した時の現象 417
プライマリ インスタンスが応答しなくなった時の現象 417
レプリカ インスタンスが応答しなくなった時の現象 418
Web Tier が応答しなくなった時の現象 418
レプリケーションの問題が発生した時の現象 418
導入環境の問題の解決 419
アプライアンスのリブート 419
レプリケーション ステータスの確認 419
レプリカ インスタンスの同期 422
キャッシュのフラッシュ 423
導入環境のバックアップ 423
今すぐバックアップ機能によるバックアップの作成 425
スケジュール バックアップによるバックアップの作成 426
プライマリ インスタンスまたはレプリカ インスタンスのスナップショット 428
プライマリ インスタンス データのリストア 428
スタンドアロン導入環境でのプライマリ インスタンス データのリストア 429
レプリケーション導入環境でのプライマリ インスタンス データのリストア 430
バックアップからのリストア 431

プライマリ インスタンスのリストア 433
プライマリ インスタンスの置換 433
レプリカ インスタンスの昇格 436
レプリカ インスタンスの昇格 439
スナップショットによるプライマリ インスタンスの復元 442
レプリカ インスタンスのリストア 444
レプリカ インスタンスの置換 444
スナップショットによるレプリカ インスタンスの復元 445
Web Tier のリストア 446
信頼関係の修復 447
バージョン 8.0 レルムとの信頼関係の修復 448
バージョン 7.1 レルムとの信頼関係の修復 450
不完全なバックアップを使用した場合のトラステッド レルムの不一致の修復 451
レガシー トラステッド レルムの修復 454

第 16 章：高度な管理 455
アプライアンスのオペレーティング システム上でのトラブルシューティングと高度な管理 455
アプライアンスの SSH の有効化 455
アプライアンスのオペレーティング システムへのログオン 456
Clam Antivirus ソフトウェアの実行 456
RSA Authentication Manager のサービス 457
自動的に開始される RSA Authentication Manager サービス 458
RSA Authentication Manager サービスの手動での管理 458
スーパー管理者のリストア 460
スーパー管理者のリストア 461
RSA Authentication Manager のアップデート 462
ソフトウェア バージョンの表示 463
IP アドレスまたはホスト名の検証 463

第 17 章：トラステッド レルムの管理 465
トラステッド レルム 465
信頼関係の作成 467
トラステッド レルムの追加 468
トラステッド レルム認証のためのエージェントの構成 469
アクセス制御のための複製エージェント レコード 471
トラステッド ユーザーの追加 472
RSA RADIUS を使用したトラステッド ユーザーの認証を許可する 473
トラステッド ユーザー グループの追加 474
トラステッド ユーザー グループへのトラステッド ユーザーの追加 474
レガシー レルムとの信頼関係の作成 475
レガシー トラステッド レルム認証のためのポートの構成 475
信頼関係の修復 477

付録 A：インスタンス ネットワーク設定の変更 479
プライマリまたはレプリカ インスタンスのネットワーク設定の更新 479
プライマリ インスタンスの IPv4 ネットワーク設定の変更 480
レプリカ インスタンスでのプライマリ インスタンスのホスト名と IP アドレスの更新 483
レプリカ インスタンスの IPv4 ネットワーク設定の変更 484
静的ルート 487
永続的な IPv4 静的ルートの追加 488
永続的な IPv6 静的ルートの追加 489
非永続的な IPv4 静的ルートの追加 490
非永続的な IPv6 静的ルートの追加 490
永続的な IPv4 または IPv6 静的ルートの削除 491
非永続的な IPv4 または IPv6 静的ルートの削除 492
不正なネットワーク設定からの復旧 493
不正な IP アドレスの変更からの復旧 493
不正なサブネット マスクからの復旧 495
不正なゲートウェイからの復旧 496

付録 B：MMC（Microsoft 管理コンソール）を使用した RSA SecurID トークンの管理 497
概要 497
RSA Token Management スナップインへのアクセス 497
RSA Token Management スナップインを使用したトークンの管理 498
RSA Token Management スナップインを使用したハードウェア トークンの割り当て 499
RSA Token Management スナップインを使用したソフトウェア トークンの割り当て 499

付録 C：IPv4/IPv6 認証エージェントの導入 501
概要 501
IPv4/IPv6 エージェント名 501
IPv4/IPv6 認証エージェントの取得 501
IPv4/IPv6 認証エージェントの導入 502
IPv4/IPv6 エージェントの構成 503
新しいノード シークレットのロード 504
一般的な IPv4/IPv6 の問題の解決 506
プライマリまたはレプリカ インスタンスでの IPv6 ネットワーク設定の追加 507
VMware インフラストラクチャ内の IPv6 の有効化 507

用語集 509

索引 519

はじめに

本書について

このガイドは、管理者およびその他の信頼できる担当者を対象に、RSA® Authentication Manager 8.0 を管理する方法について説明しています。

RSA Authentication Manager 8.0 マニュアル

RSA Authentication Manager 8.0 の詳細については、次のマニュアルを参照してください。RSA では、管理者のみがアクセス可能なネットワーク上の場所に製品マニュアルを保管することを推奨します。

リリース ノート：本リリースにおける新機能や変更点に加え、既知の不具合とその回避方法について説明しています。

Getting Started：Authentication Manager の Quick Setup プロセスを実行する方法について説明しています。

設計ガイド：Authentication Manager の上位レベルのアーキテクチャ、および既存ネットワークとの統合方法について説明しています。

セットアップと構成ガイド：Authentication Manager をセットアップおよび構成する方法について説明しています。

管理者ガイド：Authentication Manager とその機能の概要を示しています。システムを構成し、ユーザーやセキュリティ ポリシーの管理など、さまざまな管理タスクを実行する方法について説明しています。

Help Desk Administrator's Guide：ヘルプ デスク管理者が日々実行する最も一般的なタスクの手順について説明しています。

SNMP Reference Guide：SNMP（Simple Network Management Protocol）を構成して Authentication Manager のインスタンスを監視する方法について説明しています。

トラブルシューティング ガイド：RSA Authentication Manager の最も一般的なエラー メッセージと、各イベントをトラブルシューティングする適切なアクションについて説明します。

Developer's Guide：RSA Authentication Manager API（アプリケーション プログラミング インタフェース）を使用したカスタム プログラムの開発について説明しています。また、API の概要および Java API の Javadoc も含まれています。

Performance and Scalability Guide：最適なパフォーマンスを得るために環境を調整するときの考慮事項について説明しています。

6.1 から 8.0 への移行ガイド：RSA Authentication Manager 6.1 環境から RSA Authentication Manager 8.0 環境へ移行する方法について説明しています。

7.1 から 8.0 への移行ガイド：RSA Authentication Manager 7.1 環境から RSA Authentication Manager 8.0 環境へ移行する方法について説明しています。

Security Console ヘルプ：Security Console で日々実行される管理タスクについて説明しています。

Operations Console ヘルプ：Operations Console で実行される構成タスクおよび設定タスクについて説明しています。

Self-Service Console ヘルプ：Self-Service Console を使用する方法について説明しています。ヘルプを表示するには、Self-Service Console の［**Help（ヘルプ）**］タブで［**Self-Service Console Help（Self-Service Console ヘルプ）**］をクリックします。

RSA Token Management Snap-In ヘルプ：Active Directory アイデンティティソースが存在する環境で MMC（Microsoft 管理コンソール）と連携するソフトウェアを使用する方法について説明します。このスナップインを使用すると、トークンの有効化 / 無効化、トークンの割り当て、またはその他のトークン関連タスクを実行するために、Security Console にログオンする必要がなくなります。

関連ドキュメント

RADIUS リファレンス ガイド：RSA RADIUS で使用する初期設定ファイル、ディクショナリファイル、構成ファイルの使用法および設定について説明しています。

Security Configuration Guide：Authentication Manager で使用可能なセキュリティ構成設定について説明します。また、安全な導入と使用のための設定、安全な保守、物理的なセキュリティ管理に関する情報も提供します。

サポートとサービス

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
RSA Solution Gallery	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

RSA SecurCare Online では、よくある質問に対する回答や既知の問題に対する解決策を含むナレッジベースを参照できます。また、新しいリリースに関する情報や重要なテクニカル ニュース、ソフトウェアのダウンロードも利用できます。

RSA Solution Gallery では、RSA 製品との連携が検証されているサード パーティのハードウェア製品およびソフトウェア製品に関する情報を利用できます。このギャラリーには、RSA 製品とこれらのサード パーティ製品の相互運用について、連携手順を説明した Secured by RSA 実装ガイドおよびその他の情報が含まれています。

カスタマー サポートにご連絡される前に

ご連絡いただく際には、次の情報をご用意ください。

- ❑ RSA Authentication Manager アプライアンスにアクセスできることを確認してください。
- ❑ ライセンスのシリアル番号。シリアル番号は、次の方法で確認できます。
  - Security Console にログオンして、[**License Status（ライセンス ステータス**]をクリックします。[**View Installed License（インストール済みライセンスの表示）**]をクリックし、リストからライセンス ID を選択して内容を表示します。
- ❑ Authentication Manager アプライアンスのソフトウェアのバージョン情報。この情報は、Quick Setup の画面の右上隅、または Security Console に表示されます。Security Console にログオンして、[**Software Version Information（ソフトウェア バージョン情報）**]をクリックします。

1 RSA Authentication Manager 概要

RSA Authentication Manager の概要

RSA Authentication Manager は、エンタープライズ ネットワークの認証リクエストを検証し、認証ポリシーを一元管理する多要素認証ソリューションです。Authentication Manager を使用して、セキュリティ トークン、ユーザー、複数のアプリケーション、エージェント、リソースを管理し、SSL-VPN や Web ポータルなど、ネットワークと Web アクセス可能なアプリケーションに安全にアクセスするのに役立ちます。

多要素認証

パスワードは、ユーザーが選択したシークレット ワードやシークレット フレーズという 1 つの要素のみでアクセスを保護するため、弱い認証方法です。ユーザー以外の人物にパスワードが知られると、システム全体のセキュリティが危殆化することになります。多要素認証では、ユーザーの本人確認に複数の一意な要素をリクエストすることで保護を強化します。多要素認証システムには、次のような認証要素を含めることができます。

- ユーザーが知っているもの（パスワード、パスフレーズ、PIN）
- ユーザーが所有するもの（ハードウェア トークン、ラップトップ コンピュータ、携帯電話）
- ユーザーの行動（特定のアクションまたは行動パターン）

Authentication Manager は、次の強力な認証方式を提供します。

- RSA SecurID。ハードウェアトークンまたはソフトウェアトークンを使用した 2 要素認証によってアクセスを保護します。
- ODA（On-Demand 認証）。リクエストに応じて SMS テキスト メッセージまたはメール経由でユーザーにクレデンシャルを送信することにより、2 要素認証によってアクセスを保護します。
- RBA（リスク ベース認証）。ユーザーの行動パターンと認証に使用するデバイスの履歴から個々の認証試行のリスクレベルを評価し、それによってアクセスを保護します。

  RBA や ODA では、携帯電話、PC、またはラップトップといったユーザーが所有しているデバイスを活用することで、トークンを管理することなく多要素認証を実現できます。

RSA Authentication Manager の主要なコンポーネント

RSA Authentication Manager の導入環境には、次のコンポーネントが含まれます。

プライマリ インスタンス

レプリカ インスタンス

アイデンティティ ソース

RSA 認証エージェント

Web ベース リソースのリスク ベース認証

RSA RADIUS の概要

Web Tier

Self-Service

SMS プラグ イン。詳細については、263 ページの On-Demand 認証の導入 を参照してください。

ロードバランサ

注：RSA は、RSA SecurID、RBA（リスク ベース認証）、ODA（On-Demand 認証）、および SMS（Short Message Service）と多くのサード パーティ製品の統合に対応し、認定しています。認定製品のリストについては、**http://www.rsasecured.com** にアクセスして、「Authentication Manager」を検索してください。認定製品ごとに、ソリューションの設定手順を示した導入ガイドがあります。

プライマリ インスタンス

プライマリ インスタンスは、最初に導入する Authentication Manager システムです。プライマリ インスタンスを導入した後、レプリカ インスタンスを追加できます。保守や災害復旧時には、レプリカ インスタンスを昇格させ、プライマリ インスタンスと置換することができます。

導入環境の中で、Authentication Manager のすべての管理タスクを実行できるシステムはプライマリ インスタンスのみです。レプリカの昇格やログ ファイルの収集など、一部の管理タスクはレプリカ インスタンスでも実行できます。

プライマリ インスタンスの主な機能は、次のとおりです。

- ユーザーの認証。
- 内部データベースに格納されている Authentication Manager データの管理。SecurID トークンのインポートや割り当て、RBA（リスク ベース認証）の有効化、LDAP アイデンティティ ソースの追加、セルフ サービスの構成、レプリカ パッケージの生成、エージェント構成ファイル、ノード シークレットの生成などのタスクを実行できます。

- 管理や認証活動の結果生じた変更をレプリケーションする。
- プライマリ RSA RADIUS サーバをホストすること。
- セルフ サービス リクエストの処理。
- Authentication Manager データベースを最新の状態に維持する。

レプリカ インスタンス

レプリカ インスタンスは導入環境レベルでプライマリ インスタンスの冗長性を提供します。レプリカ インスタンスの管理データは、表示することはできますが更新することはできません。

レプリカ インスタンスが提供するメリットは、次のとおりです。

- すべてのユーザーおよびシステム データのリアルタイムのミラーリング
- プライマリ インスタンスの応答がない場合、認証をフェイルオーバー
- 認証リクエストを複数インスタンスに負荷分散することによるパフォーマンスの向上
- リモートロケーションへのレプリカ インスタンスの導入
- リモートへの導入は、レプリカ インスタンスの安全性を確保するよう慎重に行う必要があります。リモート レプリカ インスタンスを安全に導入する方法については、「RSA Authentication Manager 8.0 計画ガイド」の「導入シナリオ」を参照してください。
- プライマリ インスタンスの応答がない場合に、レプリカの昇格により管理機能を復旧可能

レプリカ インスタンスはオプション機能ですが、レプリカ インスタンスの導入を推奨します。

アイデンティティ ソース

導入環境の全ユーザーおよびユーザー グループは、アイデンティティ ソースに格納されます。RSA Authentication Manager がサポートするアイデンティティ ソースは、次のとおりです。

- LDAP ディレクトリ サーバ。Active Directory または Oracle Directory Server のいずれか。
- Active Directory グローバル カタログ。Active Directory フォレストの一部またはすべての Active Directory サーバをアイデンティティ ソースとして使用する場合に、使用されます。グローバル カタログは、Active Directory フォレスト内のユーザーの検索と認証、およびグループ メンバーシップの解決などのランタイム アクティビティに使用されます。グローバル カタログを使用して、管理機能を実行することはできません。
- Authentication Manager の内部データベース。ユーザーの On-Demand 認証とリスク ベース認証を有効にするなどの管理運用に使用されます。

ディレクトリ スキーマを変更することなく Authentication Manager のアイデンティティ ソースとして LDAP ディレクトリ サーバを統合できます。

RSA 認証エージェント

認証エージェントとは、認証を行うドメイン サーバ、Web サーバ、パーソナル コンピュータなどのマシンにインストールするソフトウェア アプリケーションです。

認証エージェントは、RSA Authentication Manager と通信し、認証リクエストを処理する、保護対象リソース上のコンポーネントです。SecurID 認証、ODA（On-Demand 認証）、RBA（リスク ベース認証）を使用するリソースには、すべて認証エージェントが必要です。

さまざまなタイプの認証エージェントが、異なるリソースを保護しています。たとえば、Apache Web サーバを保護する場合は、RSA Authentication Agent 5.3 for Web for Apache が必要です。RSA Authentication Agent ソフトウェアを組み込み済みの製品を購入することも可能です。このソフトウェアは、リモート アクセス サーバ、ファイアウォール、Web サーバなどのさまざまな製品に組み込まれています。該当するデバイスの実装に関する情報は、Secured By RSA Partner Program から入手できます。詳細については、**http://japan.emc.com/partnerships/rsa-partners/secured-rsa-partner-program-overview.htm** を参照してください。

注：RBA に対応するのは Web ベースの認証エージェントのみです。

Web ベース リソースのリスク ベース認証

RBA（リスク ベース認証）は、Web ベースのリソースおよびアプリケーションへのアクセスを保護します。RBA を導入するには、リソースと Authentication Manager を統合することが必須条件となります。Authentication Manager では、この統合プロセスを簡単に行うテンプレートを提供しています。統合された後、ユーザーは Web ベース リソースによって自動的に Authentication Manager にリダイレクトされ、次のいずれかが実行されます。

- ユーザーを認証して、リソースに認証の証明を返す
- リスク レベルが高い場合、認証の証明を返す前に事前構成したセキュリティ クエスチョンに対して正しく回答するなど、追加のクレデンシャルの提供をユーザーにリクエストする。

Web ベース リソースは、Authentication Manager に認証の証明を提示し、正しいことを検証した後、ユーザーのリソースへのアクセスを許可します。

RSA RADIUS の概要

RSA RADIUS と RSA Authentication Manager を共に使用すると、RADIUS 対応デバイスを通じてネットワーク リソースにアクセスしようとするユーザーを直接認証できます。RADIUS サーバは、VPN などの RADIUS クライアントからユーザー アクセス リクエストを受信します。RADIUS サーバが受信したアクセス リクエストは RSA Authentication Manager に転送され、検証されます。Authentication Manager が許可または拒否メッセージを RADIUS サーバに送信し、RADIUS サーバがそのメッセージをリクエスト送信元の RADIUS クライアントに転送します。

RADIUS は、Authentication Manager のインストール中に自動的にインストールされて構成されます。インストール後、RADIUS は Authentication Manager と同じインスタンス上で稼働するように構成されます。

RSA RADIUS の構成と、RSA RADIUS が稼働する個々のインスタンスに必要な設定の管理は、Operations Console を使用して行います。

RADIUS の日常的な運用管理に関連するほとんどのタスクは、Security Console から実行できます。

Web Tier

Web Tier は、いくつかの Authentication Manager サービスをネットワーク DMZ 内で安全にホストする軽量のアプリケーション サーバです。RBA（リスク ベース認証）、CT-KIP（Cryptographic Token Key Initialization Protocol）によるソフトウェア トークンの動的配布、Self-Service Console などのサービスは、企業ネットワークの外のユーザーからの利用が必要となる場合があります。ネットワークに DMZ がある場合、このようなサービスを DMZ に導入するために、Web Tier を使用します。

Web Tier を DMZ に導入するメリットは次のとおりです。

- Self-Service Console、CT-KIP、RBA のユーザーによって生じるフィルタリングされないインターネット トラフィックから内部ネットワークを保護します。Web Tier サーバが、プライベート ネットワークの手前で、インバウンド インターネット トラフィックを受信し、管理します。
- RBA サービスや Self-Service Console のユーザー インタフェースをカスタマイズできます。
- 一部のタスク処理をバックエンド サーバから切り離すことにより、システム パフォーマンスが向上します。

プライマリおよびレプリカ インスタンスはプライベート ネットワークのファイアウォールの内側に配置します。

Self-Service

Web ベースのワークフロー システムであるセルフサービスは、ユーザーにセルフ サービス オプションを提供するとともに、トークン導入プロセスの自動化を行います。セルフサービスには 2 つのコンポーネントがあります。

- セルフサービス：管理者のサポートなしで、ユーザー自らトークンの保守タスクやトラブルシューティングを行うことができます。ユーザーが PIN を忘れた場合、トークンが手元にない場合、エマージェンシー アクセスやトークンの再同期が必要になった場合など、導入済みトークンの保守に費やす時間を短縮できます。
- プロビジョニング：ユーザーが RSA SecurID トークンをリクエストして、トークン導入プロセスの多くの手順を実行することができ、ワークフローが自動化されます。これにより、トークンの導入（特に、大規模なトークン導入）に伴う管理オーバーヘッドを削減できます。プロビジョニングは、Enterprise Server ライセンスでのみ使用できます。

ユーザーは Self-Service Console を通じてセルフ サービスおよびプロビジョニング タスクを実行します。Self-Service Console はブラウザ ベースのインタフェースであり、ユーザーは管理者またはヘルプ デスク担当者のサポートがなくても一定のタスクを実行できるため、スタッフがユーザー支援に費やす時間を短縮できます。Self-Service Console は、ファイアウォールの内側にある Authentication Manager インスタンスにインストールできるほか、セキュリティを強化するために、DMZ（Web Tier サーバを使用）にインストールすることもできます。

Self-Service Console のデフォルトでは、ユーザーは一連のセキュリティ クエスチョンへの回答を登録した後で、システムにリクエストを送信できるようになります。さらに、ユーザーが Self-Service Console で次のタスクを実行できるように Authentication Manager を構成することもできます。

- RSA SecurID トークンをリクエストする
- RSA SecurID PIN を管理する
- ユーザー確認用のセキュリティ クエスチョンを構成する
- 携帯電話の番号やメール アドレスなど、プロファイル情報を更新する
- Self-Service Console のパスワードを変更する
- RBA（リスク ベース認証）デバイス履歴をクリアしてデバイスの登録を解除する
- ODA（On-Demand 認証）用のメール アドレスまたは電話番号を変更する
- ODA PIN を管理する
- ユーザー グループ メンバーシップを表示する

重要：ユーザーが変更できるのは、内部データベースに格納されたデータのみです。パスワードの変更を強制された場合を除き、LDAP ディレクトリに格納されたデータを Self-Service Console から変更することはできません。

ロードバランサ

RSA Authentication Manager の導入環境には、次の機能を提供するロードバランサを含めることができます。

- プライマリ Web Tier とレプリカ Web Tier に認証リクエストを分散する。
- Authentication Manager インスタンスの 1 つまたは Web Tier の 1 つがダウンした時に、フェイルオーバーを実行する。
- HTTPS ポート経由で受信した Self-Service Console へのリクエストを、Self-Service Console をホストするプライマリ Web Tier またはプライマリ インスタンスに転送する。

RSA SecurID 認証の概要

RSA SecurID では、RSA が特許を有する時間ベースの 2 要素認証メカニズムを使用して、ユーザーの正当性を検証します。RSA SecurID を使用することにより、管理者は、コンピュータ、ネットワーク、その他のリソースにアクセスしようとするユーザーが本人であることを検証できます。

RSA Authentication Manager ソフトウェアは、RSA SecurID の管理コンポーネントです。このソフトウェアは認証リクエストの検証に使用されるほか、エンタープライズ ネットワーク内での認証、ユーザー、グループに関するセキュリティ ポリシーを一元管理するために使用されます。

Authentication Manager ソフトウェアは拡張性に優れ、多数のユーザーを認証することができます。また、ネットワーク、リモート アクセス、ワイヤレス、VPN、インターネット、アプリケーションなどのさまざまな製品との相互運用性を備えています。次の表は、主な例を示しています。

製品またはアプリケーション	説明
VPN アクセス	RSA SecurID は、VPN と組み合わせて使用することにより、信頼性の高い認証を実現します。
リモート ダイヤル イン	RSA SecurID は、RADIUS などのリモート ダイヤル イン サーバと連携します。
Web アクセス	RSA SecurID は、Web ページへのアクセスを保護します。
ワイヤレス ネットワーク	Authentication Manager には、802.1 準拠の RADIUS サーバが含まれています。
Microsoft Windows への安全なアクセス	Authentication Manager を使用することで、Microsoft Windows 環境へのオンラインおよびオフライン両方のアクセスを制御できます。
ネットワーク ハードウェア デバイス	Authentication Manager を使用することで、ルータ、ファイアウォール、スイッチなど、SecurID に対応するデバイスへのデスクトップからのアクセスを制御できます。

RSA SecurID 認証プロセス

RSA SecurID 認証プロセスには、次の 3 つの製品が関与します。

- RSA SecurID トークン。ユーザーのワンタイム認証クレデンシャルを生成します。
- RSA Authentication Agent。クライアント デバイスにインストールされ、Authentication Manager に認証リクエストを送信します。
- RSA Authentication Manager。認証エージェントから送信された認証リクエストを処理し、認証クレデンシャルの検証結果に基づいてアクセスを許可 / 拒否します。

SecurID を使用してユーザーを認証するには、Authentication Manager 上に少なくとも次の情報が必要です。

要素	情報
ユーザー レコード	ユーザー ID およびユーザーに関するその他の個人情報（名前、苗字、グループに所属する場合はそのグループなど）を含みます。ユーザー レコードは、LDAP ディレクトリ サーバまたは Authentication Manager 内部データベースのいずれかに保存できます。
エージェント レコード	エージェントがインストールされているマシンの名前。Authentication Manager は、内部データベースに格納されたエージェント レコードによってエージェントを識別し、エージェントからの認証リクエストに応答します。
トークン レコード	ユーザーの RSA SecurID トークンに表示されるものと同じトークンコードを Authentication Manager で生成するために必要です。
SecurID PIN	パスコードを作成するために、トークンコードと組み合わせて使用します。

RSA SecurID トークン

RSA SecurID トークンは、ハードウェア デバイスまたはソフトウェア ベースのセキュリティ トークンです。トークンは、トークンコードと呼ばれる乱数を生成して表示します。

通常、RSA SecurID では、トークンコードに加えて PIN も必要になります。PIN は、ユーザーが作成するか、または Authentication Manager で生成されます。トークンコードと PIN の 2 要素を必要とするため、2 要素認証と呼びます。

- ユーザーが所有しているもの（トークン）
- ユーザーが知っているもの（PIN）

Authentication Manager では、トークンコードと PIN の組み合わせをパスコードと呼びます。保護されたリソースにアクセスする時、ユーザーはログオン プロンプトでパスコードを入力します （不正に取得されたパスコードが使用されないようにするために、Authentication Manager は、入力されたパスコードが以前の認証時に使用済みでないかどうかをチェックします）。

また、RSA SecurID は PIN を必要としないトークンもサポートします。ユーザーは現在のトークンコードのみを使用して認証を受けることができます。この場合、2 番目の要素の代替として、ユーザーのネットワーク パスワードなどを使用します。

トークンの納品物には、Authentication Manager にインポートするトークン シード レコード ファイルが含まれています。個々の RSA SecurID トークンに対応したトークン シード レコードが存在し、Authentication Manager が認証エージェントから認証リクエストを受け取ったときに正しい トークンコードを生成するために使用されます。

Authentication Manager は、認証に使用される SecurID トークンのシリアル番号をログに記録します。デフォルトでは、Authentication Manager は、シリアル番号をクリア テキストで記録します。ただし、Syslog への記録や SNMP を使用する際にシリアル番号をクリア テキストで記録したくない場合は、トークンのシリアル番号をマスキングすることができます。RSA では、セキュリティを向上させるために、トークンのシリアル番号をマスキングすることを推奨します。詳細については、404 ページのログ内のトークン シリアル番号のマスクを参照してください。

保護対象システムへのアクセスを許可するユーザーには、1 ユーザにつき最大 3 つの RSA SecurID トークンを割り当てることができます。

RSA SecurID ハードウェア トークン

RSA SecurID ハードウェア トークンは、多様なフォーム ファクタで提供されます。

- RSA SecurID 200 トークン

  クレジット カード サイズのこのハードウェア トークンは、持ち運びが容易で、非常に優れた耐久性を備えています。事前定義されたインターバル（通常は 60 秒間隔）で新しいトークンコードを生成して表示します。

- RSA SecurID 520 トークン

  クレジット カード サイズのこのデバイスでは、ユーザーが数字キーパッドを使用して PIN を入力します。表示されるコードは、PIN と現在のトークンコードを組み合わせ、ハッシュ暗号化により生成したものです。RSA SecurID 520 トークンは、ユーザーの PIN を盗もうとするキー ロガー タイプのマルウェアから PIN を保護します。

- RSA SecurID 700 トークン

  このハードウェア デバイスは、どのようなキー ホルダーにも簡単に取り付けることができます。ユーザーは（通常は 60 秒ごとに）変化する表示を読み取り、それをパスワードの一部として使用するだけです。

- RSA SecurID 800 ハイブリッド トークン

  RSA SecurID 800 トークンは、RSA SecurID トークンとリーダー組み込み型の USB スマート カード（USB トークン）の両方の役割を果たします。2 種類の電子機器が、相互に独立して動作します。

コンピュータに接続していない状態では、SecurID 800 は、RSA SecurID 認証に使用するトークンコードを生成して表示します。コンピュータに接続した状態では、次の 2 種類の機能を提供します。

- RSA SecurID 認証では、ユーザーは、トークンの数字を自分で読み取るのではなく、コンピュータにインストールされたミドルウェアが自動的にトークンコードを読み取ることによって認証することができます。
- トークンのスマート カード機能を使用し、複数の X.509 デジタル証明書、Windows ログオンアカウントなどのクレデンシャルを格納できます。格納されたデジタル証明書は、認証、デジタル署名、ファイル暗号化アプリケーションで使用することができます。

RSA SecurID ソフトウェア トークン

RSA SecurID トークンは、クライアント ワークステーションやモバイル デバイス上にインストールされた RSA SecurID ソフトウェア トークン アプリケーションをフォーム ファクタとすることができます。RSA Authentication Manager は、サポートするデバイス タイプに対して RSA SecurID ソフトウェア トークンを発行するための、一元化された管理インタフェースを備えています。トークンの拡張フィールドを使用すると、デバイス タイプ、デバイスのシリアル番号、トークンのニックネームなどの情報をソフトウェア トークンに追加できます。ソフトウェア トークンの詳細については、第 9 章、RSA SecurID トークンの導入と管理、および個別の RSA SecurID ソフトウェア トークン製品に付属のドキュメントを参照してください。

SecurID 認証における RSA Authentication Manager の役割

RSA Authentication Manager ソフトウェア、認証エージェント、RSA SecurID トークンは、連携してユーザーが本人であることを検証します。RSA が特許を有する RSA SecurID 時刻同期方式により、ユーザーのトークンに表示されるトークンコードが、その時間に RSA Authentication Manager ソフトウェアが生成するトークンコードと同じであることが保証されます。トークンと Authentication Manager の両方が、下記の情報に基づいてトークンコードを生成します。

- トークンの一意な識別子（「シード」と呼ばれる）。
- 現在時刻。トークンの場合はトークンの内部クロックから取得。Authentication Manager はシステムの現在時刻から取得。

認証試行が正当であることを判断するために、RSA Authentication Manager は、生成したトークンコードをユーザーが入力したトークンコードと比較します。トークンコードが一致しない場合や間違った PIN が入力された場合は、ユーザーのアクセスは拒否されます。

On-Demand 認証

ODA（On-Demand 認証）は、ユーザーの携帯電話やメール アカウントにワン タイム トークンコードを配信します。トークンコードはランダムに生成される 6 桁の番号です。ODA は、SSL-VPN や Web ポータルなど、エージェントで保護されたデバイスやアプリケーションを通じてユーザーがアクセスする会社のリソースを保護します。

また、ODA はユーザーに次の 2 要素を求めることでネットワークのセキュリティを強化します。

- ユーザーのみが知っているもの（PIN）
- ユーザーが持っているもの（トークンコード）

物理的なトークンなどの追加ハードウェアを必要としないため、ODA の導入は容易です。ほとんどの従業員はすでに携帯電話およびメール アカウントを所持し、使用しています。

On-Demand トークンコードを使用できるのは 1 回限りで、指定された期間を過ぎると有効期限が切れることでセキュリティを強化します。

ODA は SMS（Short Message Service）またはメールを使用してトークンコードを配信します。SMS を選択した場合、Authentication Manager から SMS に、中継サービスを経由して間接的にトークンコードが配信されます。SMS 配信は、SMS モデム（製品には含まれない）またはサード パーティの配信サービスを使用するようにカスタマイズできます。

On-Demand 認証ユーザー ログオンの例

単独の認証方法として使用する場合、ODA（On-Demand 認証）は、認証頻度が少ないユーザーや、契約業者のように短期間のみネットワーク アクセスが必要なユーザーの認証に適しています。ODA を使用するユーザーが企業の Web ポータルにアクセスする場合、通常次のような手順を実行します。

1. ブラウザのウィンドウを開いて、会社の Web ポータルにアクセスします。
2. プロンプトに従って、ユーザー ID と PIN を入力します。
   ワン タイム トークンコードが、ユーザーの携帯電話またはメール アカウントに送信されます。
3. ブラウザにトークンコードを入力します。
4. 保護されたリソースにアクセスできるようになります。

リスクベース認証

RBA（リスク ベース認証）は、ユーザーの行動パターンやアクセスに使用するデバイスをユーザーに気づかせることなく分析することにより、潜在的なリスクや不正な認証試行を識別します。RBA は、RSA SecurID 認証および従来のパスワード ベースの認証を強化します。評価リスクが許容できない場合、ユーザーは次のいずれかの方法によってユーザー本人であることを証明するよう要求されます。

- ODA（On-Demand 認証）。ユーザーは、PIN、および、事前に設定した携帯電話番号またはメール アカウントに送信されたワンタイム トークン コードを正確に入力する必要があります。
- セキュリティ クエスチョン。ユーザーは、1 つ以上のセキュリティ クエスチョンに正しく回答する必要があります。質問の正解は、Self-Service Console で構成するか、またはサイレント収集期間に認証を行う時に構成します。

Authentication Manager には、各ユーザーのデバイスと行動パターンに関する情報をインテリジェントに収集して分析するリスクエンジンが含まれています。ユーザーが認証を試行すると、リスクエンジンは収集したデータを参照してそのリスクを評価します。その後、リスクエンジンはユーザーの認証試行に高、中、低などの保証レベルを割り当てます。RBA は、この保証レベルを、あらかじめ構成された許容可能な最低保証レベルと比較します。保証レベルが最低保証レベルに満たない場合、このユーザーにはセキュリティ クエスチョンまたは ODA を使用したユーザー確認が求められます。

リスク ベース認証による、パスワード盗難時のデータ損失の防止

RBA（リスク ベース認証）を使用する場合、パスワード認証に慣れたユーザーは、それまでの日常のタスクをごくわずか、またはまったく変更することなく、同じように認証を続けられます。同時に、RBA はパスワードが盗まれた場合に企業のリソースを保護します。

たとえば、John のケースを考えてみてください。彼はセールス担当で、自宅から企業の SSL-VPN に定期的にアクセスしています。通常はユーザー名とパスワードのみで、同じラップトップから毎日認証を受けています。では、John のパスワードを盗んだ不正ユーザーが、別のマシンを使って別の場所から SSL-VPN にログオンしようとしたら、どうなるでしょうか。RBA は、攻撃者が不明なデバイスを使用していることを検出し、本人確認のためセキュリティ クエスチョンに回答するよう攻撃者にリクエストします。攻撃者が正解できなければ、アクセスは拒否されます。

パスワードを使用した認証に慣れたユーザーは、バックグラウンドで RBA が動作し、重要な企業リソースを保護している間、それまでと同じようにパスワードでの認証を継続できます。いつもの認証手順が中断するのは、ユーザーの行動がいつもと異なるとみなされた場合のみです。

ほとんどの場合、一般的なユーザーは、次のステップに示すように、単純にパスワードを入力するだけです。

1. ブラウザのウィンドウを開いて、会社の Web ポータルにアクセスします。
2. パスワードを入力します。
3. 保護されたリソースへのアクセスが許可されます。

パスワードが入力された後、Authentication Manager はユーザーのリスク レベルを分析して、ユーザーの行動パターンとデバイスが以前と同じかどうかを判断します。疑わしい、またはリスクが高いとみなされたユーザーには、プロンプトが表示され、次のステップでユーザーの本人確認を行います。

1. そのユーザーに対して複数の本人確認方法が構成されている場合、プロンプトに従って、ODA（On-Demand 認証）またはセキュリティ クエスチョンのいずれかを選択します。
2. ODA を選択した場合、PIN を入力します。Authentication Manager からユーザー宛に、メールまたは SMS でトークンコードが送信されます。ブラウザにトークンコードを入力し、認証を受けます。

   セキュリティ クエスチョンを選択した場合、プロンプトに従って、事前に設定した質問に答えます。正解すると、認証が成功します。

リスク ベース認証のしくみ

RBA（リスク ベース認証）は、各ユーザーの認証リスクをインテリジェントに評価し、各ユーザーのデバイスと行動パターンに関する知識を長期間にわたり蓄積して認証試行が正当かどうかを判断します。RBA には、次のような機能があります。

データ収集。RBA には、ユーザーのデバイスと行動のプロファイルを蓄積する学習期間が必要です。初期の学習期間が終了した後も、RBA は一般的なユーザーの行動から学習を続けて、リスク モデルを定期的にカスタマイズし、導入環境に応じた「正常」と「異常」の定義を調整します。

デバイス登録。ユーザーがあるデバイスからの認証に初めて成功したとき、RBA はデバイスの特性をユーザーのデバイス履歴に記録します。これによって、そのデバイスがユーザーに登録されます。登録デバイスとは、Authentication Manager が識別可能な、ユーザーが以前に認証に使用したデバイスです。

デバイス一致。認証時、RBA はユーザーのラップトップまたはデスクトップ コンピュータの特性を収集し、以前使用されたデバイスのリストと比較して近いものを検出しようとします。

保証レベル。RBA は、デバイス特性やユーザーの行動パターンを使用して保証レベルを計算します。保証レベルは、アクセス試行が正当なユーザーによる可能性の高さを示します。ユーザーが認証を試行すると、RBA は収集したデータを参照してそのリスクを評価し、その後、ユーザーの認証試行に高、中、低の保証レベルを割り当てます。

RBA の詳細については、第 12 章、リスク ベース認証の導入を参照してください。

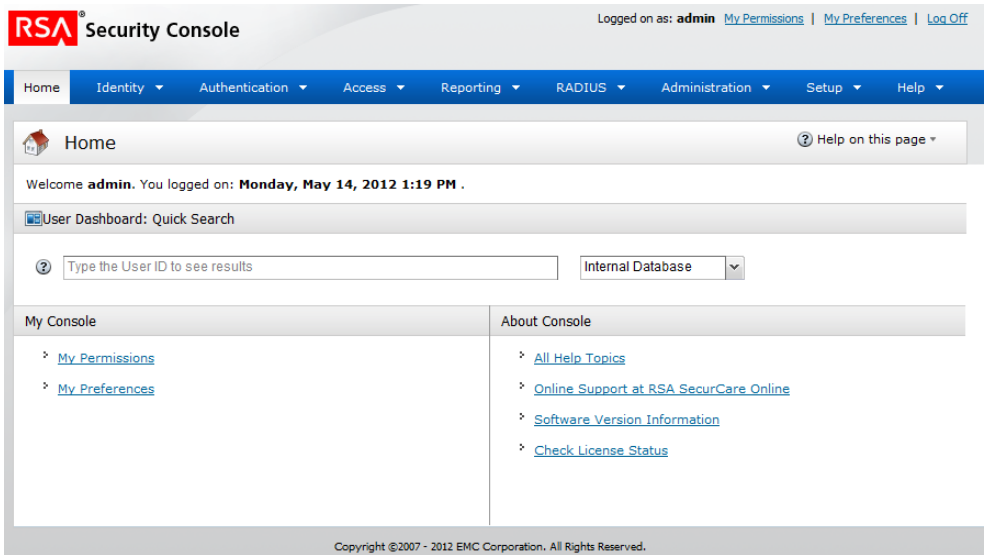
2 RSA Authentication Manager の管理の準備

RSA Authentication Manager を管理する前に、管理を行うための準備を導入環境で実施する必要があります。この章では、Security Console と組織階層について説明します。また、導入環境を管理可能な状態にするためのタスクについても説明します。

Security Console

Authentication Manager には、Security Console と呼ばれる管理用ユーザー インタフェースが付属しています。

次の図は、Security Console のホーム ページを示しています。



日常的な管理作業の大半と、セットアップおよび構成タスクの一部は、この Security Console から実行できます。たとえば、Security Console では次のような操作が可能です。

- ユーザーおよびユーザー グループの追加と管理
- 管理者の追加と管理
- RSA SecurID トークンの割り当てと管理
- ユーザーのリスク ベース認証または On-Demand 認証の有効化 / 無効化
- セキュリティ ポリシーの追加と管理
- 認証エージェントの追加と管理
- 保護対象のネットワーク リソースの指定

Authentication Manager の Quick Setup 実行時に、Security Console のスーパー管理者アカウントのユーザー ID とパスワードを作成します。スーパー管理者アカウントは、Authentication Manager のすべてのタスクを実行する権限を持っています。

Quick Setup では、Operations Console の初期ユーザー ID およびパスワードも作成します。将来 Security Console または Operations Console のいずれか一方のユーザー ID やパスワードを変更しても、他方のユーザー ID やパスワードには影響ありません。これらは別々のアカウントです。

Console のアカウントとパスワードの詳細については、190 ページの Authentication Manager 管理者アカウントを参照してください。

Security Console へのログオン

Authentication Manager の Quick Setup 後に初めてログオンするときは、Quick Setup 時に指定したユーザー ID とパスワードを使用してください。2 回目以降のログオン時には、Security Console からリクエストされるクレデンシャルを入力してください。

注：Security Console 内で前に表示したページに戻るときは、インターネットブラウザの［Back（戻る）］ボタンを使用しないでください。コンソール内の移動には、Security Console のナビゲーション用メニューやボタンを使用します。

処理手順

Security Console にログオンするには、次の URL にアクセスします。

```
https:// 完全修飾ドメイン名 :7004/console-ims
```

重要：Security Console を RSA SecurID で保護する場合は、SecurID PIN では大文字と小文字が区別される点に注意してください。

RSA SecurID による Security Console の保護の詳細については、38 ページの Security Console の保護を参照してください。

Security Console のカスタマイズ

Security Console はカスタマイズが可能で、個人用の表示設定やシステム全体の表示オプションを構成できます。表示属性は、管理者別に設定します。したがって、各管理者が Security Console セッションを自分専用に構成できます。

個人の環境設定

Security Console では、リストページに表示する項目の数、および Security Console で使用する言語を指定できます。

手順

1. Security Console のホーム ページで［**My Preferences（環境設定）**］をクリックします。
2. リスト ページに表示する項目のデフォルトの件数を指定するには、［**Items Per List Page（リストページごとの項目件数）**］ドロップダウン メニューから選択します。
3. Security Console で使用する言語を指定するには、［**Language（言語）**］ドロップダウン メニューから選択します。
4. ショートカット キーを変更するには、［Keyboard Shortcuts（**キーボード ショートカット**）］で、該当する構成要素の横に新しいキーを入力します。各ショートカットは一意に 1 つの構成要素を特定する必要があります。したがって、1 つの文字を繰り返し使用することはできません。
5. ［**Save（保存）**］をクリックします。

次のステップ

環境設定を有効にするためには、ログオフしてからもう一度ログオンし直す必要があります。

システム全体の表示オプションのカスタマイズ

Security Console の構成可能なシステム全体の表示オプションは、次のとおりです。

オプション	説明
Items Per List Page（リストページごとの項目件数）	検索結果ページに表示する 1 ページあたりの項目件数を設定できます。［25］、［50］、［100］、［250］、［All（すべて）］のいずれかを選択できます。デフォルト値は［25］です。
Language（言語）	Security Console で使用する言語を設定できます。デフォルトは［English（英語）］です。
Identity attributes（アイデンティティ属性）	デフォルトで、値を持つ属性のみをユーザー フォームに表示するか否かを選択できます。［Mobile Phone Number（携帯電話番号）］など、フォームに表示されるアイデンティティ属性の表示 / 非表示を切り替えます。
Quick User Search Criteria（クイック ユーザー検索の条件）	ホーム ページとユーザー ダッシュボード上のクイック ユーザー検索を、苗字またはユーザー ID のどちらで検索するかを構成します。デフォルトは［last name（苗字）］です。

オプション	説明
Table columns（表の列）	ユーザー リストの表の列の情報の、表示 / 非表示を切り替えます。
Search criteria（検索条件）	ユーザー リスト ページの検索パネルで、[Where（抽出条件）] ドロップダウン メニューに表示される属性の表示 / 非表示を切り替えます。
Basic user attributes（ユーザーの基本属性）	[First Name（名前）] など、フォームに表示されるユーザー属性の表示 / 非表示を切り替えます。
Table columns（表の列）	トークン リストの表の列の情報の、表示 / 非表示を切り替えます。
Search criteria（検索条件）	トークン リスト ページの検索パネルで、[Where（抽出条件）] ドロップダウン メニューに表示される属性の表示 / 非表示を切り替えます。

コンソール表示オプションの設定

Security Console 表示オプションにより、情報管理者が Security Console を使用するときに表示できる情報が決まります。これらのオプションは、導入環境全体に影響を与えます。

一部の設定は、管理者個人の環境設定で上書きできます。これらの変更が影響するのは、その管理者のみです。

管理者が追加する新しいアイデンティティ属性定義は、[**Table Columns（表の列）**] フィールドではすべてデフォルトで非表示に設定されますが、[**Search Criteria（検索条件）**] フィールドと、ユーザーフォーム表示設定の [**Identity Attributes（アイデンティティ属性）**] フィールドではデフォルトで表示に設定されます。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [Console & Session Settings（コンソールとセッションの設定）] セクションで、[**Security Console Display Options（Security Console 表示オプション）**] をクリックします。
3. [**Items Per List Page（リストページごとの項目件数）**] では、各リスト ページに表示する項目の件数を選択します。
4. [**Language（言語）**] では、Security Console で使用する言語を選択します。

5. ［**Identity Attributes（アイデンティティ属性）**］では、ユーザーフォームのデフォルト表示で、値を持つ属性のみを表示するか否かを選択します。ユーザーごとに、ユーザー フォームで表示と非表示を切り替えることができます。
6. ［**Quick User Search Criteria（クイック ユーザー検索条件）**］では、クイック ユーザー検索およびユーザー ダッシュボードにおいて苗字で検索するかユーザー ID で検索するかを選択します。
7. ［**User List Display（ユーザー リスト表示）**］セクションで、次の操作を実行します。
   a. ［**Table Columns（表の列）**］で、ユーザーを一覧表示するページに追加する列を選択します。たとえば、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックすると、選択した列がユーザー リストに表示されます。［User ID（ユーザー ID）］列は必須です。
   b. ［**Search Criteria（検索条件）**］では、ユーザーを一覧表示するページの［Search Criteria（検索条件）］ドロップダウン メニューに表示する項目を選択します。［User ID（ユーザー ID）］列は必須です。
8. ［**User Form Display（ユーザー フォーム表示）**］セクションで、次の操作を実行します。
   a. ［**Basic User Attributes（ユーザーの基本属性）**］では、ユーザー フォームに表示する属性を選択します。非表示の属性は、管理者が編集することも表示することもできません。［User ID（ユーザー ID）］フィールドと［Last Name（苗字）］フィールドは必須です。
   b. ［**Identity Attributes（アイデンティティ属性）**］では、ユーザー フォームに表示するアイデンティティ属性を選択します。非表示の属性は、管理者が編集することも表示することもできません。非表示にするアイデンティティ属性は、表示するアイデンティティ属性のリストからすべて削除してください。
9. ［**Token List Display（トークン リスト表示）**］セクションで、次の操作を実行します。
   a. ［**Table Columns（表の列）**］フィールドを使用して、SecurID トークンを一覧表示するページに追加する列を選択します。SecurID トークンのシリアル番号は、SecurID トークン リストの先頭の列に常に表示されます。
   b. ［**Search Criteria（検索条件）**］フィールドで、SecurID トークンを一覧表示するページの検索条件ドロップダウン メニューに表示する項目を選択します。SecurID トークンのシリアル番号は、検索条件ドロップダウン メニューの先頭の列に常に表示されます。
10. ［**Save（保存）**］をクリックします。

Security Console の保護

デフォルトでは、管理者は RSA パスワードか LDAP パスワードを使用して Security Console にアクセスできます。LDAP パスワードを使用する場合は、その管理者のアイデンティティ ソースが LDAP ディレクトリ サーバである必要があります。

セキュリティを強化するために、管理者が Security Console にアクセスするときに RSA SecurID パスコードを入力するよう Authentication Manager を構成できます。

次の認証方式を構成することにより、デフォルトの設定を変更できます。

- RSA パスワード
- LDAP パスワード
- RSA SecurID パスコード

コンソールへのアクセスを許可する前に SecurID パスコードの入力を求めることで、Security Console を、ネットワーク リソースの場合と同等の 2 要素認証で保護できます。Security Console を SecurID パスコードで保護する場合、SecurID PIN では大文字と小文字が区別される点に注意してください。

Security Console の認証方式として新しい認証方式を有効化するときは、変更前の認証方式の使用も一定期間許可することを推奨します。このようにすることで、以前の認証方式が使えなくなる前に、すべての管理者が新しい認証方式に移行できます。

Security Console の認証方式の構成

この手順では、管理者が Security Console にアクセスするために使用する認証方式を構成します。たとえば、Security Console にアクセスする時に、管理者に RSA SecurID パスコードの入力を求めることによって、セキュリティを高めることができます。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。
2. ［Console & Session Settings（コンソールとセッションの設定）］で、［**Security Console Authentication Methods（Security Console の認証方式）**］をクリックします。
3. ［**Console Authentication（コンソールの認証）**］フィールドに、管理者が Security Console へのログオン時に使用する認証方式を入力します。複数の認証方式を入力する場合は、演算子を使用して有効な式を作成します。次に例を挙げます。
   - RSA パスワードまたは LDAP パスワードを要求する場合は、「**RSA_Password/LDAP_Password**」と入力します。
   - RSA SecurID パスコードと LDAP パスワードの両方を要求する場合は、「**SecurID_Native+LDAP_Password**」と入力します。

- RSA パスワードを要求する場合は、「**RSA_Password**」と入力します。
- LDAP パスワードを要求する場合は、「**LDAP_Password**」と入力します。
- RSA SecurID パスコードを要求する場合は、「**SecurID_Native**」と入力します。

現在の方法よりも強力な認証方式を入力した場合は、いったんログオフした後、新しいクレデンシャルで認証を受ける必要があります。たとえば、元の方法が **RSA_Password/LDAP_Password** であるときに「**(RSA_Password/LDAP_Password)+SecurID_Native**」と入力すると、Security Console からログオフされます。その後、RSA パスワードまたは LDAP パスワードと SecurID パスコードを使用して認証を受ける必要があります。現在の方法よりも強力でない認証方法を入力した場合、変更内容は新しい認証試行にのみ作用します。

4. （オプション）複数のアイデンティティ ソースで同じユーザー ID を使用できるようにする場合は、［**Non-Unique User IDs（一意でないユーザー ID）**］で［**Identical User IDs may exist in more than one identity source（複数のアイデンティティ ソースで同一ユーザー ID を使用できる）**］を選択します。この設定は、異なるタイプのユーザーの名前を含む複数のアイデンティティ ソースがある場合に有用です。

   ここでは、従業員用と顧客用にそれぞれ 1 つのアイデンティティ ソースがあると仮定します。このオプションを使用することで、両方のアイデンティティ ソースに存在する同じユーザー ID を管理できるようになります。たとえば、ユーザー ID が jsmith の従業員と、ユーザー ID が jsmith の顧客を存在させることができます。

5. （オプション）LDAP パスワードを認証方式として有効化する場合は、［**LDAP Password（LDAP パスワード）**］で、［**Enable LDAP Password authentication method（LDAP パスワード認証方式を有効化する）**］を選択します。
6. ［**Save（保存）**］をクリックします。
7. ［**Yes, update authentication methods（はい。認証方式を更新します）**］を選択します。
8. ［**Update Authentication Methods（認証方式の更新）**］をクリックします。

アイデンティティ ソース

アイデンティティ ソースは、ユーザーおよびユーザー グループのデータが保存されているリポジトリです。導入環境のすべてのユーザーおよびユーザー グループは、アイデンティティ ソースに関連づけられています。

Authentication Manager では、次のアイデンティティ ソースをサポートしています。

- LDAP ディレクトリ

  Authentication Manager では、アイデンティティ ソースとして次のディレクトリをサポートしています。

  – Active Directory 2008 R2

  – Sun Java System Directory Server 7.0

  – Oracle Directory Server Enterprise Edition 11G

  Active Directory では、アイデンティティ ソースとしてグローバル カタログを追加できます。これは、認証時にユーザーを検索し、グループ メンバーシップを解決するために使用されます。グローバル カタログ アイデンティティ ソースを使用して、管理タスクを実行することはできません。

- Authentication Manager の内部データベース

詳細については、第 5 章、LDAP ディレクトリの統合を参照してください。

LDAP ディレクトリのデータ

Authentication Manager は、すべての LDAP ディレクトリ アイデンティティ ソースに対する read-only アクセス権を持っています。ディレクトリを Authentication Manager と統合すると、Security Console を使用して、次の操作を実行できます。

- ディレクトリに存在するユーザーおよびユーザー グループ データを表示する（ただし、追加、変更はできない）。
- Authentication Manager の管理タスクを実行する。たとえば、ODA（On-Demand 認証）および RBA（リスク ベース認証）の使用を有効化または無効化することや、ディレクトリに存在する個々のユーザーにトークンまたはユーザー エイリアスを割り当てることができます。

ディレクトリ内のデータを変更するには、LDAP ディレクトリのネイティブ ユーザー インタフェースを使用する必要があります。

内部データベースのデータ

Authentication Manager には、ユーザーおよびユーザー グループを作成できる内部データベースが付属しています。管理者は、Security Console を使用して、内部データベース内のユーザーおよびユーザー グループに対して次の操作を実行できます。

- ユーザーおよびユーザー グループのデータを追加、変更、表示する。
- 個々のユーザーに対して Authentication Manager の機能（ODA や RBA など）を有効化または無効化する。

次の情報は、内部データベースのみに格納されています。

- ポリシー、管理者ロール、認証エージェント、SecurID トークンレコードなど、Authentication Manager に固有のデータ
- LDAP ディレクトリのユーザーおよびユーザー グループ レコードを Authentication Manager にリンクするためのデータ

セキュリティ ドメインの概要

セキュリティ ドメインは、管理責任の領域を表しています。すべての Authentication Manager オブジェクトは、セキュリティ ドメインによって管理され、セキュリティ ドメインに所属します。セキュリティ ドメインを使用することで、次の操作が可能になります。

- ユーザーの編成と管理。
- システム ポリシーの適用。
- 管理者がアクセス可能なセキュリティ ドメインを制限することによる、管理者の権限適用範囲の限定。

ユーザーの編成と管理

セキュリティ ドメインを作成する時には、親セキュリティ ドメインを指定する必要があります。セキュリティ ドメインをネストすることで管理階層を構築できます。セキュリティ ドメインを使用してユーザーを編成することのメリットとして、ユーザーの検索やトークンの割り当て、ユーザー グループへの追加などが容易になるという点もあります。たとえば、ボストン セキュリティ ドメイン内のすべてのユーザーを検索し、各ユーザーにトークンを割り当てることができます。個々のユーザーは 1 つのセキュリティ ドメインにのみ所属できます。

デフォルトでは、外部 LDAP アイデンティティ ソース内のすべてのユーザーは最上位のセキュリティ ドメインに追加されます。Security Console を使用して、これらのユーザーを手動で下位のセキュリティ ドメインに移動できます。または、これらのユーザーを特定のセキュリティ ドメインに追加するようにドメイン マッピングを構成できます。ユーザーを管理する前に適切にマッピングしておけば、後からセキュリティ ドメインの間でユーザーを移動する必要がなくなります。詳細については、146 ページのセキュリティ ドメイン間でのユーザーの移動を参照してください。

管理者が Security Console を使用して内部データベース上に作成したユーザーは、その管理者がアクセス権を持つセキュリティ ドメインに作成されます。

ポリシーの適用

Authentication Manager の Quick Setup が完了すると、最上位のセキュリティ ドメインが自動的に作成されます。最上位のセキュリティ ドメイン名は編集できません。デフォルトで、Authentication Manager は、最大 1,000 個のセキュリティ ドメインをサポートしています。

Authentication Manager は、セキュリティ ドメイン レベルで認証ポリシーを適用するため、同じポリシーの対象となるユーザーを同じセキュリティ ドメインにグループ化することを検討してください。

管理者の権限適用範囲

デフォルトでは、すべての SecurID トークンは、最上位のセキュリティ ドメイン内で管理されます。管理者は Security Console を使用して、トークンを最上位のセキュリティ ドメインから導入環境内の他のセキュリティ ドメインに移動できます。

セキュリティ ドメインについては、次の点に留意してください。

- セキュリティ ドメインは階層状に編成されます。
- 通常、セキュリティ ドメインは、組織の部門構造や地理的な場所に応じて作成されます。

たとえば、経理、R&D（研究開発）、HR（人事）などの部門ごとに個別のセキュリティ ドメインを作成し、各部門のユーザーとユーザー グループを対応するセキュリティ ドメインに移動することができます。管理者が特定のセキュリティ ドメインのユーザーを管理するためには、そのセキュリティ ドメインを管理する権限を持っている必要があります。

セキュリティ ドメインを使用すると、ユーザー管理だけでなく、管理者の権限適用範囲の制限も容易になります。たとえば、ボストン、ニューヨーク、サンノゼの 3 つのセキュリティ ドメインが存在しているとします。この場合、管理者ロールの権限適用範囲をボストンのセキュリティ ドメインのみに限定するように設定することもできます。このロールが割り当てられた管理者は、その権限適用範囲をボストンのセキュリティ ドメイン内に限定され、ニューヨークのセキュリティ ドメインやサンノゼのセキュリティ ドメインは管理できません。

このように構成することで、管理者の制御が非常に容易になります。管理者の権限を、部門、地理的場所、またはその他の任意の方法で制限することができます。また、管理者は、階層構造を利用して、ユーザーとユーザーのアクセス許可およびアクセス制限をより柔軟に管理できます。

セキュリティ ドメインとポリシー

セキュリティ ドメインは、システム ポリシーの適用にも使用されます。ポリシーは、ユーザーと Authentication Manager の間のやり取りにかかわるさまざまな側面を制御します（パスワードの有効期間 / 長さ / 形式 / 変更頻度、認証失敗時の再試行回数など）。

セキュリティ ドメインには、次のポリシーが割り当てられます。

- 84 ページのトークン ポリシー
- 101 ページのロックアウト ポリシー
- 92 ページのオフライン認証ポリシー
- 96 ページのパスワード ポリシー
- 103 ページのセルフ サービス トラブルシューティング ポリシー
- 107 ページのリスク ベース認証ポリシー
- 110 ページのリスク ベース認証メッセージ ポリシー

Authentication Manager にはすべてのタイプのポリシーにデフォルトポリシーが用意されており、新しいセキュリティ ドメインを作成するときに割り当てられます。これらのデフォルト ポリシーを受け入れるか、カスタム ポリシーを作成できます。カスタム ポリシーをデフォルトポリシーとして指定すると、そのポリシーは新規作成するすべてのセキュリティ ドメインと、デフォルト ポリシーを使用するように構成されたすべての既存のセキュリティ ドメインで使用されます。

たとえば、ある管理者が「Finance Password Policy」という名前のカスタム ポリシーを作成し、デフォルトのパスワード ポリシーとして指定したとします。この Finance Password Policy は、新規作成するすべてのセキュリティ ドメインと、デフォルトのパスワード ポリシーを使用するよう構成されているすべてのセキュリティ ドメインに自動的に割り当てられます。数か月後に、「Miller and Strauss Password Policy」という新しいカスタム ポリシーを作成し、このポリシーをデフォルトのパスワード ポリシーに指定したとします。この指定以降、デフォルトのパスワード ポリシーを使用するよう構成されているすべてのセキュリティ ドメイン、および新規作成するすべてのセキュリティ ドメインに、Miller and Strauss Password Policy が自動的に適用されます。

下位のセキュリティ ドメインは、上位のセキュリティ ドメインからポリシーを継承しません。新規作成するセキュリティ ドメインには、階層内の上位のセキュリティ ドメインに割り当てられているポリシーにかかわらず、デフォルト ポリシーが適用されます。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーが割り当てられていても、その下のセキュリティ ドメインではデフォルト ポリシーが引き続き使用されます。

セキュリティ ドメインの追加

セキュリティ ドメインは、管理責任の範囲を定義するもので、通常、企業のビジネス ユニット、部署などに対応します。セキュリティ ドメインは、組織階層の 1 つの単位を表します。セキュリティ ドメイン間に関係を作成することで、階層を構築します。セキュリティ ドメインは最大 1,000 個作成できます。

開始する前に

- 使用可能なカスタム ポリシーおよびデフォルト ポリシーについて理解する。詳細については、43 ページのセキュリティ ドメインとポリシーを参照してください。
- 次のガイドラインに従う。
  - デフォルト ポリシーを使用するには、ドロップダウン リストから、［**Always Use Default**（常にデフォルトを使用する）］を選択します。デフォルト ポリシーが、セキュリティ ドメインに対して自動的に適用されます。
  - カスタム ポリシーを使用するには、ドロップダウン リストからポリシー名を選択します。明示的に変更するまで、このポリシーがこのセキュリティ ドメインに適用されます。
  - 適用したポリシーがデフォルト ポリシーでもある場合、デフォルト ポリシーを変更した場合でもそのポリシーがセキュリティ ドメインに割り当てられたままになります。デフォルト ポリシーを使用するには、［**Always Use Default（常にデフォルトを使用する）**］を明示的に指定する必要があります。

手順

1. Security Console で、［**Administration（管理）**］＞［**Security Domains（セキュリティ ドメイン）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Security Domain Name（セキュリティ ドメイン名）**］フィールドに、一意の名前を入力します。最大文字数は 100 文字です。
3. ［**Parent（親）**］ドロップダウン リストから、新しいセキュリティ ドメインの親セキュリティ ドメインを選択します。親セキュリティ ドメインは、新しいセキュリティ ドメインの所属先となるセキュリティ ドメインです。
4. ［**Password Policy（パスワード ポリシー）**］ドロップダウン リストから、新しいセキュリティ ドメインのパスワード ポリシーを選択します。パスワード ポリシーは、必要なパスワード長、文字、使用できない単語などを指定します。

5. ［**Lockout Policy（ロックアウト ポリシー）**］ドロップダウン リストから、新しいセキュリティ ドメインに割り当てるロックアウト ポリシーを選択します。ロックアウト ポリシーを使用すると、指定の時間内に一定回数以上ログオンに失敗したユーザーをロックアウトできます。ロックアウトされたユーザーは認証できません。
6. ［**Self-Service Troubleshooting Policy（セルフ サービス トラブルシューティング ポリシー）**］ドロップダウン リストから、新しいセキュリティ ドメインのポリシーを選択します。このポリシーは、ユーザーがパスワードやパスコードなどの本来の認証方法を使用できなくなった場合に Self-Service Console にログオンする方法を制御します。
7. ［**Risk-Based Authentication (RBA) Policy（RBA（リスク ベース認証ポリシー）**］ドロップダウン リストから、新しいセキュリティ ドメインのポリシーを選択します。RBA ポリシーには、ログオンに必要な最低保証レベル、および認証試行が最低保証レベルに満たない場合に使用するユーザー確認方法が含まれます。
8. ［**SecurID Token Policy**（SecurID トークン ポリシー）］ドロップダウン リストから、セキュリティ ドメインに割り当てる SecurID トークン ポリシーを選択します。トークン ポリシーでは、RSA SecurID PIN の有効期間と形式、固定パスコードの有効期間と形式を定義します。ユーザーや不正侵入者が不正なパスコードを複数回入力した場合の対処方法も定義します。
9. ［**Offline Authentication Policy**（オフライン認証ポリシー）］ドロップダウン リストから、セキュリティ ドメインに割り当てるオフライン認証ポリシーを選択します。オフライン認証ポリシーでは、ネットワークに接続できない場合のユーザー認証方法を定義します。
10. （オプション）［**Workflow Policies（ワークフロー ポリシー）**］ドロップダウン リストから、セキュリティ ドメインのワークフロー ポリシーを選択します。ワークフロー ポリシーは、メールの受信者、ワークフロー定義、承認ステップと配布ステップの数、Self-Service Console からのリクエストに関するメール通知を指定します。
11. ［**Risk-Based Authentication (RBA) Message Policy（RBA（リスク ベース認証）メッセージ ポリシー）**］ドロップダウン リストから、新しいセキュリティ ドメインのポリシーを選択します。このポリシーは、ユーザーにユーザー確認方法の構成を求めるときに伝えるメッセージを定義します。
12. ［**Save（保存）**］をクリックします。

デフォルトセキュリティ ドメイン マッピング

デフォルトでは、外部 LDAP アイデンティティ ソースのすべてのユーザーが最上位のセキュリティ ドメインに配置されます。セキュリティ ドメイン マッピングを構成すると、デフォルトの動作を上書きして、特定の LDAP アイデンティティ ソースまたはアイデンティティ ソース内の特定の組織単位のユーザーが特定のセキュリティ ドメインに配置されるようにできます。

たとえば、LDAP ディレクトリの「ou=sales,dc=example,dc=com」に格納されている営業部のユーザーを「Corporate」セキュリティ ドメインにマッピングする場合は、「Corporate」という名前のセキュリティ ドメインと「ou=sales,dc=example,dc=com」という識別名（DN）の間のマッピングを作成します。このマッピングを作成すると、「ou=sales」の下のユーザーは、最上位のセキュリティ ドメインではなく、「Corporate」セキュリティ ドメインによって管理されるようになります。

以下の点を考慮してください。

- セキュリティ ドメイン マッピングが存在しない場合、ユーザーは最上位のセキュリティ ドメインに追加される。
- 複数のセキュリティ ドメイン マッピングが存在する場合、新しいユーザー レコードには最も具体的なマッピングが適用される。

  たとえば、外部アイデンティティ ソースのユーザーに対して、「ou=sales」と「ou=commercial,ou=sales」に基づく 2 つのマッピングがあるとします。「ou=commercial,ou=sales」のユーザーには、「ou=commercial,ou=sales」のルールが適用されますが、「ou=retail,ou=sales」のユーザーは「ou=sales」のルールが適用されます。
- セキュリティ ドメイン マッピングは導入環境で今まで管理されていなかったユーザーにのみ適用される。
  - セキュリティ ドメイン マッピングを構成する前に、管理者が、ユーザーの On-Demand 認証を有効化するなど、ユーザーに影響を与える管理アクションを実行した場合、そのユーザーは最上位のセキュリティ ドメインに追加されます。
  - マッピング後も、以前から管理されているユーザーは現在属しているセキュリティ ドメイン内に残ります。ユーザーを別のセキュリティ ドメインに手動で移動するには、Security Console を使用する必要があります。アイデンティティ ソースのデフォルトのセキュリティ ドメイン マッピングを更新しても、そのアイデンティティ ソース内のすべてのユーザーが更新後のセキュリティ ドメインに移動するとは限りません。
- デフォルトセキュリティ ドメイン マッピングによって委譲管理が強化される。マッピングにより、権限適用範囲がセキュリティ ドメインに制限された特定の管理者が管理するセキュリティ ドメインにユーザーが追加されます。このように、適切な権限適用範囲が設定されている管理者のみがユーザーを管理できるため、スーパー管理者が手動でユーザーをセキュリティ ドメインに追加する必要性がありません。

- 各セキュリティ ドメイン マッピングは外部アイデンティティ ソースの識別名 (DN) を参照し、より具体的なマッピングが存在する場合を除き、DN 内のすべてのオブジェクトに適用される。

DNS（ドメイン ネーム システム）の更新計画

ユーザーが Web Tier とロードバランサ（オプション）にインターネット経由でアクセスできるようにするには、それらのシステムに対してパブリックに解決可能な名前を購入する必要があります。次の手順を実行します。

- ドメイン名を定義します（例：mydomain.com）
- ホスト名を定義します（例：myhost.mydomain.com）
- ドメイン名の登録機関に連絡して、ドメイン名とホスト名を登録します。

セルフ サービスおよびリスク ベース認証（RBA）を使用するクライアントは、DNS（ドメイン ネーム システム）を使用して仮想ホスト名を解決できる必要があります。

- 導入環境にロードバランサがある場合、仮想ホスト名はロードバランサのパブリック IP アドレスに解決される必要があります。
- 導入環境にロードバランサがない場合、仮想ホスト名は Web Tier のパブリック IP アドレスに解決される必要があります。

管理者ロールの概要

管理者は、導入環境内のユーザー、トークン、セキュリティ ドメインなどのあらゆる要素を管理します。各管理者に割り当てられる管理者ロールには、管理者権限とそれらの適用範囲が明確に規定されています。

管理者ロールにより、管理者の権限適用範囲が決まります。ユーザーは、管理者ロールを割り当てられると、管理者となります。

管理者ロールのタイプ

管理者ロールには、次の 2 つのタイプがあります。

- **事前定義ロール**。Authentication Manager には、事前に定義されたロールが用意されています。事前定義ロールをデフォルト設定のまま使用することも、ロールに割り当てられた権限を変更することも可能です。
  たとえば、ヘルプ デスクロールを持つ管理者に対して認証エージェントを表示しないようにするには、Security Console を使用してこのロールから該当する権限を削除します。

- **カスタム ロール**。組織のニーズに応じて、固有の権限とそれらの適用範囲を定義したカスタム ロールを作成できます。

  たとえば、管理対象の組織階層が、人事、研究開発、経理という 3 つのセキュリティ ドメインに分割されているとします。機密を要する経理データを保護するには、経理セキュリティ ドメイン内で経理レポートを実行および表示できるカスタム管理者を作成する方法が効果的です。

管理者ロールの割り当て

導入環境に必要なロールを決定し、必要なカスタム ロールを追加した後は、各管理者にロールを割り当てます。

管理者ロールを割り当てるときは、次の点に留意してください。

- 管理者ロールはアイデンティティ ソース内の任意のユーザーに割り当てることができます。一般的には IT（情報テクノロジー）部門のメンバー、およびその他部門の信頼できる少数のスタッフに管理者ロールを割り当てます。
- ロールをユーザーに割り当てると、そのユーザーが Authentication Manager 管理者となり、Security Console を使用して導入環境を管理できるようになります。
- ロールを管理者に割り当てると、管理者は、そのロールにより許可される管理アクションを、ロールの権限適用範囲に指定されているセキュリティ ドメイン内で実行できます。
- 割り当てることができる管理者ロールは、自分のロールと同等またはそれ以下の権限を持つ管理者ロールのみです。自分が保有していない権限を割り当てることはできません。たとえば、ユーザーの追加 / 編集 / 削除、および管理者ロールの作成と割り当てができる権限を備えたロールを持つ管理者は、On-Demand トークンコードの使用をユーザーに許可するロールを他の管理者に割り当てることはできません。
- 自分のロール以上の権限を持つ管理者ロールを編集することもできません。
- 1 人の管理者に複数のロールを割り当てることもできます。この場合、その管理者による管理アクションの実行対象は、ロールによって実行権限を付与されたセキュリティ ドメイン内に限定されます。

  たとえばある管理者が、サンノゼセキュリティ ドメイン内でユーザーを管理できる権限を備えた管理者ロールと、ニューヨークセキュリティ ドメイン内でトークンを管理できる権限を備えた管理者ロールを割り当てられているとします。Security Console でこの管理者がログオンしたときには、サンノゼセキュリティ ドメイン内のユーザー管理は許可されますが、ニューヨークセキュリティ ドメイン内のユーザー管理は許可されません。したがって、ニューヨークセキュリティ ドメイン内のユーザーは管理者には表示されません。トークンにも同じルールが適用されます。この管理者が管理し表示できるのはニューヨークセキュリティ ドメイン内のトークンのみです。

- ロールを割り当てる際は、該当するタスクの実行に最低限必要な権限とそれらの適用範囲を割り当ててください。不要な権限を備えたロールを管理者に割り当てないようにしてください。
  たとえば、ボストンセキュリティ ドメイン内のユーザーのみを担当する管理者に割り当てるロールの権限適用範囲には、サンノゼやニューヨークのセキュリティ ドメインを含めないようにします。

管理者ロールのコンポーネント

管理者ロールは、次の 2 つのコンポーネントで構成されています。

- ロールの機能に基づく権限
- 権限を適用できる権限適用範囲（セキュリティ ドメインおよびアイデンティティ ソース）

権限

管理者ロールの権限により、ユーザー、ユーザー グループ、セキュリティ ドメイン、ポリシーなどのオブジェクトに対して管理者が実行できるアクションが決定されます。権限を割り当てる際は、管理者に割り当てられたタスクを実行するために必要なすべてのオブジェクトを管理できる権限を付与すると同時に、必要のない権限は付与しないように注意してください。

次の領域を管理するよう権限を変更できます。

- ロールの基本設定
- セキュリティ ドメイン管理
- 委譲管理
- ユーザー
- ユーザー グループ
- レポート
- RSA SecurID トークン
- ユーザー認証属性
- 認証エージェント
- トラステッド レルム
- RADIUS
- On-Demand トークンコード
- プロビジョニングリクエスト

導入環境内のすべてのオブジェクトに対して次の権限を使用できます。

［**All（すべて）**］：オブジェクトに対して任意の管理アクションを実行します。

［**Delete（削除）**］：オブジェクトを削除します。

［**Add（追加）**］：オブジェクトを追加します。

［**Edit（編集）**］：オブジェクトを表示および編集しますが、追加または削除することはできません。

［**View（表示）**］：オブジェクトを表示しますが、追加、編集、削除することはできません。

権限を変更することによって、管理者ロールの権限適用範囲を拡大または縮小できます。たとえば、あなたが FocalView Software Company という企業のスーパー管理者（Super Admin の権限を持つ管理者）であるとします。この企業のボストン オフィスにいる管理者には、トークンの割り当てと管理のみが可能なロールが与えられています。あなたは、この管理者がエージェントの管理もできるようにしようと考えました。この場合、新しい権限を作成する代わりに、その管理者の現在のロールを変更できます。

これらのアクションにより、Boston セキュリティ ドメインと、Boston の下位のセキュリティ ドメイン（存在する場合）について管理者権限が追加されます。権限適用範囲に Boston セキュリティ ドメインのみが含まれる場合、管理者は、そのドメインに所属しているオブジェクト（ユーザー、トークン、エージェントなど）のみを管理できます。

ここで、トークンを管理するロールを複数の管理者が持っているとします。これらの管理者のいずれか 1 人にエージェントを管理させたい場合、ロールを変更してしまうと、そのロールを持つすべての管理者がエージェントを管理できるようになります。この場合は、トークンとエージェントの両方を管理できる新しいロールを作成し、そのロールを特定の 1 人の管理者のみに割り当てることができます。

もう 1 つの方法として、エージェントの管理が可能な別のロールを作成し、そのロールを特定の 1 人の管理者に個別に割り当てることもできます。この場合、その管理者には 2 つのロールが割り当てられることになります。

たとえば、ユーザーへのトークンの割り当てのみを担当する管理者には、次の権限を持つロールを割り当てます。

- ユーザーの表示
- トークンの表示
- ユーザーへのトークンの割り当て
- 割り当て済みのソフトウェア トークンの発行
- 割り当て済みのトークンの交換
- トークンのインポート（オプション）
- トークンの有効化 / 無効化（オプション）

オプションの権限を付与すると、管理者ロールの権限はわずかに強化され、ユーザーにトークンを割り当てる標準的なタスクを実行できるようになります。ただし、ユーザーの追加と削除、トークンの再同期、エマージェンシー オフライン認証の管理などの権限は付与しないでください。これらの権限は、ユーザーへのトークン割り当てにかかわる標準的なタスクには必要ありません。

管理者ロールの作成と権限の委譲に必要な権限

新しい管理者ロールを作成する管理者は、次の権限を持っている必要があります。

- 管理者ロールを作成する権限。
- 新しい管理者ロールに追加するものと同じ権限。
- 自身の管理者ロールに付与された権限を委譲する権限。権限の委譲が可能かどうかは、新しいロールを作成する管理者に割り当てられているロールの権限委譲設定によって決まります。
- 新しいロールに関連づけるセキュリティ ドメインを管理する権限。

ロールに権限を追加するときは、管理者のタスクの実行に必要なすべての権限を追加してください。次に例を挙げます。

- トークンをユーザーに割り当てるには、管理者は、トークンの表示と割り当て、およびユーザーの表示の権限を持っている必要があります。
- ユーザー パスワードをリセットするには、管理者は、パスワードのリセット、およびユーザー レコードの表示の権限を持っている必要があります。
- 管理者ロールをユーザーに割り当てるには、管理者は、ロールの割り当て、およびユーザー レコードの表示の権限を持っている必要があります。
- ユーザーをユーザー グループに割り当てるには、管理者は、ユーザーのユーザー グループへの割り当て、およびユーザー レコードの表示の権限を持っている必要があります。

ロールを作成したり既存のロールを他のユーザーに割り当てることがロールによって許可されている場合は、権限を他の管理者に委譲できます。［Permission Delegation（権限の委譲）］を選択する手順については、RSA Security Console ヘルプのトピック「管理者ロールの複製」を参照してください。

アイデンティティ属性定義を管理するための権限の制限

特定のカスタム定義のアイデンティティ属性定義を管理する権限を管理者ロールで制限できます。任意のアイデンティティ属性定義に対し、管理者ロールで［Modify（変更）］、［View（表示）］、［None（なし）］の権限を付与できます。詳細については、RSA Security Console ヘルプのトピック「ユーザー属性」を参照してください。

管理者ロールを追加または編集するとき、[Permissions（権限）]ページで特定のアイデンティティ属性定義の権限を設定できます。詳細については、RSA Security Console ヘルプのトピック「管理者ロールの複製」および「管理者ロールの権限の編集」を参照してください。

権限適用範囲

管理者ロールの権限適用範囲により、管理者がオブジェクトを管理できるセキュリティ ドメインと、管理者がユーザーおよびユーザー グループを管理できるアイデンティティ ソースが決定されます。詳細については、41 ページのセキュリティ ドメインの概要を参照してください。

必要なセキュリティ ドメインとアイデンティティ ソースにアクセスできるよう、十分な権限適用範囲を割り当てるようにしてください。ただし、セキュリティ上の理由から、管理者の担当外のセキュリティ ドメインやアイデンティティ ソースへのアクセスを許可するような権限適用範囲を割り当てることは避けてください。

また、管理者が特定のユーザー グループの表示と管理はできるが、そのユーザー グループ内のすべてのユーザーを表示できないという状況は避けてください。このような状況は、管理者の権限適用範囲に含まれているセキュリティ ドメイン内のユーザー グループに、権限適用範囲外のセキュリティ ドメインに所属するユーザーが含まれている場合に発生します。管理者がユーザー グループのメンバーを表示する場合、表示可能なのは管理者の権限が適用されるセキュリティ ドメインのメンバーのみです。管理者がこのグループに対して何らかのアクション、たとえば制限付きエージェントへのアクセス権の付与などを実行しようとした場合、影響を受ける一部のユーザーに気付かない恐れがあります。その結果、本来は権限を付与すべきでないユーザーに権限を与えてしまうことになります。

このような状況を避けるには、次のガイドラインに従ってください。

- すべての管理者にすべてのセキュリティ ドメインのすべてのユーザーを表示する権限を最低限、付与します。これにより管理者が、管理対象グループ内の一部のメンバーを見落とす恐れがなくなります。
- ユーザー グループとそのユーザー グループに含まれるすべてのメンバーを、同一のセキュリティ ドメインに所属させます。これにより、ユーザー グループを表示する権限およびユーザーを表示する権限を持つ管理者は、すべてのメンバー ユーザーを見ることができます。
- 表示できる情報のレポートを管理者に作成させる場合、適切な権限を付与します。一部のレポートには表示以上の権限が必要です。

管理者ロールの権限適用範囲を指定するときは、次の点に留意してください。

- 管理者ロールの権限適用範囲を最も広く設定した場合は、そのロール定義が保存されているセキュリティ ドメインと、その下位に位置するすべてのセキュリティ ドメインを管理可能です。
- 上位のセキュリティ ドメインの管理者ロールは、下位のセキュリティ ドメインを常に管理可能です。

- 管理者ロールの権限適用範囲を特定のセキュリティ ドメインに限定することも可能です。ただし、対象となるのは、管理者ロールが定義されたセキュリティ ドメインまたはその下位のセキュリティ ドメインのみです。管理者ロールは階層の下位方向のセキュリティ ドメインのみ管理でき、上位方向のセキュリティ ドメインは管理できません。
- 管理者ロールをどのセキュリティ ドメインに保存するかということは、ロールの権限適用範囲に影響します。たとえば、最上位のセキュリティ ドメインとしてボストンが、下位のセキュリティ ドメインとしてニューヨークとサンノゼが構成されているとします。ニューヨークセキュリティ ドメインに保存した管理者ロールを割り当てられた管理者は、ニューヨークセキュリティ ドメインおよびその下位に位置するセキュリティ ドメインのオブジェクトのみ管理可能です。このロールを持つ管理者が、ボストンセキュリティ ドメインやサンノゼセキュリティ ドメインのオブジェクトを管理することはできません。

  スーパー管理者ロールを最上位のセキュリティ ドメインに保存し、その他の管理者ロールを下位のセキュリティ ドメインに保存できます。これにより、たとえばヘルプ デスク管理者ロールを持つ下位の管理者が、スーパー管理者のパスワードを変更し、そのパスワードを使用して Security Console にアクセスするといった事態を防止できます。

権限適用範囲の例

たとえば、次のような階層構造を考えてみてください。

- 最上位のセキュリティ ドメインに保存された管理者ロールは、導入環境内の任意のセキュリティ ドメインを管理対象に指定できます。たとえば、セキュリティ ドメイン F のみを管理対象とすることも、すべてのセキュリティ ドメインを管理対象とすることも可能です。
- セキュリティ ドメイン A に保存された管理者ロールは、セキュリティ ドメイン A およびその下位に位置するすべてのセキュリティ ドメインを管理対象に指定できます。
- セキュリティ ドメイン C に保存された管理者ロールは、セキュリティ ドメイン E または C、あるいはその両方を管理対象に指定できます。
- セキュリティ ドメイン E に保存された管理者ロールは、セキュリティ ドメイン E のみを管理できます。

権限適用範囲内で特定の条件に一致するユーザーまたはユーザー グループを管理するように、管理者ロールを構成することも可能です。これは属性ベースのロールと呼ばれます。たとえば、場所に関するアイデンティティ属性定義を定義した場合、管理者ロールでは、セキュリティ ドメイン A とその下位のセキュリティ ドメイン（C、D、E、F）のすべてのユーザーを管理できます。

特定のカスタム ユーザー アイデンティティ属性定義の編集のみを許可する管理者ロールを作成することも可能です。この場合は、ロールが持つ権限の一部として、特定のアイデンティティ属性定義に対する権限を構成します。

特定の属性について、管理者ロールでは次のいずれかの権限を設定できます。

- ［None（なし）］
- ［Read-Only（読み取り専用）］
- ［Modify（変更）］

事前定義の管理者ロール

事前定義の管理者ロールは、次のとおりです。

- Super Admin（スーパー管理者）
- Root Domain Administrator（ルートドメイン管理者）
- Security Domain Administrator（セキュリティドメイン管理者）
- RADIUS Administrator（RADIUS 管理者）
- User Administrator（ユーザー管理者）
- Token Administrator（トークン管理者）
- Help Desk Administrator（ヘルプデスク管理者）
- Privileged Help Desk Administrator（特権ヘルプデスク管理者）
- Agent Administrator（エージェント管理者）
- Request Approver（リクエスト承認者）

- Token Distributor（トークン配布者）
- Trust Administrator（トラスト管理者）

Super Admin（スーパー管理者）

スーパー管理者ロールは、導入環境のすべてのセキュリティ ドメインに対する完全な管理者権限を持つ唯一のロールです。このロールは、他の管理者の作成およびセキュリティ ドメイン階層の作成に使用します。

特に信頼できる管理者だけにこのロールを割り当ててください。

スーパー管理者ロールを管理できるのは、スーパー管理者のみです。

スーパー管理者ロールを複製、編集、削除することはできません。

スーパー管理者は、次の操作を実行できる唯一の管理者です。

- Security Console からユーザーデータにアクセスできるよう、外部ディレクトリをアイデンティティ ソースとして構成する。
- 製品ライセンスをアップグレードする。

セッション有効期間を使用して管理セッションを制限します。詳細については、RSA Security Console ヘルプのトピック「Edit Session Lifetime Settings（セッション有効期間設定の編集）」を参照してください。

スーパー管理者の人数は、組織のニーズに基づいて決定します。スーパー管理者ロールは、その他の管理者ロールと同様の方法で割り当てることができます。詳細については、60 ページの管理者ロールの設定を参照してください。

導入環境には最低 2 人のスーパー管理者を割り当てるようにしてください。こうすることで、1 人のスーパー管理者が休暇などで長期不在となる場合でも、導入環境を完全に管理できます。

たとえば、ボストン、ニューヨーク、サンノゼにそれぞれ拠点を持つ企業の場合は、4 人のスーパー管理者を割り当てます。（ボストンに 2 人、ニューヨークとサンノゼに 1 人ずつ）。このように構成することで、大部分のシステム管理作業が発生するボストンのサイトにおいてスーパー管理者が休暇などで長期不在となる場合にも、管理作業を継続できます。また、ボストン本社から接続できなくなった場合でも、ニューヨークまたはサンノゼから導入環境の管理作業を続行できるため、管理を行えなくなることはありません。

スーパー管理者ロールを割り当てられている管理者であっても、スーパー管理者ロールを変更することはできません。

次のような状況が発生すると、導入環境内にスーパー管理者が 1 人もいなくなる可能性があります。

- スーパー管理者ロールを割り当てられていた唯一のユーザーが削除された場合。
- スーパー管理者ロールを割り当てられていた唯一のユーザーがロールを割り当て解除された場合。

- スーパー管理者ロールを割り当てられていた唯一のユーザーが Security Console からロックアウトされた場合。この状態は、Security Console のログオン要件をパスワードから SecurID に変更したにもかかわらず、事前にスーパー管理者にトークンを割り当てておかなかったときなどに発生します。

このような状況が発生した場合は、Super Admin Restoration ユーティリティを使用して、スーパー管理者をリストアする必要があります。操作手順については、461 ページのスーパー管理者のリストアを参照してください。

Root Domain Administrator（ルートドメイン管理者）

ルートドメイン管理者には、ポリシーや属性定義などの最上位のオブジェクトを含むセキュリティ ドメイン ツリーのすべての面を完全に管理する権限があります。このロールにはスーパー管理者権限の一部が含まれていません。

このロールのデフォルトの権限では、次の要素を完全に管理できます。

- ポリシー
- セキュリティ クエスチョン
- 管理の委譲
- ユーザー
- ユーザー グループ
- レポート
- トークン
- ユーザー認証属性
- 認証エージェント
- トラステッド レルム
- RADIUS
- On-Demand 認証

Security Domain Administrator（セキュリティドメイン管理者）

セキュリティドメイン管理者は、セキュリティ ドメイン階層の特定の分岐内のすべての面を管理します。このロールの管理者は、ポリシーや属性定義などの最上位のオブジェクトを除き、その分岐内のすべてのオブジェクトを管理する権限を持ちます。デフォルトでは、このロールの権限適用範囲は導入環境全体です。

このロールの権限適用範囲を下位のセキュリティ ドメインに制限する場合は、このロールを複製してからその複製したロールの権限適用範囲を編集します。このロールは、スーパー管理者と同じ権限を持ちますが、権限適用範囲がロールで指定したセキュリティ ドメインに制限されています。セキュリティドメイン管理者は、このロールの一部の権限を委譲できます。

このロールのデフォルトの権限では、次の要素を完全に管理できます。

- セキュリティ ドメイン
- 管理者ロール
- 権限
- ユーザー グループ
- レポート
- トークン
- ユーザー アカウント
- エージェント

RADIUS Administrator（RADIUS 管理者）

RADIUS 管理者ロールは、RADIUS サーバを管理するための管理責任を付与します。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、RADIUS とエージェントを完全に管理できます。

User Administrator（ユーザー管理者）

ユーザー管理者は、ユーザーの管理、ユーザーへのトークンの割り当て、制限付き認証エージェントへのアクセスの許可を行います。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- ユーザー：追加、削除、編集、表示、認証方法（RBA または ODA）の割り当て
- ユーザー グループ：ユーザー グループの表示、ユーザー グループ メンバーシップの割り当て
- レポート：追加、削除、編集、表示、実行、スケジュール
- トークン：表示、SecurID PIN のリセット、SecurID トークンの有効化 / 無効化、トークンの再同期、ユーザーへのトークン割り当て、トークンのリプレース、ソフトウェア トークンの発行、オンライン / オフライン エマージェンシー アクセス トークンコードの管理
- ユーザー アカウント：固定パスコードの管理、ログオン エイリアスの管理、デフォルト シェルの編集、不正パスコード カウントの管理、キャッシュされた Windows クレデンシャルのクリア、オフライン エマージェンシー アクセス パスコードの管理
- エージェント：表示、制限付き認証エージェントに対するアクセス権をユーザー グループに付与

ユーザー管理者は、Authentication Manager レポートのサブセットを実行できます。詳細については、386 ページのレポートを参照してください。

Token Administrator（トークン管理者）

トークン管理者は、トークンのインポートと管理、ユーザーへのトークンの割り当てを行います。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- ユーザー：表示
- レポート：レポート定義の追加、削除、編集、表示、実行、スケジュール
- トークン：トークンのインポート、トークンの削除、トークンの編集、トークンの表示、SecurID PIN のリセット、トークンの再同期、オンライン / オフライン エマージェンシー アクセス トークンコードの管理、ユーザーへのトークン割り当て、トークンのリプレース、ソフトウェア トークンの発行、不正パスコード カウントの管理。

Help Desk Administrator（ヘルプデスク管理者）

ヘルプデスク管理者は、パスワードのリセット、アカウントのロック解除、アカウントの有効化によってユーザーの アクセスの問題を解決します。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- ユーザー：表示、パスワードのリセット、アカウントの有効化 / 無効化、アクティブ セッションの終了。
- ユーザー グループ：ユーザー グループの表示
- トークン：トークンの表示、SecurID PIN のリセット、トークンの再同期、SecurID トークンの有効化 / 無効化
- エージェント：表示

Privileged Help Desk Administrator（特権ヘルプデスク管理者）

特権ヘルプデスク管理者は、パスワードのリセット、アカウントのロック解除、アカウントの有効化によってユーザーのアクセスの問題を解決します。更に、オンラインおよびオフラインの エマージェンシー アクセスに関するヘルプを提供することができます。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- ユーザー：表示、パスワードのリセット、アカウントの有効化 / 無効化、アクティブ セッションの終了
- ユーザー グループ：ユーザー グループの表示
- トークン：トークンの表示、SecurID PIN のリセット、トークンの再同期、SecurID トークンの有効化 / 無効化
- エージェント：表示

- 固定パスコード：固定パスコードの表示 / 編集
- オフライン エマージェンシー アクセス パスコード：オフライン エマージェンシー アクセス パスコードの管理

Agent Administrator（エージェント管理者）

エージェント管理者は、認証エージェントの管理、制限付き認証エージェントに対するアクセス権の付与を行います。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- ユーザー：表示
- ユーザー グループ：ユーザー グループの表示、ユーザー グループ メンバーシップの割り当て
- レポート：追加、削除、編集、レポート定義の表示、実行、スケジュール
- エージェント：追加、削除、編集、表示、ノード シークレットの管理、エージェントに対するアクセス権をユーザー グループに付与
- セキュリティ ドメイン：表示

エージェント管理者は、Authentication Manager レポートのサブセットを実行できます。詳細については、386 ページのレポートを参照してください。

Request Approver（リクエスト承認者）

リクエスト承認者は、リクエストの表示と承認を行います。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- リクエスト：表示と承認
- ユーザー：表示
- トークン：トークンの表示

ユーザーがセキュリティ ドメインへのアカウント登録をリクエストした場合、リクエスト先のセキュリティ ドメインのリクエスト承認者は、そのドメインにまだ所属していないユーザーからのリクエストを承認できます。

Token Distributor（トークン配布者）

トークン配布者は、リクエストの表示、リクエストされたトークンの配布、ユーザーへのトークンの割り当て方法および送付方法の決定を行います。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- リクエスト：表示と配布
- ユーザー：表示
- トークン：トークンの表示

Trust Administrator（トラスト管理者）

トラスト管理者は、導入環境間の信頼関係、トラステッド ユーザー、トラステッド ユーザー グループを管理できます。このロールの管理者は、自分のロールの権限を委譲できません。

このロールのデフォルトの権限では、次の要素を限定的に管理できます。

- トラステッド ユーザー：トラステッド ユーザーの追加、削除、編集、表示
- トラステッド ユーザー グループ：トラステッド ユーザー グループの追加、削除、編集、表示
- トラステッド ユーザー グループのアクセス制限：編集と表示
- トラステッド ユーザー グループへのトラステッド ユーザーの割り当て
- エージェントへのアクセス権をトラステッド ユーザー グループに付与。
- トラステッド レルムの構成。

管理者ロールの設定

次の表に、管理者ロールの設定について説明します。

管理者ロールの設定	説明
Administrative Role Name（管理者ロール名）	管理者ロールの名前。ロール名は保存先のセキュリティ ドメイン内で一意でなければなりませんが、導入環境内では重複していても構いません。 通常、管理者ロールの名前は、組織内での管理者の職務に基づいて設定します（ヘルプ デスク、IT、人事など）。
Permission Delegation（権限の委譲）	管理者ロールの権限を他の管理者に委譲できるようにする。 この設定は、管理者ロールの作成、編集、割り当てを許可されている管理者にのみ適用されます。
Notes（メモ）	ロールの簡単な説明。
Security Domain Scope（セキュリティ ドメインの権限適用範囲）	このロールを割り当てられた管理者の権限適用範囲を決定する。管理者ロールによってセキュリティ ドメインの権限を付与される場合、セキュリティ ドメイン階層でそのセキュリティ ドメインの下位に位置するセキュリティ ドメインにも権限が適用されます。

管理者ロールの設定	説明
Identity Source Scope（アイデンティティ ソースの権限適用範囲）	管理者ロールにより権限を付与するアイデンティティ ソース。
General Permissions（一般権限）	ポリシー、セキュリティ クエスチョン、委譲管理、ユーザー、ユーザー グループ、レポートに関して管理者が実行できるアクションを決定する。 ロールの権限適用範囲に最上位レベルのセキュリティ ドメインが含まれていない場合、そのロールは、アイデンティティ属性定義、パスワード ポリシー、ロックアウト ポリシー、セルフサービス トラブルシューティング ポリシー、セキュリティ クエスチョン、コンソール表示オプションを管理できません。
Authentication Permissions（認証権限）	管理者が実行できる認証に関連するタスクを決定する。このようなタスクには、RSA SecurID、ユーザー認証属性、認証エージェント、トラステッド レルム、RADIUS、On-Demand 認証の管理が含まれます。 ロールの権限適用範囲に最上位レベルのセキュリティ ドメインが含まれていない場合、そのロールは RADIUS を管理できません。
Self-Service Permissions（セルフ サービス権限）	プロビジョニングリクエストに関して管理者が実行できるアクションを決定する。
Security Domain（セキュリティ ドメイン）	管理者ロールを保存するセキュリティ ドメイン。作成中の新しい管理者ロールは、保存先のセキュリティ ドメインを権限適用範囲に含んでいる管理者によってのみ管理可能です。

管理者ロールの権限適用範囲と権限

Authentication Manager のセットアップ時に構成された事前定義の管理者ロールの権限適用範囲は、デフォルトで最上位セキュリティ ドメインに設定されます。初期スーパー管理者アカウントも最上位セキュリティ ドメインに存在するため、結果として、事前定義のロールを割り当てられた管理者はスーパー管理者アカウントを変更できるようになります。これは、Authentication Manager の初期セットアップ完了時に最上位セキュリティ ドメインが導入環境内の唯一のセキュリティ ドメインであるためです。

事前定義のロールを管理者に割り当てる前に、デフォルトの動作を維持するか、これらのロールを割り当てる管理者の権限適用範囲をスーパー管理者や他の上位権限の管理者が含まれない下位のセキュリティ ドメインに制限するかを検討してください。下位権限の管理者が上位権限の管理者のアカウントを変更できるようにしたい場合もあります。

既存の導入環境では、Security Console を使用して、管理者が使用可能な権限を監査できます。操作手順については、Security Console ヘルプのトピック「View Available Permissions of an Administrator（管理者が使用可能な権限の表示）」を参照してください。

事前定義の管理者ロールのデフォルトの権限適用範囲を使用しない場合は、次のいずれかの方法で、意図しない余分な権限を管理者に付与することを回避できます。

- 管理者の権限適用範囲に次のものが含まれないようにします。
  - 上位権限の管理者のユーザー アカウントまたはトークンが含まれるセキュリティ ドメイン。
  - 管理者自身のトークンが含まれるセキュリティ ドメイン。これは、管理者が自分のトークンや他のクレデンシャルを変更して自分のアカウントに余分な権限を追加できないようにするために必要です。
  - 管理者自身のセキュリティ ドメイン。これは、管理者が自分のアカウントを変更できないようにするために必要です。
- 管理者の権限適用範囲が意図した範囲に限定されるよう別々のセキュリティ ドメインを作成します。たとえば、スーパー管理者用に 1 つ、他の管理者用に 1 つ、管理者ロールを持たないユーザー用に 1 つのセキュリティ ドメインを作成します。下位権限の管理者の権限適用範囲を、管理者ロールを持たないユーザーのセキュリティ ドメインに制限します。

  次のモデルに従って Authentication Manager を構成します。
  - スーパー管理者用に専用のセキュリティ ドメインを作成する。
  - ユーザーまたはクレデンシャルを編集する権限を持つ管理者を含め、その他すべての管理者を下位のセキュリティ ドメインに配置する。
  - その他のすべてのユーザーを別のセキュリティ ドメインに配置する。

  - 適切なロールと権限適用範囲を管理者に割り当てる。下位権限の管理者の権限適用範囲には、その管理者が権限を持つセキュリティ ドメインのみを含める。たとえば、ヘルプ デスク管理者には、権限適用範囲としてエンド ユーザーのセキュリティ ドメインのみを割り当て、管理者自身のセキュリティドメインや、スーパー管理者のセキュリティ ドメインは割り当てないようにします。操作手順については、Security Console ヘルプのトピック「Change the Scope of an Administrative Role（管理者ロールの権限適用範囲の変更）」を参照してください。

管理者が上位権限の管理者のアカウントを管理できるようにするには、複数の方法でシステムを構成できます。

- 上位アカウントの認証データを編集する権限を削除し、下位権限の管理者が上位権限の管理者の次のアカウント設定を編集する権限を持たないようにします。
  - Security Console の認証に必要なクレデンシャル（スーパー管理者のパスワードなど）
  - セキュリティ クエスチョン
  - LDAP パスワード
  - RSA パスワード
  - 割り当てられた SecurID トークン
  - 他のユーザーを管理する権限（PIN のクリア、SecurID トークンの割り当て、On-Demand 認証を有効化する権限を含む）

  注：管理者に割り当てられた管理者ロールに、業務に必要ないタスクが含まれていないことを確認してください。詳細については、Security Console ヘルプのトピック「Edit Permissions for an Administrative Role（管理者ロールの権限の編集）」を参照してください。

- 導入環境で Self-Service Console やリスク ベース認証を使用しない場合は、次の設定を行います。
  - エンド ユーザーをサポートするヘルプ デスク管理者からパスワードのリセット権限を削除する。
  - ヘルプ デスク管理者以外の管理者にトークンの割り当て権限とパスワードのリセット権限を割り当てる。
- クレデンシャルの組み合わせを使用するよう Authentication Manager を構成する。Authentication Manager が複数のクレデンシャル（たとえば、On-Demand トークンコードとパスワード）の使用を要求する場合、その中に下位権限の管理者が編集する権限を持っていないクレデンシャルが 1 つでもあれば、下位権限の管理者が上位権限の管理者のクレデンシャルを完全に制御することはできないため、上位権限の管理者として Security Console や Operations Console にログオンすることはできません。

管理者ロールの追加

管理者ロールは、管理者に割り当てることができる一連の権限の集合です。ロールにより、管理者がユーザーやユーザー グループなどに対して持つ管理レベルが決まります。

導入環境に管理者ロールを追加し、各ユーザーに割り当てることができます。複数の管理者ロールを単一のユーザーに割り当てると、権限が結合されます。

開始する前に

管理者が管理者ロールを作成するには、次の権限を含む管理者ロールが割り当てられている必要があります。

- 管理者ロールを作成する権限。
- 新しい管理者ロールに追加する権限。
- 自信の権限を委譲する権限。権限の委譲が可能かどうかは、ロールを作成する管理者に割り当てられているロールの権限委譲設定によって決まります。

手順

1. Security Console で［**Administration（管理）**］＞［**Administrative Roles（管理者ロール）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Administrative Role Name（管理者ロール名）**］フィールドに新しい管理者ロールの名前を入力します。
3. （オプション）管理者に自身のロールの権限を他の管理者に委譲することを許可するには、［**Permission Delegation（権限の委譲）**］を選択します。
4. ［**Security Domain Scope（権限適用範囲のセキュリティ ドメイン）**］ツリー内で、新しい管理者ロールに権限を付与するセキュリティ ドメインを選択します。
5. ［**Identity Source Scope（権限適用範囲のアイデンティティ ソース）**］フィールドで、この管理者ロールに権限を付与するアイデンティティ ソースを選択します。
6. ［**Next（次へ）**］をクリックします。
7. 管理者ロールに［General Permissions（一般的な権限）］を割り当てます。
8. （オプション）属性を制限するには、［**User Attribute Restriction（ユーザー属性の制限）**］フィールドで［**May only access specific attributes（特定の属性のみアクセスを許可）**］を選択します。［**Attributes（属性）**］ドロップダウン メニューが表示されます。各属性で［**Modify（変更）**］、［**View（表示）**］、［**None（なし）**］を選択します。［**None（なし）**］を選択すると、属性が非表示になります。

注：このフィールドの値は、［Add an Identity Attribute Definition（アイデンティティ属性定義の追加）］ページの［Entry Type（エントリー タイプ）］フィールドで指定した値と矛盾しないようにしてください。属性の定義が読み取り専用の場合、［User Attribute Restriction（ユーザー属性の制限）］で［Modify（変更）］は選択できません。属性の定義が入力必須となっている場合、［User Attribute Restriction（ユーザー属性の制限）］で［View（表示）］または［None（なし）］を選択できません。選択すると、ロールを追加できなくなります。

9. ［**Next（次へ）**］をクリックします。
10. 管理者ロールに認証権限を割り当てます。
11. ［**Next（次へ）**］をクリックします。
12. 管理者ロールにセルフ サービス権限を割り当てます。
13. ［**Next（次へ）**］をクリックします。
14. ［**Security Domain（セキュリティ ドメイン）**］ドロップダウン メニューから、管理者ロールを保存するセキュリティ ドメインを選択します。
15. 管理者ロールのサマリーを確認し、［**Save（保存）**］をクリックします。

管理者ロールの割り当て

管理者ロールをユーザーに割り当てると、ユーザーは指定されたセキュリティ ドメイン内で指定されたアクションを実行できるようになります。1 人のユーザーに複数の管理者ロールを割り当てることができます。

次のガイドラインに従います。

- 管理者が、割り当ておよび追加することができる管理者ロールは、権限適用範囲が自分のロールと同等かそれよりも狭く、権限が自分のロールと同等またはそれ以下の管理者ロールのみです。
- 複数の管理者ロールを 1 人のユーザーに一度に割り当てることも、複数のユーザーに同時に割り当てることもできます。

Security Console へのアクセス時にパスワードを要求された場合、管理者は自分のユーザー レコードに割り当てられているパスワードを使用します。

手順

1. Security Console で［**Administration（管理）**］＞［**Administrative Roles（管理者ロール）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用し、割り当てる管理者ロールを検索します。
3. 割り当てる管理者ロールをクリックします。
4. コンテキスト メニューで［**Assign More（割り当て）**］をクリックします。

5. 検索フィールドを使用して、この管理者ロールを割り当てるユーザーを検索します。

   ユーザー検索では、大文字と小文字が区別されます。

6. 管理者ロールを割り当てるユーザーをクリックし、[**Assign to Role (ロールの割り当て)**] をクリックします。

管理者の利用可能な権限の表示

構成によっては、たとえば、デフォルトのヘルプ デスク管理者ロールが割り当てられた管理者のように、下位レベルの権限の管理者が、上位レベルの権限の管理者のアカウントを変更できるようになっている場合があります。管理者に割り当てれた権限を監査し、下位レベルの権限の管理者に上位レベルの権限の管理者のアカウントを変更できる権限がないことを確認するには、次の処理手順を使用します。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] の順にクリックします。
2. 検索フィールドを使用して、管理者を検索します。
3. 管理者の名前をクリックし、コンテキスト メニューから [**Available Permissions（使用可能な権限）**] を選択します。

   そのユーザーに割り当てられた管理者ロールが表示されます。それぞれのロールについて、次の情報が表示されます。

   [**Security Domain（セキュリティ ドメイン）**]：ロールを管理することができる管理者のセキュリティ ドメイン。

   [**Security Domain Scope（権限適用範囲のセキュリティ ドメイン）**]：管理者ロールの権限が適用される範囲。つまり、管理者がこの管理者ロールのタスクを実行できるセキュリティ ドメイン。

   [**Identity Source Scope（アイデンティティ ソースの権限適用範囲）**]：管理者ロールにユーザーやユーザー グループの管理が含まれている場合に、その管理者がアクセスできるアイデンティティ ソース。

   [**Permission Delegation（権限の委譲）**]：このロールを割り当てられた管理者が、このロールの権限を含む新しい管理者ロールを作成できるかどうか。

   [**Administrative Tasks and Permissions（管理タスクと権限）**]：システム内のオブジェクトを変更するために管理者に付与された権限。たとえば、ユーザーを追加する権限や、ユーザーを単純に表示する権限などです。

次のステップ

管理者に過分な権限適用範囲や権限が設定されていることが分かった場合は、次の操作を実行できます。

- 管理者に別の管理者ロールを割り当てるか、不要な管理者ロールの割り当てを解除します。詳細については、65 ページの管理者ロールの割り当てを参照してください。
- 管理者ロールを編集して、そのロールの権限適用範囲、権限のセット、またはその両方を変更します。この処理は、このロールが割り当てられたすべての管理者に影響します。詳細については、RSA Security Console ヘルプのトピック「管理者ロールの編集」を参照してください。

正しい権限適用範囲と必要な権限セットのみを含む新しい管理者ロールを作成し、管理者に割り当てます。新しいロールを作成することも、既存のロールを複製して変更することもできます。詳細については、64 ページの管理者ロールの追加を参照してください。

3 認証エージェントの導入

RSA 認証エージェント

認証エージェントは、RSA Authentication Manager との間でユーザー認証要求を安全にやり取りするために必要なソフトウェア アプリケーションです。認証エージェントは、Authentication Manager で保護するすべてのマシン（ドメイン サーバ、Web サーバ、個人用コンピュータなど）にインストールします。

たとえば、Web サーバに配置されたエージェント ソフトウェアは、保護された Web ページへのすべてのユーザーからのアクセス要求をインターセプトします。ユーザーが保護された URL にアクセスしようとすると、エージェントがユーザー ID とパスコードを要求します。エージェントは、ユーザー ID とパスコードを認証のために Authentication Manager に送信します。認証が成功すると、ユーザーは保護された Web ページにアクセスできるようになります。

認証エージェントのタイプ

エージェントを導入するときは、制限なしエージェントと制限付きエージェントのどちらにするかを指定します。

制限なしエージェント。制限なしエージェントは、エージェントと同一の導入環境に存在するすべてのユーザーからの認証要求を処理します。

制限付きエージェント。制限付きエージェントは、エージェントへのアクセスを許可されたユーザー グループのメンバーからの認証要求のみを処理します。アクセスを許可されたユーザー グループのメンバーでない場合は、制限付きエージェントで認証を受けることはできません。制限付きエージェントにより保護されるリソースは、一部のユーザーからの認証要求のみ処理されるため、より安全であると考えられます。

RSA Authentication Agent の取得

必要となるエージェントは、保護するリソースのタイプによって異なります。たとえば、Apache Web サーバを保護するには、RSA Authentication Agent for Apache をダウンロードする必要があります。

ダウンロード パッケージには、「Installation and Administration Guide」と「Readme」も含まれています。エージェントをインストールする前に、これらのドキュメントを一読してください。エージェント ソフトウェアのインストール手順については、お使いのエージェントのマニュアルを参照してください。

RSA Authentication Agent ソフトウェアが組み込まれた製品を購入することも可能です。たとえば、リモート アクセス サーバ、ファイアウォールなどの製品があります。

手順

次のいずれかの操作を実行します。

- RSA エージェントおよび RSA エージェントが必要なサード パーティ エージェントの場合は、**http://japan.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings** にアクセスします。
  お使いのプラットフォーム用のエージェント ソフトウェアを探し、エージェント ソフトウェアと RBA Integration Script（RBA 統合スクリプト）テンプレートをダウンロードします。
- RSA エージェントが組み込まれているサード パーティ エージェントの場合は、RSA Secured の Web サイト（**https://gallery.emc.com/community/marketplace/rsa?view=overview**）にアクセスし、Authentication Manager 用の導入ガイドのリストを表示します。
  お使いのエージェントに対応した Authentication Manager 用の導入ガイドをダウンロードします。

  注：導入ガイドは、認定されたパートナー ソリューションにのみ発行されます。

次のステップ

70 ページの認証エージェントの導入を参照してください。

認証エージェントの導入

認証エージェントは、RSA Authentication Manager との間でユーザー認証要求を安全にやり取りするために必要なソフトウェア アプリケーションです。認証エージェントが RSA Authentication Manager との通信を行うためには、エージェントを導入する必要があります。

手順

1. Security Console を使用して、エージェントの構成ファイルを生成します。このファイルによって、エージェントが Authentication Manager サーバを見つけることができます。詳細については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。
2. 保護する各マシンに認証エージェントをインストールします。インストール手順については、エージェントのマニュアルを参照してください。

3. Security Console を使用して、新しいエージェントのレコードを内部データベースに追加します。このステップでは、制限付きエージェントを作成するかどうかを指定できます。RSA Authentication Manager はエージェント レコードでエージェントを識別します。このプロセスはエージェントの登録と呼ばれます。詳細については、72 ページの認証エージェントの追加を参照してください。

Authentication Manager 構成ファイルの生成

認証エージェントと RSA Authentication Manager の間の通信を構成する必要があります。これを行うには、Security Console を使用して、RSA Authentication Manager 構成ファイル **sdconf.rec** を含む zip ファイル（**AM_Config.zip**）を生成します。通信を構成するには、**sdconf.rec** を各エージェント ホストにコピーします。**sdconf.rec** ファイルには、ファイル生成時のサーバ トポロジーのスナップショットが含まれています。エージェントは **sdconf.rec** ファイル内のデータをバックアップとして使用します。

生成された zip ファイルには、エージェント上で構成可能な failover.dat ファイルも含まれています。プライマリ インスタンスが使用不可になったり、NAT（ネットワーク アドレス変換）を使用するファイアウォールによってエージェント ホストから分離されたりした場合に、failover.dat ファイルを使用してエージェントの自動登録を完了できます。このファイルには、プライマリ インスタンス、レプリカ インスタンス、それぞれのエイリアス IP アドレスのリストが含まれています。

開始する前に

- エージェントが Authentication Manager に接続できることを確認します。
- 構成設定を確認します。Security Console ヘルプ トピックの「エージェント設定の構成」を参照してください。

手順

1. Security Console で、［**Access（アクセス）**］＞［**Authentication Agents（認証エージェント）**］＞［**Generate Configuration File（構成ファイルの生成）**］の順にクリックします。
2. ［**Maximum Retries（最大リトライ回数）**］ドロップダウン メニューで、認証エージェントが Authentication Manager との通信を確立する際の試行回数を選択します。この回数に達すると、「Cannot initialize agent - server communications（エージェントとサーバの通信を初期化できません）」というメッセージが返されます。
3. ［**Maximum Time Between Each Retry（最大リトライ間隔）**］ドロップダウン メニューで、認証エージェントが Authentication Manager との通信を確立する際の試行間隔（秒単位）を選択します。
4. ［**Generate Config File（構成ファイルの生成）**］をクリックします。
5. ［**Download Now（今すぐダウンロード）**］をクリックし、**AM_Config.zip** をローカル マシンに保存します。

次のステップ

- **AM_Config.zip**（**sdconf.rec** ファイルと **failover.dat** ファイルが含まれる）を各エージェント ホストにコピーします。
- 新しい **sdconf.rec** ファイルでエージェントを構成します（必要に応じて **failover.dat** ファイルも使用します）。手順については、エージェントのマニュアルを参照してください。

認証エージェントの追加

認証エージェントが Authentication Manager と通信するためには、管理者がエージェントを内部データベースに追加する必要があります。このプロセスはエージェントの登録と呼ばれます。Authentication Manager は、エージェント レコードによってエージェントを識別します。

RBA（リスク ベース認証）を使用する導入環境では、追加の構成が必要です。SSL-VPN、Web ポータル、シン クライアントなどの Web ベース アプリケーションを RBA で保護する場合は、その Web ベース アプリケーションを Authentication Manager と統合する必要があります。詳細については、319 ページのリスク ベース認証の実装を参照してください。

手順

1. Security Console で、［**Access（アクセス）**］＞［**Authentication Agents（認証エージェント）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Security Domain（セキュリティ ドメイン）**］ドロップダウン メニューから、新しいエージェントを追加するセキュリティ ドメインを選択します。
3. ［**Authentication Agent Basics（認証エージェントの基本設定）**］で、次の操作を実行します。
   a. ［**Hostname（ホスト名）**］に、新しいエージェントのホスト名を入力し、［**Resolve IP（IP の解決）**］をクリックします。
      IP アドレスが自動的に入力されます。ホスト名は、一意である必要があります。

      注：IPv4/IPv6 エージェントの場合、ホスト名にはエージェントの任意の記述名を入力することができ、必ずしも完全修飾ホスト名である必要はありません。IPv4/IPv6 エージェントでは、IP アドレスの解決はサポートされません。

   b. （オプション）［**IP Address（IP アドレス）**］フィールドに、エージェントの IP アドレスを入力します。
      既知のサーバ名を使用する場合、このフィールドには値が自動的に入力され、読み取り専用になります。アドレスが指定されていない場合、UDP エージェントは自動登録を使用してサーバにアドレスを登録します。

注：IPv6 フォーマットの IP アドレスは入力しないでください。IPv4/IPv6 エージェントはホスト名を使用してサーバにアドレスを登録します。

c. （オプション）[**Alternate IP Addresses（代替 IP アドレス）**] フィールドに、エージェントの代替 IP アドレスを入力します。

エージェントに複数のネットワーク インタフェース カードが搭載されている場合、またはエージェントが静的 NAT（ネットワーク アドレス変換）を行うファイアウォール越しに配置されている場合は、代替 IP アドレスを入力します。

既知のサーバ名を使用する場合、このフィールドには値が自動的に入力され、読み取り専用になります。

4. （オプション）[**Authentication Agent Attributes（認証エージェントの属性）**] で、次のオプションを選択します。

- エージェントのタイプを指定するには、[**Agent Type（エージェントのタイプ）**] リストからタイプを選択します。

  エージェントが Web エージェントの場合は、[**Web Agent（Web エージェント）**] を選択します。それ以外の場合は、デフォルトの [**Standard Agent（標準エージェント）**] のままにします。エージェントのタイプはラベルとして使用されるだけで、[Web Agent（Web エージェント）] と [Standard Agent（標準エージェント）] のどちらを選択しても機能上の違いはありません。

- エージェントを無効化するには、[**Agent is disabled（エージェントを無効化します）**] を選択します。

  リソースへのアクセスを一時的に停止させるには、このオプションを選択します。

- 制限付きエージェントを追加するには、[**Allow access only to members of user groups who are granted access to this agent（このエージェントへのアクセスを許可されたユーザー グループのメンバーのみにアクセスを許可する）**] を選択します。

  制限付きエージェントを使用して認証を受けることができるのは、このエージェントに対してアクセス権限のあるユーザー グループに属するユーザーのみです。制限なしエージェントでは、すべてのユーザーが認証を受けることができます。

- 手動と自動のいずれかの方法でコンタクト リストを新しいエージェントに割り当てるには、[Authentication Manager Contact List（Authentication Manager コンタクト リスト）] のボタンを選択します。

5. （オプション）トラステッド レルムのユーザーがこのエージェントで認証を受ける方法を構成する場合は、[**Enable Trusted Realm Authentication（トラステッド レルム認証を有効化する）**] を選択し、すべてのトラステッド ユーザーが新しいエージェント経由で認証を受けられるようにするか、明示的に許可されたトラステッド ユーザー グループに属するユーザーだけがエージェントを使用できるようにするかを選択します。

6. （オプション）RBA を使用するユーザーがこのエージェントで認証を受けられるようにするには、次の操作を実行します。
   - ［**Enable this agent for risk-based authentication（リスク ベース認証を有効化する）**］を選択します。
   - このエージェントへの RBA アクセスを制限するには、［**Allow access only to users who are enabled for risk-based authentication（リスク ベース認証が有効なユーザーのみにアクセスを許可する）**］を選択します。
   - RBA ユーザーの認証方式を選択します。
7. 次のオプションからいずれかを選択し、このエージェントの設定を保存します。
   - このエージェントを RBA 用のエージェントとして有効化するには、［**Save Agent and Go to Download Page（エージェントを保存してダウンロード ページに移動）**］をクリックします。

     設定が保存され、［Integration Script（統合スクリプト）］ページが表示されます。このページで、対象のエージェントの統合スクリプトを選択してダウンロードします。
   - このエージェントを RBA 用のエージェントとして有効化しない場合は、［**Save（保存）**］をクリックします。

注：ホスト名が完全修飾ホスト名でないか、IP アドレスが指定されていない場合は、ホスト名と IP アドレスを表示した［Confirmation Required（確認してください）］ダイアログが表示されます。ここでは、エージェントの詳細を編集するか、エージェント情報をそのまま保存するか選択できます。

次のステップ

- 構成設定を確認します。これについては、RSA Security Console ヘルプのトピック「エージェント設定の構成」を参照してください。
- （オプション）統合スクリプトを作成します。これについては、RSA Security Console ヘルプのトピック「Web ベース アプリケーション用統合スクリプトの生成」を参照してください。

暗号化用のノード シークレット

ノード シークレットは、認証エージェントと Authentication Manager の間でのみ使用される共有シークレットです。認証エージェントは、ノード シークレットを使用して認証リクエストを暗号化したうえで、Authentication Manager に送信します。

Authentication Manager は、エージェント上で成功した最初の認証への応答として、自動的にノード シークレットを作成し、エージェントへ送信します。

エージェントと Authentication Manager サーバの間では、ノード シークレットの状態が一致している必要があります。たとえば、サーバはエージェントがノード シークレットを持っていると認識しているが、エージェントがノード シークレットを持っていない場合や、エージェントは自身がノード シークレットを持っていると認識しているがサーバはエージェントがノード シークレットを持っていないと認識している場合、エージェントは認証を行えません。

ノード シークレットの手動送付

ほとんどの導入環境では、ノード シークレットを自動的に送付すれば問題ありません。ただし、セキュリティを高めるためにノード シークレットを手動で送付することもできます。ノード シークレットを手動で送付するときは、次の操作を実行する必要があります。

- Security Console を使用してノード シークレットを作成します。操作手順については、76 ページのノード シークレットの管理を参照してください。
- ノード シークレットを（ディスク経由などの方法で）エージェントに送付し、Node Secret Load ユーティリティを使用してエージェントにロードします。

Node Secret Load ユーティリティにより、次の処理が行われます。

- ノード シークレット ファイルが復号化されます。
- ファイル名が認証サービス名に応じた名前（通常は **securid**）に変更されます。
- 名称変更されたファイルがユーザーのマシンに格納されます。名称変更されたノード シークレット ファイルの保存場所の詳細については、お使いのエージェントのドキュメントを参照してください。

ノード シークレットを手動で送付するときは、セキュリティに配慮して次の予防措置を行ってください。

- 可能な限り長い半角英数字のパスワードを使用します。最大文字数は 16 文字です。最小文字数、必要な特殊文字の数、除外文字は、導入環境のデフォルトのパスワード ポリシーによって決まります。

- 可能な場合は、ノード シークレットを外部電子メディアに格納してエージェント管理者に渡し、パスワードを口頭で伝えます。パスワードをメモに書き留めないようにします。ノード シークレットをメールで送付する場合は、パスワードとは別に送付します。
- ノード シークレットの送付にかかわる担当者全員が信頼できるスタッフであることを確認します。

ノード シークレット ファイルの作成と送信に関する追加情報については、76 ページのノード シークレットの管理を参照してください。

ノード シークレットの管理

認証エージェント上でユーザーが初めて SecurID パスコードを使用して認証するときに、トランザクションの安全を確保するために、認証エージェントと Authentication Manager は自動的に一意のノード シークレットのハッシュ値を交換し、それをエージェント コンピュータに格納します。それ以降、各認証のやり取りでは、ノード シークレットを使用して、2 つのシステム間の通信を暗号化します。

手順

1. Security Console で、[**Access（アクセス）**] > [**Authentication Agents（認証エージェント）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索するエージェントが制限付きかどうかに応じて、[**Restricted（制限付き）**] タブまたは [**Unrestricted（制限なし）**] タブをクリックします。
3. 検索フィールドを使用して、ノード シークレットを管理するエージェントを検索します。
4. ノード シークレットを管理するエージェントをクリックし、[**Manage Node Secret（ノード シークレットの管理）**] をクリックします。
5. Manager サーバ側でノード シークレットをクリアする場合は、[**Clear Node Secret（ノード シークレットのクリア）**] チェックボックスをオンにします。
   エージェントがサーバに対して認証できるようにするには、エージェント側でもノード シークレットをクリアする必要があります。
6. （オプション）新しいノード シークレットを作成する場合は、[**Create Node Secret（ノード シークレットの作成）**] チェックボックスをオンにします。
7. （オプション）新しいノード シークレットを作成することを選択した場合は、ノード シークレット ファイルを暗号化するためのパスワードを入力し、確認します。
   パスワードを作成する場合、最大長は 16 文字です。最短の文字数、必要な文字、除外文字は、導入環境のデフォルトのパスワード ポリシーによって決まります。

8. ［**Save（保存）**］をクリックします。
9. ［**Download Now（今すぐダウンロード）**］をクリックします。

Node Secret Load ユーティリティによるノード シークレットの更新

ノード シークレットの更新が必要なことはほとんどありませんが、更新が必要となる場合もあります。ノード シークレットに問題がある場合、認証エラーまたはノード検証エラーが発生します。ノード シークレットは次の場合に更新します。

- エージェント上のノード シークレットが失われた場合。たとえば、工場出荷時の状態にリセットしたり、エージェントを再インストールした場合。
- 認証エージェント レコードが削除されたか、再追加された場合。
- ノード シークレットが接続の一端から削除されたが、もう一端からは削除されていない場合。たとえば、ノード シークレットが Authentication Manager アプライアンスから削除されていて、エージェントから削除されていない場合。

次の場合はノード シークレットを更新する必要はありません。

- エージェント名を変更する場合。
- IP アドレスを変更する場合。

Node Secret Load ユーティリティ（agent_nsload）は、RSA Authentication Manager 8.0 - Virtual Appliance DVD に含まれています。

手順

1. RSA Security Console を使用してノード シークレットを作成します。詳細については、76 ページのノード シークレットの管理を参照してください。
2. RSA Authentication Manager 8.0 - Virtual Appliance DVD の「**Node Secret Utility**」ディレクトリから、エージェントのプラットフォーム用の **agent_nsload** をエージェント ホストにコピーします。
   RSA では、次のプラットフォーム用にユーティリティを用意しています。
   - Windows
   - Linux
   - HP-UX
   - IBM AIX
3. エージェント ホスト上のコマンド ラインから、Node Secret Load ユーティリティを実行します。次のように入力します。

   ```
   agent_nsload -f パス -p パスワード
   ```

各変数の意味を以下に示します。

- パスは、ノード シークレット ファイルのディレクトリの場所とファイル名です。
- パスワードは、ノード シークレット ファイルの保護用パスワードです。

エージェントの自動登録

RSA Authentication Agent ソフトウェアに含まれる Automated Agent Registration and Update ユーティリティ（sdadmreg.exe）を使用すると、新しい認証エージェント用のエージェント レコードを Authentication Manager の内部データベースに自動的に追加できます。このプロセスはエージェントの登録と呼ばれます。認証エージェントの自己登録を有効にすると、管理者がこれらのタスクを実行する必要がなくなるため、時間と経費を節約できます。

デフォルトでは、エージェント ホストが起動した時点で Automated Agent Registration and Update ユーティリティが自動実行され、エージェントが起動する前に IP アドレスの変更が内部データベースに登録されます。このユーティリティはエージェント ホストの IP アドレスが変更されたときにも実行できます。IP アドレスの割り当てに DHCP（Dynamic Host Configuration Protocol）を使用しているシステムでは、この方法が効果的です。DHCP を使用する環境で、このユーティリティを無効にしている場合は、エージェント ホストの IP アドレスが変更されるたびに内部データベースに登録された IP アドレスを手動で更新しなければなりません。

または、エージェント ホストの IP アドレスが変更されるたびに、Automated Agent Registration and Update ユーティリティを手動で実行して、内部データベースに登録された IP アドレスを更新することも可能です。

注：RSA Authentication Agent 6.1.2 for Microsoft Windows は、IP アドレスの変更が発生する度に、内部データベースを自動更新します。このエージェントを使用している場合は、ユーティリティを手動で実行する必要はありません。

重要な IT インフラストラクチャについては、DOS（サービス妨害）攻撃への備えが必要です。システムの脆弱性を低下させるためには、次の対策が効果的です。

- 重要なマシン（メール サーバや VPN サーバなど）ではエージェント自動登録を無効化します。
- IT インフラストラクチャ内の重要なエージェントには固定 IP アドレスを割り当てます。
- Authentication Manager 内で IP アドレスを保護します。このためには、Security Console の［Authentication Agent（認証エージェント）］ページで［Protect IP Address（IP アドレスの保護）］を選択します。

エージェントの自動登録を許可する

認証エージェントは、エージェント レコードを内部データベースに自動的に追加できます。エージェント レコードを追加する処理は、「エージェントの登録」と呼ばれます。

ネットワークで DHCP（動的ホスト構成プロトコル）を使用して IP アドレスを割り当てている場合は、エージェントの自動登録を有効化することを検討してください。有効化すると、エージェント ホストの IP アドレスが変更されるたびにエージェント レコードの IP アドレスが自動的に更新されます。

認証エージェントがインストールされたコンピュータをユーザーが初めて起動すると、Auto-Registration ユーティリティによってユーザーのコンピュータが Authentication Manager データベースに自動的に登録されます。このユーティリティにより、管理者がエージェント ホスト レコードを手動で作成する必要がなくなります。

開始する前に

- 認証エージェントをインストールする。
- エージェント ホストを構成する。詳細については、エージェントのマニュアルを参照してください。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］＞［**Agents（エージェント）**］の順にクリックします。
2. ［**Allow authentication agent auto-registration（認証エージェントの自動登録を許可する）**］を選択します。
3. ［**Save（保存）**］をクリックします。

RSA Authentication Manager サーバ証明書のダウンロード

エージェント自動登録を設定するには、RSA Authentication Manager サーバ証明書が必要です。

手順

1. Security Console で、［**Access（アクセス）**］＞［**Authentication Agents（認証エージェント）**］＞［**Download Server Certificate File（サーバ証明書ファイルのダウンロード）**］の順にクリックします。
2. ［**Download Now（今すぐダウンロード）**］をクリックします。
3. ［**Save it to disk（ディスクに保存）**］を選択します。

次のステップ

エージェント自動登録をセットアップするには、エージェント ホスト マシンの自動登録ユーティリティのインストール ディレクトリにファイルをコピーし、**.exe** ファイルを実行します。

認証リクエスト用のコンタクト リスト

コンタクト リストは、認証リクエストに応答できるインスタンスを示す順序付きリストで、Authentication Manager により自動生成される以外にも管理者が手動で作成することができます。

Authentication Manager は、コンタクト リストを使用して、どのインスタンスに認証リクエストが送信されるかを決定します。エージェントと Authentication Manager 間の初期接続が完了したら、Authentication Manager は各エージェントにコンタクト リストを送信します。

Authentication Manager 導入環境では、所有するライセンス タイプに応じて、プライマリ インスタンスと、最大 15 のレプリカ インスタンスを保有できます。効率性を高めるには、コンタクト リストを使用して、エージェントからの認証リクエストに最も早く応答できるインスタンスに認証リクエストを経路指定するようにします。

その後の認証処理の中で、エージェントは新しいコンタクト リストをリクエストします。エージェントは、認証リクエストの送信先を決定するために、コンタクト リスト内の全インスタンスを定期的に検証しています。リクエストの送信先は、さまざまなメトリック（インスタンスが認証リクエストに応答するまでに要した時間など）に基づいて決定されます。

コンタクト リスト内のいずれのインスタンスも認証リクエストに応答しない場合、エージェントは Authentication Manager 構成ファイルを再確認し、構成ファイル内のいずれかの IP アドレスを使用して Authentication Manager に再接続します。

RSA RADIUS は、RADIUS サーバ エージェント用のコンタクト リストをサポートしています。RADIUS クライアント エージェントは、コンタクト リストをサポートしていません。これは、RADIUS クライアントに認証エージェント ソフトウェアがインストールされていないためです。Authentication Manager は、内部データベース内の関連するエージェント レコードにより、RADIUS サーバ経由で試行された RADIUS 認証をトラッキングします。詳細については、347 ページの RADIUS クライアントを参照してください。

IPv4/IPv6 エージェントはコンタクト リストをサポートしていません。

自動コンタクト リスト

導入環境の各インスタンスには自動コンタクト リストが割り当てられます。このリストには、コンタクト リストの割り当て先である各インスタンスの IP アドレスが含まれています（最大 11 個）。エージェントは、自動コンタクト リストをデフォルトで受信します。

Authentication Manager は、導入環境に新しいインスタンスが追加されるたびにこれらのリストを自動的に更新します。リストが更新されると、リストに関連づけられているタイム スタンプも更新されます。エージェントはこのタイム スタンプに基づいて、最新のリストをリクエストするタイミングを判断します。

スーパー管理者は、Security Console の［Edit Authentication Manager Contact List（Authentication Manager コンタクト リストの編集）］ページで自動コンタクト リストを編集できます。自動コンタクト リストに対する編集は、導入環境に新しいインスタンスが追加された時点で上書きされる可能性があります。

手動コンタクト リスト

スーパー管理者は、インスタンスの最新のリストを反映するように手動コンタクト リストを更新します。この手動リストには、導入環境内の任意のインスタンスの IP アドレスを最大 11 個含めることができます。

一般的には、自動コンタクト リストを使用するだけで十分です。ただし、認証リクエストを明示的に経路指定する必要がある場合は、手動コンタクト リストを作成してください。

たとえば、あなたがボストン、ニューヨーク、サンノゼに支店がある企業の管理者であるとします。ニューヨーク支店とサンノゼ支店は小規模で、すべての認証リクエストは、各サイトに設置された Authentication Manager のレプリカ インスタンスに経路指定されています。一方ボストン支店は大規模で、この支店にあるプライマリ インスタンスによって、ボストン支店の全ユーザーに加えて、外部ユーザーのすべての VPN リクエストも処理されています。この例の場合、手動コンタクト リストを作成して、すべての認証リクエストをレプリカ インスタンスに送信するよう経路指定することができます。このように構成することで、プライマリ インスタンスは、ニューヨーク支店とサンノゼ支店に設置したレプリカ インスタンスへのデータのレプリケーションに専念できます。

操作手順については、RSA Security Console ヘルプのトピック「Add a Manual Contact List（手動コンタクトリストの追加）」、「Assign a Manual Contact List to an Authentication Agent（認証エージェントへの手動コンタクトリストの割り当て）」、「Edit a Manual Contact List（手動コンタクトリストの編集）」を参照してください。

4 認証ポリシーの構成

ポリシー

ポリシーは、導入環境のさまざまな側面を制御します。Authentication Manager では、各ポリシー タイプのデフォルトを提供し、それらを新規作成した各セキュリティ ドメインに割り当てます。また、カスタム ポリシーを割り当てることもできます。新しいデフォルト ポリシーを指定すると、そのポリシーが、デフォルト ポリシーを使用している既存のセキュリティ ドメインおよび新しいセキュリティ ドメインに自動的に割り当てられます。

下位のセキュリティ ドメインに割り当てられるポリシーは、上位のセキュリティ ドメインから継承されません。新しいセキュリティ ドメインには、階層内の上位のセキュリティ ドメインに割り当てられているポリシーにかかわらず、セキュリティ ドメイン作成時のデフォルト ポリシーが適用されます。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを割り当てても、下位のセキュリティ ドメインではデフォルト ポリシーが引き続き使用されます。

次のポリシーを使用して、システムの管理に役立てることができます。

84 ページのトークン ポリシー：トークン ポリシーでは、ユーザーの RSA SecurID PIN の有効期間と形式、固定パスコードの有効期間と形式、連続して不正なパスコードを入力したユーザーや不正ユーザーに対処する方法を定義します。パスコードは SecurID PIN とトークンコードを組み合わせたものです。トークンコードとは、SecurID トークンの画面に表示される番号です。

92 ページのオフライン認証ポリシー：オフライン認証ポリシーでは、ネットワークに接続されていない場合のユーザー認証方法を定義します。

96 ページのパスワード ポリシー：パスワード ポリシーでは、ユーザーのパスワードの長さ、形式、変更の頻度を定義します。

101 ページのロックアウト ポリシー：ロックアウト ポリシーでは、何回ログオンに失敗するとシステムによってアカウントがロックされてしまうかを定義します。ロックアウト ポリシーは、それぞれのログオン試行で使用したクレデンシャルのタイプに関係なく、ユーザーが行ったログオン試行の合計回数に適用されます。たとえば、あるユーザーがパスワードを使用して 2 回、On-Demand 認証を使用して 1 回認証に失敗した場合、合計で 3 回の試行に失敗したことになり、ユーザーのアカウントがロックされます。

103 ページのセルフ サービス トラブルシューティング ポリシー：セルフ サービス トラブルシューティング ポリシーでは、Self-Service Console ユーザーが、パスワードやパスコードなどのプライマリ認証方式を使用して保護されたリソースにアクセスできない場合に、定型的な認証のトラブルシューティングを実施できるようにします。このポリシーでは、トラブルシューティング機能にアクセスするために使用する代替の認証方法（セキュリティ クエスチョンなど）を定義します。また、このポリシーでは、トラブル シューティング機能からユーザーをロック アウトする条件も指定します。

107 ページのリスク ベース認証ポリシー：RBA（リスク ベース認証）ポリシーには、ログオンに必要な最低保証レベル、ログオン要求の保証レベルを上げるために使用するユーザー確認方法など、すべての RBA 設定が含まれます。

110 ページのリスク ベース認証メッセージ ポリシー：RBA メッセージ ポリシーでは、ユーザーにユーザー確認方法の構成を求めるときに伝えるメッセージを定義します。

301 ページのワークフロー ポリシー：ワークフロー ポリシーでは、ユーザー リクエストを処理する方法を決定します。ワークフロー ポリシーは、導入プロセス全体に適用されます。各ユーザー リクエストは、1 つのワークフロー ポリシーで管理されます。

トークン ポリシー

トークン ポリシーでは、ユーザーの RSA SecurID PIN の有効期間と形式、固定パスコードの有効期間と形式、ユーザーまたは不正ユーザーが不正なパスコードを連続して入力した場合の対処方法を定義します。パスコードは SecurID PIN とトークンコードを組み合わせたものです。トークンコードとは、SecurID トークンの画面に表示される番号です。

トークン ポリシーはセキュリティ ドメインに対して設定します。トークン ポリシーは、そのセキュリティ ドメインに属するすべてのユーザーに適用されます。

ユーザーがトークンで認証を受ける場合、適用されるトークン ポリシーは、トークンのセキュリティ ドメインではなく、そのユーザーのセキュリティ ドメインのトークン ポリシーです。たとえば、ニューヨークのセキュリティ ドメインのユーザーが、ボストンのセキュリティ ドメインに保存されたトークンを使用して認証を受ける場合には、ニューヨークのトークン ポリシーによってポリシー要件が決定されます。

トークン ポリシーを編集する場合、既存の PIN および固定パスコードは新しい除外単語辞書や履歴要件に基づいて検証されません。ただし、その他のすべての要件については検証されます。

上位のセキュリティ ドメインに設定したトークン ポリシーは、下位のセキュリティ ドメインには継承されません。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを設定した場合でも、その下の階層に新しく作成したセキュリティ ドメインには、すべてデフォルトのトークン ポリシーが引き続き設定されます。

セキュリティの強度は、ユーザーの使い勝手を考慮して適切なレベルに調整するようにしてください。長い PIN を要求すると、記憶することが困難で、生産性を阻害すると同時に、ロックアウトされるユーザー数の増加により、ヘルプ デスクへの電話の件数が増えることにもなりかねません。

トークン ポリシー設定

以下の表は、トークン ポリシー設定について説明しています。

トークン ポリシー設定	説明
SecurID トークン ポリシー名	一意の名前。半角英数 1 ～ 128 文字の長さで指定します。

トークン ポリシー設定	説明
不正なパスコード	ユーザーが、不正なパスコードを何度も入力し、最後に正しいパスコードを入力した場合の処理方法を指定します。 ユーザーによる不正なパスコードの入力回数の上限を設定することも、無制限に許可することも可能です。不正なパスコードの入力回数の上限を超えた後に正しいパスコードを入力した場合、ユーザーには、トークンに次に表示されるトークンコード（ネクスト トークンコード）の入力を求めるプロンプトが表示されます。 これにより、不正ユーザーがパスコードを推測する状況に対処します。不正ユーザーが正しいパスコードの推測に成功したとしても、ネクスト トークンコードの入力を求めるプロンプトが表示されます。正しいネクスト トークンコードを入力できるチャンスは 1 回のみです。ネクスト トークンコードモードでは、ユーザーが正しいトークンコードを 2 回連続して入力しないと認証が成功しません。 不正なパスコードの入力を、無制限に許可することもできます。このオプションは、最終的に正しいパスコードを入力するまで、ユーザーがパスコードを何度誤って入力しても、ネクスト トークンコードの入力を求めません。ただし、セキュリティ ドメインに割り当てられているロックアウト ポリシーで、認証が特定の回数失敗した後にユーザーをロックアウトするよう設定されている場合、ユーザーはこの許容回数を超えるとロックアウトされることになります。96 ページのパスワード ポリシーを参照してください。
デフォルト ポリシー	新しいポリシーを導入環境のデフォルト ポリシーとして指定します。このセキュリティ ポリシーが、**SecurID トークン ポリシー**として［**Always Use Default（常にデフォルトを使用）**］を設定しているすべてのセキュリティ ドメインに適用されます。各セキュリティ ドメイン レベルで、デフォルト ポリシー以外のポリシーを設定することができます。
メモ	特記事項があれば記録します。

トークン ポリシー設定	説明
定期的な変更	一定期間が経過した後、ユーザーに SecurID PIN の変更を要求する場合のオプション設定です。このオプションを選択すると、[Maximum Lifetime (最長有効期間)] フィールドと [Minimum Lifetime (最短有効期間)] フィールドが有効になります。
最長有効期間	SecurID PIN を変更する頻度を指定します。たとえば、PIN の最大有効期間を 90 日間に設定したとします。ユーザーが PIN を 6 月 1 日に変更した場合は、8 月 30 日にはこれを再度変更する必要があります。
最短有効期間	ユーザーが次回 PIN を変更するまでに、現在の PIN を使用する必要のある最短期間です。たとえば、最短有効期間を 14 日間と設定したとします。ユーザーが自分の PIN を 6 月 15 日に変更した場合、6 月 29 日までは再度変更することができなくなります。 このように設定すると、以前に設定した古い PIN の再使用に関する制限をユーザーが回避できなくなります。たとえば、ユーザーに対して直近の 5 つの PIN の再使用を制限しているとします。PIN の最短有効期間を設定すると、ユーザーが PIN を即座に 6 回変更して、ある特定の PIN を再使用することを防止できます。
再使用の制限	ユーザーが 2 ～ 3 個の同じ PIN を繰り返し使用できないようにします。たとえば、直近の 3 個の PIN の使用を制限したとすると、ユーザーはそれらの PIN を入力できず、他の PIN を選択しなければならなくなります。 同じ PIN を再使用すると、不正ユーザーによって PIN が推測される可能性が高まります。特にすべての PIN が類似しているときには危険度が高まります。 制限を設けることにより、ユーザーに安易に数個の PIN を使用させないようにし、より安全な PIN を選択させるようにします。

トークン ポリシー設定	説明
PIN の作成方法	SecurID PIN を作成する方法を選択します。SecurID PIN はシステムで生成するか、ユーザーが独自の PIN を作成することができます。 **注：**RSA RADIUS を使用する場合、デフォルトではシステム生成 PIN を使用できません。システム生成 PIN を使用する場合は、RADIUS 構成ファイルの **securid.ini** を変更して、システム生成 PIN を使用可能にしない限り、認証が正しく行われません。操作手順については、Operations Console ヘルプのトピック「RADIUS サーバファイルの編集」を参照してください。
最小文字数	短すぎてブルート フォース攻撃を受ける可能性がある PIN を作成できないようにします。
最大文字数	パスコードの長さがエージェントが処理できる長さを超えないように、ユーザーが作成する PIN の長さを制限します。このフィールドを構成する場合、エージェントが処理可能なパスコードの最大長を確認してください。
除外単語辞書	ユーザーの PIN に使用できない単語のリストです。システムに対する辞書攻撃に含まれている可能性が高い、よく使用される単語（「password」など）を登録します。除外単語辞書を使用すると、ユーザーはよく使われる単語、つまり容易に推測される単語を PIN として使用できなくなります。 除外単語辞書を Authentication Manager にアップロードすることができます。除外単語辞書の最大ファイル サイズは 20 MB です。導入環境で使用できる除外単語辞書は 1 つのみです。すでに辞書がインストールされている場合は、新しい辞書を追加する前にそれを削除する必要があります。 手順については、RSA Security Console ヘルプのトピック「Add a Password Dictionary（パスワード ディクショナリの追加）」を参照してください。
文字要件	特定のタイプの文字を含めることを要件にすると、PIN の推測が難しくなります。 英字と数字の使用を要件に含めることができます。英字や数字の数を指定して要件に含めることができます。

トークン ポリシー設定	説明
SecurID PIN の有効期間の設定をコピー（固定パスコード）	固定パスコードの有効期間の設定を SecurID PIN の有効期間の設定と同じにするか、別の異なる設定を指定するかを選択します。
SecurID PIN の形式の設定をコピー（固定パスコード）	固定パスコードの形式の設定を SecurID PIN の形式の設定と同じにするか、別の異なる設定を指定するかを選択します。
エマージェンシー アクセス コードの文字要件	エマージェンシー アクセス トークンコードやパスコードは、ユーザーが自分のトークンにアクセスできないときや PIN を忘れたときに、SecurID トークンや SecurID PIN の代わりとして一時的に使用します。生成する各パスコードやトークンコードには、要件に指定された文字が含まれます。次のタイプの文字を要件に含めることができます。 • 数字 • 英字 • 特殊文字

トークン ポリシーの追加

トークン ポリシーは、RSA SecurID PIN と固定パスコードの有効期間と形式、不正なパスコードを入力するユーザーへの対処方法を決定します。

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Token Policies（トークン ポリシー）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**SecurID Token Policy Name（SecurID トークン ポリシー名）**］フィールドに、1 ～ 128 文字の一意の名前を入力します。&、%、>、<、' の各文字は使用できません。
3. ［**Incorrect Passcodes（不正なパスコード）**］で、ユーザーが不正なパスコードを入力した場合のシステムの対応を指定します。
   ユーザーが不正なパスコードを入力できる回数を制限することも、無制限にすることもできます。ユーザーが制限値を超えて不正なパスコードを入力した後に正しいパスコードを入力すると、トークンに次に表示されるトークンコード（ネクスト トークンコード）を入力するようプロンプトが表示されます。
   この設定により、許可されていない人物がパスコードを推測する行為に対する保護が提供されます。この人物が正しいパスコードの推測に成功した場合でも、ネクスト トークンコードの入力が求められます。ネクスト トークンコードを正しく入力するために与えられる機会は 1 回限りです。ネクスト トークン コードモードでは、ユーザーが正しいトークン コードを 2 回連続して入力しないと認証が成功しません。
4. 新しいポリシーをこの環境のデフォルト ポリシーとして設定する場合は、［**Default Policy（デフォルト ポリシー）**］で、［**Set as default SecurID token policy（デフォルト SecurID トークン ポリシーとして設定する）**］を選択します。このセキュリティ ポリシーは、導入環境内で、［**SecurID Token Policy（SecurID トークン ポリシー）**］を［**Always Use Default（常にデフォルトを使用する）**］に設定しているすべてのセキュリティ ドメインに適用されます。セキュリティ ドメインごとに、デフォルト ポリシーから、それ以外のポリシーに変更できます。
5. （オプション）指定した期間が経過するたびにユーザーに SecurID PIN の変更を求める場合は、［**Periodic Expiration（定期的な変更）**］で［**Require periodic SecurID PIN changes（SecurID PIN を定期的に変更する）**］を選択します。このオプションを選択する場合は、次のフィールドも指定します。

- ［**Maximum Lifetime（最長有効期間）**］で、SecurID PIN を変更する頻度を指定します。
- ［**Minimum Lifetime（最短有効期間）**］で、SecurID PIN を変更する間にユーザーが待機する必要がある期間を指定します。これにより、ユーザーが SecurID PIN を繰り返し変更することによって［Restrict Re-use（再使用の制限）］指定をバイパスすることができなくなります。

6. （オプション）［**Restrict Reuse（再使用の制限）**］で、ユーザーに再使用を禁止する直近の SecurID PIN の数を指定します。
7. ［**PIN Creation Method（PIN の作成方法）**］で、SecurID PIN の生成方法を選択します。システムによって SecurID PIN を生成するか、またはユーザーが自分で PIN を作成できるようにするかを選択できます。

注：RSA RADIUS では、デフォルトではシステム生成 PIN を使用できません。システム生成 PIN を使用する場合は、システム生成 PIN を使用できるように RADIUS 構成ファイルの **securid.ini** を変更しない限り、認証が正しく行われません。手順については、RSA Operations Console ヘルプのトピック「RADIUS サーバ ファイルの編集」を参照してください。

8. ［**Minimum Length（最小文字数）**］に、SecurID PIN に含めることができる最小文字数を入力します。
9. ［**Maximum Length（最大文字数）**］に、SecurID PIN に含めることができる最大文字数を入力します。
10. （オプション）特定の単語を PIN に使用できないようにする場合は、［**Excluded Words Dictionary（除外単語辞書）**］ドロップダウン リストから辞書を選択します。
    除外単語辞書の詳細については、RSA Security Console ヘルプのトピック「パスワード ディクショナリの追加」を参照してください。
11. ［**Character Requirements（文字の要件）**］で、SecurID PIN に使用する文字のタイプとして数字または英数字のどちらかを選択し、有効な SecurID PIN を作成するために最小限必要な文字数を各文字タイプに指定します。
12. ［**Fixed Passcode Lifetime（固定パスコードの有効期間）**］で、次のいずれかを実行します。
    - 固定パスコードと SecurID PIN とで同じ有効期間設定を使用する場合は、［**Use same settings from SecurID PIN（SecurID PIN と同じ設定を使用する）**］を選択します。
    - 固定パスコードに関して異なる有効期間設定を指定する場合は［**Define separate settings（別の設定を定義する）**］を選択し、違う設定を指定します。

13. ［**Fixed Passcode Format（固定パスコードの形式）**］で、次のいずれかを実行します。
    - 固定パスコードと SecurID PIN とで同じ形式設定を使用する場合は、［**Use same settings from SecurID PIN（SecurID PIN と同じ設定を使用する）**］を選択します。
    - 固定パスコードに関して異なる形式設定を指定する場合は［**Define separate settings（別の設定を定義する）**］を選択し、長さ、辞書、文字の要件を指定します。
14. ［**Emergency Access Code Format（エマージェンシー アクセス コードの形式）**］で、エマージェンシー コードに含める文字のタイプを指定します。
15. ［Save（保存）］をクリックします。

オフライン認証ポリシー

オフライン認証ポリシーでは、ネットワークに接続されていない場合のユーザー認証方法を定義します。

オフライン認証とは、オフィス外で作業したり、ネットワーク状況によって一時的に接続できないなどの理由から、RSA Authentication Manager に接続できないユーザーにまで、RSA SecurID 認証を拡張したものです。

オフライン認証ポリシーは、各セキュリティ ドメインに割り当てられます。1 つの導入環境に複数のオフライン認証ポリシーを作成できます。

ユーザーがあるセキュリティ ドメインに属しており、エージェント（ユーザーのコンピュータ）が別のセキュリティ ドメインに属していて、双方のセキュリティ ドメインのオフライン認証ポリシーが異なる場合は、2 つのポリシーの間で競合が生じます。

RSA では、次のトークンを使用したオフライン認証は推奨していません。

- PINPad またはソフトウェア トークン
- PIN レストークン
- 固定パスコード

このようなトークンのパスコードの長さは、オフライン認証ポリシーで設定するパスコードの最短の長さの要件よりも短い場合があります。ただし、この長さの要件を無効にし、これらのトークンを使用するオフライン認証を明示的に許可できます。

オフライン認証ポリシーの設定

以下の表は、オフライン認証 ポリシー設定ついて説明しています。

オフライン認証ポリシーの設定	説明
オフライン認証ポリシー名	一意の名前。半角英数 1 ～ 128 文字の長さで指定します。
オフライン認証	コンピュータがネットワークに接続されていないときでも、ユーザーが自分のトークンによる認証を実行することを許可します。
Windows パスワード統合	RSA SecurID を Windows のパスワード ログオン処理に統合します。ユーザーは、最初のオンライン認証の際に自分の Windows のログオン用パスワードを入力するのみです。その後、パスワードはユーザーの認証データと一緒に内部データベースに保存されます。オフライン認証の場合はオフライン データに保存されます。 これ以降の認証では、ユーザーはユーザー名と SecurID パスコードを入力するのみで Windows にログオンできます。Authentication Manager が内部データベースから Windows のパスワードを取得し、これを Windows ログオン システムに渡します。 • Windows パスワード統合の有効化 - Windows パスワード統合は、Security Console の［Add Offline Authentication Policy（オフライン認証ポリシーの追加）］ページおよび［Edit Offline Authentication Policy（オフライン認証ポリシーの編集）］ページで有効にします。 • Windows パスワード統合の削除 - ユーザーの Windows クレデンシャルのキャッシュをクリアするには、Security Console の［Assigned SecurID Tokens & Authentication Attributes（割り当てられた SecurID トークンと認証属性）］ページにある［Windows Password Integration（Windows パスワード統合）］チェックボックスをオフにします。このチェックボックスでキャッシュをクリアした場合は、ユーザーは次回以降のログオンで、Windows パスワードを入力する必要があります。
デフォルト ポリシー	新しいポリシーを導入環境のデフォルト ポリシーとして指定するオプション フィールドです。このオプションを選択した場合、新規作成するセキュリティ ドメインではこのオフライン認証ポリシーが使用されます。
メモ	特記事項があれば記録します。

オフライン認証ポリシーの設定	説明
パスコードの最短の長さ	オフライン認証ポリシーの暗号の強度が決まります。RSA では、パスコードの最短の長さを、12 文字以上に設定することを推奨しています。たとえば、RSA SecurID トークンに 6 桁の数字が表示される場合には、ユーザーは 6 文字以上の PIN を指定する必要があります。 オフライン データをダウンロードするには、ユーザーのパスコード（PIN + トークンコード）の長さは 8 文字から 16 文字である必要があります。

オフライン認証ポリシーの追加

オフライン認証ポリシーでは、ネットワークに接続されていない場合のユーザー認証方式を定義します。レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

重要：オフライン ポリシーを変更すると、以前生成されたオフライン データがすべて破棄され、再生成されます。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Offline Authentication Policies（オフライン認証ポリシー）**］＞［**Add New（新規追加）**］を順にクリックします。
2. ［**Offline Authentication Policy Name（オフライン認証ポリシー名）**］フィールドに、一意の名前を 1 ～ 128 文字で入力します。
3. （オプション）このポリシーでオフライン認証を許可する場合は、［**Enable Offline Authentication（オフライン認証の有効化）**］を選択します。有効化すると、ユーザーのコンピュータがネットワークに接続されていないときでも、ユーザーはトークンを使用して認証を受けることができます。
4. （オプション）Authentication Manager からユーザーに Windows ログイン パスワードを自動的に提供し、SecurID 認証ができるようにするには、［**Enable Windows password integration（Windows パスワード統合の有効化）**］を選択します。
5. （オプション）このポリシーをデフォルトのオフライン認証ポリシーにする場合は、［**Set as default offline authentication policy（デフォルトのオフライン認証ポリシーとして設定）**］を選択します。デフォルト ポリシーは、新規作成されるすべてのセキュリティ ドメインに適用されます。

6. ［**Minimum Passcode Length（パスコードの最短の長さ）**］ドロップダウン メニューで、日数分のオフライン データをダウンロードするときにユーザーが入力する必要があるパスコード（PIN とトークンコード）の最短の長さを選択します。
7. （オプション）PINPad トークン、ソフトウェア トークン、PIN レストークンのパスコードの長さは、指定したパスコードの最短の長さよりも短くなることがあります。RSA では、このようなタイプのトークンを使用したオフライン認証を許可しないことをお勧めします。ただし、［**Allow Offline Authentication Using（次のトークンを使用したオフライン認証を許可）**］フィールドを使用すると、選択したトークンで認証するユーザーに限り、最短の長さの要件が無効になります。
8. （オプション）RSA Authentication Manager で、ユーザーのオフライン エマージェンシー コードを生成する場合は、［**Allow offline emergency codes to be generated（オフライン エマージェンシー コードの生成を許可）**］チェックボックスをオンにします。
9. 生成するオフライン エマージェンシー コードのタイプを選択します。
   - **オフライン エマージェンシー トークンコード**：自分のトークンをなくしたユーザーに対して生成します。ユーザーがコンピュータにログオンするには、PIN に続けてエマージェンシー トークンコードを入力する必要があります。
   - **オフライン エマージェンシー パスコード**：自分の PIN を忘れてしまい、完全なパスコードを必要とするユーザーに対してのみ生成します。エマージェンシー パスコードを付与する場合は、ユーザーが本人であることを正しく確認するようにしてください。エマージェンシー パスコードを使用すると PIN なしでの認証が可能になるため、RSA ではエマージェンシー トークンコードを使用することを推奨しています。
10. ［**Lifetime（有効期間）**］フィールドに、エマージェンシー コードの有効期間を日単位で入力します。デフォルトは 30 日です。
11. ［**Maximum Days of Offline Data（オフライン データの最大日数）**］フィールドで、ユーザーに何日分のオフライン データのダウンロードを許可するかを指定します。
12. ［**Days of Offline Data Warning（オフライン データの警告の日数）**］フィールドで、オフライン認証データの残りの日数が何日になったらユーザーに警告するかを指定します。デフォルトは 7 日です。この警告を受け取ったユーザーは、ネットワークに再接続し、オフライン認証データを補充する必要があります。オフライン認証データの残り日数がゼロになった場合、ユーザーは管理者に連絡する必要があります。
13. ［**Offline Authentication Failures（オフライン認証の失敗）**］フィールドに、許容するオフライン認証の失敗回数を入力します。この回数を超えると、ユーザーはコンピュータへのログオンにエマージェンシー コードを使用しなければならなくなります。

14. （オプション）ユーザーがネットワークに再接続したときに Authentication Manager に認証ログのエントリーをアップロードする場合は、［**Offline Logging（オフライン ログ）**］チェックボックスを選択します。
15. ［**Save（保存）**］をクリックします。

パスワード ポリシー

パスワード ポリシーでは、ユーザーのパスワードの長さ、形式、変更の頻度を定義します。パスワード ポリシーはセキュリティ ドメインに割り当てます。ポリシーは、そのセキュリティ ドメインのすべてのユーザーに適用されます。Operations Console 管理者には、パスワード ポリシーは適用されません。

RSA Authentication Manager を使用するすべてのユーザーは、ユーザー レコードの一部としてパスワードを持つ必要があります。Authentication Manager の内部データベースをアイデンティティ ソースとして使用している場合、パスワードはこの内部データベースに格納されます。

パスワードの特性は、パスワード ポリシーで制御できます。

Authentication Manager のパスワード ポリシーは、内部データベースに保存されたユーザーにのみ適用されます。LDAP ディレクトリに格納されているユーザーには、そのディレクトリのパスワード ポリシーが適用されます。

Authentication Manager のインストール時には、デフォルトのパスワード ポリシーが自動的に作成されます。このポリシーは編集することが可能です。また、カスタム パスワード ポリシーを作成し、これをデフォルトとして指定することもできます。

常に 1 つのポリシーがデフォルトのパスワード ポリシーとして指定されています。セキュリティ ドメインを新しく作成すると、Authentication Manager によってそのセキュリティ ドメインに自動的にデフォルトのパスワード ポリシーが割り当てられます。そのままデフォルトのパスワード ポリシーを使用することも、各セキュリティ ドメインにカスタム ポリシーを割り当てることもできます。

上位のセキュリティ ドメインに割り当てたパスワード ポリシーは、下位のセキュリティ ドメインには継承されません。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを割り当てた場合でも、その下の階層に新しく作成したセキュリティ ドメインには、すべてデフォルトのパスワード ポリシーが引き続き割り当てられます。

システム生成パスワードを有効化した場合、ユーザーは、ユーザーのセキュリティ ドメインに適用されているパスワード ポリシーに従って、Authentication Manager が生成するパスワードを使用する必要があります。

このオプションを有効化すると、ユーザーのパスワードがランダムに生成されるため、ネットワークに不正にアクセスしようとするユーザーから推測されにくくなります。

ユーザーに最初にパスワードを割り当てる場合や、ユーザーのパスワードが期限切れになった場合、パスワードを使用しようとすると、システムで生成されたパスワードのリストからパスワードを選択することを求めるメッセージが表示されます。

セキュリティの強さは、ユーザーの使い勝手を考慮して適切に調整するようにしてください。長いパスワードを要求すると、記憶することが困難で、生産性を阻害すると同時に、ユーザーがネットワークからロックアウトされてしまい、ヘルプ デスクへの電話の数が増えることにもなりかねません。

パスワード ポリシー設定

以下の表は、パスワード ポリシー設定ついて説明しています。

パスワード ポリシー設定	説明
パスワード ポリシー名	一意の名前。半角英数 1 ～ 128 文字の長さで指定します。&、%、>、<、’ の文字は、ポリシー名として使用できません。
システム生成パスワード	ユーザーにシステムが生成したパスワードの使用を強制する場合に選択するオプション フィールドです
デフォルト ポリシー	新しいポリシーを導入環境のデフォルトとして指定するオプション フィールドです。このオプションを選択した場合、新規作成するセキュリティ ドメインではこのパスワード ポリシーが使用されます。
メモ	特記事項があれば記録します。
定期的な変更	一定期間が経過した後、ユーザーにパスワードの変更を要求する場合のオプション設定です。このオプションを選択すると、[Maximum Lifetime (最長有効期間)] フィールドと [Minimum Lifetime (最短有効期間)] フィールドが有効になります。
最長有効期間	ユーザーがパスワードの変更を要求されるまで、同じパスワードを使用できる最長期間を意味します。たとえば、このフィールドを 90 日間と設定したとします。ユーザーがパスワードを 6 月 1 日に変更した場合は、8 月 30 日にはこれを再度変更する必要があります。 このフィールドを設定すると、ユーザーが同じパスワードを継続して使用することができなくなるため、ネットワークに不正にアクセスしようとするユーザーによってパスワードが推測される危険性を低減できます。

パスワード ポリシー設定	説明
最短有効期間	ユーザーが次回パスワードを変更するまでに、現在のパスワードを使い続けなければならない最短期間です。たとえば、パスワードの最短有効期間を 14 日間と設定したとします。ユーザーが自分のパスワードを 6 月 15 日に変更した場合、6 月 29 日までは再度変更することができなくなります。 このフィールドを設定すると、ユーザーが古いパスワードの再使用に関する制限を回避できないようにできます。たとえば、ユーザーに対して直近の 5 個のパスワードの再使用を制限しているとします。このフィールドを設定すると、パスワードを即座に 6 回変更して、ある特定のパスワードを再使用することを防止できます。
再使用の制限	ユーザーが少数のパスワードを再使用できないようにします。たとえば、直近の 20 個のパスワードの使用を制限し、それらのパスワードが「password1」、「password2」、「password3」、さらに「password20」まで続くとします。ユーザーはこれら 20 個のパスワードを入力することはできなくなります。 同じパスワードを再使用すると、不正なユーザーがパスワードを推測できる可能性が高まります。特に「favoritepet1」と「favoritepet11」のように、すべてのパスワードが似通っている場合は危険度が高まります。 制限を設けることで、ペットの名前や子供の誕生日など安易なパスワードの使い回しをすることなく、より安全なパスワードをユーザーに選択させます。
最小文字数	ユーザーが、ネットワークにアクセスしようとする不正ユーザーから推測されやすい短すぎるパスワードを作成できないようにします。
最大文字数	ユーザーが覚えられないような長すぎるパスワードを作成できないようにします。
除外文字	Authentication Manager を構成して、空白を含めた最大 50 文字をパスワードで使用できる文字から除外できます。初期パスワード ポリシーでは、デフォルトで @ と ~ が除外されています。初期パスワードポリシーおよびそれ以外のポリシーを変更し、除外文字を変更することができます。

パスワード ポリシー設定	説明
除外単語辞書	ユーザーのパスワードに使用できない単語を記録したものです。システムに対する辞書攻撃に含まれている可能性が高い、よく使用される単語（「password」など）を登録します。除外単語辞書を使用すると、ユーザーはよく使われる単語、すなわち容易に推測される単語をパスワードとして使用できなくなります。 除外単語辞書を Authentication Manager にアップロードすることができます。除外単語辞書の最大ファイル サイズは 20 MB です。導入環境で使用できる除外単語辞書は 1 つのみです。すでにパスワード辞書がインストールされている場合は、新しい辞書を追加する前に削除する必要があります。 除外単語辞書を追加する手順については、RSA Security Console ヘルプのトピック「Add a Password Dictionary（パスワードディクショナリの追加）」を参照してください。
文字要件	パスワードに特定のタイプの文字を含めることを要件にすると、特に必要な文字が英数字以外の場合にはパスワードを推測することが難しくなります。 システムに対する辞書攻撃では、不正ユーザーがソフトウェアを利用して辞書に記載されているすべての単語をシステム化して入力し、有効なパスワードを推測します。パスワードに特殊文字が含まれていると、この攻撃の効果が弱まります。 たとえば、「maryland」というパスワードが辞書攻撃に含まれる可能性は、「mary%land」または「mary**land」というパスワードよりも高くなります。 次のタイプの文字を要件に含めることができます。 • 英字 • 英大文字 • 英小文字 • 数字 • 特殊文字

パスワード ポリシーの追加

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスで変更に反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Password Policies（パスワード ポリシー）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Password Policy Basics（パスワード ポリシーの基本設定）**］で、次の操作を行います。
   a. ［**Password Policy Name（パスワード ポリシー名）**］フィールドに、新しいパスワード ポリシーの一意の名前を入力します。最大文字数は 128 文字です。
   b. （オプション）ユーザーがシステム生成パスワードのみを使用するようにするには、［**Require users to use system-generated passwords（システム生成のパスワードを使用する）**］を選択します。
   c. （オプション）このポリシーをデフォルト ポリシーとして設定するには、［**Set as the default password policy（デフォルト パスワード ポリシーとして設定する）**］を選択します。このオプションを選択した場合、新規に作成されるセキュリティ ドメインでこのポリシーが使用されます。
3. ［**Lifetime（有効期間）**］で、次のいずれかを実行します。
   a. デフォルト設定の［**Require periodic password changes（パスワードを定期的に変更する）**］をオフにし、ステップ c に移動します。
   b. デフォルト設定の［**Require periodic password changes（パスワードを定期的に変更する）**］をオンにしたまま、次のオプションを指定します。
      – ［**Maximum Lifetime（最長有効期間）**］で、パスワードを使用できる期間を指定します。
      – ［**Minimum Lifetime（最短有効期間）**］で、パスワードを変更する前にユーザーが待機する必要がある期間を指定します。最短有効期間を指定した場合、ユーザーがパスワードをすぐに変更することによってパスワードの再使用制限をバイパスすることができなくなります。
   c. ユーザーが以前に使用したパスワードを使用できなくするには、［**Restrict Re-use（再使用の制限）**］を選択します。使用を禁止する以前のパスワードの数を指定することができます。

4. ［**Format（形式）**］で、次の操作を実行します。
   a. ［**Minimum Length（最小文字数）**］フィールドに、パスワードに必要な最小文字数を入力します。デフォルトは 8 です。
   b. ［**Maximum Length（最大文字数）**］フィールドに、パスワードに使用できる最大文字数を入力します。デフォルトは 32 です。
   c. （オプション）［**Excluded Characters（除外文字）**］フィールドに、ユーザーがパスワードに含めることを禁止する文字を入力します。除外文字として最大 50 文字を指定できます。
   d. ［**Excluded Words Dictionary（除外単語辞書）**］ドロップダウン リストで、使用する除外単語辞書を選択します。この辞書には、禁止されているパスワードのリストが含まれています。
   e. （オプション）［**Character Requirements（文字の要件）**］フィールドに、有効なパスワードのためにそれぞれの文字のタイプで最小限必要となる文字数を入力します。
5. ［**Save（保存）**］をクリックします。

ロックアウト ポリシー

ロックアウト ポリシーでは、何回ログオンに失敗すると Authentication Manager によってアカウントがロックされるか、アカウントのロックを解除する方法（自動または管理者の介在が必要か）を定義します 。ロックアウト ポリシーはセキュリティ ドメインに割り当てます。このポリシーは、そのセキュリティ ドメインに属するすべてのユーザーに適用されます。

Authentication Manager のインストール時には、デフォルトのロックアウト ポリシーが自動的に作成されます。デフォルトのロックアウト ポリシーでは、1 日に 5 回連続で認証試行に失敗すると、ユーザーはロックアウトされます。ユーザー アカウントのロックを解除するには、管理者の介在が必要です。このポリシーを編集するか、またはカスタム ロックアウト ポリシーを作成して、デフォルトとして指定することもできます。また、個々のセキュリティ ドメインにカスタム ポリシーを割り当てることもできます。

上位のセキュリティ ドメインに割り当てたロックアウト ポリシーは、下位のセキュリティ ドメインには継承されません。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを割り当てた場合でも、その下の階層に新しく作成したセキュリティ ドメインでは、すべてデフォルトのロックアウト ポリシーが引き続き使用されます。

ロックアウト ポリシーは、ユーザーが認証に使用するさまざまな認証方式の数に関係なく、すべてのログイン試行に対して適用されます。認証方式には、トークン、固定パスコード、Security Console または Self-Service Console に対するパスワード ベース認証、On-Demand トークンコード、リスク ベース認証があります。たとえば、あるユーザーがソフトウェア トークンを使用して 2 回、ハードウェア トークンを使用して 1 回認証に失敗した場合、合計で 3 回の試行に失敗したことになります。

ロックアウト ポリシー設定

以下の表は、ロックアウト ポリシー設定ついて説明しています。

ロックアウト ポリシー設定	説明
ロックアウト ポリシー名	一意の名前。半角英数 1 ～ 128 文字の長さで指定します。
デフォルト ポリシー	新しいポリシーを導入環境のデフォルト ポリシーとして指定するオプション フィールドです。このオプションを選択した場合、新規作成するセキュリティ ドメインでは、カスタム ポリシーを割り当てない限り、このロックアウト ポリシーが使用されます。
メモ	特記事項があれば記録します。
ユーザー アカウントのロック	認証の失敗を無制限に許可するか、認証の失敗回数が上限を超えたユーザーをロックアウトするかを指定します。デフォルトでは、1 日に連続して 5 回認証試行に失敗した後、システムによりアカウントがロックされます。
ロック解除	ロックアウト ポリシーでは、導入環境からロックアウトされた場合にユーザーを再度有効にする方法も指定します。ポリシーでユーザー アカウントを自動的にロック解除するよう構成している場合には、ロックアウトされたユーザーは指定された時間が経過した後に再び有効になります。この時間はロックアウト ポリシーで指定します。ポリシーでロックアウトされたユーザーを管理者が再度有効にするように構成している場合は、管理者がユーザーを明示的にロック解除するまでは、ユーザーはロックアウトされたままになります。

ロックアウト ポリシーの追加

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延は、ポリシー データが 10 分間キャッシュされることが原因で発生します。レプリカ インスタンスに変更が反映されるまでの時間を短縮し、遅延を最小限に抑える手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Lockout Policies（ロックアウト ポリシー）**］＞［**Add New（新規追加）**］をクリックします。
2. ［**Lockout Policy Name（ロックアウト ポリシー名）**］フィールドに、新しいロックアウト ポリシーの一意の名前を入力します。最大文字数は 128 文字です。
3. （オプション）新規作成するすべてのセキュリティ ドメインと、デフォルト ポリシーがすでに割り当てられている既存のセキュリティ ドメインに対して、このポリシーをデフォルト ポリシーとして割り当てるには、［**Default Policy（デフォルト ポリシー）**］を選択します。
4. ［**Lock User Accounts（ユーザー アカウントのロック）**］フィールドで、ユーザーの認証失敗回数を無制限に許容するか、許容される認証失敗回数を超えたらユーザーをロックアウトするかを指定します。デフォルトでは、1 日に 5 回続けて認証の試行に失敗すると、アカウントはシステムによってロックされます。
5. 認証失敗回数を制限する場合は、［**Unlock（ロック解除）**］フィールドを使用して、指定時間の経過後にユーザーのロックが自動的に解除されるようにするか、ユーザーのロックが必ず管理者によって解除されるようにするかを指定します。デフォルトは、［**Administrators unlock user accounts（管理者がユーザー アカウントをロック解除する）**］です。
6. ［**Save（保存）**］をクリックします。

セルフ サービス トラブルシューティング ポリシー

セルフ サービス トラブルシューティング機能を使用すると、Self-Service Console のユーザーは、パスワードやパスコードなどのプライマリ認証方式で保護されたリソースにアクセスできないときに、定型的な認証のトラブルシューティングを行うことができます。

セルフ サービス トラブルシューティング ポリシーでは、トラブルシューティング機能へのアクセスに使用する代替の認証方式（セキュリティ クエスチョンなど）を定義します。また、このポリシーでは、トラブルシューティング機能からユーザーをロック アウトする条件も指定します。

ユーザーのロックを解除する方法は、次のいずれかを選択する必要があります。

- 指定した時間が経過すると、システムによって自動的にユーザー アカウントのロックが解除される
- 管理者がユーザー アカウントを手動でロック解除する

管理者は、いつでも手動でユーザーのアカウントをロック解除できます。

ポリシーはセキュリティ ドメインに対して設定します。ポリシーは、そのセキュリティ ドメインのすべてのユーザーに適用されます。

上位のセキュリティ ドメインに設定したセルフ サービス トラブルシューティング ポリシーは、下位のセキュリティ ドメインには継承されません。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを設定した場合でも、その下の階層に新しく作成したセキュリティ ドメインには、すべてデフォルトのセルフ サービス トラブルシューティング ポリシーが引き続き設定されます。

セルフ サービス トラブルシューティング ポリシーでは、セカンダリ認証方式を定義できます。セカンダリ認証方式を使用すると、プライマリ認証方式で認証できなかった場合でもユーザーが Self-Service Console にアクセスできるようになります。

重要：セルフ サービス トラブルシューティング ポリシーでは、セルフ サービス トラブルシューティング機能に対するロックアウト基準のみを決定します。Self-Service Console、Security Console、Authentication Manager で保護されたリソースのロックアウト要件を設定するには、RSA Security Console ヘルプのトピック「ロックアウト ポリシー」を参照してください。

セルフ サービス トラブルシューティング ポリシーは、ユーザーが認証に使用するさまざまなトークンの数に関係なく、すべてのログイン試行に対して適用されます。たとえば、あるユーザーがソフトウェア トークンを使用して 2 回、ハードウェア トークンを使用して 1 回認証に失敗した場合、合計で 3 回の試行に失敗したことになります。

セルフ サービス トラブルシューティング ポリシー設定

以下の表は、セルフサービス トラブルシューティング ポリシー設定について説明しています。

セルフ サービス トラブルシューティング ポリシー設定	説明
セルフ サービス トラブルシューティング ポリシー名	一意の名前。半角英数 1 ～ 128 文字の長さで指定します。
デフォルト ポリシー	新しいポリシーを導入環境のデフォルト ポリシーとして指定するオプション フィールドです。このオプションを選択した場合、新規作成するセキュリティ ドメインではこのセルフ サービス トラブルシューティング ポリシーが使用されます。
メモ	特記事項があれば記録します。
認証方式	プライマリ認証方式で問題が発生した場合に、ユーザーが使用する認証方式を指定します。[Security Questions（セキュリティ クエスチョン）] を選択すると、アカウント登録時や Self-Service Console に最初にアクセスする時に、ユーザーはセキュリティ クエスチョンの回答を登録するよう要求されます。
ユーザー アカウントのロック	Self-Service Console にアクセスする際に、ユーザーに許可される認証試行の失敗の回数を制御します。失敗を無制限に許可することも、失敗回数の上限を日、時、分、秒単位で指定することもできます。失敗回数が上限に達すると、このポリシーによりユーザー アカウントがロックされます。
ロック解除	セルフサービス トラブルシューティング ポリシーでは、Self-Service Console からロックアウトされた場合にユーザーを再度有効にする方法も指定します。ポリシーでユーザー アカウントを自動的にロック解除するよう構成している場合には、ロックアウトされたユーザーは指定された時間が経過した後に再び有効になります。ポリシーでロックアウトされたユーザーを管理者が再度有効にするように構成している場合は、管理者がユーザーを明示的にロック解除するまでは、ユーザーはロックアウトされたままになります。

セルフ サービス トラブルシューティング ポリシーの追加

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Self-Service Troubleshooting Policies（セルフ サービス トラブルシューティング ポリシー）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Self-Service Troubleshooting Policy Name（セルフ サービス トラブルシューティング ポリシー名）**］フィールドで、ポリシー名を入力します。128 文字以内のを超えない一意の名前を使用してください。
3. （オプション）新しいポリシーをシステムのデフォルト ポリシーとして指定するには、［**Default Policy（デフォルト ポリシー）**］を選択します。このオプションを選択すると、新規作成されるセキュリティ ドメインはこのポリシーを使用します。
4. （オプション）［**Authentication Method（認証方式）**］で、ユーザーがプライマリ認証方式を使用できない場合に使用する認証方式を選択します。
5. ［**Lock User Accounts（ユーザー アカウントのロック）**］フィールドは、ユーザーがセルフ サービス トラブルシューティング機能にアクセスする際に許可される認証失敗回数を制御します。失敗は無制限に許可することも、一定の日数、時間、分、秒の範囲内で指定した回数許可することもできます。指定した回数に達すると、ユーザーのアカウントはトラブルシューティング機能からロック アウトされます。
6. ［**Unlock（ロック解除）**］フィールドでは、［**Lock User Accounts（ユーザー アカウントのロック）**］フィールドで指定された上限を超えてロックされたユーザーのアカウントを管理者が手動でロック解除するか、システムによって自動的にロック解除するかを構成します。自動でロック解除する場合は、何日後、何時間後、何分後、何秒後にロック解除するかを指定できます。
7. ［**Save（保存）**］をクリックします。

リスク ベース認証ポリシー

RBA が有効な場合、次の認証デバイス関連イベントによってリスク レベルが高くなる可能性があります。

- ユーザーがログオン試行失敗の閾値を超える。
- ユーザーが一時トークンコードまたは固定パスコードを使用する。
- 管理者がユーザーの PIN をクリアする。
- 管理者がユーザーの PIN を変更する。
- 管理者がトークンを紛失としてマークし、ユーザーがそのトークンでログインしようとする。導入環境で RBA を使用するには、RBA ポリシーを作成するか、デフォルトのポリシーを編集する必要があります。その後、ポリシーをセキュリティ ドメインに割り当てます。1 つのポリシーを複数のセキュリティ ドメインに割り当てることができます。詳細については、108 ページのリスク ベース認証ポリシーの追加を参照してください。

RBA（リスク ベース認証）ポリシー設定

Security Console を使用して、セキュリティ ドメインの RBA（リスク ベース認証）ポリシーを定義します。RBA ポリシーには、次のような設定があります。

リスク ベース認証ポリシー設定	説明
RBA ポリシー名	一意の名前。1 ～ 128 文字の長さで指定します。
デフォルト ポリシー	導入環境のデフォルト RBA ポリシーとして設定します。
メモ	特記事項があれば記録します。
自動有効化	ユーザーが RBA で保護されたリソースで初めて認証成功した際に、システムがユーザーの RBA を自動的に有効化するかどうかを指定します。
最低保証レベル	それぞれの認証試行が満たす必要のある信頼性の閾値です。これに満たない場合、ユーザー確認が求められます。 **注：**最低保証レベルを引き上げると、システムによる保証が強化されますが、ユーザーはより頻繁にユーザー確認を求められるようになります。

リスク ベース認証ポリシー設定	説明
サイレント収集期間	指定された期間に、システムが RBA ユーザーのベースライン認証履歴を作成することを許可します。サイレント収集期間中には、システムによりユーザーの認証デバイスが自動的に登録されます。ユーザーにユーザー確認が求められることはありません。
ユーザー確認方法	ログオン時のユーザー確認に使用できる方法です。
新規デバイス登録	未登録の認証デバイスが使用された場合のシステムの対応を指定します。
登録デバイスの合計数	各ユーザーのデバイス履歴に保存される、登録デバイスの最大数です。登録デバイスの数が制限を超えると、夜間のクリーンアップ ジョブにより最も長く使用されていないデバイスから順に削除されます。
デバイスの登録解除	非アクティブな認証デバイスをユーザーのデバイス履歴に残しておく期間を指定します。

リスク ベース認証ポリシーの追加

RBA（リスク ベース認証）は、クライアント デバイスとユーザーの行動パターンに関する情報の蓄積を利用して認証要求の潜在的なリスクを評価し、従来のパスワード ベースの認証システムを強化する多要素認証ソリューションです。RBA ポリシーにより、各セキュリティ ドメインでの RBA の動作が決まります。

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

開始する前に

最低保証レベルの概念を理解している必要があります。詳細については、316 ページの最低保証レベルを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Risk-Based Authentication Policies（リスク ベース認証ポリシー）**］＞［**Add New（新規追加）**］の順にクリックします。

2. ［**RBA Policy Basics（RBA ポリシーの基本設定）**］で、次の操作を行います。
   a. ［**RBA Policy Name（RBA ポリシー名）**］フィールドに、一意のポリシー名を入力します。最大文字数は 128 文字です。
   b. （オプション）導入環境のデフォルト RBA ポリシーとして設定するには、［**Set as default RBA policy（デフォルト RBA ポリシーとして設定）**］を選択します。
   c. （オプション）［**Notes（メモ）**］フィールドに、メモを追加します。
3. ［**Enablement and Assurance Settings（有効化および保証の設定）**］で、次の操作を実行します。
   a. （オプション）ユーザーの認証が成功した後で、自動的に RBA を有効化するには、［**Automatic Enablement（自動有効化）**］フィールドの［**Allow system to enable users for RBA automatically during authentication（認証時にユーザーの RBA を自動的に有効化する）**］を選択します。
   b. ［**Minimum Assurance Level（最低保証レベル）**］フィールドで、ユーザー確認を要求することなく認証するために必要な最低保証レベルを選択します。システムは、ユーザーのプロファイル、認証デバイス、認証履歴に基づいてそれぞれの認証試行の最低保証レベルを決定します。レベルが高くなるほど、ユーザーにユーザー確認が要求される可能性が高くなります。デフォルトの設定は［**Medium（中）**］です。

      注：この設定を変更すると、ユーザー確認を要求する頻度に影響が出ます。

4. ［**Device Registration and Identity Confirmation Settings（デバイス登録およびユーザー確認の設定）**］で、次の操作を実行します。
   a. ［**Silent Collection Period（サイレント収集期間）**］で、次のいずれかを実行します。
      - サイレント収集を有効化するには、［**Allow silent collection（サイレント収集を許可する）**］を選択します。各ユーザーに対し、サイレント収集を行う日数を入力します。
      - サイレント収集を無効化するには、［**Do not allow silent collection（サイレント収集を許可しない）**］を選択します。これはデフォルト設定です。
   b. ［**Identity Confirmation Methods（ユーザー確認方法）**］で、認証要求が最低保証レベルを満たさない場合にユーザーが選択可能な方法を選択します。少なくとも 1 つの方法を選択する必要があります。2 つの方法を選択した場合、どちらの方法を使用するかはユーザーが選択します。

c. ［**New Device Registration（新規デバイス登録）**］で、次のいずれかを選択してユーザーのデバイスを登録します。

- デバイスを自動的に追加するには、［**Register the user authentication device automatically after successful authentication（認証成功後にユーザー認証デバイスを自動的に登録する）**］を選択します。
- デバイスをデバイス履歴に追加するかどうかをユーザーが選択できるようにするには、［**Prompt the user to choose whether the system registers the device after successful authentication（認証成功後にデバイスを登録するかユーザーに確認する）**］を選択します。これはデフォルト設定です。

重要：ユーザーが共有コンピュータまたは公共のコンピュータから RBA で保護されたリソースにアクセスする場合は、このオプションを選択します。

5. ［**Device Administration Settings（デバイス管理設定）**］で、次の操作を実行します。

a. ［**Total Registered Devices（登録デバイスの合計数）**］フィールドに、各ユーザーのデバイス履歴に保持する登録済みデバイスの最大数を入力します。登録済みデバイスの数が制限を超えた場合、毎晩実行されるクリーンアップ ジョブによって、最も長く使用されていないデバイスが削除されます。

b. ［**Unregister Devices（デバイスの登録解除）**］フィールドに、システムが非アクティブ状態のデバイスをユーザーのデバイス履歴から削除する場合に、連続何日間使用しなかったら削除するか日数を入力します。

6. ［**Save（保存）**］をクリックします。

リスク ベース認証メッセージ ポリシー

RBA（リスク ベース認証）メッセージ ポリシーは、ユーザー確認方法の構成をユーザーに促すときに表示されるメッセージを定義します。このメッセージを使用して、ユーザー確認方法を構成する必要がある理由をユーザーに通知できます。このメッセージは次の条件がすべて成立している場合に表示されます。

- ユーザーが SSL-VPN、シン クライアント、Web ポータルなどの Web ベース アプリケーションの認証を受ける。
- ユーザーがユーザー確認方法を指定していない。
- ユーザーが保証レベルの高いデバイスで認証を試みた。

RBA メッセージ ポリシーは任意のセキュリティ ドメインに割り当てることができます。導入環境に複数の RBA メッセージ ポリシーを定義し、セキュリティ ドメインの編集時に割り当てることができます。セキュリティ ドメインでは、明示的に別の RBA メッセージ ポリシーを割り当てるまで、導入環境のデフォルト RBA メッセージ ポリシーを使用します。

リスク ベース認証メッセージ ポリシー設定

以下の表は、RBA（リスク ベース認証）メッセージ ポリシー設定について説明しています。

設定	説明
RBA メッセージ ポリシー名	一意の名前。1 ～ 128 文字の長さで指定します。
デフォルト ポリシー	新しいポリシーを導入環境のデフォルト ポリシーとして指定するオプション フィールドです。このオプションを選択した場合、新規作成するセキュリティ ドメインではこの RBA メッセージ ポリシーが使用されます。
メモ	特記事項があれば記録します。
メッセージ テキスト	企業ポリシーまたはビジネス ニーズに関するカスタム メッセージです。

リスク ベース認証メッセージ ポリシーの追加

RBA（リスク ベース認証）メッセージ ポリシーは、ユーザー確認方法の構成をユーザーに促すときに表示されるメッセージを定義します。RBA メッセージ ポリシーは、複数（たとえば、各セキュリティ ドメインに 1 つずつ）作成できます。このポリシーは、セキュリティ ドメインのすべてのユーザーに適用されます。

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、[**Authentication（認証）**] > [**Policies（ポリシー）**] > [**RBA Message Policies（RBA メッセージ ポリシー）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**RBA Message Policy Basics（RBA メッセージ ポリシーの基本設定）**] で、次の操作を行います。
   a. [**RBA Message Policy Name（RBA メッセージ ポリシー名）**] フィールドに、一意の名前を入力します。最大文字数は 128 文字です。
   b. （オプション）このポリシーをデフォルト ポリシーとして設定するには、[**Set as the default RBA Message Policy（デフォルト RBA メッセージ ポリシーとして設定する）**] を選択します。
   c. （オプション）[**Notes（メモ）**] フィールドに、任意のメモを入力します。
3. [**Message Confirmation（メッセージの確認）**] で、[**Message Text（メッセージ テキスト）**] フィールドのメッセージを確認し、必要に応じてメッセージを変更します。
4. [**Save（保存）**] をクリックします。

5 LDAP ディレクトリの統合

アイデンティティ ソース

アイデンティティ ソースは、ユーザーおよびユーザー グループのデータが保存されているリポジトリです。導入環境のすべてのユーザーおよびユーザー グループは、アイデンティティ ソースに関連づけられています。

Authentication Manager では、次のアイデンティティ ソースをサポートしています。

- LDAP ディレクトリ

  Authentication Manager では、アイデンティティ ソースとして次のディレクトリをサポートしています。

  – Active Directory 2008 R2

  – Sun Java System Directory Server 7.0

  – Oracle Directory Server Enterprise Edition 11G

  Active Directory では、アイデンティティ ソースとしてグローバル カタログを追加できます。これは、認証時にユーザーを検索し、グループ メンバーシップを解決するために使用されます。グローバル カタログ アイデンティティ ソースを使用して、管理タスクを実行することはできません。

- Authentication Manager の内部データベース

LDAP ディレクトリのデータ

Authentication Manager は、すべての LDAP ディレクトリ アイデンティティ ソースに対する read-only アクセス権を持っています。ディレクトリを Authentication Manager と統合すると、Security Console を使用して、次の操作を実行できます。

- ディレクトリに存在するユーザーおよびユーザー グループ データを表示する（ただし、追加、変更はできない）。
- Authentication Manager の管理タスクを実行する。たとえば、ODA（On-Demand 認証）および RBA（リスク ベース認証）の使用を有効化または無効化することや、ディレクトリに存在する個々のユーザーにトークンまたはユーザー エイリアスを割り当てることができます。

ディレクトリ内のデータを変更するには、LDAP ディレクトリのネイティブ ユーザー インタフェースを使用する必要があります。

内部データベースのデータ

Authentication Manager には、ユーザーおよびユーザー グループを作成できる内部データベースが用意されています。管理者は、Security Console を使用して、内部データベース内のユーザーおよびユーザー グループに対して次の操作を実行できます。

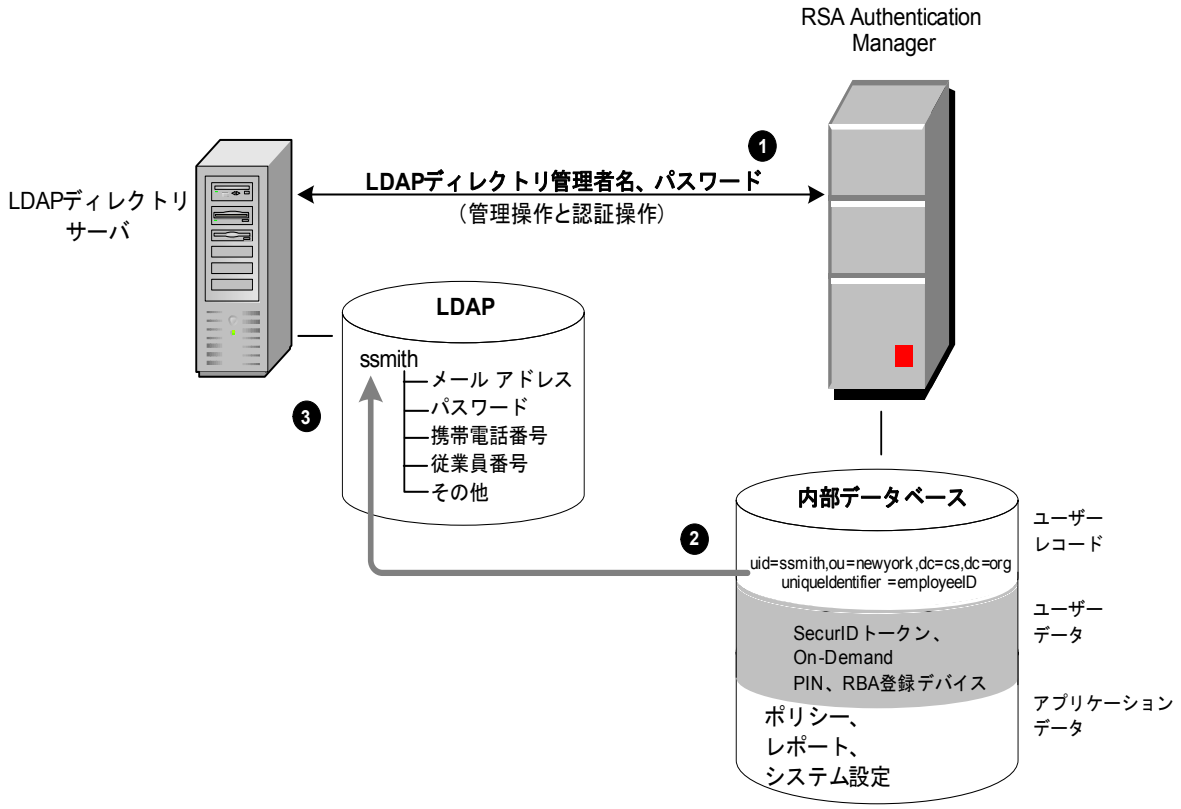
- ユーザーおよびユーザー グループのデータを追加、変更、表示する。
- 個々のユーザーに対して Authentication Manager の機能（ODA や RBA など）を有効化または無効化する。

次の情報は、内部データベースのみに格納されています。

- ポリシー、管理者ロール、認証エージェント、SecurID トークンレコードなど、Authentication Manager に固有のデータ
- LDAP ディレクトリのユーザーおよびユーザー グループ レコードを Authentication Manager にリンクするためのデータ

アイデンティティ ソース データ フロー

次の図は、データ エレメント（LDAP 属性および Authentication Manager 属性）が外部アイデンティティ ソースと内部データベースの間でどのように分散しているかを示しています。この図はまた、Authentication Manager と LDAP 外部アイデンティティ ソースの間の接続も示しています。



1. Authentication Manager は、LDAP 管理者ユーザー名とパスワードを使用して、LDAP ディレクトリと通信を行います。

   管理者アカウントに読み取り / 書き込みアクセス権が設定されている場合、エンドユーザーは、Authentication Manager 経由で表示されるパスワード更新プロンプトに直接応答することにより、自分のパスワードを更新することができます。アクセス権が読み取り専用の場合、ユーザーはパスワードの更新のために、LDAP 管理者に連絡する必要があります。

2. 内部データベースには、各ユーザーの識別名と一意識別子（LDAP ディレクトリ内でユーザーレコードを検索するために使用）への参照が保存されます。また、On-Demand 認証 PIN、セキュリティ クエスチョン、ユーザー アカウントを有効化 / 無効化するパラメータといった、Authentication Manager に特有のユーザー属性も保存されます。

3. ディレクトリ サーバには、すでに一般的な LDAP ユーザー レコードおよび属性が保存されています。Authentication Manager は複数のディレクトリ サーバと連携可能です。

アイデンティティ ソースのプロパティ

アイデンティティ ソースを追加または編集するときに、アイデンティティ ソースのプロパティを指定します。Operations Console では、アイデンティティ ソースのプロパティがカテゴリーに分類されています。

- Identity Source Basics（アイデンティティ ソースの基本設定）
- Directory Connection - Primary and Replica（ディレクトリ接続 - プライマリとレプリカ）
- Directory Settings（ディレクトリ設定）
- Active Directory Options（Active Directory オプション）
- Directory Configuration-User Tracking Attributes（ディレクトリ構成 - ユーザー トラッキング属性）
- Directory Configuration - Users（ディレクトリ構成 - ユーザー）
- Directory Configuration - User Groups（ディレクトリ構成 - ユーザー グループ）

Identity Source Basics（アイデンティティ ソースの基本設定）

[**Identity Source Name（アイデンティティ ソース名）**]：アイデンティティ ソースの一意な名前です。この名前は Security Console に表示され、アイデンティティ ソースを特定します。

[**Type（タイプ）**]：アイデンティティ ソースのタイプです。LDAP アイデンティティ ソース タイプには、たとえば、Microsoft Active Directory、Sun Java System Directory Server、Oracle Directory Server があります。アイデンティティ ソースを導入環境に追加した後で、アイデンティティ ソースのタイプを変更することはできません。サポートされるアイデンティティ ソースのリストについては、RSA Operations Console ヘルプのトピック「アイデンティティ ソース」を参照してください。

[**Notes（メモ）**]：アイデンティティ ソースに関する注釈を 255 文字以内のテキストで追加できます。

Directory Connection - Primary and Replica（ディレクトリ接続 - プライマリとレプリカ）

[**Directory URL（ディレクトリ URL）**]：新しいアイデンティティ ソースの URL です。標準の SSL-LDAP ポート 636 を使用する場合は、「ldaps://hostname/」と入力してください。その他のポートを使用する場合は、「ldaps://hostname:port/」のようにポート番号も指定してください。パスワードの管理には、SSL 接続が必須です。

Active Directory の場合、グローバル カタログは、グローバル カタログではない別のアイデンティティ ソースと同じディレクトリ URL を持つことができます。

[**Directory Failover URL（ディレクトリ フェイルオーバー URL）**]：（オプション）フェイルオーバー ディレクトリ サーバは、プライマリ ディレクトリ サーバとの接続に障害が発生した場合に使用されます。フェイルオーバー ディレクトリ サーバは、プライマリ ディレクトリ サーバのミラーである必要があります。

認証時にユーザーによるパスワードの変更を許可する場合は、LDAP ディレクトリ管理者アカウントに、アイデンティティ ソース内のユーザー レコードに対する書き込み権限が必要です。パスワード変更を許可しない場合には、ディレクトリ管理者アカウントに書き込み権限は必要ありません。

[**Directory User ID（ディレクトリ ユーザー ID）**]：LDAP ディレクトリ管理者のユーザー ID です。

たとえば、「cn=Administrator,cn=Users,dc=domain,dc=com」または「Administrator@domain.com」のように入力できます。

[**Directory Password（ディレクトリ パスワード）**]：LDAP ディレクトリ管理者のパスワードです。

このパスワードは、最新の状態を維持する必要があります。このパスワードの有効期限が切れると、接続できなくなります。

Directory Settings（ディレクトリ設定）

ディレクトリ設定では、アイデンティティ ソースの範囲を指定し、アイデンティティ ソースのサブセットのみが使用されるようにします。詳細については、123 ページのアイデンティティ ソース範囲の変更要件を参照してください。

アイデンティティ ソースの範囲を狭める場合は、内部データベースから解決不可能なユーザーやユーザー グループへの参照を削除するため、クリーンアップ ジョブをスケジュールする必要があります。詳細については、180 ページのクリーンアップ ジョブのスケジュールを参照してください。

[**User Base DN（ユーザー ベース DN）**]：ディレクトリ ユーザー定義のベース DN です。たとえば、Active Directory の場合、「cn=Users,dc=domainName,dc=com」と入力できます。

[**User Group Base DN（ユーザー グループ ベース DN）**]：ディレクトリ ユーザー グループ定義のベース DN です。たとえば、Active Directory の場合、「ou=Groups,dc=domain,dc=com」と入力できます。

次のルールに従ってください。

- 複数のアイデンティティ ソースを重複した範囲で構成してはいけません。同じユーザー ベース DN またはユーザー グループ ベース DN を指定した複数のアイデンティティ ソースがある場合は、ユーザー検索フィルタおよびユーザー グループ 検索フィルタを構成し、各ユーザーおよびユーザー グループがいずれか 1 つのアイデンティティ ソースにのみ属するようにする必要があります。不適切な構成は、解決不可能なユーザーや認証に関する問題につながる場合があります。

- 属性値にコンマや等号記号が含まれている場合は、これらの文字をバックスラッシュ（円記号）でエスケープする必要があります。たとえば、ou 属性の値が「A=B, Inc」である場合、「ou=A¥=B¥, Inc」と入力する必要があります。属性値のこれらの文字をエスケープしないと、アイデンティティ ソースへの接続が失敗します。これは属性値の中で使われているコンマまたは等号記号にのみ適用されます。識別名の要素を区切るコンマ（たとえば cn=Joe Smith, ou=Sales）や属性名と属性値の間の等号記号（たとえば ou=Sales）はエスケープしないでください。
- 「Groups」はデフォルトの組織単位ですが、Active Directory のデフォルト設定ではインストールされません。［**User Group Base DN（ユーザー グループ ベース DN）**］に対して有効なコンテナが指定されていることを確認します。

［**Search Results Time-out（検索処理タイムアウト）**］：検索の継続時間を制限します。ディレクトリ サーバ上でユーザーまたはグループの検索処理がタイム アウトになる場合は、このフィールド値を大きくするか、または個々の検索結果を絞り込むようにしてください。たとえば、「Last Name = *」の代わりに「Last Name = G*」として、検索範囲を絞り込みます。

［**User Account Enabled State（ユーザー アカウントの有効状態）**］：Authentication Manager が、ユーザー アカウントの有効 / 無効の状態を判断する場所を指定します。

- ［**Directory（ディレクトリ）**］を選択すると、外部アイデンティティ ソースのみで判断します。
  外部アイデンティティ ソースでユーザー アカウントが無効になっている場合、そのユーザー アカウントは認証できません。ユーザーの認証可否は、外部アイデンティティ ソースの［User Account Enabled State（ユーザー アカウントの有効状態）］のみに基づいて決定されます。
- 外部アイデンティティ ソースに加えて内部データベースから判断するには、［**Directory and Internal Database（ディレクトリと内部データベース）**］を選択します。
  認証を受けるユーザーは、内部データベースと外部アイデンティティ ソースの両方で、ユーザー アカウントが有効になっている必要があります。内部データベースまたは外部アイデンティティ ソースのどちらか一方でユーザー アカウントが無効になっている場合、そのユーザーは認証できません。

［**Validate Map Against Schema（マッピングをスキーマで検証）**］：アイデンティティ属性定義を作成または変更するときに、ディレクトリ スキーマに対してアイデンティティ属性定義のマッピングを検証します。

Active Directory Options（Active Directory オプション）

［**Global Catalog（グローバル カタログ）**］：アイデンティティ ソースが Active Directory グローバル カタログである場合、これを選択します。

[**User Authentication（ユーザー認証）**]：次の値のいずれかを、ユーザー認証のソースとして選択します。

- [**Authenticate users to this identity source（このアイデンティティ ソースを使用してユーザーを認証）**]：アイデンティティ ソースがグローバル カタログに関連づけられていない場合、このオプションを選択します。アイデンティティ ソースとして構成されたグローバル カタログがない場合、このオプションが自動的に選択されます。
- [**Authenticate users to a global catalog（グローバル カタログを使用してユーザーを認証）**]：アイデンティティ ソースがグローバル カタログに関連づけられている場合は、このオプションを選択し、ドロップダウン メニューからグローバル カタログを選択します。

Directory Configuration-User Tracking Attributes（ディレクトリ構成 - ユーザー トラッキング属性）

[**User ID（ユーザー ID）**]：ユーザー ID をマッピングするには、次のいずれかを選択します。

- [**Maps to（マッピング）**]：このオプションを選択すると、ユーザー ID を指定した属性にマッピングできます。
- [**Uses the same mapping as E-mail（メールと同じマッピングを使用）**]：このオプションを選択すると、ユーザー ID をメール属性にマッピングします。このオプションを選択すると、ユーザー ID とメールのフィールドに同じ値が入ります。メール属性は、ディレクトリで定義しておく必要があります。

ユーザー ID のマッピングを変更する場合、新しいフィールドはすべてのユーザーに一意であり、古いフィールドと重複しないことを確認します。これにより、一部のユーザーの管理データが誤ったユーザー レコードに関連づけられるのを防ぐことができます。たとえば、古いマッピングで、「jdoe」というユーザー ID が存在したのであれば、新しいマッピングには、「jdoe」というユーザー ID が含まれないようにします。古いユーザー ID マッピングから新しいマッピングにスムーズに移行するには、解決不可能なユーザーをクリーンアップして内部データベースのユーザー レコードを新しいユーザー ID で更新する必要があります。このタスクは、マッピングを変更したらただちに実行してください。操作手順については、「管理者ガイド」を参照してください。

[**Unique Identifier（一意識別子）**]：一意識別子は、DN が変更されたユーザーを Security Console から検索する際に役立ちます。Active Directory の場合は、デフォルトで ObjectGUID 属性が使用されます。Oracle Directory Server（または Sun Java Directory Server）の場合、デフォルト値は「nsUniqueID」です。

Security Console を使用して表示または管理する LDAP ディレクトリ ユーザーを、LDAP ディレクトリ上で移動または名前変更する前に、一意識別子を指定する必要があります。この条件が満たされていないと、システムは移動または名前変更されたユーザーのレコードを重複して作成し、それまでシステムに格納していたデータとの関連づけを解除します。

次の要件を満たすディレクトリの属性を入力してください。

- 属性には、ユーザーごとに一意なデータが格納されていることが必要です。たとえば、導入環境内のユーザーごとに一意である従業員 ID 番号や社員証番号などです。
- すべてのユーザーで、属性値が設定されている必要があります。値は空にできません。
- 属性値は変更することはできません。ユーザーの属性値を変更すると Authentication Manager はそのユーザーを追跡できなくなります。一意識別子にマッピングした属性に、他のフィールドをマッピングすることはできません。
- 属性名には最大 64 文字まで含めることができます。
- 属性値には最大 42 文字まで含めることができます。

注：サードパーティのディレクトリ管理ツールが、2 つの DN 間でユーザーを移動する操作を、ディレクトリからのユーザーの削除と新規追加の組み合わせによって処理する場合は、一意識別子のデフォルト値の使用は推奨されません。

Directory Configuration - Users（ディレクトリ構成 - ユーザー）

［**First Name（名前）**］：First Name（名前）属性にマッピングするディレクトリ属性です。デフォルトでは、［First Name（名前）］は「givenName」にマッピングされます。

［**Middle Name（ミドル ネーム）**］：Middle Name（ミドル ネーム）属性にマッピングするディレクトリ属性です。デフォルトでは、［**Middle Name（ミドル ネーム）**］は「initials」にマッピングされます。

［**Last Name（苗字）**］：Last Name（苗字）属性にマッピングするディレクトリ属性です。デフォルトでは、［Last Name（苗字）］は「sn」にマッピングされます。

［**E-mail（メール）**］：E-mail（メール）属性にマッピングするディレクトリ属性です。デフォルトでは、［E-mail（メール）］は「mail」にマッピングされます。

［**Certificate DN（証明書 DN）**］：今後の使用のために予約されています。デフォルトでは、「comment」にマッピングされます。Certificate DN（証明書 DN）属性に、「cn」や「sAMAccountName」などの重要なフィールドをマッピングしないでください。

［**Password（パスワード）**］：Password（パスワード）属性にマッピングするディレクトリ属性です。デフォルトでは、［Password（**パスワード**）］は「unicodePwd」にマッピングされます。

[**Search Filter（検索フィルタ）**]：LDAP ディレクトリ内のユーザー エントリーを絞り込むためのフィルタを入力します（ユーザー オブジェクト クラスに対するフィルタなど）。ユーザー エントリーに対する任意の有効な LDAP フィルタを指定可能です。たとえば、「(objectclass=inetOrgPerson)」と指定します。

[**Search Scope（検索スコープ）**]：LDAP ツリー内のユーザー検索の範囲です。

[**Object Classes（オブジェクト クラス）**]：Security Console を使用して管理されるアイデンティティ ソース内のユーザーのオブジェクト クラスです（「user, organizationalPerson, person」など）。

Directory Configuration - User Groups（ディレクトリ構成 - ユーザー グループ）

[**User Group Name（ユーザー グループ名）**]：User Group Name（ユーザー グループ名）属性にマッピングするディレクトリ属性です。たとえば、[User Group Name（ユーザー グループ名）] を「cn」にマッピングします。

[**Search Filter（検索フィルタ）**]：ユーザー グループ オブジェクト クラスのフィルタ（たとえば objectclass=group）のように、ユーザー グループ エントリーのみを返す LDAP フィルタです。

[**Search Scope（検索スコープ）**]：LDAP ツリー内のユーザー グループ検索の範囲。

[**Object Classes（オブジェクト クラス）**]：Security Console を使用して管理されるユーザー グループのオブジェクト クラスです。

[**Membership Attribute（メンバーシップ属性）**]：ユーザー グループに含まれるすべてのユーザーおよびユーザー グループの DN が格納される属性です。

[**Use MemberOf Attribute（MemberOf 属性の使用）**]：MemberOf 属性を使用したメンバーシップクエリーの解決を有効化します。

[**MemberOf Attribute（MemberOf 属性）**]：所属先のユーザー グループの DN が格納されるユーザー / ユーザー グループの属性です。

アイデンティティ ソース範囲

アイデンティティ ソース範囲は、アイデンティティ ソース内で管理する LDAP ディレクトリのユーザーおよびユーザー グループのサブセットを決定します。

アイデンティティ ソース範囲の設定

アイデンティティ ソースを追加する時に、ベース DN、検索フィルタ、検索スコープ（単一レベルまたはすべてのレベル）の指定によりアイデンティティ ソースの範囲を決定します。

設定	説明
ユーザー ベース DN	Authentication Manager がユーザーを検索するディレクトリの場所。
ユーザー グループ ベース DN	Authentication Manager がグループを検索する LDAP ディレクトリの場所。
ユーザー検索フィルタおよびユーザー グループ 検索フィルタ	ユーザーまたはグループ エントリーのみを返す LDAP フィルタ。例：ユーザー グループ オブジェクト クラスのフィルタ（objectclass=groupOfUniqueNames）。
ユーザー検索スコープおよびグループ検索スコープ	LDAP ツリー内のユーザーおよびユーザー グループ検索の範囲。
ユーザー オブジェクト クラスおよびグループ オブジェクト クラス	Authentication Manager がアクセスするユーザーおよびユーザー グループのオブジェクト クラス。フィールドにマッピングするカスタム属性は、オブジェクト クラスに含まれる必要があります。詳細については、136 ページのカスタム属性マッピングを参照してください。

重要：複数のアイデンティティ ソースを構成する場合は、範囲が重複しないようにする必要があります。同じユーザー ベース DN またはユーザー グループ ベース DN を指定した複数のアイデンティティ ソースがある場合は、ユーザー検索フィルタおよびユーザー グループ 検索フィルタを構成し、各ユーザーおよびユーザー グループがいずれか 1 つのアイデンティティ ソースにのみ属するようにする必要があります。構成が不適切だと、解決不可能なユーザーや認証の問題が発生することがあります。

アイデンティティ ソース範囲の変更要件

アイデンティティ ソース範囲を拡大したり、縮小することができます。アイデンティティ ソース範囲を縮小する場合は、一部のユーザーやユーザー グループが解決不可能になったり、認証できなくなったりする可能性があります。解決不可能なユーザーとは、Authentication Manager がアイデンティティ ソースとして指定された LDAP ディレクトリから検出できないユーザーのことです。

アイデンティティ ソースの範囲を狭めた後は、内部データベースから解決不可能なユーザーやユーザー グループへの参照を削除するため、クリーンアップ ジョブをスケジュールする必要があります。操作手順については、179 ページの解決不可能なユーザーおよびユーザー グループのスケジュール クリーンアップを参照してください。

スケジュール クリーンアップ ジョブを実行するときには、猶予期間およびクリーンアップ制限を設定している場合はその両方を無効化し、この 1 回のクリーンアップの実行後に再度設定を有効化する必要があります。

注：アイデンティティ ソースの範囲を拡大した場合は、スケジュール クリーンアップ を実行する必要はありません。

グローバル カタログでない Active Directory アイデンティティ ソース

Active Directory では、グローバル カタログ以外のアイデンティティ ソースが管理操作（ユーザーの On-Demand 認証やリスク ベース認証の有効化など）に使用されます。グローバル カタログを使用していない場合、このタイプのアイデンティティ ソースはユーザーの検索および認証にも使用されます。このタイプのアイデンティティ ソースはドメイン コントローラにマッピングされます。

Authentication Manager で Active Directory ドメイン ユーザーを管理する場合、Authentication Manager で認証するユーザーを格納する各ドメインをアイデンティティ ソースとして追加する必要があります。

たとえば、Active Directory フォレストに 3 つのドメインと 1 つのグローバル カタログがある場合に、そのうち 2 つのドメインのユーザーを認証するには、その 2 つのドメインをそれぞれアイデンティティ ソースとして追加する必要があります。

重要：Authentication Manager は、各導入環境で最大 30 のグローバル カタログでないアイデンティティ ソースをサポートします。内部データベースをアイデンティティ ソースとして使用する場合、この制限には、内部データベースは含まれません。

グローバル カタログでないアイデンティティ ソースでは、Active Directory の 3 つのタイプのセキュリティ グループ（ユニバーサル セキュリティ、グローバル、ドメイン ローカル）をすべてグループ メンバーシップ データとして使用できます。ただし、Authentication Manager は制限付きエージェントへのアクセスを許可する際は、すべてのグループをサポートするわけではありません。

Active Directory 内のグループ間メンバーシップのサポート

Active Directory のグループ間メンバーシップをサポートするには、ドメインの機能レベルを Windows 2003 または 2008 に設定する必要があります。ドメインの機能レベルを上げる方法の詳細については、**http://support.microsoft.com/kb/322692** を参照してください。

注：デフォルトの組織ユニット「Groups」は、デフォルトの Active Directory インストール環境には存在しません。アイデンティティ ソースを追加する場合は、ユーザーグループ ベース DN に対して有効なコンテナが指定されていることを確認します。

Active Directory グローバル カタログ アイデンティティ ソース

Active Directory フォレストがあり、その中で複数のアイデンティティ ソースを構成する場合は、必要に応じて、他の Active Directory アイデンティティ ソースがユーザーの検索 / 認証またはフォレスト内のグループ メンバーシップの解決に使用できるアイデンティティ ソースとして、Active Directory グローバル カタログを構成できます。次の操作が必要です。

- 各グローバル カタログを、別のアイデンティティ ソースとして Authentication Manager に追加すること。
- グローバル カタログをホストするドメイン コントローラ上のグローバル カタログ ポートにアイデンティティ ソースを関連づけること。

Authentication Manager では、ユーザーのパスワードの変更などの管理操作にグローバル カタログを使用しません。管理操作は、非グローバル カタログ アイデンティティ ソースに対してのみ実行されます。

グローバル カタログ使用時の導入環境の要件

これらの要件は、制限付き認証エージェントを使用する導入環境にのみ適用されます。

グローバル カタログをアイデンティティ ソースとして使用するには、導入環境が次の要件をすべて満たしている必要があります。

- 制限付き認証エージェントに対するアクセス権を付与するすべてのグループは、Windows ユニバーサル セキュリティ グループである必要があります。

- Security Console からは、Active Directory のすべてのタイプのグループ（ユニバーサル セキュリティ、ドメイン ローカル、グローバル）を表示できますが、グローバル カタログ経由で制限付きエージェントへのアクセス権の付与に使用できるのはユニバーサル セキュリティ グループのみです。
- フォレスト内のすべてのドメインは、Windows 2008 R2 を実行する必要があります。

Windows 管理者のみが Active Directory 内のグループ タイプを変更することができます。

重要：Active Directory グループのリストからグループを選択して、制限付きエージェントでユーザーをアクティブ化する場合は、ユニバーサル セキュリティ グループを選択していることを確認してください。その他のグループ タイプを選択しても、ユーザーは認証できません。

グローバル カタログのデータ レプリケーション

アイデンティティ ソースとして Active Directory グローバル カタログを使用する場合、個々の Active Directory ドメイン コントローラはグローバル カタログにドメイン変更をレプリケーションします。このような導入環境では、次のものを Authentication Manager と統合する必要があります。

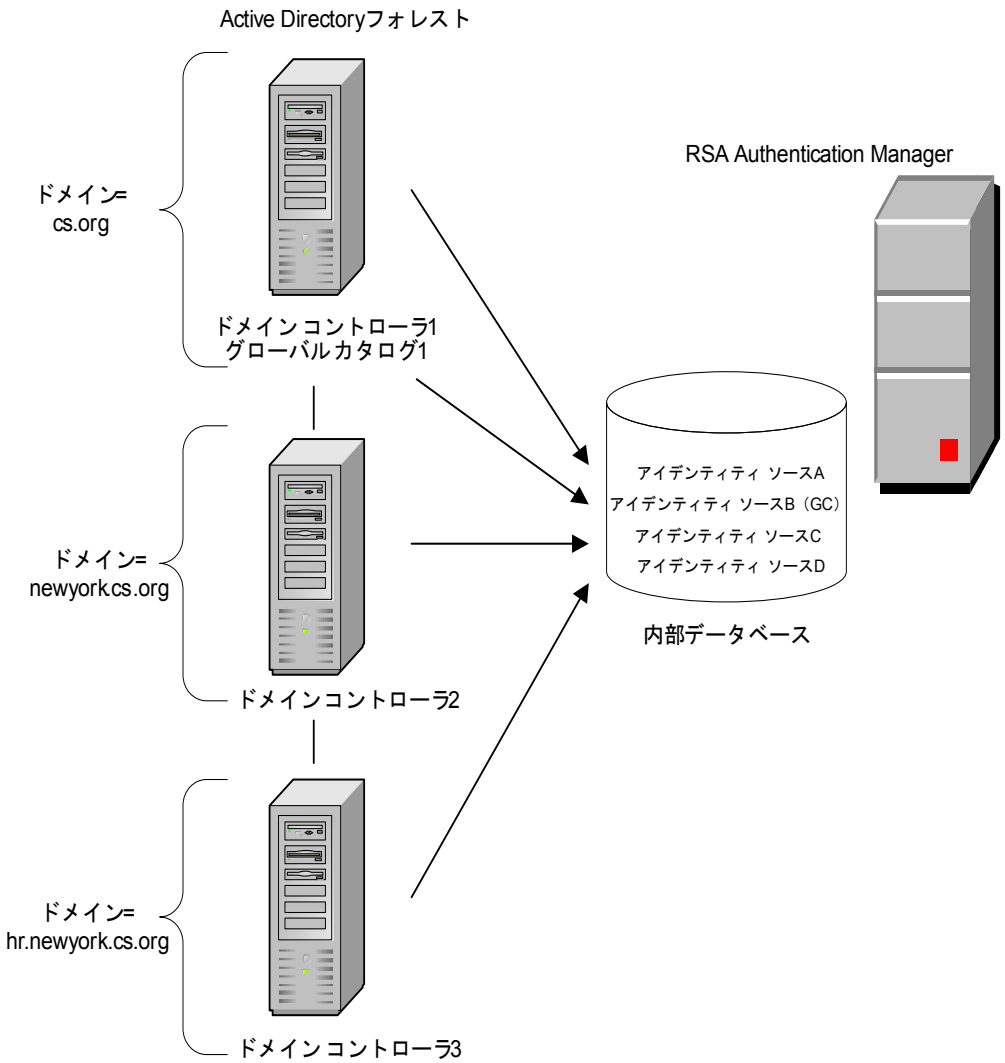
- グローバル カタログ。フォレストに 2 つ以上のグローバル カタログがある場合、1 つをフェイルオーバー用に使用できます。2 番目のグローバル カタログ用にアイデンティティ ソースを作成する必要はありません。その代わり、最初のグローバル カタログ用にアイデンティティ ソースを作成するときに、2 番目のグローバルカタログをフェイルオーバー URL として指定することができます。
- Authentication Manager から参照したいユーザーとユーザー グループが含まれるすべてのドメイン コントローラ。それぞれのドメインをアイデンティティ ソースとして追加します。

たとえば、GC1 がユーザー認証用のグローバル カタログ アイデンティティ ソースで、AD1、AD2、AD3 がそれぞれのデータのサブセットを GC1 にレプリケーションすると仮定します。その場合、各 Active Directory をアイデンティティ ソースとして登録する必要があります。統合が完了すると、Authentication Manager は認証リクエストのために GC1 に、ユーザー パスワードの更新などの管理のために AD1、AD2、AD3 にアクセスします。

グローバル カタログを含む 4 つのアイデンティティ ソースを持つ導入環境の例

次の図は 3 つのドメインからなるフォレストを示し、それぞれに 1 つのドメイン コントローラと、1 つのグローバル カタログを含みます。この例では、Authentication Manager に少なくとも 4 つのアイデンティティ ソースを登録する必要があります。

- ドメイン コントローラ用の 3 つのアイデンティティ ソースと、可能であればそれぞれのフェイルオーバー ドメイン コントローラ
- グローバル カタログ用の 1 つのアイデンティティ ソースと、可能であれば 1 つのフェイルオーバー グローバル カタログ サーバ



Active Directory 接続タイムアウトの構成

状況によっては、Authentication Manager が LDAP ディレクトリに接続を確立するにはデフォルトで設定されている LDAP 接続タイムアウトが短すぎる場合があります。Authentication Manager が接続を確立するときの待機時間を調整する必要がある場合は、Operations Console を使用してアイデンティティ ソースを編集し、[**Search Results Time-out（検索処理タイムアウト）**] フィールドの値を変更します。

LDAP ディレクトリをアイデンティティ ソースとして統合

Authentication Manager では、ディレクトリ スキーマを変更せずに LDAP ディレクトリ サーバをアイデンティティ ソースとして統合できます。統合は、アイデンティティ ソースの追加、Authentication Manager へのリンク、アイデンティティ属性定義の LDAP ディレクトリ属性名へのマッピングを行うことにより実行します。

次のガイドラインに従ってください。

- LDAP 接続情報および LDAP スキーマについての詳細な知識を必要とします。
- Authentication Manager で認証するユーザーが格納された各ディレクトリをアイデンティティ ソースとして構成する必要があります。
- 通常、プライマリ インスタンスとレプリカ インスタンスは同じディレクトリ サーバを使用しませんが、同じフェイルオーバー ディレクトリ サーバを共有することは可能です。両方のインスタンスが同じディレクトリ サーバを使用する場合、ディレクトリシステムの停止またはネットワーク停止が認証の失敗につながる可能性があります。
- 現在レプリカ インスタンスを構成していないが、将来的に計画している場合、レプリカ インスタンスを構成後、レプリカ インスタンスのアイデンティティ ソース接続情報を更新する必要があります。

次のステップは、LDAP ディレクトリ サーバをアイデンティティ ソースとして統合する方法の概要を説明します。

1. Operations Console を使用して SSL 接続をセットアップします。134 ページのアイデンティティ ソース SSL 証明書を参照してください。このステップは、Authentication Manager 経由でユーザーが自分のパスワードを変更できるよう許可する場合に必要です。
2. （オプション）パスワード ポリシーを確認し、必要に応じて調整を行います。136 ページの Active Directory のパスワード ポリシーを参照してください。このステップは、Authentication Manager 経由でユーザーが自分のパスワードを変更できるよう許可する場合にのみ必要です。

3. ディレクトリ サーバが Active Directory の場合は、ドメインの機能レベルがグループ間のメンバーシップをサポートするかを確認します。ドメイン コントローラのシステム コントロール パネルを確認します。124 ページの Active Directory 内のグループ間メンバーシップのサポートを参照してください。
4. ディレクトリ サーバのホスト名が有効な DNS 名であることを確認します。次の要件が満たされていることを確認します。
   - 正引き参照および逆引き参照の両方でホスト名が解決可能であること。
   - ディレクトリ サーバが Authentication Manager サーバから到達可能であること。
5. Operations Console を使用してアイデンティティ ソースを追加します。次の項目を正しく構成します。
   - アイデンティティ ソース名
   - LDAP 接続（ディレクトリ URL、フェイルオーバー ディレクトリ URL、ディレクトリ ユーザー ID、ディレクトリ パスワード）
   - 属性マッピング
   - （オプション）グローバル カタログ（Active Directory のみ）
6. （オプション）組織固有のカスタム ユーザー属性を定義することができます。手順については、Security Console ヘルプのトピック「Add Identity Attribute Definitions（アイデンティティ属性定義の追加）」を参照してください。
   （オプション）事前に定義したカスタム属性を LDAP ディレクトリからアイデンティティ ソースにマッピングします。カスタム属性を外部アイデンティティ ソースにマッピングすると、Authentication Manager はディレクトリから属性値を読み取るようになります。
   操作手順については、136 ページのカスタム属性マッピングを参照してください。
7. Security Console を使用してアイデンティティ ソースをシステムにリンクします。130 ページのアイデンティティ ソースとシステムのリンクを参照してください。
8. アイデンティティ ソースが正しく追加されていることを確認します。131 ページの 131 ページの LDAP ディレクトリ アイデンティティ ソースの検証を参照してください。

注：アイデンティティ ソースを無効化または削除するためには、システムとのリンク解除を実行しなければなりません。手順については、Security Console ヘルプのトピック「Unlink Identity Sources from the System（アイデンティティ ソースのシステムからのリンク解除）」を参照してください。アイデンティティ ソースの削除手順については、Operations Console ヘルプのトピック「Remove an Identity Source（アイデンティティ ソースの削除）」のトピックを参照してください。

アイデンティティ ソースの追加

既存の LDAP ディレクトリを RSA Authentication Manager で使用するには、Operations Console でディレクトリを新しいアイデンティティ ソースとして追加します。

1 つの導入環境で、最大 30 個のアイデンティティ ソースを使用できます。Active Directory を使用している場合、アイデンティティ ソースとして構成されたグローバル カタログは、この制限の対象としてカウントされません。

開始する前に

- スーパー管理者である必要があります。
- すべての機能を使用するためには、Authentication Manager とアイデンティティ ソースの間に SSL 接続を確立します。

注：ネットワークやファイアウォールの構成によっては、プライマリ インスタンス からの接続情報を検証できない場合があります。

手順

1. プライマリ インスタンスで Operations Console にログオンします。
2. ［**Deployment Configuration（導入環境の構成）**］＞［**Identity Sources（アイデンティティ ソース）**］＞［**Add New（新規追加）**］の順にクリックします。
3. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力します。
4. ［**Identity Source Basics（アイデンティティ ソースの基本設定）**］セクションで、次の項目を指定します。
   - ［**Identity Source Name（アイデンティティ ソース名）**］：Security Console に表示されるアイデンティティ ソースの名前です。
   - ［**Type（タイプ）**］：追加するアイデンティティ ソースのタイプを選択します。
   - ［**Notes（メモ）**］：アイデンティティ ソースに関する情報です。
5. ［**Directory Connection - Primary（ディレクトリ接続 - プライマリ）**］セクションで、次の操作を実行します。
   - 次のフィールドに必要な情報を入力します。詳細については、116 ページのアイデンティティ ソースのプロパティを参照してください。
     - ［**Directory URL（ディレクトリ URL）**］
     - ［**Directory Failover URL（ディレクトリ フェイルオーバー URL）**］
     - ［**Directory User ID（ディレクトリ ユーザー ID）**］
     - ［**Directory Password（ディレクトリ パスワード）**］

- ［**Test Connection（接続のテスト）**］をクリックし、プライマリ インスタンスが指定されたディレクトリに接続できるかどうかを確認します。このテストが失敗した場合は、このアイデンティティ ソースの証明書を正常にインポートしているかどうかを確認します。

6. レプリカ インスタンスがある場合は、［**Directory Connection - Replica（ディレクトリ接続 - レプリカ）**］セクションの各フィールドに入力し、［**Validate Connection Information（接続情報の検証）**］をクリックして、プライマリ インスタンスがアイデンティティ ソースに接続できるかどうかを確認します。このテストが失敗した場合は、次の操作を実行します。
   a. 正しい設定を入力したかどうかを確認します。
   b. 設定が正しい場合は、プライマリ インスタンスがアイデンティティ ソースに到達可能かどうかを確認します。
   c. プライマリ インスタンスがアイデンティティ ソースに到達可能な場合は、その他に接続エラーを引き起こしているネットワーク上の問題がないかどうか確認します。
   d. 必要な変更を行った後、［**Validate Connection Information（接続情報の検証）**］をもう一度クリックします。
7. ［**Next（次へ）**］をクリックします。
8. ［Add Identity Source - Map（アイデンティティ ソースの追加 - マップ）］ページの次のセクションに必要な情報を入力します。詳細については、116 ページのアイデンティティ ソースのプロパティを参照してください。
   - ［**Directory Settings（ディレクトリ設定）**］
   - （オプション）［**Active Directory Options（Active Directory オプション）**］
   - ［**Directory Configuration - User Tracking Attributes（ディレクトリ構成 - ユーザー トラッキング属性）**］
   - ［**Directory Configuration - Users（ディレクトリ構成 - ユーザー）**］
   - ［**Directory Configuration - User Groups（ディレクトリ構成 - ユーザー グループ）**］
9. ［**Save（保存）**］をクリックします。

アイデンティティ ソースとシステムのリンク

すべての LDAP ディレクトリ アイデンティティ ソースをシステムにリンクする必要があります。リンク後、アイデンティティ ソースのすべてのユーザーを、Security Console で表示および管理することができます。ユーザーはデフォルトで最上位のセキュリティ ドメインに表示されますが、必要に応じて他のセキュリティ ドメインに移動することもできます。さらに、システムを構成して、アイデンティティ ソースのユーザーを特定のセキュリティ ドメインに自動的に配置することができます。詳細については、46 ページのデフォルトセキュリティ ドメイン マッピングを参照してください。

開始する前に

- スーパー管理者である必要があります。
- Active Directory グローバル カタログをリンクする場合は、ユーザー データをグローバル カタログにレプリケーションする各アイデンティティ ソースもリンクする必要があります。たとえば、アイデンティティ ソース IS1 と IS2 が情報をグローバル カタログ GC1 にレプリケーションし、GC1 をアイデンティティ ソースとしてリンクする場合は、IS1 と IS2 もシステムにリンクする必要があります。

手順

1. スーパー管理者として Security Console にログオンします。
2. ［**Setup（セットアップ）**］＞［**Identity Sources（アイデンティティ ソース）**］＞［**Link Identity Source to System（アイデンティティ ソースをシステムにリンク）**］をクリックします。
3. 使用可能なアイデンティティ ソースの一覧から、リンクするアイデンティティ ソースを選択し、右矢印をクリックします。
4. ［**Save（保存）**］をクリックします。

LDAP ディレクトリ アイデンティティ ソースの検証

アイデンティティ ソースを正しく追加およびリンクできているかどうかを検証するために、Security Console を使用してアイデンティティ ソースのユーザーおよびグループを表示します。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドで適切なアイデンティティ ソースを選択し、［**Search**（検索）］をクリックします。
3. LDAP ディレクトリ アイデンティティ ソース内のユーザーが一覧表示されます。

フェイルオーバー サーバ

Operations Console を使用してアイデンティティ ソースを追加するときに、フェイルオーバー ディレクトリ サーバを指定できます。プライマリ ディレクトリ サーバが応答を停止すると、導入環境は自動的にフェイルオーバー サーバに接続します。

フェイルオーバー ディレクトリ サーバを構成する場合は、次のガイドラインに従ってください。

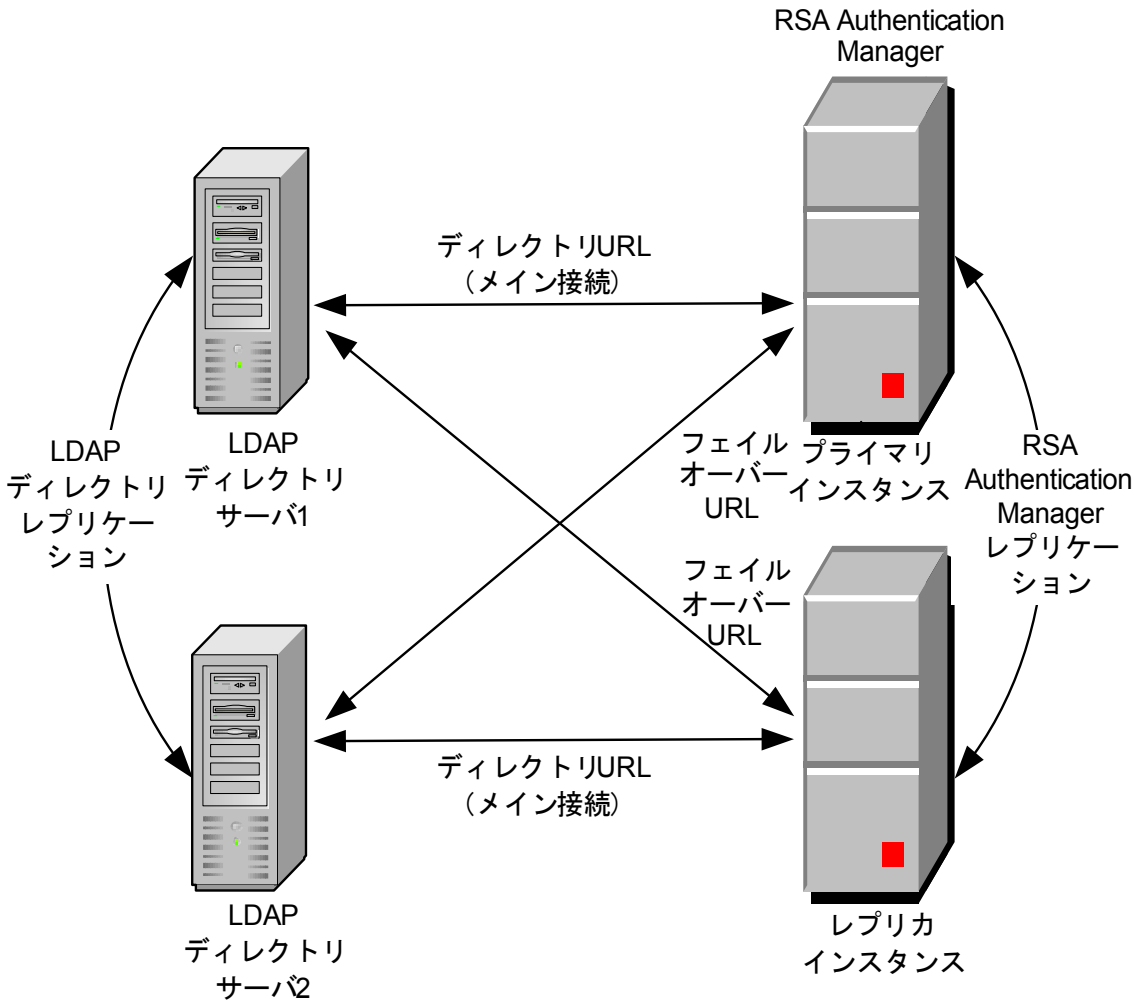
- アイデンティティ ソースを追加する時に、[Directory Failover URL（ディレクトリ フェイルオーバー URL）] フィールドにフェイルオーバー URL を入力します。操作手順については、129 ページのアイデンティティ ソースの追加を参照してください。
- フェイルオーバー ディレクトリ サーバは、プライマリ ディレクトリ サーバのレプリカである必要があります。
- プライマリ インスタンスとレプリカ インスタンスは、同じ物理ディレクトリサーバを使用すべきではありません。フェイルオーバー先を指定することなく、両方のインスタンスが同じディレクトリ サーバを使用している場合、ディレクトリサーバが使用不可となった場合には、ユーザーを認証することができません。
- 各フェイルオーバー URL は、異なる物理ディレクトリ サーバをポイントする必要があります。

Active Directory サーバのフェイルオーバー

アイデンティティ ソースが Active Directory の場合、フェイルオーバー サーバとしてグローバル カタログを指定しないでください。

フェイルオーバー ディレクトリ サーバのある導入環境の例

次の構成例では、2 つのディレクトリ サーバのいずれかが使用不可になった場合でも認証処理を継続できるよう、単一障害点を排除しています。この場合、各ディレクトリ サーバは同じドメインにあり、レプリケーションによって同じ LDAP データのコピーを保持しています。



通信パスの保護

RSA では、SSL（Secure Sockets Layer）を使用して Authentication Manager とディレクトリの間で転送中のデータを暗号化することを推奨します。

Authentication Manager で使用する予定のディレクトリ サーバごとに、SSL を構成する必要があります。詳細については、134 ページのアイデンティティ ソース SSL 証明書を参照してください。

Active Directory の場合、この他にもパスワード ポリシーとグループ メンバーシップのサポートのために、重要な注意点があります。詳細については、136 ページの Active Directory のパスワード ポリシーおよび 124 ページの Active Directory 内のグループ間メンバーシップのサポートを参照してください。

アイデンティティ ソース SSL 証明書

LDAP ディレクトリ サーバをアイデンティティ ソースとして統合する場合は、アイデンティティ ソースの SSL（Secure Sockets Layer）証明書を使用することにより、導入環境と外部アイデンティティ ソースの間の通信のセキュリティを保護します。Operations Console を使用して SSL 接続をセットアップします。SSL 接続をセットアップすることにより、ユーザーが Authentication Manager から自分のパスワードを変更できるようになります。

SSL 接続を確立する時、アイデンティティ ソースは、サーバを特定（たとえば、ホスト名を使用）する証明書を提示します。サーバ証明書を受け入れるには、その証明書自体またはその証明書のルート証明書を導入環境で信頼する必要があります。SSL 証明書を信頼するには、証明書を導入環境に追加する必要があります。

アイデンティティ ソース SSL 証明書の追加

SSL（Secure Sockets Layer）証明書を使用することにより、環境とアイデンティティ ソースの間の通信のセキュリティを保護できます。アイデンティティ ソース SSL 証明書を信頼する証明書として導入環境に追加する必要があります。

次の処理手順を実行して、アイデンティティ ソース SSL 証明書を信頼する証明書として追加します。

開始する前に

スーパー管理者である必要があります。

手順

1. SSL サーバ証明書または CA ルート証明書をプライマリ アプライアンスにインポートします。証明書は、DER（Distinguished Encoding Rules）エンコード形式である必要があります。これらの証明書にアクセスできることを確認してください。
2. プライマリ インスタンスで Operations Console にログオンします。
3. ［**Deployment Configuration（導入環境の構成）**］＞［**Identity Sources（アイデンティティ ソース）**］＞［**Identity Source Certificates（アイデンティティ ソース証明書）**］＞［**Add New（新規追加）**］の順にクリックします。
4. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。
5. 新しいアイデンティティ ソース証明書の名前を入力します。
6. SSL 証明書ファイルを選択します。証明書のファイル拡張子は、通常は .cer、.pem、.der のいずれかです。
7. ［**Save（保存）**］をクリックします。

LDAP ディレクトリ上のユーザーパスワードへの アクセス

LDAP ディレクトリに格納されているユーザーについては、Authentication Manager 管理者およびユーザー自身がユーザー パスワードを変更できるよう、システムを構成することができます。

アイデンティティ ソースの管理者アカウントが、LDAP ディレクトリ上のユーザー レコードの書き込み権限を持つ場合、管理者は LDAP ディレクトリに格納されているユーザー アカウントのパスワードを変更できます。この管理者アカウントは、Operations Console のアイデンティティ ソースの接続設定ページの［Directory User ID（ディレクトリ ユーザー ID）］および［Directory Password （ディレクトリ パスワード）］フィールドで指定するアカウントです。

次の条件が満たされている場合、認証時にプロンプトが表示されたときには、ユーザーはパスワードを変更できます。

- アイデンティティ ソース管理者アカウントが、LDAP ディレクトリ上のユーザー レコードの書き込み権限を持つこと。
- ディレクトリがユーザーによるパスワード変更を許可するよう構成されていること。

  注：ユーザーによる認証時のパスワード変更を許可しない場合は、アイデンティティ ソース管理者アカウントには、LDAP ディレクトリに対する書き込み権限は不要です。

- LDAPS 接続を Authentication Manager と LDAP ディレクトリの間で構成します。SSL 接続の設定手順については、134 ページのアイデンティティ ソース SSL 証明書を参照してください。
- 以下の条件のいずれか 1 つが適合する。
  - ユーザーのパスワードが期限切れになっている。
  - パスワードの変更を強制するために Authentication Manager 管理者がユーザー レコードを編集し、［**Require the user to change password at next logon（次回ログオン時にユーザーにパスワードの変更を要求する）**］チェックボックスをオンにしている。
  - ユーザーが次回認証時にパスワードをリセットするよう LDAP ディレクトリが構成されている。

これらの条件が満たされない場合には、ユーザーのパスワード変更の試行は失敗します。

Active Directory のパスワード ポリシー

Active Directory には、Authentication Manager のデフォルトパスワード ポリシーより厳しいデフォルトパスワード ポリシーがあります。これによって、ユーザーの追加や更新時に「Will Not Perform」などのようなエラーが引き起こされる可能性があります。

Active Directory アイデンティティ ソースのパスワード ポリシーを管理するには、次のいずれかの操作を行います。

- Authentication Manager パスワード ポリシーのパスワード要件をより厳しくします。第 4 章、認証ポリシーの構成を参照してください。
- Windows 2003、2008、2008 R2 のグループ ポリシー オブジェクト エディタで複雑な要件を緩和します。詳細については、Active Directory のドキュメントを参照してください。

注：Authentication Manager のデフォルト パスワード ポリシーは、すでに Oracle Directory Server のデフォルト パスワード ポリシーより厳しいものになっています。

カスタム属性マッピング

カスタム属性を使用する場合は、アイデンティティ ソースの追加後に、LDAP ディレクトリスキーマの物理属性名にアイデンティティ属性定義を明示的にマッピングする必要があります。

すべてのユーザー フィールドをヌル値以外のフィールドにマッピングする必要があります。ユーザー ID は、任意の一意な属性にマッピングすることができます。

詳細なマッピング手順については、Security Console の次のヘルプ トピックを参照してください。

Security Console ヘルプ トピック	説明
「ユーザー属性」	内部のデフォルト ユーザー属性の概要。
「アイデンティティ属性カテゴリーの追加」	関連するアイデンティティ属性をカテゴリーにグループ化する手順。アイデンティティ属性定義の追加時には、各属性をカテゴリーに割り当てます。 たとえば、番地、市区町村、都道府県、国などのフィールドをグループ化するために［Address（住所）］という属性カテゴリーを使用することができます。 デフォルト カテゴリーは［Attributes（属性）］です。
「アイデンティティ属性定義の追加」	カスタム ユーザー属性のマッピング手順。

アイデンティティ ソース ユーザー属性

Security Console に LDAP データを表示するには、Authentication Manager フィールドを対応する LDAP ディレクトリのフィールドにマッピングする必要があります。これらのフィールドを属性と呼びます。ユーザー属性には、次の 2 つのタイプがあります。

- コア属性
- カスタム属性

コア属性

コア属性には、ユーザー ID、名前、苗字など、基本的なユーザー属性が含まれます。Operations Console を使用してアイデンティティ ソースを作成する際、これらの属性をマッピングします。

ディレクトリのフィールドを Authentication Manager のフィールドにマッピングすると、Security Console 上に、ディレクトリに格納されているユーザーとユーザー グループのデータを表示できます。たとえば、アイデンティティ ソースを作成するときに、Authentication Manager のユーザー ID フィールドを LDAP ディレクトリ内の適切なフィールドにマッピングします。コア属性のマッピングは、Operations Console でアイデンティティ ソースを作成するときに行います。

すべてのユーザー フィールドを空でないフィールドにマッピングする必要があります。たとえば、Active Directory では、ユーザー ID はデフォルトで sAMAccountName にマッピングされますが、他の一意の空でない属性にマッピングすることもできます。

複数のアイデンティティ ソースを使用する場合は、属性のマッピングに一貫性を持たせるようにしてください。たとえば、1 つのアイデンティティ ソースでユーザー ID を sAMAccountName にマッピングするのであれば、他のアイデンティティ ソースでも同様にマッピングします。

カスタム属性

コア属性のほかに、組織固有の情報を格納するためのカスタム属性（アイデンティティ属性定義）を定義できます。カスタム属性を LDAP ディレクトリのフィールドにマッピングすると、ディレクトリからこれらの属性値を取得して Authentication Manager に表示することが可能になります。ヘルプ デスク担当者にサポート情報を提供するために、カスタム属性を使用することができます。

カスタム属性を定義する時、その値をディレクトリと内部データベースのどちらに格納するかを指定できます。ディレクトリに格納する場合、ディレクトリの既存のフィールドを指定する必要があります。

Security Console を使用してカスタム属性を作成およびマッピングします。

一意識別子の属性

アイデンティティ ソースを作成し、コア属性をマッピングするときに、一意識別子フィールドをマッピングする必要があります。このフィールドは、Authentication Manager が内部データベース レコードを対応する LDAP ディレクトリのレコードにマッピングするために使用されます。Authentication Manager はこのフィールドを、DN（識別名）が変更されたユーザーを検索するために使用します。デフォルトの一意識別子は、次のいずれかです。

- Active Directory の場合は、デフォルトで ObjectGUID 属性が使用されます。
- Oracle Directory Server（および Sun Java Directory Server）の場合は、デフォルトで nsUniqueID 属性が使用されます。

Operations Console の［Add New Identity Source（新しいアイデンティティ ソースの追加）］ページで、一意識別子フィールドをマッピングします。詳細については、129 ページのアイデンティティ ソースの追加を参照してください。

一意識別子属性は、次の要件を満たしている必要があります。

- 属性には、ユーザーごとに一意なデータが格納されていることが必要です。たとえば、導入環境内のユーザーごとに一意の従業員 ID 番号や社員証番号など。
- すべてのユーザーの属性に、データが格納されている必要があります。値が空であってはいけません。
- 値が変更不可である必要があります。値が変更されると、変更されたユーザーを Authentication Manager でトラッキングできなくなります。一意識別子としてマッピングする属性に、他のフィールドをマッピングすることはできません。
- 属性名は 64 文字を超えてはいけません。
- 属性値は 42 文字を超えてはいけません。

一意識別子をマッピングするときは次のガイドラインに従ってください。

- Security Console を使用して表示または管理するユーザーをディレクトリ上で移動または名前変更する前に、一意識別子を指定する必要があります。この条件を満たしていない場合、Authentication Manager は、移動または名前変更されたユーザーのレコードを重複して作成し、それまでシステムに保存していたデータとユーザーとの関連は無くなります。
- 一意識別子フィールドをマッピングした後は、変更できません。

ユーザー アカウントの有効状態の属性

各アイデンティティ ソースには、[User Account Enabled State（ユーザー アカウントの有効状態）] という属性があり、Authentication Manager はこの属性を参照してユーザー アカウントが有効化されているか、無効化されているかを判別します。Authentication Manager は外部 LDAP ディレクトリの属性値を常にチェックしますが、内部データベースの設定もチェックするように構成することができます。

[Enabled（有効化）] 属性は、Authentication Manager にユーザー アカウントの状態が有効または無効かをレポートし、Security Console から制御できます。他のユーザー属性の多くとは異なり、[Enabled（有効化）] 属性のマッピングは変更できません。

Operations Console を使用して LDAP アイデンティティ ソースを作成する時、ユーザーが有効化されているかどうかを Authentication Manager がどのように判別するかを制御できます。[User Account Enabled State（ユーザー アカウントの有効状態）] は、次の 2 つのいずれかに設定します。

- [**Directory**（ディレクトリ）] に設定すると、Authentication Manager は LDAP ディレクトリ内でのユーザーの有効状態だけを参照します。

  [Directory（ディレクトリ）] の設定は、ユーザーを Authentication Manager 内で有効化するか否かを LDAP だけに基づいて制御する場合に選択します。Authentication Manager 内でユーザー アカウントを無効化するには、ディレクトリ側でユーザー アカウントを無効化する必要があります。

- [**Directory and Internal Database**（ディレクトリと内部データベース）] に設定すると、Authentication Manager は LDAP ディレクトリと Authentication Manager の内部データベースの両方を参照して、ユーザーの有効状態を判別します。

  内部データベースの設定は、Authentication Manager 内でのみユーザーを無効化し、LDAP 内ではユーザーを有効化したままにしたい場合に使用します。この場合、ユーザーはリモート アクセスのために Authentication Manager の認証を受けることはできませんが、ユーザーの LDAP アカウントの状態には変更がありません。たとえば、Windows ドメイン アカウントは有効化されたままになるため、ユーザーは引き続き Windows にログオンできます。

どちらの設定でも、ユーザーが Authentication Manager の認証を受けるにはユーザーの LDAP アカウントを有効化しておく必要があります。

6 ユーザーの管理

一般的なユーザー管理タスク

Security Console を使用して、ユーザー向けの認証サービスを提供および保守します。Security Console を使用すると、次の一般的なタスクを実行できます。

- ユーザー データの管理
- 特定のリソースへのアクセスの制限
- ユーザー アクセス権限の指定
- ユーザーのアクセスの問題の解決
- ユーザーのセキュリティ問題への対応
- ユーザー データの保守

実行できる管理タスクは、管理者ロールの権限適用範囲により定義されます。

内部データベースへのユーザーの追加

LDAP ディレクトリがプライマリ アイデンティティ ソースである場合でも、Security Console を使用して、ユーザーを内部データベースに追加できます。ユーザーを内部データベースに直接追加することにより、アイデンティティ ソースのユーザーグループとは異なるユーザーグループを作成できます。たとえば、一時的な契約業者のグループや特定の管理者グループを内部データベースに保管するといったケースです。また、内部データベースを使用して、パイロット プロジェクト用に少数のユーザーを格納することもできます。

LDAP ディレクトリ内のユーザー データは読み取り専用です。ユーザーを LDAP ディレクトリに追加するには、ディレクトリ ツールを使用する必要があります。ただし、ユーザーへのトークンの割り当てやリスク ベース認証の有効化など、特定の管理機能は Security Console から実行できます。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Add New（新規追加）**] の順にクリックします。
2. [Administrative Control（管理制御）] セクションで、[**Security Domain（セキュリティ ドメイン）**] ドロップダウン リストから、ユーザーを管理するセキュリティ ドメインを選択します。ユーザーは、ここで選択したセキュリティ ドメインを権限適用範囲に含んでいる管理者によって管理されます。
3. [User Basics（ユーザーの基本設定）] セクションで、次の操作を実行します。
   a. （オプション）[**First Name（名前）**] フィールドにユーザーの名前を入力します。最大文字数は 255 文字です。
   b. （オプション）[**Middle Name（ミドル ネーム）**] フィールドにユーザーのミドル ネームを入力します。最大文字数は 255 文字です。
   c. [**Last Name（苗字）**] フィールドにユーザーの苗字を入力します。最大文字数は 255 文字です。
   d. [**User ID（ユーザー ID）**] フィールドにユーザーのユーザー ID を入力します。ユーザー ID は 48 文字以内でなければなりません。ユーザー ID がユーザーの保存先のアイデンティティ ソース内で一意であることを確認します。次の例に示すようなマルチバイト文字は使用しないでください。

   注： Security Console へのアクセスが必要な管理者のアカウントを作成する場合、ユーザー ID は導入環境内で一意でなければなりません。

   e. （オプション）[**Email（メール）**] フィールドにユーザーのメール アドレスを入力します。最大文字数は 255 文字です。
   f. （オプション）[**Certificate DN（証明書 DN）**] フィールドにユーザーの証明書 DN を入力します。証明書 DN は、認証のためにユーザーに発行される証明書のサブジェクトと一致していなければなりません。最大文字数は 255 文字です。
4. [Password（パスワード）] セクションで、次の操作を実行します。

注： このパスワードは、認証エージェントを介した認証には使用されません。

a. ［**Password（パスワード）**］フィールドにユーザーのパスワードを入力します。パスワードに対する要件は、ユーザーを管理するセキュリティ ドメインに割り当てられているパスワード ポリシーに基づいて決定されます。これはユーザーのアイデンティティ ソースのパスワードであり、アプリケーションから提供される代替パスワードとは異なります。詳細については、RSA Security Console ヘルプのトピック「パスワード ポリシーの表示」を参照してください。

b. ［Password（パスワード）］フィールドに入力したパスワードを［**Confirm Password**（パスワードの確認）］フィールドに再度入力します。

c. （オプション）ユーザーが次回にログオンしたときに、パスワードの変更を強制するには、［**Force Password Change**（パスワードの変更を強制）］を選択します。たとえば、すべての新規ユーザーに標準のパスワードを割り当てておき、システムの使用を開始する時点でユーザーにパスワードの変更を要求するには、このチェックボックスをオンにします。

5. ［Account Information（アカウント情報）］セクションで、次の操作を実行します。

a. ［**Account Starts（アカウントの開始）**］ドロップダウン リストから、ユーザーのアカウントをアクティブにする日時を選択します。タイムゾーンは、ローカル システム時間に基づいて決定されます。

b. ［**Account Expires（アカウントの有効期限）**］ドロップダウン リストからユーザー アカウントの有効期限を選択するか、または有効期限なしに構成します。タイム ゾーンは、ローカル システム時間に基づいて決定されます。

c. （オプション）新しいアカウントを無効化する場合は、［**Account is disabled（アカウントの無効化）**］を選択します。

d. ［Locked Status（ロック ステータス）］オプションが選択されている場合は、すべての選択されたオプションをオフにすることにより、ユーザーのロックを解除できます。

6. （オプション）［**Attributes（属性）**］で、ユーザーの携帯電話番号を［**Mobile Number (String)（携帯電話番号（文字列））**］フィールドに入力します。

7. ［**Save（保存）**］をクリックします。

ユーザー ステータス

セキュリティを強化するには、長期的に不在のユーザーを無効化し、ユーザーが職場に復帰したときに有効化するようにします。

ユーザーを有効化 / 無効化する前に、次のことに留意してください。

- ユーザーを無効化しても、ユーザーがアイデンティティ ソースから削除されるわけではありません。
- ユーザー アカウントを無効化しても、そのユーザーが持っているトークンは引き続き割り当てられた状態となります。ユーザー アカウントを無効化しても、ユーザーに割り当てられているトークンは割り当て解除されません。
- Authentication Manager は、ユーザー認証のたびに、ユーザーが有効か無効かを確認します。ユーザーが、リンクされたアイデンティティ ソースで無効化されている場合、そのユーザーは認証できません。

ユーザー アカウントの無効化

ユーザー アカウントを無効化すると、ユーザーの認証権限が一時停止され、保護されたリソースへのアクセスが禁止されます。ユーザーを無効化しても、ユーザーがアイデンティティ ソースから削除されるわけではありません。ユーザーを削除するには、RSA Security Console ヘルプのトピック「ユーザーの削除」を参照してください。

RSA Authentication Manager にリンクされている LDAP ディレクトリのユーザーを無効化する場合は、LDAP ディレクトリのネイティブ インタフェースを使用する必要があります。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、無効化するユーザーを検索します。一部のフィールドでは大文字と小文字が区別されます。
3. 無効化するユーザーをクリックして、［**Edit（編集）**］を選択します。
4. ［**Account Information（アカウント情報）**］セクションで、［**Account is disabled（アカウントの無効化）**］を選択します。
5. ［**Save（保存）**］をクリックします。

ユーザー アカウントの有効化

ユーザー アカウントを有効化すると、ユーザーは認証が可能になり、保護されたリソースにアクセスできるようになります。

ディレクトリ サーバのユーザーを認証するには、ディレクトリ サーバと Security Console の両方でユーザーを有効化する必要があります。ディレクトリ サーバで有効化されているユーザーだけが認証できます。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、有効化するユーザーを検索します。一部のフィールドでは大文字と小文字が区別されます。
3. 有効化するユーザーをクリックして、［**Edit（編集）**］を選択します。
4. ［**Account Information（アカウント情報）**］で、［**Account is disabled（アカウントの無効化）**］をオフにします。
5. ［**Save（保存）**］をクリックします。

セキュリティ ドメインによるユーザーの編成

セキュリティ ドメイン階層を作成し、アイデンティティ ソースをシステムにリンクすると、すべてのユーザーが最上位のセキュリティ ドメインに追加されます。ユーザーの編成、導入環境の管理、管理者の権限適用範囲の制限を容易にするために、ユーザーを階層内の別のセキュリティ ドメインに移動することができます。

通常セキュリティ ドメインは組織構造や地理的な場所に合わせて作成し、Security Console を使用して、各部門やサイトのユーザーを対応するセキュリティ ドメインに移動します。

たとえば、最上位のセキュリティ ドメインとして SystemDomain が、下位のセキュリティ ドメインとしてボストン、ニューヨーク、サンノゼが構成されている場合は、ユーザーを SystemDomain からそれぞれの勤務地のセキュリティ ドメインに移動した方が便利です。

セキュリティ ドメインの詳細については、41 ページのセキュリティ ドメインの概要を参照してください。

セキュリティ ドメイン間でのユーザーの移動

内部データベースにアカウントが格納されているユーザーは、手動で別のセキュリティ ドメインに移動できます。また、ユーザー グループも移動できます。

ユーザーを別のセキュリティ ドメインに移動すると、新しいセキュリティ ドメインのポリシーが即時適用されます。また、ユーザーを移動した後は、そのセキュリティ ドメインでユーザーを管理する権限を持つ管理者のみが移動後のユーザーを管理できます。

ユーザーを移動する際は、移動前に RBA（リスク ベース認証）が有効化されているユーザーの RBA ユーザー設定が移動後も保持されることを考慮してください。移動前に RBA が無効化されている場合は、移動後も RBA が無効化されたままになります。

LDAP ディレクトリ ユーザーは、組織単位 (ou) などのディレクトリ オブジェクトを別のセキュリティ ドメインにマッピングすることで、自動的に別のセキュリティ ドメインに移動できます。Authentication Manager は、新しいユーザー レコードがデータベースに追加されると、セキュリティ ドメイン マッピングを使用して適切なセキュリティ ドメインにユーザーを追加します。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、移動するユーザーを検索します。一部のフィールドでは大文字と小文字が区別されます。
3. 移動するユーザーを選択します。
4. ［**Action（アクション）**］メニューから、［**Move to Security Domain（セキュリティ ドメインの移動）**］をクリックし、［**Go（実行）**］をクリックします。
5. ［**Move to Security Domain（移動先のセキュリティ ドメイン）**］ドロップダウン リストから、ユーザーの移動先となるセキュリティ ドメインを選択します。
6. ［**Move（移動）**］をクリックします。

ユーザー ID の重複

同じユーザー名を持つ 2 人のユーザーが、同じ保護されたリソースにアクセスしようとすると、認証に失敗します。この状況は、複数のアイデンティティ ソースを同じ導入環境にリンクし、それぞれのアイデンティティ ソースに同じユーザー ID を持つユーザーが存在する場合に発生します。このようなケースでは、次のオプションがあります。

- ユーザー ID を、値の重複がない別のフィールドにマッピングする。たとえば、アイデンティティ ソースが Active Directory の場合であれば、UPN フィールドまたはユーザーのメール アドレスへのマッピングが可能です。

- いずれか一方のアイデンティティ ソースのユーザー ID を変更し、すべてのユーザー ID が一意になるようにする。ただし、ユーザー ID が別のアプリケーションでも使われている場合は、このオプションを使用できないことがあります。
- 重複するユーザー ID を持つユーザーの 1 人にのみトークンを割り当てる。重複するユーザー ID を持つ複数のユーザーにトークンを割り当てる必要がある場合、このオプションは役に立ちません。

ユーザー認証

Security Console を使用してユーザー認証を管理します。次の操作を実行できます。

- ユーザー認証設定の変更
- ユーザーのアクセスの問題の解決

実行できるユーザー認証タスクは、管理者ロールの権限適用範囲により定義されます。

ユーザー認証設定の管理

ユーザー認証設定では、個々のユーザーの認証ポリシーの例外を作成できます。また、これらの設定により、ユーザー認証の問題をトラブルシューティングすることもできます。

開始する前に

制限付きエージェントがあり、ユーザーがそのエージェントへのアクセス権が付与されているユーザー グループに属している。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、管理するユーザーを検索します。
3. 検索結果から、管理するユーザーをクリックします。
4. コンテキスト メニューで [**Authentication Settings（認証設定）**] をクリックします。
5. ユーザーに固定パスコードを割り当てる場合は、[**Fixed Passcode（固定パスコード）**] チェックボックスをオンにます。

   RSA では、固定パスコードでは 2 要素認証のメリットがすべて失われるため、固定パスコードを使用しないことを推奨します。

6. 不正なパスコードをクリアするには、[**Clear Incorrect Passcodes（不正なパスコードをクリアする）**] チェックボックスをオンにします。不正なパスコードのカウントがリセットされ、ユーザーにはネクスト トークンコードの入力を求めるプロンプトが表示されなくなります。ただし、ユーザーが不正なパスコードを入力し続け、ロックアウト ポリシーで許可されているログオン試行失敗回数を超えた場合、ユーザーはシステムからロックアウトされます。
7. ユーザーの Windows ユーザー ID とパスワードのハッシュ情報をクリアするには、[**Clear cached copy of selected user's Windows credential（Windows クレデンシャルのキャッシュされたコピーをクリアする）**] を選択します。
   お使いの導入環境で RSA SecurID for Windows を使用している場合、Authentication Manager はユーザーの Windows ユーザー ID とパスワードのハッシュ情報を保存します。Active Directory で Windows パスワードが変更された場合に、この情報をクリアする必要が生じる場合があります。
8. ユーザーにデフォルト シェルを割り当てる場合は、[**Default Shell（デフォルト シェル）**] フィールドにデフォルト シェルを入力します。
9. ユーザーのログオン エイリアスを構成するには、次の手順を実行します。
   a. ユーザーが自分のユーザー ID およびエイリアスを使用できるようにするかどうかを選択します。
   b. エイリアスの割り当て先となるユーザー グループを選択します。
   c. [**User ID（ユーザー ID）**] フィールドに、エイリアスのユーザー ID を入力します。[**Shell（シェル）**] フィールドに、エイリアスに割り当てるシェルを入力します。RADIUS を使用している場合は、[**RADIUS Profile（RADIUS プロファイル）**] ドロップダウン メニューから、エイリアスに割り当てる RADIUS プロファイルを選択します。[**Add（追加）**] をクリックします。
10. RADIUS を使用している場合は、ユーザーに割り当てる RADIUS プロファイルおよび RADIUS ユーザー属性を選択します。
    a. [**User RADIUS Profile（ユーザーの RADIUS プロファイル）**] ドロップダウン メニューから、ユーザーに割り当てる RADIUS プロファイルを選択します。
       ステップ 9 でユーザーのログオン エイリアスを設定したが、各エイリアスに RADIUS プロファイルを指定しなかった場合は、各エイリアスにユーザーの RADIUS プロファイルが割り当てられます。
    b. [**RADIUS User Attributes（RADIUS ユーザー属性）**] でユーザーに割り当てる属性を選択し、[**Value（値）**] フィールドに属性の値を入力して、[**Add（追加）**] をクリックします。RADIUS ユーザー属性は、RADIUS プロファイルの属性より優先して適用されます。
       RADIUS ユーザー属性はアイデンティティ ソース属性にマッピングできます。詳細については、367 ページのアイデンティティ ソース属性への RADIUS ユーザー属性定義のマッピングを参照してください。
11. [**Save（保存）**] をクリックします。

ログオン エイリアス

ログオン エイリアスを使用すると、ユーザーはユーザー グループ ID を使用してログオンできます。ユーザー グループ ID は、制限付きエージェントへのアクセス権を持つユーザー グループに関連づけられます。

たとえば、ユーザーは、“kmiller” のように、名前の頭文字と苗字を組み合わせたユーザー ID や、“root” などの特定の名前を持つ管理者ユーザー ID を持つことができます。ログオン エイリアスが設定されている場合、ユーザーがオペレーティング システムにログオンするために入力したユーザー ID に関係なく、Authentication Manager は、認証のためユーザーのパスコードを検証します。下位互換性を確保するために、シェル値もシステムによって保持されます。

ログオン エイリアスは、Security Console の［Authentication Settings（認証設定）］ページから割り当てることができます。このページにアクセスするには、ユーザーのコンテキスト メニューを使用します。

操作手順については、147 ページのユーザー認証設定の管理を参照してください。

ユーザーのロック解除

RSA Authentication Manager は、ロックアウト ポリシーに違反したユーザーをロックアウトします。ロックアウトされたユーザーは、ロック解除されるまで認証を受けられません。

ロックアウト ポリシーでは、認証の試行失敗回数の上限を指定します。この回数を超えたユーザーのアカウントはシステムからロックアウトされます。また、ロックアウト ポリシーでは、一定期間の経過後にユーザーをロック解除することができます。または、管理者にユーザーを手動でロック解除するように依頼することもできます。

手順

1. Security Console で、**［Identity（アイデンティティ）］＞［Users（ユーザー）］＞［Manage Existing（既存項目の管理）］**の順にクリックします。
2. 検索フィールドを使用して、ロック解除するユーザーを検索します。一部のフィールドでは大文字と小文字が区別されます。
3. ロック解除するユーザーをクリックして、**［Edit（編集）］**を選択します。
4. **［Account Information（アカウント情報）］**セクションで、**［Locked Status（ロック ステータス）］**に移動し、選択されているオプションをすべてクリアします。
5. **［Save（保存）］**をクリックします。

不正なパスコード カウント

トークンを割り当てられたユーザーが不正なパスコードを入力するたびに、システムはその回数をカウントします。このカウントは、ユーザーが正しいパスコードを入力するたびに自動的にクリアされます。不正なパスコードを入力した回数が SecurID トークン ポリシーで許容される回数を超え、その後そのユーザーが正しいパスコードを入力すると、ネクスト トークンコードの入力を求めるプロンプトが表示されます。管理者が Security Console を使用して、ユーザーの不正パスコードの入力回数をクリアすると、ネクスト トークンコードの入力を求めるプロンプトは表示されなくなります。

この操作では、既存のカウントのみをクリアします。将来またカウントのクリアが必要になったときは、同じ手順を繰り返す必要があります。

操作手順については、147 ページのユーザー認証設定の管理を参照してください。

セキュリティ クエスチョンの管理

セキュリティ クエスチョンは、認証のための質問に回答することをユーザーに要求する認証方式です。アカウント登録時や Self-Service Console に初めてアクセスするときに、ユーザーは、質問の回答を登録するよう要求されます。後で認証を受けるときに、ユーザーは、これらの質問のサブセットに対してアカウント登録時と同じ回答を示す必要があります。

セキュリティ クエスチョンは、次のような場合に使用されます。

- プライマリ認証方式が失敗した場合
- RBA（リスク ベース認証）のユーザー確認を行う場合

ユーザーに回答の変更を許可する場合は、既存の回答をクリアする必要があります。たとえば、ユーザーが回答を忘れた場合や、回答が漏洩したと考えられる場合などにこれを行う必要があります。管理者がユーザーの回答をクリアすると、ユーザーは次回のログオン時に新しい回答を登録するよう要求されます。操作手順については、RSA Security Console ヘルプのトピック「ユーザー ダッシュボードでセキュリティ クエスチョンの回答をクリアする」を参照してください。

質問のファイルは英語圏のユーザー向けに用意されていますが、管理者はこれを変更して新しい質問ファイルを作成できます。また、英語以外の言語で質問のファイルを作成することもできます。新しい質問のセットを作成した場合や、質問を 1 つだけ変更した場合は、既存のファイルが新しいファイルに置き換わります。

アカウント登録時または Self-Service Console に初めてアクセスしたときにユーザーが回答を登録する必要のある質問の数を指定します。また、ユーザーが認証時に回答する必要がある質問の数も指定します。登録用に指定する質問の数は、認証用に指定する質問の数よりも多くなければなりません。認証用に指定する質問の数が、アカウント登録用に指定する質問の数よりも少なければ、ユーザーは認証時に回答する質問を選択することができます。

セルフ サービス トラブルシューティングでは、用意される質問の数は認証に必要な質問の数よりも多くなければなりません。

セキュリティ クエスチョンの要件の設定

アカウント登録時または Self-Service Console に初めてアクセスしたときにユーザーが回答を登録する必要のある質問の数、および認証時にユーザーが正しく回答する必要のある質問の数を指定します。アカウント登録用に指定された質問の総数が認証用に指定された質問の数よりも多ければ、ユーザーは認証の際に回答する質問を選択することができます。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。
2. ［**Security Questions Requirements（セキュリティ クエスチョン要件）**］をクリックします。
3. ［**Enrollment（アカウント登録）**］フィールドで、アカウント登録時にユーザーが回答を登録する必要のある質問の数を指定します。この設定を変更しても、現在アカウント登録済みのユーザーには影響しません。
4. ［**Authentication（認証）**］フィールドで、認証時にユーザーが正しく回答する必要のある質問の数を指定します。
5. ［**Save（保存）**］をクリックします。

カスタムのセキュリティ クエスチョン

セキュリティ クエスチョンのテキストと言語は、カスタマイズした XML ファイルの作成と、データベースへのインポートによってカスタマイズできます。新しいセキュリティ クエスチョン ファイルを作成する場合は、次の手順に従います。

- **既存の英語テキストを変更する**。既存の XML ファイルを編集して、既存の質問の文言を変更したり、独自の新しい質問を追加します。
- **言語を変更する**。提供されるテンプレートを参考に、新しい XML ファイルを作成します。言語 ID を指定して、選択した言語でセキュリティ クエスチョンを入力します。

RSA Authentication Manager 8.0 - Virtual Appliance DVD には、テンプレートとして使用できるセキュリティ クエスチョン サンプル ファイル（**SecurityQuestionsSample.xml**）が含まれます。ファイルには、次のようなサンプルが含まれます。

```
<?xml version="1.0" encoding="UTF-8"?>
 <SECURITY_QUESTIONS>
   <LANGUAGE id="en_US">
     <QUESTION>first question</QUESTION>
     <QUESTION>second question</QUESTION>
     <QUESTION>third question</QUESTION>
   </LANGUAGE>
 </SECURITY_QUESTIONS>
```

RSA Authentication Manager 8.0 - Virtual Appliance DVD またはダウンロード キットの **Security Questions Sample** フォルダには、変更または新規作成した セキュリティ クエスチョン ファイルの妥当性検査をするためのセキュリ ティ クエスチョン ファイル スキーマ（**SecurityQuestions.xsd**）も含まれます。

1 つの導入環境でアクティブにできるセキュリティ クエスチョン ファイルは 1 つだけです。既存のセキュリティ クエスチョンを変更して、変更したファ イルをインポートした場合、ユーザーは、セキュリティ クエスチョンの回答 を再度登録する必要があります。

セキュリティ クエスチョンをカスタマイズする際は、次のガイドラインに 従ってください。

- 言語ごとに個別の XML ファイルを作成します。たとえば、3 言語の質問 が必要な場合、3 つのファイルを作成する必要があります。
- 各 XML ファイルには、質問を記述した言語を識別するため、XML 言語 属性を含める必要があります。サポートされている言語 ID コードのリス トは、RSA Security Console ヘルプのトピック「Language Codes for Security Questions（セキュリティ クエスチョンの言語コード）」を参照し てください。
- 質問のテキストは実際の言語で記述する必要があります。Authentication Manager は、言語の翻訳は行いません。
- 1 つのセキュリティ クエスチョンは 255 文字以内である必要があります。
- セキュリティ クエスチョン ファイルには、少なくともアカウント登録用 に指定したセキュリティ クエスチョンの数と同じ数のセキュリティ クエ スチョンが含まれている必要があります。手順については、RSA Security Console ヘルプのトピック「Enrollment Requirements for Security Questions（セキュリティ クエスチョンのアカウント登録時の要件）」を参照してく ださい。
- セキュリティ クエスチョンのファイルは削除できません。

セキュリティ クエスチョン ファイルの変更

セキュリティ クエスチョンは、XML ファイルからデータベースに格納され ます。デフォルトの一連の質問は、英語圏のユーザー向けになっています。 デフォルトの質問は、質問自体を変更することや、質問を追加することで変 更できます。作業が終了したら、変更した XML ファイルをデータベースに インポートします。新しいファイルをインポートすると、新しいファイルの 言語セットでシステム内の対応する言語セットの質問が置き換えられます。 たとえば、新しいファイル内のすべての英語の質問で以前のすべての英語の 質問が置き換えられます。そのため、既存のファイル内の質問を 1 つだけ変 更した場合でも、ファイル全体を再インポートする必要があります。

既存のセキュリティ クエスチョン ファイルを変更するかどうかは、慎重に決定してください。ファイルをインポートして、既存の質問を変更するたびに、以前の質問に対するユーザーの回答がすべて削除されます。ユーザーは回答を再度入力する必要があります。RSA では、ユーザーが回答を入力する前に、セキュリティ クエスチョンをカスタマイズすることを推奨します。

手順

1. RSA Authentication Manager 8.0 - Virtual Appliance DVD 内のセキュリティ クエスチョンのサンプル ファイル（**SecurityQuestionSample.xml**）の例を表示します。
2. LANGUAGE 要素ごとにセキュリティ クエスチョンの XML ファイルを作成します。たとえば、3 言語の質問が必要な場合、言語ごとにファイルを作成します。
3. それぞれの言語で、ファイルにセキュリティ クエスチョンを入力します。Authentication Manager は、言語の翻訳は行いません。セキュリティ クエスチョンには 255 字まで入力できます。ファイルには、セキュリティ クエスチョン要件で指定したアカウント登録に必要な回答の数と同じかそれ以上のセキュリティ クエスチョンを追加します。
4. それぞれの XML ファイルに、テキストの言語と一致する言語 ID が含まれていることを確認します。サポートする言語 ID のリストについては、RSA Security Console ヘルプのトピック「セキュリティ クエスチョンの言語コード」を参照してください。
5. RSA Authentication Manager 8.0 - Documentation DVD 内のセキュリティ クエスチョン ファイル スキーマ（**SecurityQuestions.xsd**）を使用して、各ファイルを検証します。

次のステップ

新しいセキュリティ クエスチョン ファイルをインポートします。操作手順については、RSA Security Console ヘルプのトピック「セキュリティ クエスチョンのインポート」を参照してください。

エマージェンシー オンライン認証

オンライン認証は、トークンを紛失したか破損したユーザーのために、エマージェンシー アクセスを提供します。トークンを紛失した場合でも、ユーザーは引き続き、オンライン エマージェンシー アクセス トークンコード、つまり Authentication Manager が生成する 8 文字の英数字コードを使用して 2 要素認証を行うことができます。

オンライン エマージェンシー アクセス トークンコードの形式は、セキュリティ ドメインのトークン ポリシーによって決まります。たとえば、セキュリティ ドメインのトークン ポリシーで特殊文字の使用が許可されている場合は、オンライン エマージェンシー アクセス トークンコードに特殊文字を含めることができます。

ユーザーのトークンが期限切れの場合は、新しいトークンを割り当ててから、一時的なアクセスを許可します。オンライン エマージェンシー アクセス トークンコードを、期限切れのトークンを持つユーザーに割り当てることはできません。操作手順については、159 ページのオフライン エマージェンシー パスコードの提供を参照してください。

次の表は、オンライン エマージェンシー アクセス トークンコードのタイプを示しています。どちらのタイプも、ユーザーのトークンにより生成されるトークンコードの代替として使用します。

トークンコードの種類	説明
一時固定トークンコード	• 2 回以上使用できる。 • ユーザーの RSA SecurID PIN と組み合わせてパスコードを作成する必要がある。 • Self-Service Console に表示される。
ワン タイム トークンコード	• セットで発行される。セットに含めるトークンコードの数は、管理者が決定できる。 • ユーザーの RSA SecurID PIN と組み合わせてパスコードを作成する必要がある。 • Self-Service Console に表示される。 • ユーザーは、ワン タイム トークンコードのセットをファイルとしてダウンロードできる。 • セット内の各トークンコードは 1 回しか使用できない。

また、ユーザーは、管理者の援助がなくても、Self-Service Console を使用して Authentication Manager への一時的なアクセスをリクエストすることができます。詳細については、283 ページの RSA セルフサービスを参照してください。

ワン タイム トークンコードのセットの割り当て

トークンの完全な紛失や破損が生じたユーザーに対しては、ワン タイム トークンコードのセットを割り当てることで、一時的なアクセスを提供できます。ワン タイム トークンコードは、ユーザーが紛失したトークンによって生成されるトークンコードに代わるものです。ユーザーは、PIN とワン タイム トークンコードを入力して、2 要素認証を実行する必要があります。

セットに含まれる各ワン タイム トークンコードは 1 回限り使用できます。トークンコードがセットで提供されるため、ユーザーは、その都度管理者に問い合わせをする必要なく複数回認証を行うことができます。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、適切なトークンを検索します。
3. 検索結果から、操作するトークンをクリックします。
4. コンテキスト メニューから、[**Emergency Access Tokencodes（エマージェンシー アクセス トークンコード）**] をクリックします。
5. [Manage Emergency Access Tokencodes（エマージェンシー アクセス トークンコードの管理）] ページで、[**Online Emergency Access（オンライン エマージェンシー アクセス）**] チェックボックスをオンにして、オンライン エマージェンシー アクセス トークンコードによる認証を有効化します。
6. [**Set of One-Time Tokencodes（ワン タイム トークンコードのセット）**] を選択します。
7. 生成するトークンコードの数を入力します。
8. [**Generate Codes（コードの生成）**] をクリックします。[Generate Codes（コードの生成）] ボタンの下に、トークンコードのセットが表示されます。
9. ユーザーに通知するために、ワン タイム トークンコードのセットを記録します。
10. [**Emergency Access Tokencode Lifetime（エマージェンシー アクセス トークンコードの有効期間）**] で、次のいずれかのオプションを選択します。
    - [No expiration（有効期限なし）]。
    - トークンコードの有効期限を設定する。
11. [**If Token Becomes Available（トークンが使用可能になった場合）**] フィールドで、紛失または使用不可能と識別されていたトークンが使用可能になった場合に Authentication Manager がどのように対処するかを構成します。
    - 回収されたトークンによる認証を拒否する。
      トークンの完全な紛失や破損が生じた場合、回収されたトークンによる認証を拒否します。これにより、権限のない人物によって回収された場合に、そのトークンを使用して認証を行うことはできなくなります。紛失したトークンが PIN レストークンの場合、この設定は必須です。
    - 回収されたトークンによる認証を許可し、同時にエマージェンシー アクセス トークンコードを無効化する。
    - エマージェンシー アクセス トークンコードの有効期間が経過した後にのみ回収されたトークンによる認証を許可する。
12. [**Save（保存）**] をクリックします。

一時固定トークンコードの割り当て

場合によっては、RSA SecurID で保護されたリソースに対する一時的なアクセスをユーザーに許可することが必要になることがあります。たとえば、既存のトークンの紛失や破損が生じたユーザーに対して、一時的なアクセスを許可することができます。一時的なアクセスが許可されたユーザーは、交換用トークンが支給されるのを待つ間も保護されたリソースにアクセスできます。

この手順では、一時固定トークンコードを使用して、ユーザーに一時エマージェンシー アクセスを許可します。

一時固定トークンコードは、ユーザーのトークンによって生成されるトークンコードに代わるものです。通常のトークンコードと同様、一時固定トークンコードをユーザーの PIN とともに入力して、パスコードを作成します。PIN と一時固定トークンコードを併用することで、ユーザーの 2 要素認証を実現します。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Assigned（割り当て済み）**］タブで、検索フィールドを使用して、紛失または破損したトークンを検索します。
3. 検索結果から、紛失または破損したトークンをクリックし、コンテキスト メニューから［**Emergency Access Tokencodes（エマージェンシー アクセス トークンコード）**］をクリックします。
4. ［Manage Emergency Access Tokencodes（エマージェンシー アクセス トークンコードの管理）］ページで、［**Online Emergency Access（オンライン エマージェンシー アクセス）**］を選択します。
5. ［Type of Emergency Access Tokencode(s)（エマージェンシー アクセス トークンコードのタイプ）］で、［**Temporary Fixed Tokencode（一時固定トークンコード）**］を選択します。
6. ［**Generate New Code（新しいコードの生成）**］をクリックします。［**Generate New Code（新しいコードの生成）**］ボタンの横にトークンコードが表示されます。
7. ユーザーに通知するために、エマージェンシー アクセス トークンコードを記録します。
8. ［**Emergency Access Tokencode Lifetime（エマージェンシー アクセス トークンコードの有効期間）**］で、［**No expiration（有効期限なし）**］を選択するか、または［**Expire on（有効期限）**］を選択し、有効期限を指定します。

   セキュリティ上の理由により必要に応じて、一時固定トークンコードの有効期間を制限できます。一時固定トークンコードは固定コードであるため、トークンによって生成される擬似乱数ほど安全性が高くありません。

9. ［**If Token Becomes Available（トークンが使用可能になった場合）**］で、次のオプションのいずれかを選択します。
   - ［**Deny authentication with token（トークンによる認証を拒否する）**］。
     トークンの完全な紛失や破損が生じた場合にこのオプションを選択します。これにより、トークンが回収された場合にそのトークンを使用して認証を行うことはできなくなります。トークンを不正に取得した第三者が保護対象リソースに無許可でアクセスするのを阻止できます。
   - ［**Allow authentication with token at any time and disable online emergency tokencode（トークンによる認証を常時許可し、オンライン エマージェンシー トークンコードを無効化する）**］。
     このオプションは、トークンが一時的に使用できない（ユーザーの自宅への置き忘れなど）場合に選択します。ユーザーはトークンを回収した後、ただちにトークンによる認証を再開できます。オンライン エマージェンシー アクセス トークンコードは、回収したトークンを使用した時点でただちに無効化されます。
   - ［**Allow authentication with token only after the emergency code lifetime has expired and disable online emergency tokencode（有効期間が経過し、オンライン エマージェンシー トークンコードが無効化した後にのみトークンによる認証を許可する）**］。
     このオプションは、トークンが手元にない場合に選択できます。ただし、ユーザーはトークンを回収しても、オンライン エマージェンシー アクセス トークンコードが期限切れになるまで、トークンを認証に使用することはできません。
10. ［**Save（保存）**］をクリックします。

エマージェンシー オフライン認証

オフライン認証は、オフライン認証時にエマージェンシー アクセスを必要とする RSA SecurID for Windows ユーザーに対して提供します。トークンの紛失または盗難にあったユーザーか、PIN を忘れたユーザーが対象となります。一時エマージェンシー アクセスを次の 2 通りの方法で許可できます。

- **オフラインエマージェンシー アクセス トークンコード**。このオプションは、ユーザーのトークンが使用不可の場合に使用します。オフライン エマージェンシー アクセス トークンコードは、ユーザーの PIN と組み合わせて使用します。
- **オフライン エマージェンシー パスコード**。このオプションは、自分の PIN を忘れたユーザーに対して使用します。オフライン エマージェンシー パスコードは、ユーザーの PIN およびトークンコードの代わりに使用します。

RSA SecurID for Windows ユーザーは、オフラインでの作業中に認証を受けることができるように一時エマージェンシー アクセスを必要とすることがあります。一時エマージェンシー アクセスは、トークンが一時的に手元にない場合、トークンを紛失したり、盗難にあった場合、ユーザーが PIN を忘れた場合に必要となります。

オフライン認証の場合、システムは、ユーザーが必要とする前にオフライン パスコードまたはトークンコードを生成しユーザーのマシンにダウンロードしておく必要があります。オフライン エマージェンシー認証コードは、事前に提供する必要があります。認証コードを、オフラインのユーザーに送信することはできません。

オフライン エマージェンシー アクセス トークンコードの提供

オフライン エマージェンシー アクセス トークンコードは、ユーザーのトークンが生成するトークンコードを置き換えます。通常時に使用するトークンコードと同様に、ユーザーがオフライン エマージェンシー アクセス トークンコードと PIN を入力してパスコードを作成することで、2 要素認証が実現されます。

次の項目を構成できます。

- ユーザーが次回オンラインで認証するときに新しいオフライン エマージェンシー アクセス トークンコードがダウンロードされるように指定する。
- オフライン エマージェンシー アクセス トークンコードをオンラインとオフラインの認証に使用できるようにする。

開始する前に

- ユーザーのセキュリティ ドメインで、オフライン認証が許可され、オフライン エマージェンシー アクセス トークンコードのダウンロードが許可されている。
- オフライン認証を行うエージェントでユーザーが過去に認証を行っており、エージェント上に有効な日数のオフライン認証データがダウンロード済みである。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、オフライン エマージェンシー アクセス トークンコードが必要なユーザーのトークンを検索します。
3. 検索結果から、トークンをクリックします。
4. コンテキスト メニューから、［**Emergency Access Tokencodes（エマージェンシー アクセス トークンコード）**］をクリックします。

5. ［Manage Emergency Access Tokencodes（エマージェンシー アクセス トークンコードの管理）］ページで、オフライン エマージェンシー アクセス トークンコードとその有効期限を確認します。
6. ユーザーが次回オンラインで認証するときに新しいオフライン エマージェンシー アクセス トークンコードをダウンロードするようにする場合は、［**Reset Offline Emergency Access Tokencode（オフライン エマージェンシー アクセス トークンコードのリセット）**］を選択します。選択した場合は、新しいトークンコードが自動的にダウンロードされます。
7. オンライン認証にオフライン エマージェンシー アクセス トークンコードを使用する必要がある場合は、［**Use offline code for online access（オンライン アクセスにオフライン コードを使用する）**］をクリックします。
8. ［**Save（保存）**］をクリックします。

オフライン エマージェンシー パスコードの提供

オフライン エマージェンシー パスコードは、ユーザーが通常入力するパスコード（PIN + トークンコード）の代わりに使用します。ユーザーは、トークンを所持したり、PIN を知っていなくてもオフライン認証を受けられます。

開始する前に

次を確認してください。

- ユーザーのセキュリティ ドメインで、オフライン認証が許可され、オフライン エマージェンシー アクセス トークンコードのダウンロードが許可されている。
- オフライン認証を行うエージェントでユーザーが過去に認証を行っており、エージェント上に有効なオフライン認証データがダウンロード済みである。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、オフライン エマージェンシー パスコードが必要なユーザーを検索します。
3. 検索結果から、ユーザーをクリックします。
4. コンテキスト メニューで［**Manage Emergency Offline Access（エマージェンシー オフライン アクセスの管理）**］をクリックします。
5. ［Manage Emergency Access Passcodes（エマージェンシー アクセス パスコードの管理）］ページで、オフライン エマージェンシー パスコードとその有効期限を確認します。

6. ユーザーが次回オンラインで認証するときに新しいオフライン エマージェンシー パスコードをダウンロードするようにする場合は、[**Reset Offline Emergency Access Passcode（オフライン エマージェンシー アクセス パスコードのリセット）**]を選択します。選択した場合は、新しいパスコードが自動的にダウンロードされます。
7. [**Update（更新）**]をクリックします。

RSA SecurID PIN

暗証番号（PIN）は、ユーザーを認証するために使用する数字のパスワードです。

セキュリティを強化するために、トークン ポリシーの設定により、文字と数字の両方が含まれる PIN を作成することや定期的な PIN の変更をユーザーに要求できます。84 ページのトークン ポリシーを参照してください。

PIN が紛失または漏洩すると、保護されたリソースはリスクにさらされることになります。そのため、ユーザーには、PIN が危殆化した場合はすぐに報告するよう指示する必要があります。

ユーザーから PIN の危殆化の報告があった場合、次回認証に成功した時に PIN を変更するようユーザーに要求することができます。

PIN の変更をユーザーに要求する場合、そのユーザーは、現在の PIN を把握している必要があります。PIN を変更するためには、ユーザーは、既存の PIN とトークンコードを使用して認証する必要があります。認証が成功した後、新しい PIN の作成を指示するプロンプトがユーザーに表示され、新しい PIN がユーザーのトークンに割り当てられます。

たとえば、あるユーザーから、地元のコーヒー ショップでコンピュータを使用していたときに、入力した PIN を誰かに見られたおそれがあるとの報告があったとします。報告を受けたら、管理者は Security Console を使用してユーザーに PIN の変更を要求します。操作手順については、162 ページのユーザーに対する RSA SecurID PIN 変更の強制を参照してください。

トークン ポリシーによっては、ユーザーが PIN を作成するのではなく、システムによって生成された PIN をユーザーが使用しなければならない場合があります。次回の認証の後に、システムによって生成された PIN がユーザーに提供されます。ユーザーは、その後、システムによって生成された新しい PIN を使用して認証を行います。

ユーザーが PIN を忘れた場合、PIN の変更を要求する方法では新しい PIN を作成できません。PIN を変更するには、ユーザーが現在の PIN を把握している必要があるためです。ユーザーが PIN を忘れた場合、新しい PIN を作成する前に元の PIN をクリアする必要があります。操作手順については、163 ページの RSA SecurID PIN のクリアを参照してください。

ユーザーが Self-Service Console を使用して自分の PIN をリセットすることもできます。

On-Demand 認証の初期 PIN の設定

ODA（On-Demand 認証）では、トークンコードを要求するための PIN が常に必要です。管理者は、ユーザーの初期 PIN を設定できます。次の処理手順は、まだ ODA を有効化していないユーザー向けです。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、ODA を有効化するユーザーを検索し、初期 PIN を設定します。
3. ユーザーをクリックします。
4. ［**SecurID Tokens（SecurID トークン）**］を選択します。
5. ［**On-Demand Authentication（On-Demand 認証）**］で、［**Enable User（ユーザーの有効化）**］を選択します。
6. ［**Expiration Date（有効期限）**］では、［**No expiration（有効期限なし）**］または On-Demand 認証が期限切れになる日付を指定します。
7. ［**Send On-Demand Tokencodes to（On-Demand トークンコードの送信先）**］では、配布方法を指定します。
8. ［**Associated PIN（PIN の割り当て）**］では、次のいずれかを実行します。
   - ［**Require user to setup the PIN through RSA Self-Service Console（ユーザーが RSA Self-Service Console を使用して PIN を設定する）**］を選択します。
   - ［**Set initial PIN to（初期 PIN の設定）**］を選択し、初期 PIN を入力します。
9. ［**Save（保存）**］をクリックします。
10. 初期 PIN を設定した場合は、安全性の高い方法でその初期 PIN をユーザーに伝えます。

ユーザーの On-Demand 認証 PIN のクリア

ユーザーの ODA（On-Demand 認証）PIN をクリアすることができます。たとえば、PIN のセキュリティが侵害された場合、ユーザーが PIN を忘れた場合、会社のポリシーで PIN の変更が必要になった場合などにこの操作が必要になります。ODA では PIN が必須であるため、ユーザーの PIN をクリアするときは一時 PIN を必ず設定する必要があります。

ユーザーは、初回使用時に一時 PIN を変更する必要があります。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、一時 PIN を設定するユーザーを検索します。
3. ユーザーをクリックします。
4. コンテキスト メニューから [**SecurID Tokens（SecurID トークン）**] を選択します。
5. [**On-Demand Authentication（On-Demand 認証）**] のセクションの、[**Associated Pin（PIN の割り当て）**] で、[**Clear existing PIN and set a temporary PIN for the user（既存の PIN をクリアし、一時 PIN を設定する）**] を選択します。
6. 一時 PIN を入力します。
7. [**Save（保存）**] をクリックします。
8. 安全性の高い方法でこの一時 PIN をユーザーに伝える必要があります。

ユーザーに対する RSA SecurID PIN 変更の強制

SecurID PIN の変更をユーザーに要求する場合は、トークンを使用して認証に成功した後に、新しい PIN の作成を求めるメッセージがユーザーに対して表示されます。

PIN の変更を要求できるのは、ユーザーが既存の PIN を知っている場合だけです。たとえば、現在の PIN が危殆化した場合に、ユーザーに SecurID PIN の変更を要求することがあります。ユーザーが PIN を忘れた場合は、PIN をクリアする必要があります。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. [**Assigned（割り当て済み）**] タブをクリックします。
3. 検索フィールドを使用して、編集するトークンを検索します。
4. 検索結果から、ユーザーに変更を要求する PIN を使用するトークンをクリックします。
5. [**Require SecurID PIN Change（SecurID PIN の変更を要求する）**] を選択します。

RSA SecurID PIN のクリア

ユーザーが SecurID PIN を忘れた場合は、ユーザーが新しい PIN を作成できるように、PIN をクリアすることができます。ユーザーの PIN をクリアすると、ユーザーは次回のユーザー認証時に新しい PIN を作成できます。

たとえば、PIN を忘れたユーザーからヘルプデスクに問い合わせがあったとします。管理者は、ユーザーの本人確認を行ったうえで、PIN をクリアします。ユーザーに対しては、次回のユーザー認証時にパスコードの入力プロンプトが表示されたら、トークンコードのみを入力するよう指示します。トークンコードの入力後、新しい PIN を作成するように求めるメッセージがユーザーに対して表示されます。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、PIN をクリアするユーザーを検索します。
3. ユーザーをクリックします。
4. コンテキスト メニューから [**SecurID Tokens（SecurID トークン）**] を選択します。
5. ユーザーに割り当てられているトークンのシリアル番号をクリックします。
6. コンテキスト メニューから [**Clear SecurID PIN（SecurID PIN のクリア）**] を選択します。
7. ユーザーに対して、次回の認証時にトークンコードのみを入力するよう指示します。トークンコードの入力後、新しい PIN を作成するように求めるメッセージがユーザーに対して表示されます。

RSA SecurID 800 トークンの PIN ロック解除キーの取得

SecurID 800 トークンを使用しているユーザーが PIN を忘れてしまった場合、トークンにアクセスするには PIN ロック解除キーが必要になります。スマートカードの詳細の表示および PIN ロック解除キーの取得は、Security Console を使用して行います。

開始する前に

SecurID 800 トークン データを表示する前に、SecurID 800 トークン データを RSA Authentication Manager にロードする。操作手順については、164 ページの PIN ロック解除キーのインポートを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Assigned（割り当て済み）**］タブをクリックします。
3. 検索フィールドを使用して、表示するスマートカードを検索します。
4. 検索結果から、表示するスマートカードをクリックします。
5. コンテキスト メニューで［**Edit（編集）**］をクリックします。
6. ［**SID800 Smart Card Details（SID800 スマート カードの詳細）**］セクションを表示して、PIN ロック解除キーを取得します。

PIN ロック解除キーのインポート

RSA SecurID 800 ハイブリッド トークンの PIN ロック解除キーを Authentication Manager にインポートするには、Import PIN Unlocking Key ユーティリティ（import-puk）を使用します。XML データをインポートすると、Security Console の［Token Properties（トークンのプロパティ）］ページで PIN ロック解除キーを表示できます。

開始する前に

- この手順を実行するには、SecurID 800 Smart Card Details（SecurID 800 スマートカード詳細）権限が許可された管理者ロールが必要です。詳細については、RSA Security Console ヘルプのトピック「Edit Administrative Roles（管理者ロールの編集）」を参照してください。
- アプライアンスで、SSH（セキュア シェル）が有効化されている必要があります。操作手順については、455 ページのアプライアンスの SSH の有効化を参照してください。

手順

1. SSH クライアントを使用してアプライアンスにログオンします。操作手順については、456 ページのアプライアンスのオペレーティング システムへのログオンを参照してください。
2. ディレクトリを **/opt/rsa/am/utils** に変更します。次のように入力します。

   ```
   cd /opt/rsa/am/utils/
   ```

   Enter キーを押します。
3. import-puk を実行して、PIN ロック解除キーをインポートします。次のように入力します。

   ```
   ./rsautil import-puk -f filename
   ```

   ここで、filename は PUK.xml ファイルへのパスを表します。（例：-f /opt/rsa/am/PUK.xml）。

4. プロンプトが表示されたら、管理者ユーザー ID を入力して Enter キーを押します。
5. プロンプトが表示されたら、パスワードを入力して Enter キーを押します。
6. インポート プロセスが完了したら、次のメッセージが表示されます。

   ```
   Status:IMPORTED < 個数 > PIN UNLOCK KEY (PUK) RECORDS
   SUCCESSFULLY.
   ```

7. SSH クライアントを閉じます。次のように入力します。

   ```
   exit
   ```

   Enter キーを押します。

ユーザー グループ

ユーザーをグループ化すると、保護されたリソースへのアクセスの管理が容易になります。ユーザー グループは、ユーザー、他のユーザー グループ、またはその両方の集合です。ユーザー グループに属するユーザーおよびユーザー グループは、メンバー ユーザーおよびメンバー ユーザー グループと呼ばれます。

ユーザー グループの編成

組織のニーズに従ってグループを編成できます。

- 地理的位置。地理に従ってグループを作成できます。
  - 市区町村、都道府県、国
  - 複数の市区町村、都道府県、国を含む地域
- 社内の部門。社内の機能分野に従ってグループを作成できます。
  - 部課
  - プロジェクト
  - ジョブ
- リソース。特定のリソースに従ってグループを作成できます。
  - 研究開発に関するファイル
  - 医療記録

ユーザー グループの特徴

ユーザー グループの特徴は、次のとおりです。

- 各ユーザー グループは、LDAP ディレクトリまたは内部データベースのいずれかのアイデンティティ ソースに格納されます。
- 各ユーザー グループは、1 つのセキュリティ ドメインに関連づけられます。

- 1 つのユーザー グループには、複数のユーザーおよびユーザー グループを含めることができます。
  外部アイデンティティ ソースに格納されているユーザー グループには、同じアイデンティティ ソースに属するユーザーとユーザー グループのみを含めることができます。
- 1 つのユーザー グループには、異なるセキュリティ ドメインで管理されているユーザーやユーザー グループを含めることができます。
  たとえば、セキュリティ ドメイン A に属するユーザーとセキュリティ ドメイン B に属するユーザーを同じユーザー グループのメンバーとし、同じ保護されたリソースへのアクセスを許可することができます。
- ユーザー グループ名は、1 つのアイデンティティ ソース内で一意でなければなりません。
  Authentication Manager では、別々のアイデンティティ ソースに保存されていれば、同じ名前の 2 つのユーザー グループを使用できます。
- 管理者は、セキュリティ ドメイン間でユーザー グループを移動して、グループに対する管理責任を別の管理者に移動できます。操作手順については、RSA Security Console ヘルプのトピック「ユーザーグループのセキュリティ ドメイン間の移動」を参照してください。
- ユーザーまたはユーザー グループは、複数のユーザー グループに所属できます。
- ［User Dashboard（ユーザー ダッシュボード）］ページを使用して、ユーザーをユーザー グループに追加したり、ユーザーグループから削除することができます。操作手順については、RSA Security Console ヘルプのトピック「ユーザー ダッシュボード」を参照してください。

ユーザー グループの作成

ユーザー グループは、次のいずれかの方法で作成できます。

- 内部データベースにユーザー グループを作成するには、Security Console を使用します。操作手順については、168 ページのユーザー グループの追加および 169 ページのユーザー グループへのユーザーの追加を参照してください。
- 外部アイデンティティ ソースにユーザー グループを作成するには、LDAP ディレクトリのネイティブ インタフェースを使用します。

内部ユーザー グループ

外部アイデンティティ ソースのユーザーとユーザー グループを内部データベースのユーザー グループに追加できます。この操作には、次のメリットがあります。

- 外部アイデンティティ ソースのユーザーの認証パフォーマンスが向上する。
  これらのユーザーを内部データベースのグループに直接含めると、ユーザー認証時の外部アイデンティティ ソースへのアクセスの必要性が減少し、ディレクトリ サーバへのネットワーク トラフィックが軽減される。ユーザー グループのメンバー グループに属するユーザーは、このパフォーマンス向上のメリットを受けることができません。
- ユーザー編成の管理が非常に容易になる。特に、LDAP ディレクトリのユーザーの場合、Security Console からはディレクトリのグループ構造を管理できないため管理が容易になります。
- 次の理由により、管理上の負荷が軽減されます。
  - 1 つの制限付きエージェントに 1 つのユーザー グループを作成できます。このとき、アイデンティティ ソースごとに個別のグループを作成するのではなく、エージェントへのアクセス権を付与するすべてのユーザーを 1 つのグループに含めることができます。
  - LDAP 管理者が LDAP 内のグループを変更した場合に、制限付きエージェントを再構成する必要性を最小限、またはゼロにすることができます。アクセス権は、内部データベースに存在するユーザー グループを通じて付与されるため、ディレクトリ内のグループに対する変更の影響を受けないためです。

外部アイデンティティ ソースに存在するユーザー グループのメンバーシップは、引き続き、当該ユーザー グループと同一の外部アイデンティティ ソースに属するメンバー ユーザーとメンバー ユーザー グループに制限されています。

ユーザー グループのネスト

制限付きエージェントへのアクセスを許可するユーザー グループを構成する際、1 つのユーザー グループに複数のユーザー グループを追加し、“ ネスト ” することができます。これにより、制限付きエージェント上でいくつかのグループを有効化できます。ネストされたグループを使用すると、管理者が認証エージェントへのアクセスを制限するために要する負荷は軽減されますが、グループのネストが深かったり、大量のユーザーが含まれている場合は、認証のパフォーマンスに影響する可能性があります。

ネストされたユーザー グループの特徴は、次のとおりです。

- 内部データベースのユーザー グループに、内部データベースまたは外部アイデンティティ ソースに存在するユーザー グループを含めることができます。外部アイデンティティ ソースのユーザー グループに、他のアイデンティティ ソースのユーザー グループを含めることはできません。

- ユーザー グループのネストは、次のいずれかの方法で行うことができます。
  - Security Console を使用して、内部データベースに格納されている 2 つ以上のユーザー グループをネストする。
  - LDAP ディレクトリ ユーザー インタフェースを使用して、同じ外部アイデンティティ ソースに格納されている 2 つ以上のユーザー グループをネストする。
  - Security Console を使用して、内部データベースに格納されているユーザー グループの下に、外部アイデンティティ ソースに格納されているユーザー グループをネストする。
- ネストされたユーザー グループのメンバーは、制限付きエージェントへのアクセス権を付与されている親ユーザー グループから、制限付きエージェントへのアクセス権を継承します。ネストされたグループも同じエージェントへのアクセスを許可されている場合、そのメンバーは、追加のアクセス権限を得ている可能性があります。

ユーザーがネストされたグループのメンバーの場合は、次の 2 種類の理由により、制限付きエージェントに対するアクセス権が付与されます。

- ユーザーが、制限付きエージェントへのアクセス権を持つユーザー グループのメンバーである
- ユーザーが、制限付きエージェントへのアクセス権を持つユーザー グループにネストされたユーザー グループのメンバーである

一般的に、ネストされたユーザー グループのメンバーは、親ユーザー グループと同じアクセス権限を持っています。ネストされたユーザー グループのメンバーは、そのグループが、エージェントへのアクセスを許可された別のユーザー グループの下にネストされている場合そのエージェントにアクセスできます。

ユーザー グループの追加

ユーザー グループは内部データベースに追加できます。外部アイデンティティ ソースにすでに存在するユーザー グループは追加する必要はありません。外部アイデンティティ ソースに存在するグループは、アイデンティティ ソースがリンクされるときに追加されます。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**User Groups（ユーザー グループ）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**Security Domain**（セキュリティ ドメイン）] ドロップダウン リストから、新しいユーザー グループのセキュリティ ドメインを選択します。新しいユーザー グループは、このセキュリティ ドメインを権限適用範囲に含んでいる管理者によって管理されます。

3. ［**User Group Name（ユーザー グループ名）**］フィールドに、ユーザー グループの一意の名前を入力します。最大文字数は 64 文字です。&、%、>、<、' の各文字は使用できません。
4. ［**Save（保存）**］をクリックします。

ユーザー グループへのユーザーの追加

どのアイデンティティ ソースのユーザーでも追加できるのは、内部データベースのユーザー グループのみです。外部 LDAP アイデンティティ ソースのグループのメンバーシップを変更するには、ネイティブ ツールを使用する必要があります。

ユーザーは、単独のユーザー グループまたは複数のユーザー グループに追加できます。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、ユーザー グループに追加するユーザーを検索します。いくつかの検索フィールドでは大文字と小文字が区別されます。
3. ユーザー グループに追加するユーザーの横のチェックボックスをオンにします。
4. ［Action（アクション）］メニューから、［**Add to User Groups（ユーザー グループに追加）**］を選択し、［**Go（実行）**］をクリックします。
5. 検索フィールドを使用して、ユーザーを追加するユーザー グループを検索します。いくつかの検索フィールドでは大文字と小文字が区別されます。
6. ユーザーを追加するユーザー グループの横のチェックボックスをオンにします。ユーザーを複数のグループに追加するには、複数のチェックボックスをオンにします。
7. ［**Add to Group（グループに追加）**］をクリックします。

認証エージェントによるユーザー アクセスの制御

エージェントをインストールした後は、保護されたリソースへのユーザー アクセスを制御するための構成をエージェントに対して実施します。次の表は、各エージェントの構成がユーザー アクセスをどのように制御するかを示しています。

エージェントの構成	認証されるユーザー	メリット
制限なし	エージェントと同一の導入環境に存在するすべてのユーザー。	エージェントを制限付きエージェントとして構成する操作、ユーザー グループをエージェントに関連づける操作、エージェントに関連づけられたユーザー グループのユーザー メンバーシップを管理する操作が不要になるため、管理上の負担が小さくなる。
制限付き	制限付きエージェントへのアクセスを直接許可されたすべてのグループのメンバー。 制限付きエージェントへのアクセスを直接許可されたグループにネストしているグループのメンバー。	エージェントは一部のユーザーの認証のみ許可するため、特定のネットワーク リソースへのアクセスを制限でき、セキュリティが向上する。
制限付き（グループのアクセス時間制限付き）	指定期間中に認証されるグループまたはネストされているグループのメンバー。	指定期間外の認証を禁止することにより、エージェントへのアクセスをさらに制限できる。

ユーザー アクセスを制御するための制限付きエージェントの構成

制限付きエージェントは、1 つ以上の指定されたグループのメンバーのみが保護されたリソースにアクセスできるようにします。たとえば、個人データへのアクセスを提供する制限付きエージェントを作成し、人事部門のメンバーのみがこのエージェントで認証されるようにした場合、人事部門のメンバーのみが個人データにアクセスできるようになります。認証を行う期間を指定することによって、さらにアクセスを制限できます。

この手順には、制限付きエージェントを構成するために必要な高度なタスクが含まれています。

手順

1. 認証エージェントを追加し、エージェントを制限付きエージェントとして構成します。
   操作手順については、72 ページの認証エージェントの追加を参照してください。
2. Authentication Manager 構成ファイルを生成します。
   手順については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。
3. ユーザー グループを設定します。
   手順については、165 ページのユーザー グループを参照してください。
4. 制限付きエージェントへのアクセスをユーザー グループに許可します。
   操作手順については、171 ページの制限付きエージェントでのユーザー グループの認証を許可するを参照してください。
5. （オプション）ユーザー グループに対してアクセス時間制限を設定します。
   手順については、RSA Security Console ヘルプのトピック「ユーザー グループのアクセス時間制限を設定する」を参照してください。

制限付きエージェントでのユーザー グループの認証を許可する

制限付きエージェントは、制限付きエージェントへのアクセスが許可されたユーザー グループのメンバーであるユーザーと、アクセスが許可されたユーザー グループのメンバーであるユーザー グループのユーザーからの認証要求のみを処理します。指定されたユーザー グループのメンバーでないユーザーは、制限付きエージェントを使用して認証を行うことはできません。

制限付きエージェントを使用すると、リソースに対して認証を受けるユーザーをより細かく制御できます。ただし、制限付きエージェントを使用すると、管理者が各ユーザー グループとエージェントを明示的に関連づける必要があるため、管理オーバーヘッドがそれだけ増加します。

手順

1. Security Console で、［**Access（アクセス）**］＞［**Authentication Agents（認証エージェント）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Restricted（制限付き）**］タブをクリックします。
3. 検索フィールドを使用して、アクセスを許可する制限付きエージェントを検索します。
4. アクセスを許可する制限付きエージェントの横のチェックボックスをオンにします。
5. ［**Action（アクション）**］メニューの［**Grant** Access to User Groups...（ユーザー グループにアクセスを許可 ...）］をクリックし、［**Go（実行）**］をクリックします。

6. 検索フィールドを使用して、アクセスを許可するユーザー グループを検索します。
7. アクセスを許可するユーザー グループの横のチェックボックスをオンにします。
8. ［**Grant Access to Restricted Agent（制限付きエージェントへのアクセスを許可する）**］をクリックします。

ユーザー グループに対するアクセス時間制限

ユーザー グループに対してアクセス時間制限を割り当てることも可能です。アクセス時間制限により、ユーザー グループのメンバーが制限付きエージェントにアクセス可能な日時を制御できます。

たとえば、企業のリソースにアクセスするユーザーがボストンにいて、このユーザーがアクセスできる時間を通常の就業時間内に制限するとします。この場合、ボストンのユーザーを 1 つのグループに追加し、そのグループのアクセス時間を、午前 8 時から午後 5 時に制限することができます。Authentication Manager には、エージェントへのアクセスを制限するときの典型的な時間帯を反映した、アクセス時間テンプレートが用意されており、時間制限の構成にかかる負担を軽減できます。この例では、時間を手動で構成する代わりに、「8am - 5pm Weekdays（平日午前 8 時～午後 5 時）」テンプレートを使用するように選択できます。

アクセス時間制限には、次のような動作上の特徴と制限事項があることに注意してください。

- すべての時間は、アクセス時間制限を構成するときに選択するタイム ゾーンに相対した時間になります。

  地理的に離れた場所にユーザーが存在する環境でアクセス時間制限を適用する場合は、この動作上の特徴を考慮する必要があります。詳細については、173 ページの地理的に離れた場所にいるユーザー向けのアクセス時間制限を参照してください。
- Authentication Manager では、30 分単位のタイム ゾーンはサポートしていません。その場合は、使用可能なタイム ゾーンのうち、目的のタイム ゾーンに最も近いものを使用してください。
- Authentication Manager では、サマータイム期間に伴う変更の自動調整は行いません。

地理的に離れた場所にいるユーザー向けのアクセス時間制限

アクセス時間制限で指定する時間は、プライマリ インスタンスのタイム ゾーンに相対しています。地理的に離れた複数の場所にいるユーザーのアクセス時間を制限する場合、それぞれの場所の時差を考慮する必要があります。時差に対処するためには、グループ メンバーシップとアクセス時間制限を次の 2 種類の方法で構成することができます。

- **地理的な場所に基づいて 2 つ以上のユーザー グループを構成し、各グループに異なるアクセス時間を設定する**。メンバーの場所に基づいてユーザー グループを構成する場合は、プライマリ インスタンスの場所と、ユーザーの場所との時差は、グループごとに別々のアクセス時間制限を構成することで相殺する必要があります。

  たとえば、導入環境にボストンのユーザーとロンドンのユーザーがいる場合は、ボストンのために 1 つのユーザー グループを作成し、ロンドンのために別のユーザー グループを作成します。グループごとに異なるアクセス時間制限を指定します。プライマリ インスタンスが設置されているボストンのグループに対しては、アクセス時間を午前 8 時～午後 5 時に制限し、ロンドンのグループには、午前 3 時～正午（ロンドンの時刻では午前 8 時～午後 5 時に相当）に制限することができます。

  あるいは、アクセス時間制限の構成時にローカル タイム ゾーンを選択することもできます。前の例では、アクセス時間制限を構成する前に、各ユーザー グループに対してローカルのタイム ゾーンを指定することができます。

  RSA では、アクセス時間と制限付きエージェントへのユーザー アクセスをより厳密に管理できるため、この方法を推奨しています。

- **複数の地理的な場所に存在するユーザー用の 1 つのユーザー グループを構成し、両方のグループに同じアクセス時間を設定する**。異なる場所にいるメンバーが含まれる 1 つのグループを構成する場合、ユーザー グループの全メンバーの就業時間が全て含まれるようにアクセス時間制限を設定する必要があります。

  たとえば、グループに、ボストンのユーザーとロンドンのユーザーが含まれているとします。プライマリ インスタンスが設置されているボストン（タイム ゾーンは東部標準時）で、ボストンのアクセス時間を午前 8 時～午後 5 時に制限した場合、ロンドンのユーザーは、ロンドン時刻で午後 1 時～午後 10 時の間しかエージェントにアクセスできないため、グループのアクセス時間を東部標準時の午前 3 時～午後 5 時に拡大する必要があります。これにより、ボストンのユーザーとロンドンのユーザーの両方が、就業時間にエージェントにアクセスできます。

詳細については、172 ページのユーザー グループに対するアクセス時間制限を参照してください。

複数のユーザー グループに属するユーザーのアクセス時間制限

1 人のユーザーが複数のグループのメンバーである場合、複数のグループに同一の制限付きエージェントへのアクセス権が付与される場合があります。このような場合、複数のグループの時間制限が組み合わされ、ユーザーに許可されるエージェントへのアクセス時間が延長される可能性があります。

たとえば、あるユーザーが 2 つのユーザー グループのメンバーだとします。2 つのユーザー グループは、マーケティングとセールスです。両方のグループが、同じ制限付きエージェントにアクセスできます。マーケティング グループのメンバーのアクセス時間制限が午前 8 時～午後 5 時で、セールスグループのメンバーのアクセス時間制限が午前 9 時～午後 7 時の場合、このユーザーはエージェントに午前 8 時～午後 7 時までアクセスすることができます。

詳細については、RSA Security Console ヘルプのトピック「Set Restricted Access Times for User Groups（ユーザー グループのアクセス時間制限の設定）」を参照してください。

ネストされたユーザー グループに属するユーザーのアクセス時間制限

一般的に、1 つの親グループにネストされたユーザー グループは、親ユーザー グループと同じアクセス時間制限を共有します。ただし、親ユーザー グループとネストされたユーザー グループの両方が、同じエージェントへのアクセス権を付与されている場合、アクセス時間制限は、複数のユーザー グループに属するユーザーの場合と同様に合計されます。

たとえば、あるユーザーが 2 つのユーザー グループのメンバーだとします。2 つのユーザー グループは、マーケティングとセールスです。マーケティングはセールスの下にネストされており、両グループとも同じ制限付きエージェントに対するアクセス権を持ちます。マーケティング グループのメンバーのアクセス時間制限が午前 8 時～午後 5 時で、セールスグループのメンバーのアクセス時間制限が午前 9 時～午後 7 時の場合、マーケティングのメンバーは制限付きエージェントに午前 8 時～午後 7 時までアクセスすることができます。

Active Directory グループによる制限付きエージェントへのアクセス

Active Directory は、複数のグループ タイプをサポートしています。Active Directory をアイデンティティ ソースとして構成した場合、Authentication Manager では、ユニバーサル グループしかサポートしません。

制限付きエージェントへのアクセスを許可するために Active Directory グループを選択する際は、必ずユニバーサル グループを選択してください。その他のタイプの Active Directory グループを使用すると、ユーザーを認証できません。Security Console 上には、グループ タイプにかかわらず、すべての Active Directory グループが一覧表示されます。

Security Console には、ユーザーのプライマリ Active Directory ユーザー グループ（Domain Users など）のメンバーは表示されません。このようなグループは、メンバーが存在していても空の状態で示されます。

制限付きエージェントで認証が許可されたユーザー グループの表示

Security Console を使用して、制限付きエージェントで認証が許可されたユーザー グループを表示します。検索結果には、制限付きエージェントへのアクセス権を直接付与されたユーザー グループのみが表示されます。ネストされたユーザー グループは表示されません。

手順

1. Security Console で、[**Access（アクセス）**] > [**Authentication Agents（認証エージェント）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. [**Restricted（制限付き）**] タブをクリックします。
3. 検索フィールドを使用して、ユーザー グループを表示するエージェントを検索します。
4. エージェントをクリックし、[**User Groups with Access（アクセスを許可されたユーザー グループ）**] を選択します。
5. 表示するユーザー グループをクリックし、[**View（表示）**] を選択します。

LDAP ディレクトリ内のユーザー データ

LDAP ディレクトリ側でのユーザー データの変更により、ユーザーの識別名（DN）、ユーザー ID、またはその両方が変更されると、そのユーザーの認証および管理に影響が生じる可能性があります。ユーザーの DN またはユーザー ID が変更された場合、Authentication Manger は、アイデンティティ ソースとして指定された LDAP ディレクトリでそのユーザーを検出できなくなります。この状態のユーザー（またはユーザー グループ）は、“ 解決不可能 ” と呼びます。解決不可能なユーザーであっても、トークンが割り当てられているかぎりライセンス上のユーザー数制限の対象としてカウントされるため、RSA では、解決不可能なユーザーおよびユーザー グループへの参照を削除することを推奨します。

ユーザーが解決不可能になる仕組み

解決不可能なユーザーとは、アイデンティティ ソースとして指定された LDAP ディレクトリから検出できなくなったユーザーです。

ユーザーが解決不可能となるのは、次のいずれかの場合です。

- ユーザーが LDAP ディレクトリから削除された場合。
- ユーザーがアイデンティティ ソースのベース DN の範囲外に移動された場合。
- ユーザーがすべてのアイデンティティ ソースの範囲外に移動された場合。
- アイデンティティ ソースの範囲を縮小したため、ユーザーが含まれなくなった場合。

- アイデンティティ ソースの検索フィルタが変更されたため、ユーザーが含まれなくなった場合。
- ユーザーが削除と追加操作の組み合わせによって同じ物理ディレクトリ内のアイデンティティ ソースに移動され、なおかつ一意の識別子としてデフォルト値を使用する構成になっている場合。
- ユーザーが物理的に異なるディレクトリのアイデンティティ ソースに移動された場合。

解決不可能になるユーザーは、アイデンティティ ソースに存在していないものとして報告されます。

別のアイデンティティ ソースに移動したユーザーをクリーンアップしたら、認証の有効化や管理者ロールの割り当てなど、Authentication Manager 内でそれらのユーザーを再設定する必要があります。

一部のディレクトリ管理ツールは、ディレクトリからいったんユーザーを削除し、ユーザーを再度追加することでユーザーを移動します。このような場合、デフォルトの一意識別子を使用していると、Authentication Manager は移動後のユーザーを検出できません。ディレクトリからいったんユーザーを削除し、ユーザーを再度追加すると、デフォルトの一意識別子である ObjectGUID に新しい値が設定されます。ユーザーの一意識別子の値を変えずに保持するには、カスタム属性を一意識別子として構成します。

ユーザー グループが解決不可能になる仕組み

解決不可能なユーザー グループとは、アイデンティティ ソースとして指定された LDAP ディレクトリで検索できなくなったユーザー グループです。

ユーザー グループが解決不可能となるのは、次のいずれかの場合です。

- ユーザー グループが LDAP ディレクトリから削除された場合。
- ユーザー グループが移動された場合。
- アイデンティティ ソースの範囲を縮小したため、ユーザー グループが含まれなくなった場合。
- アイデンティティ ソースの検索フィルタを変更したため、ユーザー グループが含まれなくなった場合。

解決不可能なユーザーの手動クリーンアップ

次のような理由があるため、解決不可能なユーザーをクリーンアップすることを推奨します。

- 解決不可能なユーザーでも、ライセンスのユーザー数制限の対象としてカウントされます。解決不可能なユーザーをクリーンアップすると、このカウントが減り、導入環境内に登録できるユーザー数が増えます。

- 解決不可能なユーザーに割り当てられているトークンは、割り当てられたまま残されます。解決不可能なユーザーをクリーンアップすると、それらのユーザーのトークンを他のユーザーに割り当てることが可能になります。

  ユーザーが物理的に異なるディレクトリのアイデンティティ ソースに移動された場合は、トークンを同じユーザーに再割り当てしてください。ユーザーに移動前に割り当てられていた固定パスコード、On-Demand トークンコード設定、管理者ロールがある場合は、それらも再割り当てする必要があります。

手動クリーンアップ処理を実行すると、LDAP ディレクトリのユーザーと内部データベースの RSA 固有のデータの間の関連づけが削除されます。操作手順については、177 ページの解決不可能なユーザーの手動クリーンアップを参照してください。

手動クリーンアップを開始すると、Authentication Manager によって、リンクされたアイデンティティ ソースの解決不可能なユーザーのリストが生成されます。すべてのユーザーの参照を削除する前に、クリーンアップの対象となるユーザーをプレビューできます。デフォルトでは、リンクされたアイデンティティ ソース内の解決不可能なユーザーがすべてクリーンアップされます。手動クリーンアップでは、ユーザー グループはクリーンアップされません。

手動クリーンアップ処理は、システムにリンクされている LDAP ディレクトリ アイデンティティ ソースにのみ適用されます。アイデンティティ ソースがリンクされない場合、ユーザーは解決不可能ではなく、手動クリーンアップは必要ありません。

解決不可能なユーザーの手動クリーンアップ

解決不可能なユーザーを必要に応じて手動でクリーンアップできます。クリーンアップ処理を実行すると、LDAP ディレクトリのユーザーと内部データベースの RSA 固有のデータの間の関連づけが削除されます。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Identity Sources（アイデンティティ ソース）**] > [**Clean Up Unresolvable Users（解決不可能なユーザーのクリーンアップ）**] の順にクリックします。
2. クリーンアップするアイデンティティ ソースの名前または [**All（すべて）**] を選択します。

3. ［**Grace Period（猶予期間）**］フィールドで、次のいずれかを実行します。
   - 指定した日数を超えて解決不可能なユーザーをクリーンアップする場合は、チェックボックスをオンにします。
   - 解決不可能であることが判明したユーザーを直ちに削除する場合は、チェックボックスをオフにします。

   ［Grace Period（猶予期間）］を使用すると、誤ってディレクトリから削除されたり、アイデンティティ ソースの範囲外の OU に移動された可能性があるユーザーおよびユーザー グループをクリーンアップすることを回避できます。ユーザーをクリーンアップするための条件として解決不可能な状態が続く日数を指定することにより、事前に修正アクションを取ることができます。このフィールドは、デフォルトで、解決不可能なユーザーを 7 日後にクリーンアップするよう設定されています。
4. ［**Next（次へ）**］をクリックします。

   解決不可能なユーザーのリストが作成されます。処理が完了すると、リストがプレビュー パネルに表示されます。プレビュー パネルには、一度に最大 500 件の結果が表示されます。500 件の結果が表示された場合は、さらに多くのユーザーをクリーンアップする必要がある可能性があります。その場合は、「Users and User Groups Missing From Identity Source（アイデンティティ ソース上に見つからないすべてのユーザーおよびグループ）」レポート テンプレートを使用してレポートを実行して、解決不可能なユーザーの完全なリストを表示することをお勧めします。詳細については、391 ページのレポートの追加を参照してください。
5. プレビュー パネルで、ユーザーのリストを確認します。列名をクリックすると、リストをソートできます。リストが空の場合、解決不可能なユーザーはいません。
6. ［**Clean Up Now（今すぐクリーンアップ）**］をクリックします。

   重要：クリーンアップはキャンセルできません。［**Clean Up Now（今すぐクリーンアップ）**］をクリックすると、ユーザーと内部データベース内のオブジェクトとの関連づけがすべて削除されます。

   クリーンアップ プロセスが完了すると、処理が正常に完了したことを示すメッセージが［Configure Settings（設定の構成）］パネルに表示されます。

解決不可能なユーザーおよびユーザー グループのスケジュール クリーンアップ

スケジュール クリーンアップ ジョブでは、解決不可能なユーザーおよびユーザー グループへの参照を内部データベースから削除します。

スケジュール クリーンアップ ジョブは、リンクされたアイデンティティ ソースおよびリンク解除されたアイデンティティ ソースに対して実行します。毎日、毎週、毎月のいずれかの頻度で実行するように構成できます。解決不可能なユーザーの数が［Cleanup Limit（クリーンアップ制限）］で指定した値を超えている場合、このジョブはキャンセルされます。これにより、LDAP ディレクトリ側で直接多数のユーザーに対して変更が行われた時に、それらの多数のユーザーと認証データの関連づけが誤って解除されるのを防ぐことができます。デフォルトの制限は、50 ユーザーです。

次のような理由があるため、解決不可能なユーザーをクリーンアップすることを推奨します。

- 解決不可能なユーザーでも、ライセンスのユーザー数制限の対象としてカウントされます。解決不可能なユーザーをクリーンアップすると、このカウントが減り、導入環境内に登録できるユーザー数が増えます。
- 解決不可能なユーザーに割り当てられているトークンは、割り当てられたまま残されます。解決不可能なユーザーをクリーンアップすると、それらのユーザーのトークンを他のユーザーに割り当てることが可能になります。

  ユーザーが物理的に異なるディレクトリのアイデンティティ ソースに移動された場合は、トークンを同じユーザーに再割り当てしてください。ユーザーに移動前に割り当てられていた固定パスコード、On-Demand トークンコード設定、管理者ロールがある場合は、それらも再割り当てする必要があります。

次のような状況で、クリーンアップをスケジュール設定することを推奨します。

- アイデンティティ ソースを削除する前

  アイデンティティ ソースを削除するには、まずアイデンティティ ソースとシステムのリンクを解除し、スケジュール クリーンアップを実行します。その後で、Operations Console を使用してアイデンティティ ソースを削除します。スケジュール クリーンアップでは、リンク解除されたアイデンティティ ソースに関連づけられたユーザーとグループへのすべての参照を内部データベースから削除します。詳細については、RSA Security Console ヘルプのトピック「システムからのアイデンティティ ソースのリンク解除」を参照してください。

  アイデンティティ ソースを一時的にリンク解除する場合（たとえば、関連するグローバル カタログを追加する場合）、クリーンアップ ジョブは実行しないでください。アイデンティティ ソースを再度リンクしたときに、そのアイデンティティ ソースのすべてのユーザーは再度解決可能になります。Authentication Manager は、リンク解除操作の前と同じように、これらのユーザーを検出できるようになります。

- アイデンティティ ソースの範囲を縮小した後

  アイデンティティ ソースの範囲を小さくした場合、一部のユーザーおよびユーザー グループは、解決不可能になり、認証できなくなることがあります。アイデンティティ ソースの編集後は、スケジュール クリーンアップ ジョブを実行する必要があります。このジョブを実行するときは、設定していた猶予期間およびクリーンアップ制限を無効化し、この 1 回のクリーンアップの実行後に、これらの設定を再度有効化する必要があります。

次のオプションを使用して、クリーンアップ プロセスを変更できます。

[Cleanup Limit（クリーンアップ制限）]：［Cleanup Limit（クリーンアップ制限）］で指定した値を超える数の解決不可能なユーザーがデータベース内に見つかった場合、自動クリーンアップはキャンセルされます。この制限を使用すると、多数のユーザーに対してアイデンティティ ソース側で直接変更が行われた場合に、多数のユーザーと認証データの関連づけが誤って解除されるのを防ぐことができます。

クリーンアップがキャンセルされた場合は、「Users and User Groups Missing From Identity Source（アイデンティティ ソース上に見つからないすべてのユーザーおよびグループ）」レポートを実行して、解決不可能なユーザーのリストを表示できます。このリストには、クリーンアップする必要がないユーザーが含まれている可能性があります。たとえば、ディレクトリから誤って削除されたユーザーや、ある場所から同じディレクトリ内の別の場所に移動されたユーザーなどが考えられます。

[Grace Period（猶予期間）]：［Grace Period（猶予期間）］を使用すると、指定した日数を超えて解決不可能な状態が続いているユーザーだけをクリーンアップの対象にすることができます。［Grace Period（猶予期間）］を指定しておけば、ディレクトリ内のユーザーに対する不適切な変更を修正する時間的猶予を確保できます。たとえば、誤ってユーザーが削除または移動される場合があります。

リンクされたアイデンティティ ソース内で誤って次のいずれかの変更が発生した場合は、［Grace Period（猶予期間）］を使用すると、その変更が行われたユーザーのクリーンアップを回避できます。

- ユーザーが削除された場合
- ユーザーが導入環境のアイデンティティ ソースの外にある OU（組織単位）に誤って移動された場合
- ユーザー名が変更された場合

クリーンアップ ジョブのスケジュール

スケジュール クリーンアップ ジョブでは、内部データベースの解決不可能なユーザーおよびユーザー グループへの参照を修復または削除します。解決不可能なユーザーとは、指定されたアイデンティティ ソースに自身のレコードが含まれなくなったユーザーです。ユーザーが同じ LDAP ディレクトリ内の別の ID に移動した場合は、クリーンアップ ジョブによって参照が修復されます。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Identity Sources（アイデンティティ ソース）**] > [**Schedule Cleanup（スケジュール クリーンアップ）**] の順にクリックします。
2. クリーンアップ ジョブの実行をスケジュール設定するには、[**Cleanup Status（クリーンアップ ステータス）**] セクションで、[**Enable scheduled cleanup of unresolvable users and user groups from linked identity sources, and all users and user groups from unlinked identity sources（スケジュール クリーンアップを有効化し、リンクされたアイデンティティ ソースの解決不可能なユーザーとユーザー グループ、およびリンク解除されたアイデンティティ ソースのすべてのユーザーとユーザー グループをクリーンアップする）**] をオンにします。デフォルトでは、このチェックボックスはオフになっており、無効化されています。
   構成したクリーンアップを無効化すると、次回このページにアクセスしたときに、すべてのフィールドはデフォルト値にリセットされ、以前に実行した構成の変更はすべて失われます。
3. [**Cleanup Limit（クリーンアップ制限）**] フィールドで、次のいずれかを実行します。
   - デフォルトのままにします。
     デフォルトでは、このフィールドは有効で、制限は 50 ユーザーです。この制限値は、ゼロより大きい正の数である必要があります。指定値を超える数の解決不可能なユーザー参照やリンク解除されたユーザー参照が見つかった場合、クリーンアップはキャンセルされます。この制限を使用すると、多数のユーザーに対してアイデンティティ ソース側で直接変更が行われた場合に、多数のユーザーと認証データの関連づけが誤って解除されるのを防ぐことができます。
   - 解決不可能なユーザーおよびユーザー グループをすべてクリーンアップする場合は、[**Cleanup Limit（クリーンアップ制限）**] チェックボックスをオフにします。

     重要：リンク解除されたアイデンティティ ソースを削除する前に、クリーンアップを実行する場合は、このチェックボックスをオフにします。
4. [**Grace Period（猶予期間）**] フィールドで、次のいずれかを実行します。
   - デフォルトのままにします。
     デフォルトでは、このフィールドは有効で、7 日間に設定されています。この値は、ゼロより大きい正の数である必要があります。リンク解除されたアイデンティティ ソースの場合は、このフィールドは無視されます。指定した日数を超えて解決不可能な状態が続いているユーザーだけがクリーンアップされます。このフィールドを使用すると、誤ってディレクトリから削除されたり、アイデンティティ ソースの範囲外の OU に移動された可能性があるユーザーがクリーンアップされるのを回避できます。クリーンアップを行う前に、修正アクションを取ることができます。

- 解決不可能であることが判明したユーザーを直ちに削除する場合は、［**Grace Period（猶予期間）**］チェックボックスをオフにします。

注：猶予期間は、ユーザー グループには適用されません。ユーザー グループは、解決不可能であることが判明すると直ちに削除されます。

5. クリーンアップ制限の値を超え、クリーンアップがキャンセルされた場合は、「Users and User Groups Missing From Identity Source（アイデンティティ ソース上に見つからないすべてのユーザーおよびグループ）」レポートを実行して、クリーンアップする必要があるユーザーを判別します。このレポートを確認したら、クリーンアップが成功するように適切な制限値を設定するか、手動クリーンアップを実行することもできます。詳細については、RSA Security Console ヘルプのトピック「レポート テンプレートの表示」および 179 ページの解決不可能なユーザーおよびユーザー グループのスケジュール クリーンアップを参照してください。

注：リンク解除されたアイデンティティ ソースを削除する前にスケジュール クリーンアップを実行する場合、制限を適用しないよう、［Cleanup Limit（クリーンアップ制限）］チェックボックスがオフになっていることを確認します。また、アイデンティティ ソースの範囲を縮小した後でこのジョブを実行する場合も、このチェックボックスをオフにします。

6. ［**Schedule（スケジュール）**］で、［**Start（開始）**］フィールドを使用して、クリーンアップを最初に実行する日付を選択します。
7. ［**Frequency（頻度）**］フィールドを使用して、クリーンアップを実行する頻度と曜日を指定します。
8. ［**Run Time（実行時間）**］フィールドを使用して、クリーンアップを実行する時刻を指定します。
9. 特定の日付で設定を期限切れにする場合は、［**Expire（期限切れ）**］フィールドを使用します。日付を選択しない場合、設定に期限はありません。
10. クリーンアップのスケジュール設定が終了したら、［**Save（保存）**］をクリックします。

次のステップ

別のアイデンティティ ソースに移動したユーザーをクリーンアップしたら、管理者ロールの割り当てや認証の有効化など、Authentication Manager 内でそれらのユーザーを再設定する必要があります。

LDAP ディレクトリ内でのユーザーの移動

アイデンティティ ソースとしてリンクされた LDAP ディレクトリ上でユーザーを移動した場合、Authentication Manager がその移動を検出してユーザー データを更新できるのは、次のいずれかの場合です。

- スケジュール クリーンアップが実行された場合。
- すべてのアイデンティティ ソースか、またはそのユーザーが格納されているアイデンティティ ソースに対して、管理者が手動クリーンアップを実行した場合。
- 管理者が Security Console でそのユーザーのレコードを変更した場合。
- そのユーザーが認証を試行した場合。

アイデンティティ ソース内でのユーザーの移動

ユーザーが LDAP ディレクトリ内で移動され、同じアイデンティティ ソース内に残るのであれば、ユーザーの一意識別子が変更されない限り、そのユーザーの認証と管理が引き続き可能になります。しかし、一部のディレクトリ管理ツールでは、ユーザーをいったん削除してからディレクトリに再追加することにより移動を行うため、一意識別子が変更されることになります。

このような場合、Authentication Manager は移動後のユーザーを検出できません。ユーザーを削除してからディレクトリに再追加すると、デフォルトの一意識別子として指定されている属性（Active Directory では ObjectGUID、Oracle Directory Server では nsUniqueID）に新しい値が作成されるからです。この問題を回避するには、一意識別子としてカスタム属性を使用するよう構成します。

元のアイデンティティ ソースの範囲外へのユーザーの移動

ユーザーが LDAP ディレクトリ内で移動され、元のアイデンティティ ソースの範囲外にいる場合は、次の基準が満たされていれば、そのユーザーの認証と管理が引き続き可能になります。

- ユーザーがまだ同じ物理ディレクトリ内に存在すること。
- 次の基準を満たす別のアイデンティティ ソースが Authentication Manager 内で構成されていること。
  - 元のアイデンティティ ソースと同じ物理ディレクトリ内に存在するアイデンティティ ソースであること。
  - ユーザーの新しい DN が格納されているアイデンティティ ソースであること。
  - 両方のアイデンティティ ソースで同じ属性をユーザー ID に使用していること。

  - 両方のアイデンティティ ソースで同じ属性を一意識別子に使用していること。

  ユーザーの移動後にアイデンティティ ソースを構成することもできますが、アイデンティティ ソースを構成する前にユーザーが認証を試みると、その後 1 時間はアクセスが拒否されます。

- アイデンティティ ソースがデフォルトの一意識別子を使用するように構成されている場合は、ユーザーの移動方法がユーザーの削除と再追加によるものでないこと。

これらの基準が満たされていないと、移動の結果としてユーザーが解決不可能な状態になります。解決不可能なユーザーを管理する方法については、176 ページの解決不可能なユーザーの手動クリーンアップを参照してください。

LDAP ディレクトリ内でのユーザーの移動の影響

ディレクトリ内でユーザーが移動されると、Authentication Manager に次のような影響が生じます。

- ユーザーの最初の認証試行が失敗する場合があります。この認証失敗は、ロックアウト ポリシーのカウントに含まれません。

  初回の認証が失敗するユーザーの数を最小化するには、定期的なクリーンアップをスケジュールします。操作手順については、180 ページのクリーンアップ ジョブのスケジュールを参照してください。

- レプリケーションの同期ずれが発生したり、レプリカ インスタンスが使用不可の状態になると、システムがユーザーの新しいアイデンティティ ソースを更新するのに遅延が生じることがあります。その場合は、レプリケーションが復旧されるまでユーザーのアクセスが拒否されます。

- エイリアスで認証を受けるユーザーが異なるアイデンティティ ソースに移動された場合は、グループとの関連づけが維持されません。

  ユーザー エイリアス、シェル、およびエイリアスに割り当てられている RADIUS プロファイルは古いアイデンティティ ソースに設定されたまま残ります。

  新しいアイデンティティ ソース内のグループに、エイリアス、シェル、および RADIUS プロファイルを再度設定する必要があります。これを行うには、ユーザーの認証設定を編集し、新しいアイデンティティ ソース内のグループを選択し、そのグループにエイリアスを関連づける必要があります。

  認証設定の更新の詳細については、147 ページのユーザー認証設定の管理を参照してください。

- ユーザーが異なるアイデンティティ ソースに移動された場合、そのユーザーは制限付きエージェントでの認証ができなくなることがあります。

  Oracle Directory Server/Sun Java System Directory Server でユーザーの識別名（DN）が変更された場合、そのユーザーはすべての LDAP グループ メンバーシップから削除されます。このユーザーが、制限付きエージェントでの認証が許可されたグループに所属していた場合、制限付きエージェントで認証できなくなります。

  ユーザーが、制限付きエージェントでの認証を許可された新しいアイデンティティ ソースのグループのメンバーである場合は、いかなるアクションも必要ありません。ユーザーが、制限付きエージェントでの認証を許可された新しいアイデンティティ ソースのグループのメンバーでない場合は、新しいアイデンティティ ソースとして指定されているディレクトリ内のグループにユーザーを追加し、そのグループを制限付きエージェントに関連づける必要があります。

  Authentication Manager ではグループ メンバーシップがキャッシュされているため、LDAP ディレクトリ内でグループ メンバーシップが直接変更された場合、これらの変更をすぐに認識できないことがあります。その結果、キャッシュに保存した値が期限切れになるまで（通常は 10 秒後）Authentication Manager は、そのユーザーを、元のアイデンティティ ソースのグループのメンバーと見なします。

  制限付きエージェントに関連づけられているすべてのグループからユーザーが削除された場合でも、移動後の短い間、ユーザーは制限付きエージェントで認証を受けることができてしまいます。グループ メンバーシップの変更が即時に認識されるようにするには、ディレクトリ内で変更を行った後、キャッシュをフラッシュしてください。詳細については、423 ページのキャッシュのフラッシュを参照してください。

- ユーザーが別の管理者の管理対象になることがあります。

  元の管理者の権限適用範囲に新しいアイデンティティ ソースが含まれていない場合、その管理者はユーザーを管理できなくなります。代わりに、新しいアイデンティティ ソースを管理する権限を持つ管理者が、そのユーザーを管理できるようになります。

- ユーザーが異なるアイデンティティ ソースに移動されると、Security Console は、新しいアイデンティティ ソース内でそのユーザーをただちに認識します。

  移動により何らかの問題が生じて管理者による対応が必要になった場合は、古いアイデンティティ ソースではなく新しいアイデンティティ ソース内でユーザーを検索するように管理者に伝達する必要があります。

LDAP ディレクトリ内のユーザーの変更

ユーザーのユーザー ID が LDAP ディレクトリ側で変更された場合、Authentication Manager がその変更を自動検出してユーザーデータを更新できるのは、次のいずれかの場合です。

- スケジュール クリーンアップが実行された場合。
- すべてのアイデンティティ ソースか、またはそのユーザーが格納されているアイデンティティ ソースに対して、管理者が手動クリーンアップを実行した場合。
- 管理者が Security Console でそのユーザーのレコードを変更した場合。
- ユーザーが古いユーザー ID で認証を試みた場合。

ディレクトリ側でユーザー ID が変更されると、Authentication Manager に次のような影響が生じます。

- そのユーザーの最初の認証が失敗する可能性があります。

  他のイベントによりユーザー ID が更新される前にユーザーが認証を試みた場合に、認証が失敗することがあります。ユーザーがアクセスを拒否された場合は、変更後の最初の認証には古いユーザー ID を使用し、それ以降の認証には常に新しいユーザー ID を使用するように指示してください。

  ユーザー ID がユーザーのメールに関連づけられている場合、初回の認証が失敗する可能性は低くなります。

- Security Console では、新しいユーザー ID が即時に認識されます。

  ユーザー ID の変更により何らかの問題が生じて管理者による対処が必要になった場合は、古いユーザー ID ではなく新しいユーザー ID でユーザーを検索するように管理者に伝達してください。

  管理者がユーザー レコードの表示など、ユーザーを管理する操作を実行すると、ユーザー ID が更新され、ユーザーが新しいユーザー ID で認証を受けることが可能になります。

- Sun Java System Directory Server/Oracle Directory Server Enterprise Edition アイデンティティ ソース内でデフォルト設定が使用されている場合は、制限付きエージェントで認証ができなくなる可能性があります。

  Sun Java System Directory Server/Oracle Direcory Server Enterprise Edition のデフォルト設定では、uid 属性をネーミング属性として使用します。Authentication Manager のデフォルト設定では、ユーザー ID を uid 属性にマッピングします。Sun Java System Directory Server/Oracle Directory Server Enteprise Edition アイデンティティ ソースでこれらのデフォルト設定が構成されている場合は、ユーザー ID（UID）が変更されると、ユーザーの識別名も変更されるため、そのユーザーの LDAP グループ メンバーシップがすべて削除されます。

DN が変更されたユーザーが、制限付きエージェントでの認証が許可されたグループに所属していた場合、ユーザーは、制限付きエージェントで認証できなくなります。ユーザーが引き続き制限付きエージェントを通じて認証を受けることができるようにするには、制限付きエージェントに関連づけられているグループにユーザーを再追加する必要があります。

LDAP ディレクトリ内のグループ メンバーシップの変更

パフォーマンスを最適化し、Authentication Manager と LDAP ディレクトリの間のトラフィックを最小限にするために、Authentication Manager はユーザーのグループ メンバーシップに関する情報をキャッシュします。ユーザーのグループ メンバーシップが LDAP ディレクトリで変更された場合、キャッシュを更新するまで、Authentication Manager はその変更を認識できません。変更内容は、キャッシュ更新間隔の時間が経過した後、有効になります。変更されてからキャッシュ更新までの間、次の状況が発生する可能性があります。

- 制限付きエージェントへのアクセス権を持つグループに追加されたユーザーが、制限付きエージェントで認証できない。
- 制限付きエージェントへのアクセス権を持つグループから削除されたユーザーが、制限付きエージェントで引き続き認証できる。

キャッシュは、Operations Console を使用してただちにフラッシュできます。詳細については、423 ページのキャッシュのフラッシュを参照してください。

キャッシュの構成の詳細については、RSA Security Console ヘルプのトピック「Configure the Cache（キャッシュの構成）」を参照してください。

7 RSA Authentication Manager の管理

システム管理の委任

スーパー管理者と Operations Console 管理者が、Authentication Manager システム コンポーネントを保守します。

スーパー管理者

スーパー管理者は、導入環境のすべてのレルムとセキュリティ ドメインに対する完全な管理者権限を持つ唯一のロールです。スーパー管理者は、他の管理者、セキュリティ ドメイン階層を作成し、アイデンティティ ソースを導入環境にリンクします。

Operations Console 管理者

Operations Console 管理者は、Operations Console へのアクセス権もつ管理者アカウントです。Operations Console 管理者は、スーパー管理者がシステムにアクセスできない場合にスーパー管理者アカウントをリストアするなど、重要なコマンド ライン ユーティリティの手順を実行できます。

スーパー管理者のロールと同様に、Operations Console 管理者アカウントは最も信頼できる管理者にのみ付与する必要があります。多くの Operations Console タスクには、スーパー管理者と Operations Console 管理者の両方のクレデンシャルが必要です。

初期 Operations Console 管理者アカウントは Quick Setup 中に作成します。Operations Console 管理者は Security Console で作成および管理できます。Operations Console 管理者アカウントを表示または管理できるのは、スーパー管理者だけです。同様に、スーパー管理者をリストアできるのは、Operations Console 管理者のクレデンシャルを持つユーザーだけです。

Authentication Manager では、ユーザー データベースと別の場所に Operations Console 管理者アカウントを格納します。Operations Console 管理者には、パスワード ポリシーは適用されません。

システム管理者アカウント

次のアカウントは、Authentication Manager 導入環境の変更、保守、修復を行う権限を持っています。これらのアカウントは Quick Setup 中に作成されます。

- Authentication Manager 管理者アカウント
- アプライアンス オペレーティング システム アカウント

これらのアカウントのログオン クレデンシャルを媒体に記録する場合は、保存方法と保存場所が安全であることを確認します。

Authentication Manager 管理者アカウント

次の表に、Authentication Manager の管理者アカウントを示します。プライマリ インスタンスを導入する管理者が、Quick Setup 中にこれらのアカウントを作成します。

名前	権限の内容	管理
スーパー管理者	スーパー管理者は、導入環境内のすべてのセキュリティ ドメインで完全な管理者権限を持ち、Security Console 内のすべての管理タスクを実行できます。	すべてのスーパー管理者は、Security Console で他のスーパー管理者ユーザーを作成できます。 Operations Console 管理者は、すべてのスーパー管理者アカウントがシステムにアクセスできなくなった場合にいずれかのスーパー管理者アカウントをリストアできます。

名前	権限の内容	管理
Operations Console 管理者	Operations Console 管理者は Operations Console 内の管理タスクを実行できます。また、コマンド ライン ユーティリティを使用して、スーパー管理者アカウントのリストアなどの処理を実行できます。コマンド ライン ユーティリティを使用するには、アプライアンス オペレーティング システム アカウントのパスワードが必要です。 **注：**Operations Console の一部のタスクの実行には、スーパー管理者のクレデンシャルも必要になります。Operations Console が許可するのは、ユーザーレコードが内部データベースに格納されたスーパー管理者のみです。	すべてのスーパー管理者は、Security Console で Operations Console 管理者を作成して管理できます。たとえば、紛失した Operations Console 管理者パスワードを復旧することはできませんが、スーパー管理者であれば新しいパスワードを作成できます。 Operations Console 管理者アカウントは、Authentication Manager 内部データベースの外に格納されます。そのため、データベースが接続不能になっても、Operations Console 管理者は引き続き Operations Console とコマンド ライン ユーティリティにアクセスできます。

スーパー管理者と非管理者ユーザーのユーザー ID は同じ規則で検証されます。有効なユーザー ID は一意の識別子でなければならず、1 ～ 255 文字の ASCII 文字を使用できます。&、%、>、<、' の各文字は使用できません。

Operations Console 管理者の有効なユーザー ID は一意の識別子でなければならず、1 ～ 255 文字の ASCII 文字を使用できます。@、~ の各文字とスペースは使用できません。

注：Operations Console を使用するユーザーごとに Operations Console 管理者アカウントを作成します。複数の管理者の間で、アカウント情報（特にパスワード）を共有しないでください。

アプライアンス オペレーティング システム アカウント

アプライアンス オペレーティング システム アカウントのユーザー ID は rsaadmin です。このユーザー ID は変更できません。オペレーティング システム アカウントのパスワードは、Quick Setup 中に指定します。このアカウントは、高度な保守またはトラブルシューティング タスクの実行時にオペレーティング システムにアクセスするために使用します。

すべてのアプライアンスには root ユーザー アカウントもあります。このアカウントは通常のタスクでは必要ありません。このアカウントを使用してアプライアンスにログオンすることはできません。

オペレーティング システムには、SSH（Secure Shell）または VMware vSphere Client を使用してアクセスできます。SSH でアプライアンス オペレーティング システムにアクセスするには、事前に Operations Console を使用してアプライアンスの SSH を有効化する必要があります。手順については、455 ページのアプライアンスの SSH の有効化を参照してください。

Operations Console 管理者は、rsaadmin のパスワードを変更できます。手順については、Operations Console ヘルプ トピックの「Change the Operating System Account Password（オペレーティング システム アカウントのパスワードの変更）」を参照してください。

セキュリティ上の理由から、オペレーティング システム パスワードを復旧するためのユーティリティは提供していません。

スーパー管理者の追加

各導入環境には、少なくとも 1 人のスーパー管理者が必要です。管理上の役割を分担するために、別のユーザーをスーパー管理者として割り当てることができます。スーパー管理者の追加は Security Console で行います。

開始する前に

この手順を実行するユーザーは、スーパー管理者であることが必要です。

手順

1. Security Console で、**［Identity（アイデンティティ）］＞［Users（ユーザー）］＞［Manage Existing（既存項目の管理）］**の順にクリックします。
2. 検索フィールドを使用して、スーパー管理者ロールを割り当てるユーザーを検索します。
3. そのユーザーをクリックし、**［Administrative Roles（管理者ロール）］**を選択します。
4. **［Assign Role（ロールの割り当て）］**＞**［SuperAdminRole］**＞**［Assign Role（ロールの割り当て）］**の順にクリックします。

Operations Console 管理者の追加

Operations Console 管理者は、Operations Console で管理タスクを実行する権限といくつかのコマンド ライン ユーティリティを実行する権限が与えられたユーザーです。Operations Console 管理者は、Security Console で作成します。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、［**Administration（管理）**］＞［**Manage OC Administrators（OC 管理者の管理）**］の順にクリックします。
2. ［**Add New（新規追加）**］をクリックします。
3. ［**Create User ID（ユーザー ID の作成）**］フィールドに、Operations Console 管理者のユーザー ID を入力します。ユーザー ID は、1 ～ 255 文字で指定する必要があります。ユーザー ID には、スペース、@、~ を除く ASCII 文字のみを含めることができます。
4. ［**Create Password（パスワードの作成）**］フィールドに、Operations Console 管理者のパスワードを入力します。パスワードは、8 ～ 32 文字で指定する必要があります。パスワードには、1 文字以上の英字と 1 文字以上の特殊文字を含める必要があります。パスワードには、スペース、@、~ を除く ASCII の文字のみを含めることができます。ユーザー ID と同じパスワードを指定することはできません。
5. ［**Confirm Password（パスワードの確認）**］フィールドにパスワードをもう一度入力します。
6. ［**Save（保存）**］をクリックします。

注： 新しい Operations Console 管理者のアカウントがレプリカ インスタンスにレプリケーションされるのに 15 ～ 30 分かかる場合があります。

Operations Console

Operations Console は、次の Authentication Manager コンポーネントの追加および管理に使用します。

- アイデンティティ ソース
- インスタンス
- 証明書

- Web Tier
- ネットワーク設定

Operations Console を使用して、導入環境データのバックアップを作成し、リストアにより、応答しなくなったインスタンスを修復することもできます。

Operations Console へのログオン

Operations Console にログオンするには、Operations Console 管理者のクレデンシャルが必要です。初期の Operations Console 管理者アカウントは、Quick Setup で作成されます。スーパー管理者は、追加の Operations Console 管理者アカウントを作成することができます。

Operations Console のページのナビゲーションは、ブラウザのナビゲーション機能ではなく、Operations Console のメニューおよびボタンを使用するようにしてください。

開始する前に

Operations Console 管理者のクレデンシャルが必要です。

手順

1. ブラウザを開きます。
2. 次の URL にアクセスします。

   ```
   https:// 完全修飾
   ホスト名 :7072/operations-console/
   ```

   完全修飾ホスト名には、アプライアンスの FQHN を指定します。

セッション有効期間の制限

セッション有効期間は、セッション継続時間を定義します。管理者がセッションを無期限に開かれたままにすると、不正アクセスの危険がありますが、セッション有効期間によりこれを防ぐことができるため、重要なセキュリティ機能と言えます。セッション有効期間を編集する場合は、最長セッション有効期間や、セッションが自動的に閉じられるまでの許容アイドル時間などの設定を変更できます。

管理者が SecurityConsole、Operations Console、Self-Service Console にログオンするたびに、次のセッションが作成されます。

- ログオン セッション
- EAP32 セッション
- コンソールおよびコマンド API セッション

同時にログオンできる管理者は最大 10 人です。

プライマリ インスタンスとレプリカ インスタンスにそれぞれ異なるセッション属性を設定できます。

ログオン セッション

ログオン セッションの設定により、認証プロセスの途中で放置されたセッションや、認証プロセスが完了していないセッションの有効期間が制御されます。次のタイプのログオン セッションに影響します。

- Security Console（管理者）
- Operations Console（管理者）
- Self-Service Console（管理者以外）
- リスク ベース認証を行うユーザー（管理者以外）

これらの設定のデフォルト値は、アイドル タイムアウトが 3 分、最長有効期間が 8 分です。

EAP32 セッション

EAP（拡張認証プロトコル）セッションの設定により、EAP32 セッションの初回セッション有効期間が制御されます。

コンソールおよびコマンド API セッション

コンソールおよびコマンド API セッションの設定により、Web ベース コンソールまたはコマンド API（Application Programming Interface）を経由した、管理者の認証済みのアクティブなセッションが制御されます。デフォルト設定は、アイドル タイムアウトが 30 分、最長有効期間が 8 時間です。

Authentication Manager の Web ベース管理コンソールは、Security Console と Operations Console です。コマンド API は、Authentication Manager システムとやり取りするカスタム ソフトウェア アプリケーションの開発を担当するプログラマ、Web 開発者、システム エンジニアが使用します。コマンド API の詳細については、「RSA Authentication Manager 8.0 Developer's Guide」を参照してください。

セッション有効期間の制限のタイプ

セッションの設定は、Web ベース管理コンソール、「RSA Authentication Manager 8.0 Developer's Guide」に記載されているコマンド API インタフェース、エンド ユーザーによる RBA（リスク ベース認証）ログオン試行のそれぞれのログオン ページに適用されます。セッションがタイムアウトするか、最長有効期間に達すると、ログオン ページが再表示され、ユーザーは再度ログオンしなければなりません。

管理者は、セッションに関する次の設定を構成できます。

［**Time-out（タイムアウト）**］：指定した期間非アクティブな状態が続くと、セッションが終了します。デフォルト設定は 30 分です。

［**Maximum Lifetime（最長有効期間）**］：セッションの最長期間です。コンソール セッションが最長有効期間に達すると、アクティブかどうかにかかわらずセッションは終了し、管理者はログオフされます。デフォルト設定は 8 時間です。

最長有効期間の設定は、セッションの非アクティブ状態を考慮しません。たとえば、コンソールおよびコマンド API セッション有効期間が 8 時間に設定されていれば、管理者はセッションを開始してから 8 時間後に自動的にログオフされます。そのセッション中に非アクティブな時間があったかどうかは考慮されません。

コンソールおよびコマンド API セッションの設定を変更できるのはスーパー管理者のみです。

セッション有効期間の設定の編集

セッション有効期間を編集する場合は、セッションの最長有効期間や、セッションが自動的に閉じられるまでのアイドルタイム アウトなどの設定を変更できます。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。
2. ［Console & Session Settings（コンソールとセッションの設定）］で、［**Session Lifetime（セッション有効期間）**］をクリックします。
3. 編集するセッション タイプをクリックし、コンテキスト メニューから［**Edit（編集）**］を選択します。
4. ［**Session Lifetime Settings（セッション有効期間の設定）**］セクションで、次の操作を実行します。
   a. 非アクティブな状態が一定期間継続した場合にセッションをタイムアウトする場合は、［**Time out idle sessions（アイドル セッションのタイムアウト）**］を選択し、タイムアウトまでの時間を入力します。
   b. ［**Limit session lifetime（セッション有効期間の制限）**］を選択し、セッションの最長有効期間を入力します。
5. ［**Save（保存）**］をクリックします。

アイデンティティ ソース プロパティの更新

アイデンティティ ソースを Authentication Manager にリンクした後で、アイデンティティ ソースのプロパティを更新する必要が生じる場合があります。アイデンティティ ソース プロパティのディレクトリ構成マッピング セクションの設定により、アイデンティティ ソースのフィールドを、内部データベースで使用できるようになります。Operations Console を使用してディレクトリ構成マッピングを編集します。

Security Console を使用して、カスタム ユーザー属性を作成することもできます。Security Console を使用して、カスタム ユーザー属性のアイデンティティ属性定義を編集します。詳細については、RSA Security Console ヘルプのトピック「Edit Identity Attribute Definitions（アイデンティティ属性定義の編集）」を参照してください。

手順

1. ユーザー ID のマッピングを変更する予定の場合は、Authentication Manager とアイデンティティ ソースをリンク解除します。操作手順については、197 ページのシステムからのアイデンティティ ソースのリンク解除を参照してください。
2. アイデンティティ ソース プロパティを編集します。操作手順については、198 ページのアイデンティティ ソースの編集を参照してください。
3. アイデンティティ ソースをリンク解除してユーザー ID のマッピングを変更した場合は、編集が終わった後、アイデンティティ ソースを Authentication Manager に再リンクします。操作手順については、199 ページのアイデンティティ ソースとシステムのリンクを参照してください。

システムからのアイデンティティ ソースのリンク解除

アイデンティティ ソースをシステムにリンクすると、そのアイデンティティ ソース内のすべてのユーザーおよびユーザー グループを Security Console で表示して管理できるようになります。アイデンティティ ソースをリンク解除すると、これらのユーザーおよびユーザー グループは Security Console で管理できなくなります。

アイデンティティ ソースを再度リンクしたときに、そのアイデンティティ ソースのすべてのユーザーは再度解決可能になります。Authentication Manager は、リンク解除操作の前と同じように、これらのユーザーを検出できるようになります。

開始する前に

スーパー管理者である必要があります。

注：内部データベースおよび自分が属するアイデンティティ ソースはリンク解除できません。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Identity Sources（アイデンティティ ソース）**] > [**Link Identity Source to System（システムへのアイデンティティ ソースのリンク）**] の順にクリックします。
2. [**Link Identity Source（アイデンティティ ソースのリンク）**] セクションにあるリンクされたアイデンティティ ソースのリストから、リンク解除するアイデンティティ ソースを選択し、左矢印をクリックしてリンク解除します。
3. [**Save（保存）**] をクリックします。
4. [Unlink Identity Source Confirmation（アイデンティティ ソースのリンク解除確認）] の画面で、[**Yes, unlink the identity source(s)（はい、アイデンティティ ソースをリンク解除します）**] を選択します。
5. [**Unlink（リンク解除）**] をクリックします。

次のステップ

アイデンティティ ソースのユーザー属性マッピングを編集します。操作手順については、198 ページのアイデンティティ ソースの編集を参照してください。

アイデンティティ ソースの編集

アイデンティティ ソースをシステムにリンクする前または後で、アイデンティティ ソースのプロパティを編集できます。ユーザー ID のマッピングを編集する前に、Authentication Manager からアイデンティティ ソースのリンクを解除する必要があります。

重要：アイデンティティ ソースのプロパティを編集するときは十分に注意してください。アイデンティティ ソースの範囲を縮小したり、ユーザー ID を再マッピングする場合は、116 ページのアイデンティティ ソースのプロパティを参照してください。

開始する前に

スーパー管理者である必要があります。

手順

1. プライマリ インスタンスの Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Identity Sources（アイデンティティ ソース）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力します。

3. 編集するアイデンティティ ソースをクリックして、[**Edit（編集）**]を選択します。
4. [**Connection(s)（接続）**]タブまたは[**Map（マップ）**]タブをクリックして、プロパティを表示します。フィールドに対して必要な変更を行います。各フィールドの詳細については、116 ページのアイデンティティ ソースのプロパティを参照してください。
5. 以下のいずれかをクリックします。
   - [**Reset（リセット）**]。保存していない場合は、[**Reset（リセット）**]をクリックして、アイデンティティ ソースを編集前の状態にリセットできます。
   - [**Save（保存）**]。クリックして変更を保存すると、確認メッセージが表示されます。
   - [**Save and Finish（保存して終了）**]。クリックして変更内容を保存すると、アイデンティティ ソースのリストが示され、確認メッセージが表示されます。

次のステップ

変更によってユーザーまたはグループのセットに変更が生じる場合は、アイデンティティ ソースのリンク解除、手動クリーンアップの実行、アイデンティティ ソースの再リンクが必要になる場合があります。詳細については、175 ページの LDAP ディレクトリ内のユーザー データを参照してください。

アイデンティティ ソースとシステムのリンク

すべての LDAP ディレクトリ アイデンティティ ソースをシステムにリンクする必要があります。リンク後、アイデンティティ ソースのすべてのユーザーを、Security Console で表示および管理することができます。ユーザーはデフォルトで最上位のセキュリティ ドメインに表示されますが、必要に応じて他のセキュリティ ドメインに移動することもできます。さらに、システムを構成して、アイデンティティ ソースのユーザーを特定のセキュリティ ドメインに自動的に配置することができます。詳細については、46 ページのデフォルトセキュリティ ドメイン マッピングを参照してください。

開始する前に

- スーパー管理者である必要があります。
- Active Directory グローバル カタログをリンクする場合は、ユーザー データをそのグローバル カタログにレプリケーションする各アイデンティティ ソースもリンクする必要があります。たとえば、アイデンティティ ソース IS1 と IS2 が情報をグローバル カタログ GC1 にレプリケーションし、GC1 をアイデンティティ ソースとしてリンクする場合は、IS1 と IS2 もシステムにリンクする必要があります。

手順

1. スーパー管理者として Security Console にログオンします。
2. ［**Setup（セットアップ）**］＞［**Identity Sources（アイデンティティ ソース）**］＞［**Link Identity Source to System（アイデンティティ ソースをシステムにリンク）**］をクリックします。
3. 使用可能なアイデンティティ ソースの一覧から、リンクするアイデンティティ ソースを選択し、右矢印をクリックします。
4. ［**Save（保存）**］をクリックします。

LDAP ディレクトリ アイデンティティ ソースの検証

アイデンティティ ソースを正しく追加およびリンクできているかどうかを検証するために、Security Console を使用してアイデンティティ ソースのユーザーおよびグループを表示します。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドで適切なアイデンティティ ソースを選択し、［**Search**（検索）］をクリックします。
3. LDAP ディレクトリ アイデンティティ ソースのユーザーが一覧表示されます。

SSL 証明書の管理

SSL（Secure Sockets Layer）は、RSA Authentication Manager の管理とレプリケーションに使用する通信ポートに対してデフォルトで有効になっています。Authentication Manager インスタンスの導入時に、長期使用可能な SSL 証明書によって通信が保護されます。この証明書は導入環境ごとに一意で、内部 RSA 認証局（CA）によって署名されます。

この SSL 証明書は内部 RSA CA によって署名されるため、ブラウザによっては、証明書を確認できないとの警告メッセージが出される場合があります。これは予期された動作です。

続行するには、ブラウザで提供されている、信頼できないサイトへの接続を許可するオプションをクリックします。たとえば、ブラウザによっては、「危険性を理解した上で接続する」などのリンクをクリックするように求められる場合があります。

この警告メッセージが表示されるのを防ぐには、内部 RSA CA を、ブラウザが信頼するルート証明機関のリストに追加するか、証明書を、ブラウザが信頼する認証局によって署名された証明書に置き換える必要があります。

内部 RSA CA を、ブラウザが信頼するルート証明機関のリストに追加する手順については、ブラウザのマニュアルを参照してください。

コンソール証明書

RSA Authentication Manager のインスタンスの導入時に、ブラウザと Security Console、Operations Console、Self-Service Console の間の通信は、長期間有効な SSL（Secure Socket Layer）証明書によってセキュリティが保護されます。この証明書は、内部の RSA CA（認証局）によって署名されます。この CA は自己署名認証局であるため、このデフォルトの証明書を検証できないという警告メッセージがブラウザに表示される場合があります。

コンソール証明書をサードパーティの CA が発行した証明書に交換することも選択できます。ただし、コンソールの証明書を交換する必要があるのは、次の理由がある場合です。

- ネットワーク ポリシーにより、別の CA が発行した証明書を使用する必要がある。
- 既存の証明書が期限切れである。

サードパーティの CA から取得した証明書チェーンに含まれる各 X.509 バージョン 3 CA 証明書の基本制限拡張フィールドでは、CA フラグが TRUE に設定されている必要があります。基本制限拡張フィールドの設定が適切でない X.509 バージョン 3 CA 証明書がチェーン内にある場合、Authentication Manager はこの証明書を拒否します。この状態になった場合は、認証局に連絡し、問題を解決してください。

サードパーティの CA が発行した証明書の有効期限は 1 ～ 2 年しかない可能性があります。サードパーティの証明書は、有効期限が切れる前に交換する必要があります。コンソール証明書の有効期限が切れると、Authentication Manager サービスを停止後に起動できなくなります。

証明書の有効期限が切れたインスタンスでサービスを停止した場合は、その期限切れの証明書を、インスタンスの導入時にインストールされたデフォルトの証明書に交換する必要があります。操作手順については、206 ページの有効期限の切れたコンソール証明書の置換を参照してください。

置換処理の概要については、201 ページのコンソール証明書の置換を参照してください。

コンソール証明書の置換

この手順を完了すると、ブラウザと Security Console、Operations Console、Self-Service Console との通信のセキュリティを保護するために使用する既存の SSL（Secure Socket Layer）証明書を置き換えることができます。

既存の SSL 証明書の置き換えが必要なインスタンスで、これらのタスクを実行します。

開始する前に

- Operations Console 管理者である必要があります。
- CA（認証局）に問い合わせて、CSR（証明書署名リクエスト）に必要な情報を確認し、情報を準備します。

手順

1. 次のいずれかを実行して、CSR を生成します。
   - Operations Console を使用し、RSAAuthentication Manager で鍵ペアおよび CSR を生成します。操作手順については、202 ページの Operations Console による証明書署名リクエストの生成を参照してください。
   - 任意のサード パーティ ツールを使用して、鍵ペアおよび CSR を生成します。
2. CSR を CA に送信し、SSL サーバ証明書をリクエストします。
   - CA で SSL サーバ証明書のオプションが用意されていない場合は、証明書の拡張鍵使用法に「鍵暗号化」を指定するようリクエストしてください。
   - 鍵アルゴリズムは RSA 公開鍵である必要があります。
3. 証明書ファイル（.cer または .p7b）を CA からダウンロードします。証明書ファイルには、通常、証明書の完全な署名チェーンが含まれています。
   - 発行された証明書のサブジェクトには、CN（共通名）として、SSL 証明書を置き換えるインスタンスの FQHN（完全修飾ホスト名）の値が指定されている必要があります。
   - 証明書ファイルに、署名チェーンのすべての証明書が含まれていない場合は、証明書の完全な署名チェーンを 1 ファイルで、または個別にダウンロードする必要があります。
4. サード パーティ ツールを使用して CSR を生成した場合は、CA から発行された証明書および新しい証明書の秘密鍵を含む、PKCS#12 ファイル（.pfx または .p12）を作成します。
5. 204 ページのコンソール証明書のインポートを参照してください。
6. 205 ページの新しい SSL コンソール証明書のアクティブ化を参照してください。

Operations Console による証明書署名リクエストの生成

コンソール証明書をサード パーティ CA（認証局）が発行する証明書で置き換えるには、CSR（証明書署名リクエスト）を生成し、CA に送信する必要があります。次のような理由で、コンソール証明書を置き換えることが必要な場合があります。

- ネットワーク ポリシーにより、別の CA により発行された証明書を使用する必要がある。
- 既存の証明書が期限切れである。

CSR を CA に送信して、署名済み証明書を取得します。CSR は Operations Console を使用して生成します。

開始する前に

- Operations Console 管理者である必要があります。
- CA に問い合わせて、CSR に必要な情報を確認し、情報を準備します。

手順

1. Operations Console で、**［Deployment Configuration（導入環境の構成）］＞［Certificates（証明書）］＞［Console Certificate Management（コンソール証明書の管理）］**の順にクリックします。
2. ［Console Certificate Management（コンソール証明書の管理）］ページで、**［Generate CSR（CSR の生成）］**をクリックします。
3. ［Generate Certificate Signing Request（証明書署名リクエストの生成）］ページの**［Certificate Basics（証明書の基本設定）］**で、必須情報を入力します。
   CA によっては、次の情報の一部またはすべてを入力する必要があります。
   - **（必須）［Alias（エイリアス）］**：証明書の名前です。この名前は、［Console Certificate Management（コンソール証明書の管理）］ページの［Alias（エイリアス）］列に表示されます。使用できる文字は、a ～ z、A ～ Z、スペース、コンマのみです。
   - **［Country Name（国名）］**：組織の所在地の国です。CA に送信する値は、2 文字の国コードです。
   - **［State or Province Name（都道府県名）］**：組織がの所在地の都道府県名です。
   - **［City or Locality Name（市区町村名）］**：組織の所在地の市区町村名です。
   - **［Organization Name（組織名）］**：組織の正式名称です。
   - **［Organizational Unit Name（部門名）］**：証明書を注文する組織の部門です（たとえば、エンジニアリング、経理、マーケティングなど）。
   - **［E-mail Address（メール アドレス）］**：検証に使用する正式なメールアドレスです（administrator@mycompany.com など）。
4. **［Generate File（ファイルの生成）］**をクリックします。
5. **［Download File（ファイルのダウンロード）］**ページで、**［Download（ダウンロード）］**をクリックします。
6. ブラウザ プロンプトに従い、CSR ファイルを保存します。
7. **［Download File（ファイルのダウンロード）］**ページで、**［Done（完了）］**をクリックします。

コンソール証明書のインポート

CA（認証局）の署名チェーンに含まれる証明書をすべてインポートした後で、新しい SSL（Secure Socket Layer）証明書で既存の証明書を置き換えることができます。

開始する前に

- Operations Console 管理者である必要があります。
- CSR（証明書署名リクエスト）を作成して CA に送信します。
- CA ルート証明書をダウンロードします。
- SSL 証明書に完全な証明書チェーンが含まれていない場合は、署名チェーンに含まれる他の CA の証明書をすべてダウンロードします。
- SSL 証明書をダウンロードします。

手順

1. Operations Console で、**［Deployment Configuration（導入環境の構成）］＞［Certificates（証明書）］＞［Console Certificate Management（コンソール証明書の管理）］**の順にクリックします。
   次のステップを実行し、まず最初にルート証明書をインポートします。続けて、署名チェーンの各証明書を順番にインポートします。
2. ［Console Certificate Management（コンソール証明書の管理）］ページで、**［Import Certificate（証明書のインポート）］**をクリックします。
3. ［Import Certificate（証明書のインポート）］ページの**［Certificate Basics（証明書の基本設定）］**で、次のいずれかを実行します。
   Operations Console で作成した CSR に対して発行されたコンソール証明書の場合
   - **［Import Certificate（証明書のインポート）］**フィールドで、証明書ファイルの場所を参照します。このファイルには、CA から入手した CA ルート証明書または SSL 証明書が含まれています。
   - **［Type of Certificate to Import（インポートする証明書のタイプ）］**で、**［PKCS #7 (*.cer or *.p7b)］**を選択します。

   他の証明書ツールで作成した CSR に対して発行されたコンソール証明書の場合
   - **［Import Certificate（証明書のインポート）］**フィールドで、証明書ファイルの場所を参照します。このファイルには、1 個以上の証明書および新しい証明書のための秘密鍵が含まれています。以下のいずれかの操作を実行します。
     - SSL 証明書ファイルに、CA ルート証明書までの完全な証明書チェーンが含まれている場合は、PKCS #12 ファイルをインポートします。**［Password（パスワード）］**フィールドに、PKCS#12 ファイルのパスワードを入力します。

– SSL 証明書ファイルに、CA ルート証明書までの完全な証明書チェーンが含まれていない場合は、PKCS #12 ファイルの SSL 証明書をインポートする前に、PKCS #7 ファイルで証明書チェーンに含まれるすべての CA 証明書をインポートします。［**Password（パスワード）**］フィールドに、PKCS#12 ファイルのパスワードを入力します。

4. ［**Import**（インポート）］をクリックします。

次のステップ

新しい証明書をアクティブ化し、既存の SSL 証明書を置き換えます。操作手順については、205 ページの新しい SSL コンソール証明書のアクティブ化を参照してください。

新しい SSL コンソール証明書のアクティブ化

RSA Authentication Manager のインスタンスを導入する際、Security Console、Operations Console、Self-Service Console の各コンソールとブラウザの間の通信は、有効期間の長い SSL（Secure Socket Layer）証明書で保護されます。コンソール証明書を置換するため新しい証明書をインポートした場合は、その新しい証明書をアクティブ化し、使用できるようにする必要があります。

SSL（Secure Socket Layer）証明書をアクティブ化するには、証明書のサブジェクト フィールドの CN（共通名）として、管理対象のインスタンスの FQHN（完全修飾ホスト名）が含まれていなければなりません。

開始する前に

- スーパー管理者であり、Operations Console 管理者でもあること。
- アクティブ化する SSL 証明書をインポートするには、204 ページのコンソール証明書のインポートを参照してください。

手順

1. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Certificates（証明書）**］＞［**Console Certificate Management（コンソール証明書の管理）**］の順にクリックします。
2. ［Console Certificate Management（コンソール証明書の管理）］ページの［**Alias（エイリアス）**］列で、新しい SSL 証明書の名前をクリックします。
3. コンテキスト メニューから［**Activate（アクティブ化）**］を選択します。
4. ［Activate Certificate Confirmation（証明書のアクティブ化の確認）］ページで、［**Certificate Details（証明書の詳細）**］を確認し、正しい証明書を選択していることを確かめます。

5. ［**Yes, make this the active certificate（はい、この証明書をアクティブにします）**］を選択し、［**Activate Certificate（証明書のアクティブ化）**］をクリックします。
   証明書がアクティブ化されたら、アプライアンス サービスが自動的に再起動し、アクティブ化処理が完了します。これには数分かかる場合があります。
6. すべてのサービスが開始されたら、Operations Console にログオンします。
7. Operations Console で、［**Deployment Configuration（導入構成）**］＞［**Certificates（証明書）**］＞［**Console Certificate Management（コンソール証明書の管理）**］の順にクリックし、新しい証明書のステータスが［**Active（アクティブ）**］になっていることを確認してください。

有効期限の切れたコンソール証明書の置換

オリジナルのコンソール証明書をサード パーティの CA（認証局）によって発行された証明書に置換した場合は、そのサード パーティの証明書が有効期限切れになる前に交換する必要があります。コンソール証明書の有効期限が切れると、Authentication Manager サービスを停止後に起動できなくなります。

証明書の有効期限が切れた導入環境で Authentication Manager サービスを停止した場合は、次の手順を実行してサービスを起動します。

手順

1. SSH クライアントまたは VMware vSphere Client を使用して、ユーザー ID rsaadmin と現在のオペレーティング システム パスワードでアプライアンスにログオンします。
2. ディレクトリを utils に変更します。次のように入力します。

   ```
   cd /opt/rsa/am/utils
   ```

   Enter キーを押します。
3. 次のコマンドを実行して、コンソール証明書をサード パーティの証明書からオリジナルの証明書に変更します。次のように入力し、Enter キーを押します。

   ```
   ./rsautil reset-server-cert -u oc_admin_UserID
   -p oc_admin_password
   ```

   各パラメータの意味を以下に示します。
   - oc_admin_UserID は Operations Console 管理者のユーザー名
   - oc_admin_password は Operations Console 管理者のパスワード

次のステップ

Authentication Manager サービスを起動します。操作手順については、458 ページの RSA Authentication Manager サービスの手動での管理を参照してください。

ライセンス

各 Authentication Manager 導入環境には、ライセンスがインストールされている必要があります。このライセンスは、Authentication Manager アプライアンスを使用する権利を付与します。

次のライセンス タイプがあります。

Base Server：Authentication Manager の 1 つのプライマリ インスタンスと 1 つのレプリカ インスタンスを許可する永久ライセンス。

Enterprise Server：Authentication Manager の 1 つのプライマリ インスタンスと最大 15 個のレプリカ インスタンスを許可する永久ライセンス。Enterprise Server ライセンスには、トークンのプロビジョニング機能も含まれます。

各ライセンス タイプは、インストール可能な Authentication Manager のインスタンス数を制限します。ユーザー数の制限は、お客様の要件により異なります。

たとえば、従業員数 10,000 人のお客様の場合は、現在の従業員に加えて、将来的に雇用することになる従業員の数を考慮に入れて、11,000 ユーザー分のライセンスを購入されることが考えられます。

次の点を理解しておくことが重要です。

- 複数のライセンスをインストールできます。
- アカウント ID は、すべてのライセンスで同じである必要があります。
- ライセンス ID はスタック ID とも呼ばれ、各ライセンスで一意である必要があります。同じ ID のライセンスを 2 回インストールすることはできません。
- ライセンスの対象としてカウントされるのは、トークンが割り当てられているユーザーだけです。複数のトークンを割り当てられたユーザーは、1 回だけカウントされます。
- Security Console には、ユーザー数制限が近づくと警告メッセージが表示されます。メッセージが表示されるのは、ユーザー数制限が 85、95、100% を超えたときです。
- ユーザー カウントは毎時間システムによって更新されます。また、ユーザーが Security Console で［License Status（ライセンス ステータス）］ページを表示する度に更新されます。

次の表は、各ライセンス タイプの属性を示しています。

ライセンス機能	Base Server	Enterprise Server
トークンを割り当てるユーザー数	購入時にお客様が指定	購入時にお客様が指定
インスタンス数	2[1]	16（1 つのプライマリ インスタンスと 15 のレプリカ インスタンス）
RBA/ODA	オプション	オプション
事業継続	オプション	オプション
RADIUS	はい	はい
オフライン認証	はい	はい
トークン	はい	はい
セルフ サービス	はい	はい
トークン プロビジョニング	いいえ	はい

[1] インスタンス数が 2 までに制限されたライセンスでも、災害復旧用として 3 番目のインスタンスを使用できます。

事業継続オプションでは、ライセンスで通常許可されるユーザー数を超えるユーザーに一時的に RSA SecurID 認証を使用させることができます。RSA では、事業継続オプションを使用して作成したユーザーについては、トークンを割り当てて送付する必要が生じないように、On-Demand トークンコードの受信を有効にすることを推奨します。ただし、必要に応じて、RSA SecurID トークンをこれらのユーザーに割り当てることもできます。

特定の機能を追加したり、ユーザー数を追加する必要がある場合は、追加のライセンスを取得する必要があります。

手順については、ライセンスのインストールおよびインストール済みライセンスの表示を参照してください。

ライセンスのインストール

次のいずれかのタスクを実行する場合は、新しいライセンスをインストールする必要があります。

- 評価版ライセンスから Base Server ライセンスまたは Enterprise Server ライセンスにアップグレードする。
- 既存のライセンスの制限および機能をアップグレードする。

ライセンスを購入すると、XML ライセンス ファイルを含む .zip ファイルが提供されます。Security Console を使用して、XML ライセンス ファイルをインストールする必要があります。

新しいライセンスをインストールすると、[License Status（ライセンスのステータス）] ページに、インストールされているすべてのライセンスの制限および機能がまとめて表示されます。

開始する前に

- スーパー管理者である必要があります。
- 評価版ライセンスからアップグレードする場合は、新しいライセンスをインストールする前に評価版ライセンスをアンインストールする必要があります。詳細については、RSA Security Console ヘルプのトピック「Uninstall a License（ライセンスのアンインストール）」を参照してください。
- ライセンスのバージョンと現在の RSA Authentication Manager バージョンに互換性がある必要があります。
- ライセンスのシリアル番号が導入環境の他のすべての既存のライセンスと同じである必要があります。
- ライセンス ID またはスタック ID は、すべてのライセンスを通じて一意である必要があります。

手順

1. .zip ファイルから XML ライセンス ファイルを抽出します。
2. Security Console で、[**Setup（セットアップ）**] > [**Licenses（ライセンス）**] > [**Add New（新規追加）**] の順にクリックします。
3. インストールする XML ライセンス ファイルを参照し、選択します。
4. [**Next（次へ）**] をクリックします。
5. [**Install（インストール）**] をクリックします。
   [License Status（ライセンスのステータス）] ページに、インストールされているすべてのライセンスの制限および機能がまとめて表示されます。

インストール済みライセンスの表示

ライセンスを表示すると、ライセンスの機能、制限、ステータスに関する詳細を確認できます。重要な機能の 1 つとして挙げられるのが、ライセンスが許可するユーザー数です。

トークンを割り当てられたユーザーは、このライセンス制限の対象としてカウントされます。無効化されたトークンや、期限切れのトークンが割り当てられたユーザーも、このライセンス制限の対象としてカウントされます。複数のトークンが割り当てられたユーザーは、1 回だけカウントされます。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Licenses（ライセンス）**] > [**Status（ステータス）**] の順にクリックします。

   [License Status（ライセンスのステータス）] ページに、インストールされているすべてのライセンスについて次の情報が表示されます。

   [**Status（ステータス）**]：ユーザー数の制限と製品の機能ごとにライセンスのステータスを示します。有効な値は、[OK]、[Approaching Limit（制限間近）]、[Limit Exceeded（制限超過）] です。

   [**License Features（ライセンス機能）**]：ライセンスで有効化される機能の名前を示します。

   [**Limit（制限）**]：この機能を使用できるユーザーの最大数を示します。このフィールドは、セルフ サービスなどのライセンスによる数の制限がない機能には適用されません。

   [**Actual（現在値）**]：トークンが割り当てられたユーザー数など、制限がある機能の場合、このフィールドには、ライセンス制限の対象としてカウントされるユーザー数の現在の値が示されます。セルフ サービスなど、制限がない機能の場合、このフィールドには、その機能を使用できるかどうかが示されます。

2. [**View Installed Licenses（インストール済みライセンスの表示）**] をクリックします。

3. [Installed Licenses（インストール済みライセンス）] ページで、ライセンス ID をクリックして [**View（表示）**] を選択すると、そのライセンスについて次の詳細情報が表示されます。

   [**License Details（ライセンスの詳細）**]：シリアル番号、製品、バージョン、発行日およびインストール日などのライセンスの詳細情報。

   [**License Features（ライセンス機能）**]：ライセンスされた機能の詳細情報。

8 Web Tier 導入環境の管理

Web Tier 導入環境の管理

Web Tier のインストール後に構成を変更する必要がある場合は、Operations Console を使用してこの章のタスクを実行してください。Web Tier 構成を変更した後、Web Tier を更新する必要があります。操作手順については、215 ページの Web Tier の更新を参照してください。

Web Tier のアンインストール手順については、215 ページの Windows での Web Tier のアンインストールと 216 ページの Linux での Web Tier のアンインストールを参照してください。

Web Tier の SSL 証明書の置換手順については、219 ページのデフォルトの RSA 仮想ホスト証明書の置換を参照してください。

Web Tier の構成の編集

Operations Console を使用して、既存の Web Tier の構成および Web Tier サービスのオプションを変更できます。たとえば、優先 RBA インスタンスを変更し、Self-Service Console、リスク ベース認証、動的シード配布をオンまたはオフにすることができます。

仮想ホスト名または仮想ホスト ポート番号を編集する場合は、RSA Operations Console ヘルプのトピック「ロードバランサと仮想ホストの構成」を参照してください。

開始する前に

- スーパー管理者である必要があります。
- ダウンタイムがユーザーに与える影響について考慮してください。
- Linux システムで、ローカル ユーザーに対するオープン可能ファイル数のハード制限が 4,096 以上であることを確認します。

手順

1. プライマリ インスタンスの Operations Console で、**［Deployment Configuration（導入環境の構成）］＞［Web-Tier Deployments（Web Tier の導入）］＞［Manage Existing（既存項目の管理）］**の順にクリックします。
2. **［Web Tier Name（Web Tier 名）］**リストで、Web Tier の名前をクリックします。
3. コンテキスト メニューで**［Edit（編集）］**をクリックします。

4. ［Edit（編集）］ページの［**Details（詳細）**］セクションで、次の情報を変更できます。
   - ［**Deployment name（導入名）**］：Web Tier 導入環境の名前です（0 ～ 255 文字、&、%、>、<、’、” の各文字は使用できません。
   - ［**Hostname（ホスト名）**］：Web Tier をインストールした Web Tier サーバの完全修飾ホスト名です。
   - ［**Preferred RBA Instance（優先 RBA インスタンス）**］：この Web Tier に接続し、RBA（リスク ベース認証）トラフィックの宛先となるインスタンスです。
5. ［**Web-Tier Service Options（Web Tier サービスのオプション）**］セクションで、以下の任意のサービスをオンまたはオフにします。
   - Self-Service Console
   - リスク ベース認証
   - 動的シード配布
6. ［**Save（保存）**］をクリックします。

次のステップ

導入名や優先 RBA インスタンスを変更した場合、またはサービスのオンまたはオフを切り替えた場合は、変更が有効になるまで 3 分以上かかります。

Web Tier サーバの IP アドレスの変更

ネットワークの再構成などにより変更が必要になった場合には、Web Tier サーバの IP アドレスを変更できます。IP アドレスを変更する場合は、Web Tier を再インストールする必要があります。この手順の実行中は、Web Tier サーバをできません。

開始する前に

- ダウンタイムがユーザーに与える影響について考慮してください。
- スーパー管理者である必要があります。
- Linux システムの場合は、ローカル ユーザーに対するオープン可能ファイル数のハード制限が 4,096 以上であることを確認します。

手順

1. Web Tier サーバの IP アドレスを変更します。詳細については、ご使用のサーバのマニュアルを参照してください。
2. Web Tier をアンインストールします。操作手順については、215 ページの Windows での Web Tier のアンインストールおよび 216 ページの Linux での Web Tier のアンインストールを参照してください。

3. 使用しているプラットフォーム用の Web Tier インストーラを使用して Web Tier を再インストールします。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
4. カスタム証明書で証明書を置き換えた場合は、Web Tier を再インストールした後でカスタム証明書をアクティブ化します。
5. 新しい Web Tier サーバの IP アドレスを DNS サーバまたはローカルの hosts ファイルに登録します。操作手順については、DNS サーバおよびローカル ホストのドキュメントを参照してください。

ロードバランサと仮想ホストの更新

Operations Console を使用して、仮想ホスト名、IP アドレス、リスニング ポートを変更できます。たとえば、仮想ホスト名の変更、IP アドレスの競合の解決、別のポートを使用する場合、変更が必要になります。

導入環境にロードバランサがある場合、仮想ホスト名はロード バランサのパブリック IP アドレスに解決される必要があります。

導入環境にロードバランサがない場合、仮想ホスト名は Web Tier のパブリック IP アドレスに解決される必要があります。

ロードバランサの名前を変更する場合、または別のロード バランサを使用する場合は、それに応じて仮想ホスト名を変更する必要があります。

開始する前に

- スーパー管理者である必要があります。
- 仮想ホスト名は、ロードバランサを指すように DNS（ドメイン名システム）で構成する必要があります。

手順

1. プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Virtual Host & Load Balancing（仮想ホストとロード バランシング）**］の順にクリックします。
2. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。
3. ［Virtual Host と Load Balancing（仮想ホストとロード バランシング）］ページで、以下のいずれかを変更します。
   a. 完全修飾仮想ホスト名
   b. デフォルト ポート番号
   c. ロードバランサの IP アドレス ロードバランサを使用しない場合は、IP アドレスは空白のままにします。

4. ［**Save（保存）**］をクリックします。
   システムにより、仮想ホスト名とキー指定要素がキーストアファイルに保存されます。
5. 確認ページで、［**Mandatory Next Steps（次の必須ステップ）**］を読みます。
6. ［**Done（終了）**］をクリックします。

次のステップ

Operations Console で、該当する次の必須ステップを実行します。

- ロードバランサの詳細を更新した場合は、プライマリおよびレプリカ インスタンスを再起動する必要があります。Operations Console で、［**Maintenance（保守）**］＞［**Reboot Appliance（アプライアンスのリブート）**］の順にクリックし、各インスタンスをリブートします。
- 仮想ホスト名を更新した場合は、RBA を使用する各 Web ベース アプリケーション用に新しい統合スクリプトを生成し、統合スクリプトを再導入します。詳細については、「管理者ガイド」を参照してください。
- 導入環境に Web Tier が含まれている場合は、Web Tier を更新します。Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。各 Web Tier の更新リンクをクリックします。
- 導入環境に Web Tier が含まれている場合は、ロードバランサとファイアウォールの証明書を仮想ホスト証明書で置き換えます。
- 導入環境で動的シード配布を使用する場合は、CT-KIP URL のホスト名とポートが、仮想ホストのホスト名とポートを指すよう更新します。Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。［**Tokens（トークン）**］をクリックします。
- 導入環境で RSA Self-Service Console を使用する場合は、Self-Service Console URL が仮想ホストのホスト名とポートを指すよう更新します。Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。［**E-Mail Notifications for User Account Changes（ユーザー アカウント変更のメール通知）**］をクリックします。

Web Tier バージョンの確認

Web Tier のバージョンは、Authentication Manager のバージョンと同じである必要があります。Authentication Manager を更新した後で、Web Tier のバージョンを必ず確認します。Web Tier のバージョンは、Operations Console または Web Tier インストール ディレクトリで確認できます。

手順

Web Tier のバージョンを確認するには、以下のいずれかを実行します。

- Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Web-Tier Deployments（Web Tier の導入）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
- Web Tier インストール ディレクトリ配下で、**webtier.properties** ファイルを探し、ファイル内に記述された **webtier.version=<VERSION NUMBER>** を確認します。

Web Tier の更新

Authentication Manager のバージョン アップデートや Web Tier ページのカスタマイズなどの変更を行うときは、Web Tier を更新する必要があります。Authentication Manager は、最新ではない各 Web Tier に対して、Operations Console に更新ボタンを表示します。複数の Web Tier を更新する場合は、一度に 1 つずつ更新します。更新はそれぞれ完了まで最長 20 分かかります。

手順

1. Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Web-Tier Deployments（Web Tier の導入）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. [Web Tiers] ページの [**Status（ステータス）**] 列で、更新する Web Tier の [**Update（更新）**] をクリックします。

   更新が完了すると、更新された Web Tier の [**Status（ステータス）**] 列に [**Online（オンライン）**] と表示されます。更新が完了するまでには最長で 20 分かかります。

Windows での Web Tier のアンインストール

アンインストールするには、Web Tier サーバで RSA Authentication Web-Tier Uninstaller for Windows を実行します。Web Tier をアンインストールすると、Web Tier と RSA Authentication Manager のすべての機能とコンポーネントが Web Tier サーバから削除されます。

Web Tier をアンインストールしても、Web Tier 導入レコードは削除されません。

開始する前に

プログラムをアンインストールできる Windows クレデンシャルを持っていることを確認します。

手順

1. Web Tier サーバで、［**スタート**］＞［**コントロール パネル**］＞［**プログラムと機能**］の順にクリックします。
2. ［**RSA Authentication Web Tier**］を右クリックし、［**アンインストール**］をクリックします。
3. コマンド ライン上で、次のように入力します。

   ```
   y
   ```

   Enter キーを押します。

   完了すると、アンインストーラ スクリーンに［Uninstall finished（アンインストール完了）］と表示されます。
4. Enter キーを押します。

   システムから、Web Tier サービスおよびインストール フォルダが削除されます（トップ レベル フォルダを除く）。

次のステップ

- プライマリ インスタンスで、Operations Console を使用して、Web Tier 導入レコードを削除します。操作手順については、RSA Operations Console ヘルプのトピック「Web Tier 導入レコードの削除」を参照してください。
- （オプション）DNS サーバ上で、アンインストールした Web Tier のホスト名と IP アドレスを削除します。

Linux での Web Tier のアンインストール

アンインストールするには、Web Tier サーバ上で RSA Authentication Web-Tier Uninstaller for Linux を実行します。Web Tier をアンインストールすると、Web Tier および RSAAuthentication Manager のすべての機能とコンポーネントが、Web Tier サーバから削除されます。

Web Tier をアンインストールしても、Web Tier 導入レコードは削除されません。

開始する前に

- root 権限を持っていることを確認します。
- ローカル ユーザーに対するオープン可能ファイル数のハード制限が 4,096 以上であることを確認します。

手順

1. Web Tier サーバにログオンします。
2. ディレクトリを **Web Tier インストール ディレクトリの下の、/uninstall** に変更します。

3. コマンド ライン上で、次のコマンドを入力します。

   ```
   ./uninstall.sh
   ```

4. Enter キーを押します。
5. ［Welcome］画面で、次のように入力します。

   ```
   yes
   ```

6. Enter キーを押します。
   システムにより、Web Tier がアンインストールされ、完了すると［Uninstall Complete（アンインストール完了）］と表示されます。

次のステップ

- プライマリ インスタンスで、Operations Console を使用して、Web Tier 導入レコードを削除します。操作手順については、RSA Operations Console ヘルプのトピック「Web Tier 導入レコードの削除」を参照してください。
- （オプション）DNS サーバ上で、アンインストールする Web Tier のホスト名と IP アドレスを削除します。

Web Tier サービスの管理

Bootstrapper Server と Web Tier サービスは、Web Tier のインストール時に自動的に起動して実行されます。レプリカ インスタンスの昇格後は、それらを手動で起動する必要があります。

Web Tier のステータスをレポートしたり更新を Web Tier にプッシュするには、Web Tier サーバ上で Bootstrapper Server が実行中である必要があります。セルフ サービス、RBA（リスク ベース認証）、動的シード配布などの Web Tier 機能を提供するためには、Web Tier サービスが実行中である必要があります。Web Tier サーバを別のマシンに移行するために停止するなどの場合は、Bootstrapper Server および Web Tier サービスを手動で停止、開始、再起動できます。

操作については、次の手順を参照してください。

- 217 ページの Windows での RSA Web Tier Bootstrapper Server の管理
- 218 ページの Linux での RSA Web Tier Bootstrapper Server の管理

Windows での RSA Web Tier Bootstrapper Server の管理

RSA Web Tier Bootstrapper Server を停止、開始、再起動するには、この処理手順を実行してください。この処理手順は、サポートされるすべてのバージョンの Windows に適用されます。

処理手順

1. Web Tier サーバで、**［スタート］＞［ファイル名を指定して実行］**をクリックします。
2. 次のように入力します。
   services.msc
3. Enter キーを押します。
4. ［**RSA Webtier Bootstrapper Server**］を右クリックします。
5. 目的に応じて次のいずれかをクリックします。
   - **停止**
   - **開始**
   - **再起動**

Linux での RSA Web Tier Bootstrapper Server の管理

RSA Web Tier Bootstrapper Server を停止、開始、再起動するには、この処理手順を実行してください。この処理手順は、サポートされるすべてのバージョンの Linux に適用されます。

開始する前に

- インストール時に指定したローカル ユーザーとしてログオンします。
- ローカル ユーザーのオープン可能ファイル数のハード制限が 4,096 以上であることを確認します。

処理手順

1. Web Tier サーバで、**RSA_WT_HOME/webtierBootstrapper/server** に移動します。
   ここで、RSA_WT_HOME は Web Tier のインストール ディレクトリです。
2. 次のうちの適切なコマンドを入力します。
   ./rsaserv start all
   ./rsaserv stop all
   ./rsaserv restart all
   ./rsaserv status all

デフォルトの RSA 仮想ホスト証明書の置換

各 Web Tier には仮想ホスト名に基づく証明書があります。リスク ベース認証などの一部の機能では、ロードバランサの使用を許可するために仮想ホスト名が使用されます。Self-Service Console などの他の機能では、仮想ホスト名を使用して、プライマリ インスタンスに関連づけられた Web Tier サーバに接続します。

オプションで、デフォルトの RSA 仮想ホスト証明書を置換できます。次のような場合、証明書を置換する必要があります。

- ネットワーク ポリシーで、信頼するルート CA（認証局）が発行した証明書を使用することが必須となっている。
- 信頼するルート CA が発行した現在の証明書の期限が切れた。
- ブラウザにデフォルトの RSA 仮想ホスト証明書が信頼されていないという警告が表示されるため、置換したい。

認証局証明書ファイル

認証局の証明書は、1 つまたは複数のファイルで送信されます。考えられる組み合わせは、次の 3 とおりです。

1 ファイル。親ルート証明書から、中間証明書（存在する場合）、ホスト証明書までの証明書チェーン全体を含んだ 1 つの証明書ファイル。この場合、1 つのファイルにすべてが含まれているため、最も便利です。ただし、個々の証明書を切り離すことができないので、柔軟性に欠ける面があります。

証明書ファイルを Web Tier にインポートする際、証明書が信頼されていないという警告がシステムにより表示されます。これは、インポートするルート証明書がまだ信頼されたルート証明書ストアに保存されていないためです。インポート後、警告は表示されなくなります。

2 ファイル。署名済み仮想ホスト証明書ファイルとルート証明書ファイル。この場合は次のメリットがあります。

- ルート証明書は、今後発行されるすべての証明書の検証に使用できます。
- ルート証明書は、RSA のデフォルト ルート証明書を信頼していない Web ブラウザの信頼されたルート証明書ストアにインポートできます。

まず、ルート証明書をインポートする必要があります。

2 つ以上のファイル。複数のファイルのそれぞれに個別の証明書が含まれています。この場合、ユーザーがルート認証局までの信頼を構築でき、最も柔軟性に優れます。Web Tier 証明書と仮想ホスト証明書の両方を置換する場合、これらの証明書が同じ信頼される認証局によって署名されていれば、認証局の証明書をインポートする回数は 1 回で済みます。各証明書は、次の順序でインポートする必要があります。

- 信頼する親ルート証明書
- 中間証明書
- ホスト証明書

デフォルトの仮想ホスト証明書の置換

デフォルトの仮想ホスト証明書を置換する処理手順は、次のとおりです。

1. 次のいずれかの方法で証明書署名リクエストを生成します。
   - RSA Security Console：操作手順については、220 ページの Web Tier の CSR（証明書署名リクエスト）の生成を参照してください。
   - サードパーティ製のツール：サードパーティ製ツールで秘密鍵と署名リクエストを生成します。CN（共通名）には、仮想ホストの FQHN（完全修飾ホスト名）を指定します。正しい値を指定しないと、仮想ホスト証明書をアクティブ化できません。操作手順については、サードパーティ製ツールのドキュメントを参照してください。
2. 証明書署名リクエストを CA（認証局）に送信します。
3. 信頼するルート証明書と署名済みの仮想ホスト証明書をインポートし、アクティブな証明書にします。操作手順については、221 ページの署名済み仮想ホスト証明書のインポートを参照してください。
4. 新しい証明書をインポートした後、各 Web Tier を更新します。操作手順については、215 ページの Web Tier の更新を参照してください。

Web Tier の CSR（証明書署名リクエスト）の生成

証明書署名リクエストを CA に送信する前に、Authentication Manager で証明書署名リクエスト ファイルを生成する必要があります。Authentication Manager が、秘密鍵および証明書署名リクエストを生成します。

開始する前に

- Operations Console 管理者である必要があります。
- 仮想ホストを定義する必要があります。

手順

1. Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Certificates（証明書）**] > [**Virtual Host Certificate Management（仮想ホスト証明書の管理）**] の順にクリックし、[**Generate CSR（CSR の生成）**] をクリックします。
2. [Generate Virtual Host Certificate Signing Request（仮想ホスト証明書の署名リクエストの生成）] ページで、以下を実行します。
   - [**Virtual Host（仮想ホスト）**] の名前を確認する。
   - [**Alias（エイリアス）**] を入力する。
   - （オプション）[**Country Name（国名）**] を入力する。
   - （オプション）[**State or Province name（都道府県名）**] を入力する。
   - （オプション）[**City or Locality name（市区町村名）**] を入力する。
   - （オプション）[**Organization Name（組織名）**] を入力する。
   - （オプション）[**Organizational Unit Name（部門名）**] を入力する。
   - （オプション）[**E-mail Address（メール アドレス）**] を入力する。
3. [**Generate File（ファイルの生成）**] をクリックします。
4. [Download File（ファイルのダウンロード）] ページの [**Download（ダウンロード）**] をクリックします。
5. 証明書署名リクエスト ファイルをローカル マシンに保存します。

次のステップ

- 証明書署名リクエスト ファイルを CA に送信し、署名された証明書をローカル マシンに保存します。
- 信頼するルート証明書および署名された証明書を仮想ホストにインポートし、アクティブ化します。操作手順については、221 ページの署名済み仮想ホスト証明書のインポートを参照してください。

署名済み仮想ホスト証明書のインポート

既存の仮想ホスト証明書を新しい証明書で置換するためには、署名チェーンのすべての証明書ファイルを CA（認証局）からダウンロードし、インポートする必要があります。

開始する前に

- Operations Console 管理者である必要があります。
- CA ルート証明書、署名チェーンに含まれる他のすべての証明書、新しい仮想ホスト証明書をダウンロードします。

手順

1. Operations Console で、**［Deployment Configuration（導入構成）］＞［Certificates（証明書）］＞［Virtual Host Certificate Management（仮想ホスト証明書の管理）］**の順にクリックします。
   次のステップを実行し、まず最初にルート証明書をインポートします。続けて、署名チェーンの各証明書を順番にインポートします。
2. ［Virtual Host Certificate Management（仮想ホスト証明書の管理）］ページで、**［Import Certificates（証明書のインポート）］**をクリックします。
3. ［Import Certificate（証明書のインポート）］ページの**［Certificate Basics（証明書の基本設定）］**で、次のいずれかを実行します。
   Operations Console で作成した CSR に対して発行された証明書の場合
   - **［Import Certificate（証明書のインポート）］**フィールドで、証明書ファイルの場所を参照します。このファイルには、CA から入手した CA ルート証明書または SSL 証明書が含まれています。
   - **［Type of Certificate to Import（インポートする証明書のタイプ）］**で、**［PKCS #7 (*.cer or *.p7b)］**を選択します。

   他の証明書ツールで作成した CSR に対して発行されたコンソール証明書の場合
   - **［Import Certificate（証明書のインポート）］**フィールドで、証明書ファイルの場所を参照します。このファイルには、1 個以上の証明書および新しい証明書のための秘密鍵が含まれています。
   - **［Type of Certificate to Import（インポートする証明書のタイプ）］**で、**［PKCS#12 (*.pfx or*.p12)］**を選択します。
   - **［Password**（パスワード）］フィールドに、PKCS#12 ファイルのパスワードを入力します。
4. **［Import**（インポート）］をクリックします。

次のステップ

仮想ホスト証明書のアクティブ化

仮想ホスト証明書のアクティブ化

仮想ホストで新しい証明書を使用できるようにするには、その証明書をアクティブ化する必要があります。

仮想ホスト証明書をアクティブ化するには、証明書のサブジェクト フィールドの CN（共通名）として、仮想ホストの FQHN（完全修飾ホスト名）が含まれていなければなりません。

開始する前に

- Operations Console 管理者である必要があります。
- アクティブ化する署名済み仮想ホスト証明書のインポート

手順

1. Operations Console で、［**Deployment Configuration（導入構成）**］＞［**Certificates（証明書）**］＞［**Virtual Host Certificate Management（仮想ホスト証明書の管理）**］の順にクリックします。
2. ［Virtual Host Certificate Management（仮想ホスト証明書の管理）］ページの［**Alias（エイリアス）**］で、新しい証明書の名前をクリックします。
3. ［**Activate（アクティブ化）**］をクリックします。
4. ［Activate Certificate Confirmation（証明書アクティブ化の確認）］ページで、詳細を確認し、［**Yes, make this the active default certificate（はい、この証明書をアクティブにします）**］を選択します。
5. ［**Activate Certificate（証明書のアクティブ化）**］をクリックします。

次のステップ

Web Tier を更新します。操作手順については、215 ページの Web Tier の更新 を参照してください。

Web Tier 上の Self-Service Console のログアウト エラー

Web Tier サーバと関連づけられたインスタンスの時刻のずれが 15 分を超えると、ユーザーが Self-Service Console からログアウトするときに次のエラーが表示されることがあります。

「Error:Internal Server Error.The server encountered an unexpected condition, which prevented it from fulfilling your request.」

システム ログには、次のように記録されます。

「Caused by:com.rsa. common.SystemException:Logout request exceeds the configured time window.The web tier time is not in sync with the biz-tier or a possible replay.」

考えられる原因は、ログアウト リクエストが許容されるタイム ウィンドウ外で行われたことです。この問題を解決するには、次の操作のいずれかを実行します。

- 導入環境に NTP（ネットワーク タイム プロトコル）サーバがない場合は、Web Tier サーバのシステム時刻を関連づけられたインスタンスと同期します。
- 導入環境に NTP サーバがある場合は、Web Tier サーバを NTP サーバと同期します。

タイム ゾーンが同じである必要はありません。たとえば、Web Tier サーバの時刻を午前 7:00（GMT）、関連づけられたインスタンスの時刻を午前 9:00（GMT + 2）に設定することができます。

9 RSA SecurID トークンの導入と管理

RSA SecurID トークン

RSA SecurID トークンは、RSA SecurID の 2 要素認証で使用します。RSA SecurID トークンは、トークンコードと呼ばれる 6 桁または 8 桁の擬似乱数を定期的に生成します。トークンコードを PIN（暗証番号）と組み合わせた場合、これをパスコードと呼びます。ユーザーは、Authentication Manager で保護されているリソースにアクセスする際、本人であることを証明するために、パスコードをその他のセキュリティ情報とともに入力します。Authentication Manager がパスコードが正しいことを確認すると、ユーザーはアクセスを許可されます。パスコードが正しくない場合、ユーザーはアクセスを拒否されます。

SecurID トークンには、ハードウェア トークンとソフトウェア トークンの 2 種類があります。ハードウェア トークンは、内蔵クロック、および工場でエンコードされた「シード」と呼ばれるトークンのランダム キーを使用して、トークンコードを生成します。ハードウェア トークンには、キー フォブや PINPad などの複数のモデルがあります。ソフトウェア トークンは、個別にインストールされる 2 個のコンポーネントで構成されています。つまり、対象とするデバイス プラットフォームに固有のアプリケーションとトークン シード レコードです。ソフトウェア トークン アプリケーションは、デバイス上でトークンコードを生成し、ハードウェア トークンと同じパスコード機能を備えています。対応するデバイスには、スマート フォン、コンピュータ、タブレットなどがあります。

ハードウェア トークンとソフトウェア トークンには、同じような管理タスクが必要です。導入後に、Security Console のユーザー ダッシュボードを使用することで、トークン関連の管理タスクを実行できます。詳細については、RSA Security Console ヘルプのトピック「ユーザー ダッシュボード」を参照してください。

デフォルトで、RSA は PIN が必要なトークンを提供し、すべてのトークンで PIN を使用することを強く推奨します。PIN は、RSA SecurID の 2 要素認証における 2 番目の要素となります。また、RSA Authentication Manager は、RSA SecurID PIN が必要ないトークンを使用した認証もサポートします。

RSA SecurID トークンの導入

次のステップは、RSA SecurID トークンの導入に必要なタスクの概要を示しています。

処理手順

1. 226 ページのトークン レコード ファイルのインポートを実行します。
2. （オプション）227 ページの新しいセキュリティ ドメインへのトークン レコードの移動を実行します。
3. 228 ページのユーザーへのトークンの割り当てを実行します。
4. ソフトウェア トークンの場合、232 ページのソフトウェア トークン プロファイルの追加を実行します。それ以外の場合は、ステップ 5 に進みます。
5. トークンを配布します。以下のいずれかを選択します。
   - 234 ページのハードウェア トークンの配布
   - 234 ページのファイル ベースの配布を使用した複数のソフトウェア トークンの配布
   - 236 ページのファイル ベースの配布を使用した単一のソフトウェア トークンの配布
   - 238 ページの動的シード配布（CT-KIP）を使用した複数のソフトウェア トークンの配布
   - 240 ページの動的シード配布を使用した単一のソフトウェア トークンの配布
   - 242 ページの CTF（Compressed Token Format）を使用した複数のソフトウェア トークンの 配布
   - 244 ページの CTF（Compressed Token Format）を使用した単一のソフトウェア トークンの 配布

トークン レコード ファイルのインポート

トークンを購入すると、トークンと一緒にトークン レコードが格納された XML ファイルが RSA から提供されます。個々のトークン レコードを操作するには、トークン レコード XML ファイルを Authentication Manager にインポートする必要があります。

ハードウェア トークンの場合は、ファイル内の各トークン レコードが購入したハードウェア トークンに対応しています。

ソフトウェア トークンの場合は、ファイル内の各トークン レコード データが最終的にはソフトウェア トークン アプリケーションに転送されます。すべてのトークン レコードには、トークン シード、トークンのシリアル番号、有効期限、トークンコードの桁数とインターバルなどのメタデータが含まれます。

開始する前に

- インポートされたトークンを所有するセキュリティ ドメインを決定する。そのセキュリティ ドメインは、トークンを導入および管理する管理者の権限適用範囲内にある必要があります。
- 管理者ロールによって、トークンの管理が許可されている。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Import Tokens Job（インポートトークン ジョブ）**] > [**Add New（新規追加）**] の順にクリックします。
2. インポート ジョブの名前を入力します。ジョブはここで入力した名前で保存され、後でジョブの詳細を表示できます。名前は 1 ～ 128 文字の長さで指定します。&、%、>、< の各文字は使用できません。
3. [**Security Domain（セキュリティ ドメイン）**] ドロップダウン メニューから、このトークンのインポート先となるセキュリティ ドメインを選択します。このセキュリティ ドメインを権限適用範囲に含む管理者が、このトークンを管理することになります。デフォルトでは、トークンは最上位のセキュリティ ドメインにインポートされます。
4. インポートするトークン ファイルを参照し、選択します。
5. ファイルがパスワード保護されている場合は、[**File Password（ファイルのパスワード）**] フィールドに、パスワードを入力します。
6. 重複したトークンの処理を指定するには、[**Import Options（インポート オプション）**] ラジオ ボタンを使用します。
7. [**Submit Job**（ジョブの実行）] をクリックします。

次のステップ

- トークンをユーザーに割り当てる。詳細については、228 ページのユーザーへのトークンの割り当てを参照してください。

新しいセキュリティ ドメインへのトークン レコードの移動

トークンレコードのセキュリティ ドメインを移動することができます。インポート先のセキュリティ ドメインを選択しない場合、トークン レコードはデフォルトで最上位のセキュリティ ドメインにインポートされます。Security Console を使用して、導入環境内のセキュリティ ドメイン間でトークン レコードを移動できます。トークン レコードを管理するために管理者の権限適用範囲を変更することや、トークンを使用する場所のセキュリティ ドメインにトークン レコードを移動することもできます。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、移動するトークンを検索します。
3. 移動するトークンの横にあるチェックボックスをオンにします。
4. [**Action（アクション）**] メニューから、[**Move to Security Domain（セキュリティ ドメインの移動）**] をクリックします。
5. [**Go（実行）**] をクリックします。
6. [**Move to Security Domain（移動先のセキュリティ ドメイン）**] ドロップダウン リストから、トークンの移動先となるセキュリティ ドメインを選択します。
7. [**Move（移動）**] をクリックします。

ユーザーへのトークンの割り当て

トークンを割り当てると、トークンが特定のユーザーに関連づけられます。ユーザーを認証するためには、事前にトークンをユーザーに割り当てておく必要があります。1 ユーザーに対し、最大 3 つのトークンを割り当てることができます。ユーザーがトークンの紛失や盗難を報告する可能性が高くなるため、ユーザーには複数のハードウェア トークンを割り当てないことを推奨します。ソフトウェア トークン アプリケーションの中には、複数のトークンが許可されないものもあります。プラットフォームに固有のトークンの制限事項にについては、RSA SecurID ソフトウェア トークンのマニュアルを参照してください。

トークンはユーザー ダッシュボードを使用して割り当てることもできます。詳細については、ユーザー ダッシュボードを参照してください。

開始する前に

- トークン レコード ファイルから内部データベースにトークン レコードをインポートする。詳細については、226 ページのトークン レコード ファイルのインポートを参照してください。
- トークンを割り当てるすべてのユーザーについて、Authentication Manager 内にユーザー レコードが存在することを確認する。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、トークンを割り当てるユーザーを検索します。
3. 検索結果から、トークンを割り当てるユーザーをクリックします。
4. コンテキスト メニューから、[**SecurID Tokens（SecurID トークン）**] の下の [**Assign More（割り当て）**] をクリックします。

5. ［Assign SecurID Tokens（SecurID トークンの割り当て）］ページで、利用可能な RSA SecurID トークンのリストから、割り当てるトークンのチェックボックスをオンにします。後で配布できるように、割り当てたトークンを記録します。
6. ［**Assign（割り当て）**］をクリックします。

次のステップ

ソフトウェア トークン プロファイルの追加

ソフトウェア トークン プロファイル

ソフトウェア トークン プロファイルは、ソフトウェア トークンの構成および配布プロセスを指定します。ソフトウェア トークン プロファイルは、ソフトウェア トークンを配布する予定のプラットフォームごとに必要です。ソフトウェア トークン プロファイルを導入環境に追加できるのは、スーパー管理者だけです。ソフトウェア トークン プロファイルは、導入環境全体で使用することができ、セキュリティ ドメインに固有のものではありません。

デバイス定義ファイル

デバイス定義ファイルは、Android プラットフォームや iOS プラットフォームなど、特定のプラットフォームで使用するソフトウェア トークンの機能と属性を定義する XML ファイルです。このファイルは、サポートされるトークンコードの特性、トークン タイプ、トークンが CT-KIP 対応であるかどうか、CT-KIP リンク形式、トークンが CTF 対応であるかどうか、サポートされるバインド属性を特定します。

RSA が新しいタイプのソフトウェア トークン アプリケーションをリリースした場合、多くの場合、そのアプリケーション用の新しいデバイス定義ファイルもリリースされます。新しいトークン タイプのソフトウェア トークン プロファイルを作成する場合は、新しいデバイス定義ファイルをインポートする必要があります。新しいデバイス定義ファイルをインポートする必要があるかどうかについては、使用するソフトウェア トークン アプリケーションの管理者ガイドを参照してください。

ソフトウェア トークンの構成

RSA SecurID ソフトウェア トークンは、出荷時に、PIN タイプは PINPad（PIN をトークンコードに統合する）、トークンコードの長さは 8 桁、トークンコードの間隔は 60 秒に設定されています。ただし、ソフトウェア トークンのトークンコードの間隔、PIN タイプ、トークンコードの長さは、作成するソフトウェア トークン プロファイルごとに構成できます。デバイス定義ファイル内の構成オプション セットに応じて、トークンコードの長さは 6 桁または 8 桁に、トークンコードの間隔は 30 秒または 60 秒に設定できます。また、キーフォブ トークンと同じ動作になるよう PIN タイプを変更することができます。トークンを PIN なしでトークンコードのみで使用するよう再構成することもできます。

ソフトウェア トークンの配布方法

トークン データをソフトウェア トークン アプリケーションに提供するために、次の方法が用意されています。

動的シード配布（CT-KIP）。動的シード配布方法では、4 パス CT-KIP（Cryptographic Token Key Initialization Protocol）を使用することにより、モバイル デバイスやデスクトップで実行中の RSA SecurID クライアント アプリケーションと、Authentication Manager サーバのコンポーネントである CT-KIP サーバとの間で情報を交換します。クライアントとサーバの間で交換した情報を使用して、共有される一意のシークレット情報（トークン シード）が生成されます。シードを生成する上で重要な情報は、公開鍵と秘密鍵のペアを使用して転送時に暗号化されます。生成されたトークン シード値そのものがネットワーク経由で転送されることはありません。動的シード配布は、ファイル ベースの配布よりも推奨される方法です。4 パス CT-KIP プロトコルの使用によって、配布処理の途中でトークンのシードが傍受される可能性を回避することができるからです。

アクティベーション コードの有効期限を構成した場合、ユーザーは、コードの有効期限が切れる前にアクティベーション コードをクライアント アプリケーションに入力する必要があります。有効期限が切れる前にアクティベーション コードが使用されなかった場合は、トークンを再配布し、CT-KIP URL と新しいアクティベーション コードをユーザーに送信する必要があります。

4 パス CT-KIP プロトコルは、ユーザーがクライアント デバイスでトークンのインポート オプションを選択した時に、クライアント アプリケーションから CT-KIP サーバへのリクエストによって開始します。動的シード配布では、配布用に生成された一回限り有効な一意のアクティベーション コードを使用して、リクエストの正当性を確認します。アクティベーション コードは、クライアント アプリケーションにユーザーが手動で入力するか、ユーザーのデバイスに送信する URL 文字列に追加する必要があります。CT-KIP サーバがアクティベーション コードを評価し、リクエストが有効であると判断すると、4 パス プロセスを続行し、最終的にインポートの動作が成功します。

ファイル ベースの配布。ファイル ベースの配布では、Authentication Manager がトークン データを生成します。このデータは、ダウンロードできるよう ZIP ファイルに格納されます。この方法を使用して配布するソフトウェア トークン ファイルには、.sdtid という拡張子が付きます。トークン ファイル内のデータには、SecurID アルゴリズムで使用されるシードと、その他のメタデータ（トークンのシリアル番号、有効期限、トークンコードの桁数など）が含まれています。攻撃から保護するため、シードは AES アルゴリズムで暗号化されており、オプションとして、構成プロセスの際に管理者がパスワードを設定することができます。「RSA Authentication Manager 8.0 Security Configuration Guide」に記載されているガイドラインに従った強力なパスワードを使用して、ファイル ベースのトークンを保護することを推奨します。

CTF（Compressed Token Format）配布。一部のモバイル デバイス プラットフォームのメール プログラムでは、添付された .sdtid ファイルを解釈できません。このような場合は、CTF（Compressed Token Format）を使用してファイル ベースのトークンを配布することができます。Authentication Manager は、CTF URL 文字列の形式でトークン データを生成します。このデータは、URL リンクとしてメールでユーザーのデバイスに配布することができます。CTF URL 文字列には、ソフトウェア トークン アプリケーションが必要とするトークン データをエンコードした情報が含まれています。このエンコードされたデータには、SecurID アルゴリズムで使用されるシードと、その他のメタデータ（シリアル番号、有効期限、トークンコードの桁数など）が含まれています。URL 形式によって、ソフトウェア トークン アプリケーションに関連するデータが URL リンクに含まれていることをデバイスに伝えます。「RSA Authentication Manager 8.0 Security Configuration Guide」に記載されているガイドラインに従った強力なパスワードを使用して、CTF 形式のトークンを保護することを推奨します。

デバイス属性

デバイス属性を使用して、ソフトウェア トークンに情報を追加します。［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドを使用すると、特定のデバイス プラットフォームまたは特定のデバイスにトークンをインストールするよう制限できます。デバイス タイプに関連づけられたデフォルトの［**DeviceSerialNumber（デバイスのシリアル番号）**］の値により、トークンが特定のプラットフォームにバインドされます。デバイス プラットフォームへのバインドにより、ユーザーは、サポートされる Android デバイスなど、任意のデバイスにトークンをインストールできるようになります。Apple iOS などの異なるプラットフォームにそのトークンをインストールすることはできなくなります。

セキュリティを強化するために、トークンをデバイス固有の単一の ID 番号にバインドすることができます。たとえば、RSA SecurID ソフトウェア トークン アプリケーションがデバイスに割り当てる一意のデバイス ID にバインドすることができます。この場合、トークンは特定のデバイス ID を持つデバイスにのみインストールすることができます。ユーザーがトークンを別のデバイスにインポートしようとすると、そのインポートは失敗します。管理者は、トークンを配布する前にバインドしておく必要があります。デバイスのバインドに使用する情報をユーザーから入手する必要があります。ユーザーは、バインドに使用する情報を提供する前に、ソフトウェア トークン アプリケーションをインストールしておく必要があります。詳細については、使用する RSA SecurID ソフトウェア トークンのドキュメントを参照してください。

［**Nickname（ニックネーム）**］フィールドを使用すると、ユーザーが判別しやすい名前をトークンに付けることができます。トークンをデバイス上のアプリケーションにインストールすると、そのアプリケーションにトークンのニックネームが表示されます。ニックネームを割り当てない場合、アプリケーションにはデフォルトの名前が表示されます。たとえば、トークンのシリアル番号などです。すべてのソフトウェア トークン アプリケーションがニックネームをサポートするわけではありません。

ソフトウェア トークン プロファイルの追加

ソフトウェア トークン プロファイルは、ソフトウェア トークンの構成および配布オプションを指定します。ソフトウェア トークン プロファイルは、ソフトウェア トークンを配布する予定のプラットフォームごとに構成する必要があります。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Software Token Profiles（ソフトウェア トークン プロファイル）**］＞［**Add New（新規追加）**］の順にクリックします。
2. **プロファイル名**を入力します。プロファイル名にはデバイス タイプまたは配布方法を含めるようにしてください。たとえば、「Android_CT_KIP」のような名前にします。
3. 以下のいずれかの操作を実行します。
   - 既存のデバイス タイプを選択するには、［**Device Type（デバイス タイプ）**］ドロップダウン リストからデバイス タイプを選択します。
   - 新しいデバイス タイプをロードするには、［**Import New Device Definition File（新しいデバイス定義ファイルのインポート）**］をクリックした後、目的のデバイス定義ファイルを参照し、［**Submit（送信）**］をクリックします。
4. デバイス タイプの該当するフィールドに値を入力します。デバイスタイプに応じて、次の設定を構成する必要があります。
   a. ［**Tokencode Duration（トークンコード間隔）**］フィールドで、トークンコードの更新間隔を選択します。
   b. ［**Tokencode Length（トークンコード桁数）**］フィールドで、トークンコードの桁数を選択します。
   c. ［**Authentication Type（認証タイプ）**］を選択します。以下の認証タイプを利用できます。
      – PINPad 形式。ユーザーは、ソフトウェア トークン アプリケーションに PIN を入力して、パスコードを生成する必要があります。

- フォブ形式 ユーザーは、SecurID で保護されたリソースのログオン画面で、PIN に続けてトークンコードを入力する必要があります。
- トークンコード。ユーザーは、トークンコードを入力します。PIN は必要ありません。

d. ［**Delivery Method（配布方法）**］を選択します。ソフトウェア トークン ファイルは、次の 3 つのうちのいずれかの方法で配布できます。

- 動的シード配布。CT-KIP（Cryptographic Token-Key Initialization Protocol）を使用します。この方法は、CT-KIP に対応した SecurID ソフトウェア トークンの場合にのみ使用します。CT-KIP 対応の SecurID ソフトウェア トークンは、常に 128 ビット トークンです。
- CTF（Compressed Token Format）配布。Authentication Manager によって URL が生成され、これをユーザーのデバイスに配布します。この URL には、ソフトウェア アプリケーションが必要とするトークン情報がエンコードされています。この方法は、CTF に対応した SecurID ソフトウェア トークンの場合にのみ使用します。CTF 配布は、64 ビット トークンに対応していません。
- ファイル ベースの配布。Authentication Manager によってソフトウェア トークン配布ファイル（.sdtid）が生成されます。このファイルは、ダウンロード用に .zip ファイルで提供されます。このソフトウェア トークン配布ファイルには、SecurID アルゴリズムによって使用される共有シークレット（「シード」）と、その他のメタデータ（有効期限、シリアル番号、トークンコードの桁数など）が含まれています。

e. ［**Device Specific Attributes（デバイス固有の属性）**］セクションで、次のいずれかを実行します。

- このデバイス タイプのすべてのソフトウェア トークンをデバイス クラスにバインドする場合は、［**DeviceSerialNumber**］フィールドの値をデフォルト値（classGUID）のままにしておきます。
- このデバイス タイプのすべてのソフトウェア トークンをデバイス クラスにバインドしない場合は、［**DeviceSerialNumber**］フィールドの値を消去するか、デフォルト値のままにしておきます。後でトークンを配布するときに、デフォルト値をデバイスに固有の ID で置き換えることができます。

f. 配布するすべてのトークンに同じニックネームを設定する場合はニックネームを入力します（たとえば、会社名）。実際にトークンを配布するとき、各トークンに個別のニックネームを設定できます。

5. ［**Save（保存）**］をクリックします。

次のステップ

選択した方法を使用して、トークンをユーザーに配布します。手順については、以下のいずれかを参照してください。

- 234 ページのファイル ベースの配布を使用した複数のソフトウェア トークンの配布
- 236 ページのファイル ベースの配布を使用した単一のソフトウェア トークンの配布
- 238 ページの動的シード配布（CT-KIP）を使用した複数のソフトウェア トークンの配布
- 240 ページの動的シード配布を使用した単一のソフトウェア トークンの配布
- 242 ページの CTF（Compressed Token Format）を使用した複数のソフトウェア トークンの 配布
- 244 ページの CTF（Compressed Token Format）を使用した単一のソフトウェア トークンの 配布

ハードウェア トークンの配布

開始する前に

ユーザーへのトークンの割り当て

処理手順

以下のいずれかの操作を実行します。

- ユーザーが近くにいる場合は、トークンを直接手渡す方法を指示します。
- 組織が大規模で地理的に分散している場合は、トークンを送付します。

ファイル ベースの配布を使用した複数のソフトウェア トークンの配布

ファイル ベースの配布を使用して、ソフトウェア トークンを配布する場合、トークン データはトークン配布ファイル（SDTID ファイル）に格納されます。SDTID ファイルは、ダウンロード用の ZIP ファイルに追加されます。

開始する前に

- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションの管理者ガイドを参照してください。
- ソフトウェア トークン プロファイルの追加。スーパー管理者がソフトウェア トークン プロファイルを追加する必要があります。
- ユーザーへのトークンの割り当て。

重要：この方法で、トークンを再配布すると、再配布したトークンの既存のユーザーは認証できなくなります。ユーザーは、認証する前に、新しいトークン データをインポートする必要があります。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Distribute Software Tokens in Bulk（ソフトウェア トークンの一括配布）**] > [**Generate Software Token Files（ソフトウェア トークン ファイルの生成）**] の順にクリックします。
2. [**Job Name（ジョブ名）**] フィールドにジョブの名前を入力するか、デフォルトの名前を使用します。ジョブはここで入力した名前で保存され、後でジョブの詳細を表示できます。名前には 1 ～ 128 文字の一意の名前を入力します。&、%、>、< の各文字は使用できません。
3. [**Software Token Profile（ソフトウェア トークン プロファイル）**] ドロップダウン リストから、配布方法としてファイル ベースの配布を使用するソフトウェア トークン プロファイルを選択します。
4. [**DeviceSerialNumber（デバイスのシリアル番号）**] フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
5. [**Nickname（ニックネーム）**] フィールドにニックネームを入力するか、空白のままにします。
6. トークン ファイルのパスワード保護を選択できます。ユーザーは、デバイス上の SecurID アプリケーションにトークンを追加するときに、パスワードを入力する必要があります。次のオプションを選択できます。
   - [**Password（パスワード）**]：任意のパスワードを入力します。このパスワードは、トークン配布ファイル内のすべてのソフトウェア トークンに適用されます。パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
   - [**No password（パスワードなし）**]：ユーザーはパスワードを入力する必要がありません。
   - [**User ID（ユーザー ID）**]：ユーザーは自分のユーザー ID を入力します。
   - [**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**]：ユーザーは、自分のユーザー ID と、管理者が設定したパスワードを入力します。ユーザー ID とパスワードの組み合わせを選択した場合、パスワードとして、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。

7. ［**Password（パスワード）**］を選択した場合は、［**Password（パスワード）**］フィールドおよび［**Confirm Password（パスワードの確認）**］フィールドにパスワードを入力します。
8. ［**Next（次へ）**］をクリックします。
9. トークンの選択基準を入力して、配布するトークンを検索します。たとえば、配布するトークンのシリアル番号の範囲を入力します。
10. ［**Next（次へ）**］をクリックします。
11. 配布のサマリーを確認し、［**Submit Job（ジョブの実行）**］をクリックします。
12. ［**Completed（完了）**］タブをクリックして、完了したジョブを表示します。
13. コンテキスト メニューで［**Download Output File（出力ファイルのダウンロード）**］をクリックします。
14. 出力ファイルをローカルマシンに保存します。
15. トークン ファイルをユーザーに安全に配布します。

ファイル ベースの配布を使用した単一のソフトウェア トークンの配布

ファイル ベースのプロビジョニングを使用して、ソフトウェア トークンを配布する場合、トークン データはトークン配布ファイル（SDTID ファイル）に格納されます。SDTID ファイルは、ダウンロード用の ZIP ファイルに追加されます。

開始する前に

- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションの管理者ガイドを参照してください。
- ソフトウェア トークン プロファイルの追加。ソフトウェア トークン プロファイルを追加できるのは、スーパー管理者だけです。
- ユーザーへのトークンの割り当て。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、配布するソフトウェア トークンを検索します。
3. 検索結果から、配布するソフトウェア トークンをクリックします。
4. コンテキスト メニューで［**Distribute（配布）**］をクリックします。
5. ［**Software Token Profile（ソフトウェア トークン プロファイル）**］ドロップダウン リストから、配布方法としてファイル ベースの配布を使用するソフトウェア トークン プロファイルを選択します。

6. ［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
7. ［**Nickname（ニックネーム）**］フィールドにニックネームを入力するか、空白のままにします。
8. トークン ファイルのパスワード保護を選択できます。次のオプションを使用できます。
   - ［**Password（パスワード）**］：任意のパスワードを入力します。このパスワードは、トークン配布ファイル内のすべてのソフトウェア トークンに適用されます。パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
   - ［**No password（パスワードなし）**］：ユーザーはパスワードを入力する必要がありません。
   - ［**User ID（ユーザー ID）**］：ユーザーは自分のユーザー ID を入力します。
   - ［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］：ユーザーは、自分のユーザー ID と、管理者が設定したパスワードを入力します。ユーザー ID とパスワードの組み合わせを選択した場合、パスワードとして、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
9. ［**Password（パスワード）**］または［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］を選択した場合は、［**Password（パスワード）**］フィールドおよび［**Confirm Password（パスワードの確認）**］フィールドにパスワードを入力します。
10. ［**Save and Distribute（保存して配布）**］をクリックします。
11. ［**Download Now（今すぐダウンロード）**］をクリックします。
12. トークン ファイルをユーザーに安全に配布します。
13. ［**Done（終了）**］をクリックします。

動的シード配布（CT-KIP）を使用した複数のソフトウェア トークンの配布

動的シード配布では、CT-KIP プロトコルを使用して、トークン データを生成するため、トークン ファイルは必要ありません。配布ステップが完了すると、RSA Authentication Manager が CT-KIP サーバの URL リンクと一回限り有効な一意のトークン アクティベーション コードを表示します。トークンを URL 経由でデバイスに配布するには、これら 2 つの情報が必要です。Authentication Manager 8.0 では、特定のモバイル プラットフォーム デバイス タイプ用にカスタムの CT-KIP URL が生成されるようになりました。Android、iPhone、Nokia、Browser Toolbar、Windows Phone などに対応しています。

開始する前に

- CT-KIP サーバの URL リンクと CT-KIP アクティベーション コードをユーザーに安全に配布する方法を決定する。RSA Authentication Manager では、メールは暗号化されません。安全に配布するために、以下を実行できます。
  - ユーザーに電話するなど、オフラインで情報を提供する。
  - 情報をメールにコピーし、メールを暗号化する。
  - エンド ユーザーのデバイスで暗号化メールがサポートされている場合は、SMTP（Simple Mail Transfer Protocol）メール暗号化ゲートウェイを使用する。
- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションのマニュアルを参照してください。
- ソフトウェア トークン プロファイルの追加。
- ユーザーへのトークンの割り当て。
- RSA では、Authentication Manager のデフォルトの証明書を信頼する証明書に置き換えることを推奨しています。デフォルトの証明書を置き換えない場合は、CT-KIP の処理を続行する前に、信頼されていない証明書を受け入れるかどうかを確認するメッセージがエンド ユーザーに表示されます。CT-KIP で動的シード配布を使用する場合は、Authentication Manager サーバまたは Web Tier に信頼された証明書が必要です。

重要：この方法で、トークンを再配布すると、再配布したトークンの既存のユーザーは認証できなくなります。ユーザーは、認証する前に、新しいトークン データをインポートする必要があります。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Distribute Software Tokens in Bulk（ソフトウェア トークンの一括配布）**］＞［**Generate Dynamic Seed Provisioning Credentials（動的シード配布クレデンシャルの生成）**］の順にクリックします。

2. ［**Job Name（ジョブ名）**］フィールドにジョブの名前を入力するか、デフォルトの名前を使用します。ジョブはここで入力した名前で保存され、後でジョブの詳細を表示できます。名前には 1 ～ 128 文字の一意の名前を指定する必要があります。&、%、>、< の各文字は使用できません。
3. ［**Software Token Profile（ソフトウェア トークン プロファイル）**］ドロップダウン リストから、配布方法として動的シード配布を使用するソフトウェア トークン プロファイルを選択します。
4. ［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
5. ［**Nickname（ニックネーム）**］フィールドにニックネームを入力するか、空白のままにします。
6. ［**Next（次へ）**］をクリックします。
7. トークンの選択基準を入力して、配布するトークンを検索します。たとえば、配布するトークンのシリアル番号の範囲を入力します。
8. ［**Next（次へ）**］をクリックします。
9. 配布のサマリーを確認し、［**Submit Job（ジョブの実行）**］をクリックします。
10. ［**Completed（完了）**］タブをクリックして、完了したジョブを表示します。
11. 操作するジョブをクリックします。
12. コンテキスト メニューで［**Download Output File（出力ファイルのダウンロード）**］をクリックします。
13. 出力ファイルをローカルマシンに保存します。
14. 出力ファイルを開き、アクティベーション コードと CT-KIP URL をコピーして、ユーザーに安全に配布します。

注：出力ファイルをダウンロードした場合、一部のスプレッドシート アプリケーションでは、アクティベーション コードの先頭の 0 が削除されます。アクティベーション コードを正常にインポートするには、テキスト エディタなど、文字が削除されないアプリケーションでファイルを開いて、アクティベーション コードを正確にコピーします。

15. トークンをインポートする方法をユーザーに指示します。
    アクティベーション コードの有効期限を構成した場合は、有効期限が切れる前にトークンをインポートするようにユーザーに指示します。有効期限が切れる前にアクティベーション コードが使用されなかった場合は、トークンを再配布し、CT-KIP URL と新しいアクティベーション コードをユーザーに送信する必要があります。
    詳細については、お使いのプラットフォーム用のソフトウェア トークンの管理者ガイドを参照してください。

動的シード配布を使用した単一のソフトウェア トークンの配布

動的シード配布では、CT-KIP プロトコルを使用して、トークン データを生成するため、トークン ファイルは必要ありません。配布ステップが完了すると、RSA Authentication Manager が CT-KIP サーバの URL リンクと一回限り有効な一意のトークン アクティベーション コードを表示します。トークンを URL 経由でデバイスに配布するには、これら 2 つの情報が必要です。
Authentication Manager 8.0 では、特定のモバイル プラットフォーム デバイス タイプ用にカスタムの CT-KIP URL が生成されるようになりました。
Android、iPhone、Nokia、Browser Toolbar、Windows Phone などに対応しています。

開始する前に

- CT-KIP サーバの URL リンクと CT-KIP アクティベーション コードをユーザーに安全に配布する方法を決定する。RSA Authentication Manager では、メールは暗号化されません。より安全な配布オプションとして、以下を実行できます。
  - ユーザーに電話するなど、オフラインで情報を提供する。
  - 情報をメールにコピーし、メールを暗号化する。
  - SMTP（Simple Mail Transfer Protocol）メール暗号化ゲートウェイを使用する。
- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションのマニュアルを参照してください。
- ソフトウェア トークン プロファイルの追加。ソフトウェア トークン プロファイルを追加できるのは、スーパー管理者だけです。
- ユーザーへのトークンの割り当て。
- RSA では、Authentication Manager のデフォルトの証明書を信頼する証明書に置き換えることを推奨しています。デフォルトの証明書を置き換えない場合は、CT-KIP の処理を続行する前に、信頼されていない証明書を受け入れるかどうかを確認するメッセージがエンド ユーザーに表示されます。特定のモバイル デバイス プラットフォームでは、信頼する証明書がインストールされたサーバの SSL 証明書のみをサポートしています。
  CT-KIP で動的シード配布を使用する場合は、Authentication Manager サーバに信頼された証明書が必要です。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、配布するソフトウェア トークンを検索します。
3. 検索結果から、配布するソフトウェア トークンをクリックします。
4. コンテキスト メニューで［**Distribute（配布）**］をクリックします。
5. ［**Software Token Profile（ソフトウェア トークン プロファイル）**］ドロップダウン リストから、配布方法として動的シード配布を使用するソフトウェア トークン プロファイルを選択します。
6. ［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
7. ［**Nickname（ニックネーム）**］フィールドにニックネームを入力するか、空白のままにします。
8. ［**CT-KIP Activation Code（CT-KIP アクティベーション コード）**］ドロップダウン リストから、ソフトウェア トークンのアクティベーション コードを選択します。
9. ［**Save and Distribute（保存して配布）**］をクリックします。
10. アクティベーション コードと CT-KIP URL をコピーして、ユーザーに安全に配布します。
11. トークンをインポートする方法をユーザーに指示します。
    アクティベーション コードの有効期限を構成した場合は、有効期限が切れる前にトークンをインポートするようにユーザーに指示します。有効期限が切れる前にアクティベーション コードが使用されなかった場合は、トークンを再配布し、CT-KIP URL と新しいアクティベーション コードをユーザーに送信する必要があります。
    詳細については、お使いのプラットフォーム用のソフトウェア トークンの管理者ガイドを参照してください。

CTF（Compressed Token Format）を使用した複数のソフトウェア トークンの配布

CTF（Compressed Token Format）を使用してソフトウェア トークンを配布する場合は、URL を生成し、それをユーザーに配布します。この URL には、ソフトウェア トークン アプリケーションで必要なトークン データが含まれています。

開始する前に

- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションのマニュアルを参照してください。
- ソフトウェア トークン プロファイルの追加。ソフトウェア トークン プロファイルを追加できるのは、スーパー管理者だけです。
- ユーザーへのトークンの割り当て。

重要：この方法でトークンを再配布した場合、再配布したトークンのユーザーは、新しいトークン データをインポートするまで認証できません。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Distribute Software Tokens in Bulk（ソフトウェア トークンの一括配布）**］＞［**Generate Compressed Token Format Credentials（Compressed Token Format クレデンシャルの生成）**］の順にクリックします。
2. ［**Job Name（ジョブ名）**］フィールドにジョブの名前を入力するか、デフォルトの名前を使用します。ジョブはここで入力した名前で保存され、後でジョブにアクセスして詳細を表示できます。名前には 1 ～ 128 文字の一意の名前を指定する必要があります。&、%、>、< の各文字は使用できません。
3. ［**Software Token Profile（ソフトウェア トークン プロファイル）**］ドロップダウン リストから、配布方法として CTF を使用するソフトウェア トークン プロファイルを選択します。
4. ［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
5. ［**Nickname（ニックネーム）**］フィールドにニックネームを入力するか、空白のままにします。

6. トークン ファイルのパスワード保護を選択できます。次のオプションを使用できます。
   - ［**Password（パスワード）**］：任意のパスワードを入力します。このパスワードは、トークン配布ファイル内のすべてのソフトウェア トークンに適用されます。パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
   - ［**No password（パスワードなし）**］：ユーザーはパスワードを入力する必要がありません。
   - ［**User ID（ユーザー ID）**］：ユーザーは自分のユーザー ID を入力します。
   - ［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］：ユーザーは、自分のユーザー ID と、管理者が設定したパスワードを入力します。ユーザー ID とパスワードの組み合わせを選択した場合、パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
7. ［**Password（パスワード）**］または［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］を選択した場合は、［**Password（パスワード）**］フィールドおよび［**Confirm Password（パスワードの確認）**］フィールドにパスワードを入力します。
8. ［**Next（次へ）**］をクリックします。
9. トークンの選択基準を入力して、配布するトークンを検索します。たとえば、配布するトークンのシリアル番号の範囲を入力します。
10. ［**Next（次へ）**］をクリックします。
11. 配布のサマリーを確認し、［**Submit Job（ジョブの実行）**］をクリックします。
12. ［**Completed（完了）**］タブをクリックして、完了したジョブを表示します。
13. 操作するジョブをクリックします。
14. コンテキスト メニューで［**Download Output File（出力ファイルのダウンロード）**］をクリックします。
15. 出力ファイルをローカルマシンに保存します。
16. 出力ファイルを開き、CTF URL をコピーして、それらをユーザーに安全に配布します。
17. トークンをインポートする方法をユーザーに指示します。詳細については、お使いのプラットフォーム用のソフトウェア トークンの管理者ガイドを参照してください。

CTF（Compressed Token Format）を使用した単一のソフトウェア トークンの配布

CTF（Compressed Token Format）を使用してソフトウェア トークンを配布する場合は、URL を生成し、それをユーザーに配布します。この URL には、ソフトウェア トークン アプリケーションで必要なトークン データが含まれています。

開始する前に

- デバイス上にソフトウェア トークン アプリケーションをインストールするようユーザーに指示する。インストール手順については、ソフトウェア トークン アプリケーションのマニュアルを参照してください。
- ソフトウェア トークン プロファイルの追加。ソフトウェア トークン プロファイルを追加できるのは、スーパー管理者だけです。
- ユーザーへのソフトウェア トークンの割り当て。詳細については、RSA Security Console ヘルプのトピック「Assign a Software Token to a User（ユーザーへのソフトウェア トークンの割り当て）」を参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Assigned（割り当て済み）**］タブをクリックします。
3. 検索フィールドを使用して、配布するソフトウェア トークンを検索します。
4. 検索結果から、配布するソフトウェア トークンをクリックします。
5. コンテキスト メニューで［**Distribute（配布）**］をクリックします。
6. ［**Software Token Profile（ソフトウェア トークン プロファイル）**］ドロップダウン リストから、配布方法として CTF（Compressed Token Format）を使用するソフトウェア トークン プロファイルを選択します。
7. ［**DeviceSerialNumber（デバイスのシリアル番号）**］フィールドで、次のいずれかを実行します。
   - デバイス クラスにトークンをバインドするには、デフォルトの設定のままにする。
   - 特定のデバイスにトークンをバインドするには、フィールドをクリアし、ユーザーから取得したデバイス ID を入力する。
8. ［**Nickname（ニックネーム）**］フィールドにニックネームを入力するか、空白のままにします。

9. トークン ファイルのパスワード保護を選択できます。次のオプションを使用できます。
   - ［**Password（パスワード）**］：任意のパスワードを入力します。このパスワードは、トークン配布ファイル内のすべてのソフトウェア トークンに適用されます。パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
   - ［**No password（パスワードなし）**］：ユーザーはパスワードを入力する必要がありません。
   - ［**User ID（ユーザー ID）**］：ユーザーは自分のユーザー ID を入力します。
   - ［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］：ユーザーは、自分のユーザー ID と、管理者が設定したパスワードを入力します。ユーザー ID とパスワードの組み合わせを選択した場合、パスワードは、128 ビットトークンの場合は最長 24 文字、64 ビットトークンの場合は最長 8 文字まで指定できます。
10. ［**Password（パスワード）**］または［**Combination User ID followed by Password（ユーザー ID とパスワードの組み合わせ）**］を選択した場合は、パスワードを作成し、［**Password（パスワード）**］フィールドおよび［**Confirm Password（パスワードの確認）**］フィールドに入力します。
11. ［**Save and Distribute（保存して配布）**］をクリックします。
12. CTF URL をコピーして、ユーザーに安全に配布します。

    注：CTF URL をコピーする前にこのページから移動した場合は、配布プロセスを最初から実行し直して、新しい URL を生成する必要があります。

13. トークンをインポートする方法をユーザーに指示します。詳細については、お使いのプラットフォーム用のソフトウェア トークンの管理者ガイドを参照してください。

RSA SecurID トークンの管理

トークンの管理には、トークンの管理とユーザーへの一時エマージェンシー アクセスの提供が含まれます。トークンに関する以下のタスクを実行できます。

- 246 ページの トークンの有効化
- 247 ページの トークンの無効化
- 247 ページの トークンの削除
- 248 ページの トークンの編集
- 249 ページの 交換用トークンの割り当て

トークンの有効化または無効化

有効化されたトークンは認証に使用できます。無効化されたトークンは認証に使用できません。

Authentication Manager をインストールした後、トークンを導入環境にインポートする必要があります。インポートしたすべてのトークンは自動的に無効化されます。ユーザーがトークンを紛失した場合や盗難に遭った場合に、このセキュリティ機能が導入環境を保護します。

トークンは、管理者がユーザーに割り当てたときに自動的に有効化されます。

セルフサービス経由で提供されるトークンコードのみ（PIN レス）のソフトウェア トークンは、デフォルトで無効化されています。ユーザーは、Self-Service Console からトークンを有効化する必要があります。

トークンが無効化されても、ユーザーのアカウントはロックされません。ロックアウトはユーザーのアカウントに適用されます。トークンはロックアウトされません。トークンを無効化しても、ユーザーのアカウントが導入環境から削除されるわけではありません。無効化したトークンは、Security Console に表示できます。

有効化 / 無効化できるのは、管理者の権限適用範囲のセキュリティ ドメインのトークンのみです。

次のような状況では、割り当てられたトークンを無効化する必要があります。

- ハードウェア トークンをユーザーに送付する前。割り当て先のユーザーにトークンが届いたことを確認したら、トークンを再度有効化します。
- ユーザーが長期間認証する必要がないことが分かっている場合。たとえば、割り当て先のユーザーが長期休暇を取る前に、必要に応じてトークンを無効化します。トークンを無効化すると、再有効化されるまでユーザーがそのトークンを使用して認証を受けることができなくなります。

トークンの有効化

ユーザーが割り当てられたトークンで認証できるようにするには、トークンを有効化する必要があります。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Assigned（割り当て済み）**］タブまたは［**Unassigned（未割り当て）**］タブをクリックして、有効化するトークンのリストを表示します。
3. 有効化するトークンの横にあるチェックボックスをオンにします。
4. ［**Action（アクション）**］メニューから、［**Enable（有効化）**］をクリックします。
5. ［**Go（実行）**］をクリックします。

トークンの無効化

トークンを無効化すると、割り当てられているユーザーはそのトークンを使用して、認証することができなくなります。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. [**Assigned（割り当て済み）**] タブまたは [**Unassigned（未割り当て）**] タブをクリックして、無効化するトークンのリストを表示します。
3. 無効化するトークンの横にあるチェックボックスをオンにします。
4. [**Action（アクション）**] メニューから、[**Disable（無効化）**] をクリックします。
5. [**Go（実行）**] をクリックします。

トークンの削除

トークンを削除すると、トークンは内部データベースから削除され、割り当てることができなくなります。すでにユーザーに割り当てられている場合、ユーザーはそのトークンを使用して認証することができなくなります。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 削除するトークンがユーザーに割り当てられているかどうかに応じて、[**Assigned（割り当て済み）**] タブまたは [**Unassigned（未割り当て）**] タブをクリックします。
3. 検索フィールドを使用して、削除するトークンを検索します。
4. 検索結果で、削除するトークンの横にあるチェックボックスをオンにします。
5. [Action（アクション）] メニューから、[**Delete（削除）**] をクリックします。
6. [**Go（実行）**] をクリックします。
7. 削除ダイアログ ボックスで [**OK**] をクリックして、削除を確定します。

トークンの編集

トークンの割り当て先のセキュリティ ドメインなど、トークンに関する情報を更新するためにトークンを編集します。また、以下の操作も可能です。

- トークンを有効化または無効化する。
- SecurID PIN をクリアする。
- ユーザーが次回トークンを使用して認証するときに、SecurID PIN を変更するように要求する。トークンがユーザーに割り当てられている場合にのみ、PIN の表示、クリア、変更などのオプションが表示されます。
- ユーザーが SecurID PIN を入力する必要があるかどうかを指定する。

手順

1. Security Console で、［**Authentication（認証）**］＞［**SecurID Tokens（SecurID トークン）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 編集するトークンがユーザーに割り当てられているかどうかに応じて、［**Assigned（割り当て済み）**］タブまたは［**Unassigned（未割り当て）**］タブをクリックします。
3. 検索フィールドを使用して、編集するトークンを検索します。
4. 検索結果から、編集するトークンをクリックします。
5. コンテキスト メニューで［**Edit（編集）**］をクリックします。
6. トークン レコードに必要な変更を加えます。
7. ［**Save（保存）**］をクリックします。
   保存していない場合は、［**Reset（リセット）**］をクリックして、トークン レコードを編集前の状態にリセットできます。

トークンの紛失、盗難、破損、有効期限切れに関するユーザー支援

ユーザーは Self-Service Console を使用して、交換用トークンと一時エマージェンシー アクセス トークンコードをリクエストできます。

トークンの破損、紛失、一時的な置き忘れ、盗難、期限切れが発生した場合には、ユーザーに対して一時エマージェンシー アクセス トークンコードを提供できます。Authentication Manager がエマージェンシー アクセス トークンコードを生成します。ユーザーはトークンの問題が解決するまでの間、このコードを使用して 2 要素認証による認証を受けることができます。詳細については、導入環境間でのユーザーとトークンのエクスポートおよびインポートを参照してください。

注：期限切れのトークンに対してエマージェンシー アクセス トークンコードを割り当てることはできません。一時アクセスを提供する前にトークンをリプレースしてください。

トークンを完全に紛失したり、盗難に遭ったり、破損したり、期限切れになった場合は、トークンをリプレースする必要があります。詳細については、交換用トークンの割り当てを参照してください。

交換用トークンの割り当て

トークンの完全な紛失、破損、期限切れが生じたユーザーに対しては、交換用トークンを割り当てることができます。

手順

1. Security Console で、[**Authentication（認証）**] > [**SecurID Tokens（SecurID トークン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、交換が必要なトークンを検索します。
3. 検索結果から、交換が必要なトークンをクリックします。
4. [**Replace with Next Available Token（次に使用可能なトークンに交換）**] をクリックします。

トークンの再同期

トークンに表示されているトークンコードと、Authentication Manager によって生成されたトークンコードが一致しない場合は、トークンを再同期する必要があります。トークンコードが一致しない場合、認証が失敗します。構成に応じて、ユーザーが Self-Service Console でトークンを再同期できます。トークンを再同期する場合も Security Console を使用できます。

開始する前に

トークンコードにアクセスする必要があります。ユーザーは、トークンコードを読み取って管理者に電話で伝える必要があります。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、トークンを再同期する必要があるユーザーを検索します。
3. 検索結果から、トークンを再同期する必要があるユーザーをクリックします。
4. コンテキスト メニューから [**SecurID Tokens（SecurID トークン）**] をクリックします。
5. 再同期するトークンをクリックします。
6. [**Resynchronize Token（トークンの再同期）**] をクリックします。

7. ユーザーのトークンに表示されたトークンコードを入力します。
8. トークンコードが変わるのを待ち、新しいトークンコードを入力します。
9. ［**Resynchronize（再同期）**］をクリックします。

導入環境間でのユーザーとトークンのエクスポートおよびインポート

2 つの Authentication Manager 8.0 導入環境間で、トークン レコードとユーザー レコードをエクスポートおよびインポートできます。2 つの導入環境をマージする場合や、導入環境間でトークンを移動する場合に、この操作を実行します。トークンをエクスポートおよびインポートすることや、ユーザーとそのユーザーに割り当てられたトークンをエクスポートおよびインポートすることができます。ソース導入環境からエクスポートし、ターゲット導入環境にインポートできます。割り当て済みまたは未割り当てのトークンを移動し、ターゲット導入環境の別のユーザーにそのトークンを再割り当てすることができます。Authentication Manager は、処理を安全に実行するために、エクスポート ファイルを暗号化します。

エクスポートおよびインポートによる認証への影響

新しい導入環境にユーザーを移動しても、ソース導入環境からエクスポートしたデータは削除されないため、認証が中断されることはありません。ユーザー レコードをターゲット導入環境にインポートした後でも、ユーザーは引き続きソース導入環境で認証できます。ソース導入環境からユーザーを手動で削除する必要があります。

エクスポートおよびインポートによるアイデンティティ ソースへの影響

Authentication Manager は、ユーザーのエクスポートおよびインポートを処理する際、内部と外部のアイデンティティ ソースで異なった処理をします。

注： ［Identity Source Mapping（アイデンティティ ソース マッピング）］ページでアイデンティティ ソースを選択します。

外部アイデンティティ ソースからエクスポートし、外部アイデンティティ ソースにインポートする

ソース導入環境とターゲット導入環境の両方で、ユーザー レコードが外部アイデンティティ ソース（LDAP ディレクトリ サーバ）に格納されている場合、Authentication Manager は LDAP ディレクトリ サーバの各ユーザー レコードを参照する参照レコードをターゲット導入環境に作成します。移動するユーザーは、ソース導入環境とターゲット導入環境で同じユーザー ID を持つ必要があります。

次の事項が適用されます。

- ターゲット導入環境にユーザー レコードがすでに存在しており、ユーザーに 1 つ以上のトークンがすでに割り当てられている場合、Authentication Manager はユーザーとトークンをインポートしません。代わりに、例外メッセージをログに記録します。
- ターゲット導入環境にユーザー レコードがすでに存在しており、ユーザーにトークンが割り当てられていない場合、Authentication Manager はターゲット導入環境のユーザー レコードを更新し、トークンをインポートします。また、システム ログに警告メッセージを書き込みます。

内部アイデンティティ ソースからエクスポートし、内部アイデンティティ ソースにインポートする

ユーザー レコードがソース導入環境とターゲット導入環境の両方の内部データベースに格納されている場合、Authentication Manager は、同一レコードが存在しない場合のみ、ターゲット導入環境の内部データベースに新しいレコードを追加します。ターゲット導入環境に同一ユーザー レコードがすでに存在している場合は、レコードが複製されることはなく、そのユーザーおよびリンクされたすべてのトークンは無視されます。

内部アイデンティティ ソースからエクスポートし、外部アイデンティティ ソースにインポートする

ソース導入環境で内部アイデンティティ ソースを使用しており、ターゲット導入環境で外部アイデンティティ ソースを使用している場合は、次の事項が適用されます。

- ターゲット導入環境にユーザー レコードがすでに存在しており、ユーザーに 1 つ以上のトークンが割り当てられている場合、Authentication Manager はユーザーとトークンをインポートしません。代わりに、例外メッセージをログに記録します。
- ターゲット導入環境にユーザー レコードがすでに存在しており、ユーザーにトークンが割り当てられていない場合、Authentication Manager はターゲット導入環境のユーザー レコードを更新し、トークンをインポートします。また、システム ログに警告メッセージを書き込みます。

外部アイデンティティ ソースからエクスポートし、内部アイデンティティ ソースにインポートする

ソース導入環境で外部アイデンティティ ソースを使用している場合、ユーザーの LDAP パスワードはエクスポートされません。ユーザー レコードはパスワードなしで内部データベースにインポートされ、パスワード認証が無効化されます。ユーザーがパスワード認証を行う必要がある場合は、パスワードをリセットするか、ユーザーが Self-Service Console を使用して、パスワードを作成する必要があります。詳細については、RSA Security Console ヘルプのトピック「ユーザーとトークンのエクスポート後にユーザーのパスワードリセットを有効化する」を参照してください ターゲット導入環境に同一ユーザー レコードがすでに存在している場合は、レコードが複製されることはなく、そのユーザーおよびリンクされたすべてのトークンは無視されます。

エクスポートおよびインポートによるユーザーへの影響

エクスポートおよびインポート操作は、次のような影響をユーザー レコードに与えます。

- エクスポートされたユーザーの RBA（リスク ベース認証）がソース導入環境で有効化されているが、ターゲット導入環境に RBA のライセンスがない場合は、インポート後にユーザーの RBA が無効化されます。ターゲット導入環境に RBA のライセンスがある場合、ユーザーはインポート後にソース導入環境のステータスに従って RBA が有効化または無効化されます。
- エクスポートされたユーザーがソース導入環境で RADIUS プロファイルまたはユーザー エイリアスを持っている場合、ターゲット導入環境では RADIUS プロファイルおよびエイリアスが無効化されます。ユーザーは、RADIUS を使用して認証できなくなります。詳細については、354 ページの RADIUS プロファイルおよび RSA Security Console ヘルプのトピック「RADIUS プロファイルへのユーザーエイリアスの割り当て」を参照してください。
- ソース導入環境とターゲット導入環境で PIN ポリシーが異なる場合は、異なる PIN 標準に準拠するために、各ユーザーが初めてターゲット導入環境にログオンするときに、PIN の変更が必要になります。
- ターゲット導入環境が次の条件を満たしている場合は、ユーザーのセキュリティ クエスチョンと回答がインポートされる。
  - 言語が両方の導入環境で同じである。言語が一致しない場合、ユーザーはセキュリティ クエスチョンの回答なしでインポートされます。RSA では、ソース導入環境とターゲット導入環境で同じ言語を使用することを推奨します。
  - 同じセキュリティ クエスチョンが両方の導入環境に存在する必要があります。質問が異なる場合、ユーザーはセキュリティ クエスチョンの回答なしでインポートされます。
  - ターゲット導入環境でユーザーが回答する必要がある質問の数が、ソース導入環境で必要な数と同じかそれよりも少ない場合、ユーザーと回答がインポートされる。ターゲット導入環境でソース導入環境よりも多くの質問に回答する必要がある場合、ユーザーは回答なしでインポートされます。ユーザーは、初めてターゲット導入環境にログオンするときに、セキュリティ クエスチョンと回答を再構成する必要があります。詳細については、150 ページのセキュリティ クエスチョンの管理を参照してください。
  - 外部アイデンティティ ソースのユーザーがすでにターゲット導入環境に登録されている場合、ユーザーおよびユーザーの回答はインポートされない。

- Mobile Number（携帯電話番号）属性定義がアイデンティティ属性定義に含まれており、SMS（Short Message Service）サービス プロバイダを使用している場合は、ODA（On-Demand 認証）がサポートされます。Mobile Number（携帯電話番号）がエクスポートされる唯一の拡張属性です。Mobile Number（携帯電話番号）は、ユーザー レコードに含まれている場合に、エクスポートされ、除外することはできません。SMS がターゲット導入環境で構成されている場合、ユーザーは携帯電話番号を使用して ODA 認証できます。
- ソフトウェア トークン プロファイルはインポートされません。ソース導入環境とターゲット導入環境に同じプロファイルが存在する場合は、プロファイルとトークンの間の関連づけがインポートされます。Authentication Manager では、ソフトウェア トークン プロファイルのインポートを次のように処理します。
  - ソース導入環境とターゲット導入環境でソフトウェア トークン プロファイルの名前が一致する場合、トークンはソフトウェア トークン プロファイルの関連づけを保持したままインポートされます。
  - ソース導入環境とターゲット導入環境でソフトウェア トークン プロファイルの名前が一致しない場合、トークンはインポートされるが、ソフトウェア トークン プロファイルはトークンに関連づけられません。ソフトウェア トークン プロファイルは認証に影響しませんが、トークンの配布に影響します。デフォルトでは、これらのトークンを紛失、破損した場合や、交換が必要な場合に、Self-Service Console を使用して交換することはできません。RSA では、これらのトークンを交換する必要がある場合は、ユーザーが新しいトークンをリクエストすることを推奨します。また、代替策として、管理者が新しいプロファイルを使用して Security Console から現在のトークンを再配布すれば、ユーザーは Self-Service Console から、交換をリクエストできるようになります。ただし、この方法を使用すると再配布されたトークンの認証に影響します。詳細については、229 ページのソフトウェア トークン プロファイルを参照してください。
  - ソース導入環境のソフトウェア トークン プロファイルに、ターゲット導入環境にはない新しいデバイス タイプが含まれている場合は、トークンのインポート時に新しいデバイス タイプがトークンから削除されます。
  - 割り当て済みのトークンをユーザーなしでインポートした場合、ソフトウェア トークン プロファイルの関連づけは削除され、デバイス タイプはデフォルトのデバイス定義タイプにリセットされます。

暗号化キーのダウンロード

暗号化キーは、RSA 公開鍵ペアの公開鍵です。暗号化キーにより、次のことが保証されます。

- エクスポートしたトークンとユーザー レコードをターゲット導入環境にのみインポートできる。
- エクスポート データが暗号化されるため、転送中のデータの読み取りや改ざんが防止される。
- ソース導入環境とターゲット導入環境の間だけで通信可能になる。

ソース導入環境からユーザーまたはトークンをエクスポートする前に、ターゲット導入環境から暗号化キーをダウンロードする必要があります。

手順

1. ターゲット導入環境の Security Console で、[**Administration（管理）**] > [**Export/ Import Tokens and Users（トークンおよびユーザーのエクスポート / インポート）**] > [**Download Encryption Key（暗号化キーのダウンロード）**] の順にクリックします。
2. [**Download Now（今すぐダウンロード）**] をクリックします。
3. [**File Download（ファイルのダウンロード）**] ダイアログ ボックスを使用して、暗号化キーの保存場所を選択し、[**Save（保存）**] をクリックします。
4. お使いのブラウザで必要なローカル ディレクトリへの保存操作を完了します。
5. [**Done（終了）**] をクリックします。

次のステップ

ソース導入環境からトークンまたはユーザーとトークンをエクスポートします。254 ページのトークンのエクスポートおよび 257 ページのトークンを割り当てられたユーザーのエクスポートを参照してください。

トークンのエクスポート

導入環境からトークン レコードをエクスポートするには、Security Console を使用します。その後、レコードを別の導入環境にインポートできます。

重要：トークンは、ソース導入環境でユーザーに割り当て済みであった場合でも、ターゲット導入環境には未割り当ての状態でインポートされます。

開始する前に

- トークンをインポートするターゲット導入環境から暗号化キーをダウンロードする。254 ページの暗号化キーのダウンロードを参照してください。
- エクスポートするトークンが属するセキュリティ ドメインを選択する。そのセキュリティ ドメインからすべてのトークンがエクスポートされます。特定のトークンをエクスポートする場合は、一時的なセキュリティ ドメインにトークンを移動し、そのセキュリティ ドメインのみをエクスポートします。

手順

1. ソース導入環境の Security Console で、[**Administration（管理）**] > [**Export/Import Tokens and Users（トークンおよびユーザーのエクスポート / インポート）**] > [**Export Tokens and Users（トークンおよびユーザーのエクスポート）**] の順にクリックします。
2. [**Encryption Key Location（暗号化キーの場所）**] フィールドで、ターゲット導入環境からダウンロードした暗号化キーを参照します。
3. [Export Job Name（エクスポート ジョブ名）] フィールドで、エクスポート タスクを処理するジョブの名前を指定します。RSA では、デフォルトのジョブ名のままにすることを推奨します。ジョブ名を編集する場合は、一意にする必要があります。
4. [**Export Type（エクスポート タイプ）**] フィールドで、[**Tokens Only（トークンのみ）**] を選択します。
5. [**Next（次へ）**] をクリックします。
6. [Token Selection（トークンの選択）] セクションの [**Security Domain（セキュリティ ドメイン）**] フィールドで、ソース セキュリティ ドメインを選択します。このセキュリティ ドメインのトークンのみがエクスポートされます。
7. 選択したセキュリティ ドメインのサブドメインを含める場合にのみ、[**Subdomains（サブドメイン）**] フィールドで、[**Include subdomains（サブドメインを含める）**] を選択します。
8. [**Status（ステータス）**] フィールドで、エクスポートするトークンのステータスを選択します。
9. [**Export（エクスポート）**] をクリックします。

   [Export/Import Status（エクスポート / インポート ステータス）] ページに移動します。エクスポートの進行状況が自動的に更新されます。ページを更新する必要はありません。
10. [**Download File（ファイルのダウンロード）**] をクリックして、エクスポート ファイルをダウンロードし、ローカル マシンに保存します。
11. System Log Report（システム ログ レポート）を実行して、エクスポートの結果を表示します。詳細については、386 ページのレポートを参照してください。

次のステップ

ターゲット導入環境にトークンをインポートします。256 ページの別の導入環境からのトークンのインポートを参照してください。

別の導入環境からのトークンのインポート

別の導入環境からエクスポートされたトークンをインポートできます。トークン データと一緒にカスタム トークン属性はインポートされません。標準のトークン属性はインポートされます。ソフトウェア トークン プロファイルはインポートされません。ソース導入環境とターゲット導入環境にまったく同じプロファイルが存在する場合は、プロファイルとトークンの間の関連づけがインポートされます。トークンのインポートがソフトウェア トークン プロファイルの関連づけに与える影響については、252 ページのエクスポートおよびインポートによるユーザーへの影響を参照してください。ソース導入環境でユーザーに割り当てられていない重複するトークンは、ターゲット導入環境にインポートされません。

このトピックでは、別の導入環境からエクスポートされたトークンをインポートする方法について説明します。新しいトークン レコード ファイルをインポートするには、226 ページのトークン レコード ファイルのインポートを参照してください。

開始する前に

- ソース導入環境からトークンをエクスポートする。254 ページのトークンのエクスポートを参照してください。
- RSA では、インポートするトークン用の新しいセキュリティ ドメインをターゲット導入環境に作成することを推奨します。これにより、簡単に新しいデータを分離し、その正確性を検証できます。インポートが正しいことを確認したら、別の適切なセキュリティ ドメインにこのデータを移動できます。

手順

1. ターゲット導入環境の Security Console で、［**Administration（管理）**］＞［**Export/Import Tokens and Users（トークンおよびユーザーのエクスポート / インポート）**］＞［**Import Tokens and Users（トークンおよびユーザーのインポート）**］の順にクリックします。
2. ［**Import Job Name（インポート ジョブ名）**］フィールドで、インポート ジョブの名前を指定します。
3. インポート ファイルの場所を選択します。
4. ［**Next（次へ）**］をクリックします。
5. ［**Security Domain Selection（セキュリティ ドメインの選択）**］ページで、インポート後のトークンのターゲット セキュリティ ドメインを選択します。選択できるセキュリティ ドメインは 1 つだけです。
6. ［**Next（次へ）**］をクリックします。

7. ［**Pre-Import Summary（インポート前のサマリー）**］ページで、インポート操作の詳細が正しいことを確認します。
8. ［**Import（インポート）**］をクリックします。［**Export/Import Status（エクスポート / インポート ステータス）**］ページに移動します。インポートのステータスが自動的に更新されます。

   インポートが完了すると、トークンが未割り当ての状態で選択したセキュリティ ドメインに追加されます。
9. レポートを実行して、インポート ジョブの結果を表示します。「**Imported Users and Tokens Report（インポートされたユーザーおよびトークン レポート）**」テンプレートを使用します。詳細については、386 ページのレポートを参照してください。

注：RSA では、「Imported Users and Tokens Report（インポートされたユーザーおよびトークン レポート）」テンプレートの［**Job Name（ジョブ名）**］フィールドで、特定のインポート ジョブの名前を選択しないことを推奨します。レポートを実行するときにのみ、インポート ジョブの名前を選択します。テンプレートでインポート ジョブの名前を選択すると、実行するすべてのレポートで同じジョブ名が使用されます。

トークンを割り当てられたユーザーのエクスポート

導入環境からユーザーとトークンをエクスポートするには、Security Console を使用します。その後、レコードを別の環境にインポートできます。トークンが割り当てられているユーザーのみがエクスポートされます。

グループにユーザーを追加し、エクスポート時にこれらのグループのみを選択できます。グループを使用してユーザーをフィルタできますが、グループはエクスポートされません。グループ メンバーシップもエクスポートされません。

ユーザーのエクスポートが RBA（リスク ベース認証）、ODA（On-Demand 認証）、RADIUS の使用状況に与える影響については、250 ページのエクスポートおよびインポートによるアイデンティティ ソースへの影響を参照してください。

開始する前に

- ユーザーとトークンをインポートするターゲット導入環境から暗号化キーをダウンロードする。254 ページの暗号化キーのダウンロードを参照してください。
- この操作がアイデンティティ ソースに与える影響を理解する。250 ページのエクスポートおよびインポートによるアイデンティティ ソースへの影響を参照してください。
- エクスポートするユーザー レコードが属するセキュリティ ドメインを選択する。ユーザー レコードと異なるセキュリティ ドメインにトークンが存在していても構いません。トークンは、ユーザー レコードに従います。

手順

1. ソース導入環境の Security Console で、[**Administration（管理）**] > [**Export/Import Tokens and Users（トークンおよびユーザーのエクスポート / インポート）**] > [**Export Tokens and Users（トークンおよびユーザーのエクスポート）**] の順にクリックします。
2. [**Encryption Key Location（暗号化キーの場所）**] フィールドで、ターゲット導入環境からダウンロードした暗号化キーを参照します。
3. [**Export Job Name（エクスポート ジョブ名）**] フィールドで、エクスポート ジョブの名前を指定します。RSA では、ジョブ名をデフォルトのままにすることを推奨します。ジョブ名を編集する場合は、新しい名前が一意である必要があります。
4. [**Export Type（エクスポート タイプ）**] フィールドで、[**Users with Tokens（ユーザーとトークン）**] を選択します。
5. [**Next（次へ）**] をクリックします。
6. [Security Domain（セキュリティ ドメイン）] セクションの [**Security Domain（セキュリティ ドメイン）**] フィールドで、エクスポートするユーザーが属するセキュリティ ドメインを選択します。
7. 選択したセキュリティ ドメインのサブドメインを含める場合にのみ、[**Subdomains（サブドメイン）**] フィールドで、[**Include subdomains（サブドメインを含める）**] を選択します。
8. [**User Selection（ユーザーの選択）**] セクションで、次のいずれかを実行します。
   - 選択したセキュリティ ドメイン内のすべてのユーザーをエクスポートする。
   - エクスポートするユーザーのグループを検索する。選択したグループに属する、選択したセキュリティ ドメインとそのサブドメインのユーザーのみがエクスポートされます。他のセキュリティ ドメインのユーザーは無視されます。セキュリティ ドメインに関係なく、エクスポートされるユーザーに割り当てられているトークンがエクスポートされます。

   グループ単位でエクスポートするユーザーを選択する場合は、エクスポートするユーザーが含まれているグループを検索し、矢印ボタンを使用して、[**Available Groups（選択可能なグループ）**] ボックスから [**Selected Groups（選択したグループ）**] に移動します。
9. [**Export（エクスポート）**] をクリックします。

   [Export/Import Status（エクスポート / インポート ステータス）] ページに移動します。エクスポートの進行状況が自動的に更新されます。

10. ［Export/Import Status（エクスポート / インポート ステータス）］ページで、［**Download File（ファイルのダウンロード）**］をクリックして、エクスポート ファイルをダウンロードし、ローカル マシンに保存します。
11. System Log Report（システム ログ レポート）を実行して、エクスポートの結果を表示します。詳細については、386 ページのレポートを参照してください。

次のステップ

ターゲット導入環境にユーザーとトークンをインポートします。259 ページのトークンを割り当てられたユーザーのインポートを参照してください。

トークンを割り当てられたユーザーのインポート

別の導入環境からエクスポートしたトークン レコードおよびユーザー コードをインポートできます。ユーザーは、グループ メンバーシップなしで、1 つのセキュリティ ドメインにインポートされます。ターゲット導入環境で割り当てられていないトークンは、エクスポート ファイル内の一致する割り当て済みトークンによって上書きされます。

ユーザーのエクスポートが RBA（リスク ベース認証）、ODA（On-Demand 認証）、RADIUS の使用状況に与える影響については、250 ページのエクスポートおよびインポートによるアイデンティティ ソースへの影響を参照してください。

ソフトウェア トークン プロファイルはインポートされません。ソース導入環境とターゲット導入環境に同じプロファイルが存在する場合は、プロファイルとトークンの間の関連づけがインポートされます。ユーザーとトークンをインポートする際にソフトウェア トークン プロファイルの関連づけを保持する方法については、252 ページのエクスポートおよびインポートによるユーザーへの影響を参照してください。

次の情報もインポートされません。

- カスタム トークン属性
- 拡張ユーザー属性
- リスク ベース認証デバイス履歴

開始する前に

- この操作がアイデンティティ ソースに与える影響を理解する。250 ページのエクスポートおよびインポートによるアイデンティティ ソースへの影響を参照してください。
- ソース導入環境からユーザーとトークンをエクスポートする。
- インポート対象のユーザーがターゲット導入環境の外部アイデンティティ ソースに格納される場合は、ターゲット導入環境で使用する LDAP ディレクトリ サーバにそのユーザーがすでに存在することを確認する。

- ソース導入環境とターゲット導入環境で同じユーザー ID 命名規則を使用する。
- RSA では、追加するユーザーとトークン用に新しいセキュリティ ドメインをターゲット導入環境に作成することを推奨します。これにより、簡単に新しいデータを分離し、その正確性を検証できます。インポートが正しいことを確認したら、別の適切なセキュリティ ドメインにこのデータを移動できます。

手順

1. ターゲット導入環境の Security Console で、**［Administration（管理）］＞［Export/Import Tokens and Users（トークンおよびユーザーのエクスポート / インポート）］＞［Import Tokens and Users（トークンおよびユーザーのインポート）］**の順にクリックします。
2. **［Import Job Name（インポート ジョブ名）］**フィールドで、インポート ジョブの名前を指定します。
3. インポート ファイルの場所を選択します。
4. **［Next（次へ）］**をクリックします。
5. ［Security Domain Selection（セキュリティ ドメインの選択）］ページで、ユーザーとトークンのターゲット セキュリティ ドメインを選択します。選択できるセキュリティ ドメインは 1 つだけです。
6. **［Next（次へ）］**をクリックします。
7. ［Identity Source Mapping（アイデンティティ ソース マッピング）］ページで、システムがユーザーを検索するターゲット導入環境のアイデンティティ ソースを選択します。内部データベースを選択した場合、ユーザーはターゲット導入環境の内部データベースに作成されます。
8. **［Next（次へ）］**をクリックします。
9. ［Pre-Import Summary（インポート前のサマリー）］ページで、インポート操作の詳細が正しいことを確認します。
10. **［Import（インポート）］**をクリックします。［Export/Import Status（エクスポート / インポート ステータス）］ページに移動します。インポートのステータスが自動的に更新されます。

    インポートが完了すると、ユーザーが割り当てられているトークンと一緒に選択したセキュリティ ドメインに配置されます。
11. レポートを実行して、インポート ジョブの結果を表示します。**「Imported Users and Tokens Report（インポートされたユーザーおよびトークン レポート）」**テンプレートを使用します。詳細については、386 ページのレポートを参照してください。

注：レポートを実行するときに、インポート ジョブの名前を指定します。「Imported Users and Tokens Report（インポートされたユーザーおよびトークン レポート）」テンプレートの［Job Name（ジョブ名）］フィールドには、特定の名前を指定しないでください。テンプレートでインポート ジョブの名前を選択すると、実行するすべてのレポートで同じジョブ名が使用されます。

次のステップ

初めてターゲット導入環境にログオンするときに、セキュリティ クエスチョンと回答を構成する必要があることをユーザーに伝えます。

10 On-Demand 認証の導入

On-Demand 認証

ODA（On-Demand 認証）は、テキスト メッセージまたはメールで送付される On-Demand トークンコードをユーザーが受信できるサービスです。ODA を使用して、SSL-VPN、シン クライアント、Web ポータルなどのリソースを保護できます。

ユーザーが有効な PIN を使用してエージェントにログオンすると、システムからユーザーにテキスト メッセージまたはメールでトークンコードが送信されます。ユーザーは、保護されたリソースにアクセスするために、トークンコードの入力を求められます。

プライマリ認証方式として ODA を使用する場合は、保護対象のリソースに RSA Authentication Agent ソフトウェアをインストールする必要があります。

注：SMS 配信を使用するには、SMS プロバイダとの関係を確立し、SMS を Manager と統合する必要があります。

On-Demand 認証の計画

ODA（On-Demand 認証）を使用する計画がある場合は、On-Demand トークンコードの配信方法を導入環境に構成する必要があります。ユーザーの On-Demand 認証を有効化し、ユーザーが On-Demand トークンコードを受信できるようにする必要があります。

Authentication Manager は、On-Demand トークンコードを次の 2 つの方法で配信できます。

- 携帯電話にテキスト メッセージで配信する。On-Demand トークンコードをユーザーの携帯電話に配信するには、Authentication Manager に SMS プロバイダやモデムを統合する必要があります。SMS プロバイダやモデムのベンダーが要求するパラメータを使用して Authentication Manager を構成してください。操作手順については、264 ページのテキスト メッセージによる On-Demand トークンコード配信の構成を参照してください。
- メール アカウントに配信する。SMTP（Simple Mail Transfer Protocol）サーバへの接続を構成する必要があります。操作手順については、271 ページのメールによる On-Demand トークンコード配信の構成を参照してください。

注：配信方法は、各ユーザーごとに、携帯電話とメールのいずれか 1 つだけを選択できます。

ユーザーが On-Demand トークンコードを受信できるようにするには、ユーザーに対して ODA を有効化しておく必要があります。操作手順については、276 ページの On-Demand 認証を使用するためのユーザーの構成を参照してください。

テキスト メッセージによる On-Demand トークンコード配信の構成

テキスト メッセージを使用して On-Demand トークンコードを携帯電話に送信するには、次のタスクを実行します。

1. Authentication Manager が携帯電話番号を格納しているアイデンティティ ソースの属性にアクセスできることを確認します。Authentication Manager は、内部データベースと LDAP ディレクトリの携帯電話番号属性を自動的にマッピングします。
   （オプション）Security Console を使用して、内部データベースと LDAP ディレクトリのカスタム属性にマッピングすることもできます。264 ページの On-Demand トークンコードをテキスト メッセージで配信するためのアイデンティティ属性定義を参照してください。
2. 266 ページの On-Demand トークンコードの配信のための HTTP プラグ インの構成。

On-Demand トークンコードをテキスト メッセージで配信するためのアイデンティティ属性定義

Authentication Manager 8.0 から携帯電話番号およびメール アドレスを格納しているアイデンティティ ソース属性にアクセスできる必要があります。Authentication Manager は、内部データベースと LDAP ディレクトリのメール属性とモバイル属性を自動的にマッピングします。Security Console を使用して、内部データベースと LDAP ディレクトリのカスタム属性にマッピングすることもできます。

On-Demand トークンコードをテキスト メッセージで配信する場合は、次の表を使用して、Authentication Manager からユーザーの携帯電話番号にアクセスできることを確認するために必要な属性の構成を判断してください。

導入環境内のアイデンティティ ソース	構成
内部データベース	属性マッピングは必要ありません。
LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つあり、LDAP ディレクトリの［mobile（携帯電話）］属性フィールドにある携帯電話番号の値を使用する場合。	属性マッピングは必要ありません。 外部アイデンティティ ソースを追加する時に、Authentication Manager は、LDAP ディレクトリの［mobile（携帯電話）］属性を自動的にリンクします。 On-Demand トークンコードの配信を構成する場合は、［SMS Configuration（SMS の構成）］ページにある［User Attribute to Provide SMS Destination（SMS の宛先を保存するユーザー属性）］ドロップダウン メニューから［Mobile Number（携帯電話番号）］を選択します。
LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つあり、LDAP ディレクトリの［mobile（携帯電話）］属性フィールド以外の属性フィールドにある携帯電話番号の値を使用する場合。	「Mobile Number（携帯電話番号）」アイデンティティ属性を編集し、ユーザーの携帯電話番号を格納している LDAP ディレクトリ属性にマッピングするか、新しいアイデンティティ属性定義を作成することができます。 On-Demand トークンコードの配信を構成する場合は、［SMS Configuration（SMS の構成）］ページにある［User Attribute to Provide SMS Destination（SMS の宛先を保存するユーザー属性）］ドロップダウン メニューから［Mobile Number（携帯電話番号）］または新しく作成した属性を選択します。
LDAP ディレクトリが少なくとも 1 つあるが、LDAP ディレクトリに携帯電話番号が格納されていないために、ユーザーの携帯電話番号を内部データベースに保存する場合。	常に内部データベースに格納される、ユーザーの携帯電話番号のアイデンティティ属性定義を作成する必要があります。 On-Demand トークンコードの配信を構成する時に、［SMS Configuration（SMS の構成）］ページにある［User Attribute to Provide SMS Destination（SMS の宛先を保存するユーザー属性）］ドロップダウン メニューから作成した属性を選択します。

On-Demand トークンコードの配信のための HTTP プラグ インの構成

導入環境を構成して、HTTP、HTTPS、XML-over-HTTP 経由で SMS（Short Message Service）プロバイダまたはモデムと統合することにより、On-Demand トークンコードをユーザーの携帯電話に配信することができます。

HTTP リクエストにより、次の配信情報を SMS プロバイダまたはモデムに送信します。

- On-Demand トークンコードを含むテキスト メッセージ
- 携帯電話番号
- SMS プロバイダまたはモデムで必要とされるその他の情報

テキスト メッセージの最大長は 140 バイトです。文字数は、SMS プロバイダで使用される文字エンコーディングのタイプに依存します。140 バイトのフル ペイロードで 7 ビット文字を 160 文字、8 ビット文字を 140 文字、16 ビット文字を 70 文字サポートできます。$OTT 変数と $Lifetime 変数は、使用可能な文字を使用して、実際の値に置き換えられます。

重要：HTTP 接続は安全ではありません。トークンコードなどの機密情報が漏洩する可能性があります。接続をセキュリティで保護するには、HTTPS を構成します。

開始する前に

- http://www.securedbyrsa.com にアクセスして、サポートされる SMS プロバイダとモデムの構成値とパラメータが記載されている導入ガイドをダウンロードします。各 SMS プロバイダから独自の導入ガイドが提供されています。プロバイダは名前で検索できます。また、サイトで［**Product Category（製品カテゴリー）**］＞［**SMS Providers（SMS プロバイダ）**］に移動すると、完全なリストを入手できます。導入ガイドは、各プロバイダの［**Collateral（関連資料）**］タブで見つけることができます。
- デジタル証明書が必要な SMS プロバイダの場合、または HTTP 接続が HTTPS サイトにリダイレクトされる場合は、使用しているプロバイダから証明書を入手して、ローカルの場所に保存します。証明書をインポートすると、Authentication Manager が、On-Demand トークンコードの送信先のサーバを検証できるようになります。Authentication Manager は、この証明書によって署名されているすべての接続を許可します。手順については、RSA Security Console ヘルプのトピック「デジタル証明書のインポート」を参照してください。

- すべてのユーザーの宛先携帯電話番号が次の要件を満たすことを確認します。
  - 携帯電話番号に国番号が含まれる。ユーザーの宛先携帯電話番号が国番号なしですでに格納されている場合は、携帯電話への On-Demand トークンコードの配信を構成するときに国番号を選択します。
  - 携帯電話番号は数字で終わる。
  - 携帯電話番号はプラス（+）文字で始めることもできる。
  - 区切り文字には、次の文字か空白を使用する。.（ピリオド）、-（ハイフン）、(（右括弧）、)（左括弧）
  - アルファベット文字またはこのリストに示されていないその他の文字を使用しない。

  有効な宛先携帯電話番号の例を次に示します。

  +1 123 123 1234
  +44 1234-123-123-1
  123 123 1234
  123.123.1234
  (123) 123-1234

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。
2. ［Authentication Settings（認証設定）］で、［**On-Demand Tokencode Delivery（On-Demand トークンコードの配信）**］をクリックします。
3. ［**SMS Configuration（SMS の構成）**］タブをクリックします。
4. ［**Tokencode Delivery by SMS（SMS によるトークンコードの配信）**］で、次の操作を実行します。
   a. ［**Enable the delivery of on-demand tokencodes using SMS service（SMS サービスを使用した On-Demand トークンコードの配信を有効化する）**］を選択します。
   b. ［**User Attribute to Provide SMS Destination（SMS の宛先を保存するユーザー属性）**］ドロップダウン メニューで、On-Demand トークンコードをユーザーに配信するための携帯電話番号が保存されたユーザー属性を選択します。
      ユーザー情報管理に内部データベースを使用する場合は、データベース内の属性（電話番号など）と関連づけたり、カスタム属性を作成することが可能です。外部アイデンティティ ソースを使用する場合は、外部アイデンティティ ソースの属性（電話番号など）にマッピングされた属性を選択できます。

c. ［**Default country code（デフォルトの国番号）**］ドロップダウン メニューから、宛先携帯電話番号の前に付加する国番号を選択します。On-Demand トークンコードの配信先となる携帯電話番号には、常に国番号が必要です。国番号は、On-Demand トークンコードの送信先の携帯電話番号に国番号が含まれていない場合にのみ選択してください。

d. ［**SMS Plug-In（SMS プラグ イン）**］ドロップダウン メニューから、［**HTTP**］を選択します。

5. ［**SMS Provider Configuration（SMS プロバイダの構成）**］で、次の操作を実行します。

a. ［**Base URL（ベース URL）**］フィールドに、SMS プロバイダまたはモデムのベース URL を入力します。

b. デジタル証明書を要求する SMS プロバイダの場合や、HTTP 接続を HTTPS サイトにリダイレクトする場合は、証明書をインポートします。手順については、RSA Security Console ヘルプのトピック「デジタル証明書のインポート」を参照してください。

注：SMS プロバイダがデジタル証明書を必要としない場合やベース URL に HTTPS が使用されない場合、このステップは不要です。

c. ［**HTTP Method（HTTP メソッド）**］ドロップダウン メニューで、SMS プロバイダへのリクエストに使用するメソッドを選択し、次のいずれかを構成します。

– GET または POST の場合：SMS プロバイダが指定したパラメータを入力します。

– XML の場合：SMS プロバイダが指定した XML リクエスト本文を入力します。

注：SMS プロバイダが XML-over-HTTP を使用している場合は、［**HTTP Method（HTTP メソッド）**］で［**XML**］を選択します。

d. ［**Parameters（パラメータ）**］フィールドに、Authentication Manager と SMS プロバイダまたはモデムが必要とするパラメータを入力します。詳細については、270 ページの SMS HTTP プラグ イン構成パラメータを参照してください。

e. ［**Account User Name（アカウントのユーザー名）**］フィールドに、SMS サービス プロバイダのアカウントのユーザー名を入力します。これはサービス プロバイダから提供されます。

f. ［**Account Password（アカウントのパスワード）**］フィールドに、SMS サービス プロバイダ アカウントのパスワードを入力します。これはサービス プロバイダから提供されます。

g. ［**Connection Timeout（接続タイムアウト）**］フィールドに、1,000 ～ 3,600,000 ミリ秒の接続タイムアウトを入力します。デフォルト値は 5,000 ミリ秒です。

h. ［**Success Response Code（成功応答コード）**］フィールドに、SMS プロバイダが指定する成功応答コードを入力します。

i. ［**Response Format（応答フォーマット）**］フィールドに、SMS プロバイダの成功応答フォーマットを入力します。

注：正規表現の詳細については、標準の JDK のマニュアルを参照してください。

6. （オプション）［**SMS HTTP(S) Proxy Configuration（SMS HTTP(S) プロキシ構成）**］で、次の操作を実行します。

a. ［**Proxy Hostname（プロキシ ホスト名）**］フィールドに、HTTP プロキシのホスト名を入力します。

b. ［**Proxy Port（プロキシ ポート）**］フィールドに、プロキシ ポート番号を入力します。

c. ［**Proxy User（プロキシ ユーザー）**］フィールドに、プロキシ ユーザー名を入力します。

d. ［**Proxy Password（プロキシ パスワード）**］フィールドに、プロキシ パスワードを入力します。

7. （オプション）［**Test SMS Provider Integration（SMS プロバイダ統合のテスト）**］で、次の操作を実行します。

a. ［**Mobile phone number to test（テストする携帯電話番号）**］フィールドで、国番号を選択し、テスト メッセージを受信する携帯電話の番号を入力します。

b. ［**Send Test Text Message（テスト テキスト メッセージの送信）**］をクリックします。

テストを実行する前に、変更した内容がシステムによってすべて保存されます。接続が失敗すると、エラー メッセージが表示されます。

8. ［**Tokencode Settings（トークンコードの設定）**］タブで、次の項目を構成します。

a. ［**On-Demand Tokencode Message（On-Demand トークンコード メッセージ）**］フィールドに、On-Demand トークンコードを含むテキスト メッセージに表示するテキストを入力します。

$OTT 変数は削除しないでください。この変数の場所に、On-Demand トークンコードが挿入されます。

b. ［**On-Demand Tokencode Lifetime（On-Demand トークンコードの有効期間）**］フィールドに、ユーザーに配信された On-Demand トークンコードが有効な期間を入力します。

9. ［**Save（保存）**］をクリックします。

SMS HTTP プラグ イン構成パラメータ

パラメータの構成値には可変要素が含まれています。可変要素は、SMS 転送時に対応する値に置き換わります。たとえば、${cfg.user} は［Account User Name（アカウントの ユーザー名)］フィールドに指定した値に置き換わります。

パラメータ文字列には次の構成要素が必須です。

構成要素	構成要素に対応するフィールド
$msg.address	SMS の宛先を指定するユーザー属性
$msg.message	On-Demand トークンコード メッセージ
$cfg.user	アカウントのユーザー名
$cfg.password	アカウントのパスワード

+、&、= の各文字は、パラメータ文字列の値ペアで使用するために予約されています。たとえば、text=${msg.message}&clientid=${cfg.user} のようになります。

+、&、または = 文字がパラメータ文字列の値データに使用される場合、各文字に対応する構成要素をパラメータ文字列に入力する必要があります。

文字	構成要素
+	${plus}
&	${ampersand}
=	${equal}

たとえば、外国の電話番号に + 文字を含める場合は、構成要素 ${plus} を次のように使用します。destaddr=${plus}${msg.address}

構成例

この例では、SMS プロバイダには次の形式のメッセージ データを送信する必要があります。

```
https://sms.rsa.com/http/send?user=john&password=doe123&extr
aparam=123456&to=2223334444&text=Meet+me+at+home
```

この例の場合、次のように各フィールドを構成する必要があります。

フィールド名	値
Base URL（ベース URL）	https://sms.rsa.com/http/send
HTTP Method（HTTP メソッド）	GET
Parameters（パラメータ）	user=$cfg.user&password=$cfg.password&extraparam=123456&to=$msg.address&text=$msg.message
アカウントのユーザー名	john
アカウントのパスワード	doe123
成功レスポンス コード	RESULT:OK
レスポンス フォーマット	RESULT:OK

SMS サービス プロバイダの変更

SMS サービス プロバイダを変更できます。

処理手順

以下のいずれかの操作を実行します。

- HTTP プラグ インを再構成する。詳細については、266 ページの On-Demand トークンコードの配信のための HTTP プラグ インの構成を参照してください。
- カスタム プラグ インを実装する。詳細については、RSA 製品の販売代理店にお問い合わせください。

メールによる On-Demand トークンコード配信の構成

On-Demand トークンコードをメール アカウントに送信するには、次のタスクを実行します。

1. 272 ページの SMTP メール サービスの構成
2. Authentication Manager が、ユーザーのメール アドレスを格納する属性にアクセスできることを確認します。273 ページの On-Demand トークンコードをメールで配信するためのアイデンティティ属性定義を参照してください。
3. 275 ページの On-Demand トークンコードの配信のためのメールの構成

SMTP メール サービスの構成

メールを使用して On-Demand トークンコードを配信することを計画している場合は、SMTP（Simple Mail Transfer Protocol）メッセージを送信するようにすべての Authentication Manager インスタンスを構成する必要があります。

SMTP の設定は、レプリカ インスタンスでは直ちに表示できない可能性があります。データは 10 ～ 20 分でレプリケーションされます。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [**E-Mail (SMTP)（メール（SMTP））**] をクリックします。
3. インスタンスを選択します。
4. [**Next（次へ）**] をクリックします。
5. [**Hostname（ホスト名）**] フィールドに、このインスタンスがメッセージを送信するメール サーバのホスト名を入力します。
6. [**Port（ポート）**] フィールドに、メール サーバの宛先ポート番号を入力します。
7. [**From E-mail Address（送信元のメール アドレス）**] フィールドに、このインスタンスから発信されるすべてのメールの送信者として表示するメール アドレスを入力します。ユーザーが返信を返すことができるメール アドレスを使用してください。
8. （オプション）メール サーバへの接続にユーザー ID とパスワードが必要な場合は、[**Logon Required（ログオンが必要）**] を選択します。
9. ログオンが必要な場合は、次の操作を実行します。
   a. [**User ID（ユーザー ID）**] フィールドに管理者のユーザー ID を入力します。このユーザー ID は、すでに SMTP メール サーバで定義されている必要があります。
   b. [**Password（パスワード）**] フィールドに、ユーザー ID のパスワードを入力します。
   c. [**Confirmed Password（パスワードの確認）**] フィールドに、パスワードを再度入力します。
10. [**Test E-mail Address（テスト用メール アドレス）**] フィールドに、このインスタンスのテストに使用する宛先メール アドレスを入力します。
11. [**Test Connection（接続のテスト）**] をクリックして、メール サービスをテストします。

12. プライマリ インスタンスを構成した後は、同じ設定をレプリカ インスタンスに適用できます。
13. テスト用メールを受信したら、[**Save（保存）**] をクリックします。

On-Demand トークンコードをメールで配信するためのアイデンティティ属性定義

On-Demand トークンコードをメールで配信する場合は、ユーザーのメールアドレスを格納する属性に Authentication Manager 8.0 からアクセスできる必要があります。

追加構成が必要かどうかについては、下の表を参照して判断してください。

導入環境内のアイデンティティ ソース	構成
内部データベース	[E-Mail（メール）] を選択して、内部データベースに格納するユーザーのメールアドレスを使用します。 構成されたメール アドレスにアクセスするために、On-Demand トークンコードを使用して認証する必要がないことを確認します。 On-Demand トークンコードによる認証が必要なメール アドレスの場合、ユーザーはトークンコードを取得できません。該当する場合は、On-Demand トークンコードによる認証が必要ないメールアドレスを格納できるアイデンティティ属性定義を内部データベースに作成します。
メール アドレス属性を格納する LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つ存在する場合	[E-Mail（メール）] を選択します。アイデンティティ ソースの構成時に [E-Mail（メール）] フィールドにこの属性をマッピングしておく必要があります。 構成されたメール アドレスにアクセスするために、On-Demand トークンコードを使用して認証する必要がないことを確認します。 ディレクトリ内に構成されているメールアドレスへのアクセスに On-Demand トークンコードによる認証が必要な場合は、ユーザーはトークンコードを取得できません。該当する場合は、アイデンティティ属性定義を作成し、On-Demand トークンコードによる認証が必要ないメール アドレスを格納している LDAP 属性をマッピングします。

導入環境内のアイデンティティ ソース	構成
LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つあり、LDAP ディレクトリの［mail（メール）］属性フィールドに格納されたメール アドレスの値を使用する場合。	属性マッピングは必要ありません。 Authentication Manager 8.0 は、LDAP ディレクトリを追加する時に、LDAP ディレクトリの［mail（メール）］属性を自動的にリンクします。 On-Demand トークンコードの配信を構成する場合は、［E-mail Configuration（メールの構成）］ページにある［User Attribute to Provide E-mail Destination（メールの宛先を保存したユーザー属性）］ドロップダウン メニューから［E-mail（メール）］を選択します。
LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つあり、LDAP ディレクトリの［mail（メール）］属性フィールド以外の属性フィールドにあるメール アドレスの値を使用する場合。	Authentication Manager 8.0 で［E-mail（メール）］フィールドへの LDAP ディレクトリ属性のマッピングを変更するか、新しい属性定義を作成して、メール アドレスに使用する LDAP ディレクトリの属性をその属性定義にマッピングします。詳細については、RSA Operations Console ヘルプのトピック「LDAP ディレクトリ アイデンティティ ソースの編集」を参照してください。 On-Demand トークンコードの配信を構成する場合は、［E-mail Configuration（メールの構成）］ページにある［User Attribute to Provide E-mail Destination（メールの宛先を保存したユーザー属性）］ドロップダウン メニューから［E-mail（メール）］または新しく作成した属性を選択します。
LDAP ディレクトリ アイデンティティ ソースが少なくとも 1 つあるが、LDAP ディレクトリにメール アドレスが格納されていないために、ユーザーのメール アドレスを内部データベースに保存する場合。	常に内部データベースに格納される、ユーザーのメール アドレス用のアイデンティティ属性定義を作成する必要があります。 On-Demand トークンコードの配信を構成する場合は、［E-mail Configuration（メールの構成）］ページにある［User Attribute to Provide E-mail Destination（メールの宛先を保存したユーザー属性）］ドロップダウン メニューから作成した属性を選択します。

On-Demand トークンコードの配信のためのメールの構成

ユーザーのメール アドレスに On-Demand トークンコードを送信するように環境を構成できます。最初に、メール サーバ接続をインスタンスごとに構成する必要があります。

開始する前に

- 以下の情報があることを確認する。
  - **ホスト名**。メール通知を送信するために使用するメールサーバのホスト名です。
  - **SMTP ポート**。メールの送信に使用するポートです。
  - **メール アドレス**。メール通知の送信元アドレスです。
  - **ログオン**。メール サーバにユーザー ID とパスワードが必要かどうかを示します。
- ユーザーごとに宛先メール アドレスを構成する。

  On-Demand 認証を使用しなければアクセスできないメール アドレスは使用しないでください。たとえば、ユーザーが仕事用のメール アカウントにアクセスするためにトークンコードが必要な場合は、ユーザーの個人用メール アドレスを宛先にします。
- 272 ページの SMTP メール サービスの構成を参照してください。導入環境内の各インスタンスに対してこの操作を行う必要があります。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [**On-Demand Tokencode Delivery（On-Demand トークンコードの配信）**] をクリックします。
3. [**E-mail Configuration（メールの構成）**] タブをクリックします。
4. [**Enable the delivery of On-demand Tokencodes through e-mail（メールによる On-Demand トークンコードの配信を有効化する）**] を選択します。
5. [**User Attribute to Provide E-mail Destination（メールの宛先を保存するユーザー属性）**] ドロップダウン メニューで、On-Demand トークンコードをユーザーに配信するためのメール アドレスが保存された属性を選択します。
6. [**Save（保存）**] をクリックします。
7. （オプション）[**Tokencode Settings（トークンコードの設定）**] タブで、次の操作を実行します。

a. ［**On-Demand Tokencode Message（On-Demand トークンコード メッセージ）**］フィールドに、On-Demand トークンコードを含むテキスト メッセージに表示するテキストを入力します。
$OTT 変数は削除しないでください。この変数の場所に、On-Demand トークンコードが挿入されます。

b. ［**On-Demand Tokencode Lifetime（On-Demand トークンコードの有効期間）**］フィールドに、ユーザーに配信された On-Demand トークンコードが有効な期間を入力します。

8. ［**Save（保存）**］をクリックします。

On-Demand 認証を使用するためのユーザーの構成

ユーザーが On-Demand トークンコードを受信するには、ODA（On-Demand 認証）が有効化されている必要があります。ユーザーの ODA を有効化する時に、トークンコードの配信方法、On-Demand トークンコードを使用可能な期間、Self-Service Console を使用して初期 PIN を設定できるかどうかを指定できます。操作手順については、276 ページのユーザーの On-Demand 認証の有効化を参照してください。

管理者は、ユーザーが PIN を忘れたり、PIN の有効期限が切れたり、PIN が危殆化した場合に、PIN をクリアし、ユーザーに一時 PIN を提供できます。管理者は、ユーザーに PIN の変更を強制できます。詳細については、278 ページの On-Demand 認証用の PIN を参照してください。

ユーザーが宛先の電話番号やメール アドレスを更新できるように Self-Service Console を構成できます。この構成オプションにより、管理者の時間や労力を削減できます。操作手順については、279 ページのユーザーによる電話番号およびメール アドレスの更新の有効化を参照してください。

ユーザーの On-Demand 認証の有効化

ODA（On-Demand 認証）は、ユーザーの携帯電話やメール アカウントにワン タイム トークンコードを配信します。On-Demand トークンコードは、指定された期間を過ぎると有効期限が切れることでセキュリティを強化します。ODA は、ユーザーが SSL-VPN、Web ポータル、ブラウザ ベースのシンクライアントを介してアクセスする会社のリソースを保護します。

ユーザーが On-Demand トークンコードを受信できるように ODA を有効化します。

開始する前に

On-Demand トークンコードの配信。

手順

1. Security Console で、[**Authentication（認証）**] > [**On-Demand Authentication（On-Demand 認証）**] > [**Enable Users（ユーザーの有効化）**] の順にクリックします。
2. 検索フィールドを使用して、ODA を有効化するユーザーを検索します。一部のフィールドでは大文字と小文字が区別されます。
3. ユーザーの ODA を有効化します。

   1 人のユーザーを有効化するには、次の手順を実行します。

   a. 検索結果から、ODA を有効化するユーザーをクリックします。

   b. コンテキスト メニューで [**Enable for ODA（ODA の有効化）**] をクリックします。

   複数のユーザーを有効化するには、次の手順を実行します。

   a. 利用可能なユーザーのリストで、ODA を有効化するユーザーの横にあるチェックボックスをオンにします。

   b. [**Enable for ODA（ODA の有効化）**] をクリックします。
4. 必要に応じて、[**Send On-Demand Tokencodes to（On-Demand トークンコードの送信先）**] オプションを使用して、On-Demand トークンコードの配信方法を選択します。必要に応じて、メール アドレスまたは電話番号を指定します。

   重要：On-Demand トークンコードをユーザーのメール アドレスに送信することを選択する場合、ユーザーがメール アカウントにアクセスするために、On-Demand トークンコードによる認証が必要ないことを確認してください。
5. [**Expiration Date（有効期限）**] オプションを使用して、ユーザーが On-Demand トークンコードを要求できる期間を指定します。正確な日付または有効期限なしを指定できます。
6. [**Associated PIN（PIN の割り当て）**] オプションを使用して、ユーザーの初期 PIN を作成する方法を指定します。必要に応じて、初期 PIN を作成します。
7. [**Save（保存）**] をクリックします。

On-Demand 認証用の PIN

ユーザーは ODA（On-Demand 認証）用の PIN を持っている必要があります。PIN には、ユーザーのセキュリティ ドメインの PIN ポリシーが適用されます。ODA 用の PIN に関連して次のタスクがあります。

- PIN の設定

  ユーザーは、Self-Service Console を使用して初期 PIN を設定できます。ユーザーに PIN を設定させる場合は、ユーザーの ODA を構成するときにこのオプションを選択する必要があります。ユーザーに初期 PIN を設定させない場合は、管理者が Security Console を使用してユーザーの初期 PIN を設定できます。

- PIN のクリア

  ユーザーが PIN を忘れたり、PIN の有効期限が切れたり、PIN が危殆化した場合は、PIN をクリアすることができます。ユーザーの PIN をクリアする場合は、ユーザーが ODA で保護されるリソースへのログオンを試行できるように一時 PIN をユーザーに割り当てる必要があります。PIN のクリアとユーザーへの一時 PIN の割り当ては、Security Console を使用して行います。

- PIN の変更

  ODA が有効になっているユーザーは、Self-Service Console にログオンした後か認証時に ODA PIN を変更できます。ユーザーは、PIN の有効期限が切れたとき、または管理者から PIN の変更を強制されたときに PIN を変更する必要があります。PIN が危殆化したと考えられる場合は、ユーザーに強制的に PIN を変更させることができます。PIN の変更を強制する場合は、Security Console を使用してユーザーの PIN をクリアして、一時 PIN を設定します。

ユーザーに初期 PIN を設定させるための操作手順については、278 ページのユーザーによる On-Demand 認証の初期 PIN の設定の有効化を参照してください。ユーザーの一時 PIN をクリアして初期 PIN を設定するよう強制する方法については、279 ページの On-Demand トークンコードの一時 PIN の設定を参照してください。

ユーザーによる On-Demand 認証の初期 PIN の設定の有効化

ユーザーが ODA（On-Demand 認証）を使用して、保護されたリソースにアクセスするには、PIN が必要です。ユーザーの初期 PIN を設定できます。また、ユーザーが自分の初期 PIN を設定できるようにして、管理者の労力を軽減させることもできます。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、有効化するユーザーを検索します。
3. 有効化するユーザーをクリックします。

4. ［**SecurID Tokens（SecurID トークン）**］をクリックします。
5. ［**On-Demand Authentication（On-Demand 認証）**］セクションで、ユーザーの ODA が有効化されていない場合は、［**Enable user for on-demand authentication（On-Demand 認証を有効化する）**］を選択します。
6. ［**Require user to set the PIN through the RSA Self-Service Console（ユーザーが RSA Self-Service Console を使用して PIN を設定する）**］を選択します。
7. ［**Save（保存）**］をクリックします。

On-Demand トークンコードの一時 PIN の設定

Security Console を使用して、ユーザーの On-Demand トークンコード PIN をクリアし、一時 PIN を割り当てます。

手順

1. Security Console で、［**Identity（アイデンティティ）**］＞［**Users（ユーザー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 検索フィールドを使用して、On-Demand トークンコードの一時 PIN を設定するユーザーを検索します。
3. ユーザーをクリックします。
4. ［**SecurID Tokens（SecurID トークン）**］をクリックします。
5. ［**Clear existing PIN and set a temporary PIN for the user（既存の PIN をクリアして一時 PIN を設定する）**］を選択します。
6. 一時 PIN を入力します。
7. ［**Save（保存）**］をクリックします。
8. 安全性の高い方法でこの一時 PIN をユーザーに伝える必要があります。

ユーザーによる電話番号およびメール アドレスの更新の有効化

ユーザーが On-Demand トークンコードの宛先となる自分の電話番号およびメール アドレスを更新できるように Self-Service Console を構成できます。

次の点に注意してください。

- ユーザーは、電話番号とメール アドレスが内部データベースに格納されている場合にのみ情報を更新できます。
- 外部アイデンティティ ソースに格納されたユーザー属性は、すべて読み取り専用です。ユーザーが Self-Service Console を使用して情報を変更することはできません。
- 必須入力フィールドは編集できます。

開始する前に

- Self-Service Console 上に［Change Delivery Option（配信オプションの変更）］リンクを表示するように Authentication Manager 8.0 を構成する。このリンクは、ユーザーの On-Demand 認証を有効化すると、［My Account（マイ アカウント）］ページに表示されます。
- 少なくとも 1 つの属性（SMS 電話番号またはメール アドレス）が編集および表示できること、または両方の属性（SMS 電話番号とメール アドレス）が表示できるが、編集できないことを確認する。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**Customization（カスタマイズ）**］セクションで、［**User Profile（ユーザー プロファイル）**］をクリックします。
3. ［**Choose an Identity Source（アイデンティティ ソースの選択）**］ドロップダウン リストから、［**Internal Database（内部データベース）**］を選択します。
4. ［**Next（次へ）**］をクリックします。
5. 次のどちらかまたは両方の操作を実行します。
   ユーザーが電話番号を更新できるようにするには：
   a. ［**Custom Attributes（カスタム属性）**］セクションで、［**Mobile Number（携帯電話番号）**］の［**View and manage user profile attribute details（ユーザー プロファイル属性の詳細の表示および管理）**］を選択します。
   b. ［**Make Field (for Update Profile)（プロファイル更新時のフィールド ステータス）**］ドロップダウン リストから、［**Editable（編集可能）**］を選択します。
   c. ［**Display Label（表示ラベル）**］で、デフォルトのラベルを受け入れるか、任意のラベルに置き換えます。
   ユーザーがメール アドレスを更新できるようにするには：
   a. ［**Core Attributes（コア属性）**］で、［**Email（メール）**］の［**View and manage user profile attribute details（ユーザー プロファイル属性の詳細の表示および管理）**］を選択します。
   b. ［**Make Field (for Update Profile)（プロファイル更新時のフィールド ステータス）**］ドロップダウン リストから、［**Editable（編集可能）**］を選択します。
   c. ［**Display Label（表示ラベル）**］で、デフォルトのラベルを受け入れるか、任意のラベルに置き換えます。
6. ［**Save（保存）**］をクリックします。

認証エージェントまたは RADIUS クライアントでの On-Demand 認証

認証エージェントまたは RADIUS クライアントを通じて On-Demand トークンコードをリクエストして認証する場合の認証プロセスは、Self-Service Console から On-Demand トークンコードをリクエストして認証する場合や、RSA SecurID ハードウェアまたはソフトウェア トークンを使用して認証する場合と異なります。いずれの場合も、認証エージェントはユーザー ID とパスコードの入力をユーザーに求めます。ただし、On-Demand トークンコードの場合は、次のようなプロセスになります。

1. 保護されているリソースにユーザーがアクセスしようとすると、エージェントはユーザーにユーザー ID とパスコードの入力を求めます。
2. ユーザーは自分のユーザー ID を入力し、パスコード プロンプトに対してはパスコードではなく ODA（On-Demand 認証）PIN を入力します。

   On-Demand トークンコード サービスが有効化されているユーザーがパスコード プロンプトに ODA PIN を入力すると、Authentication Manager はそのユーザーが実際には On-Demand トークンコードをリクエストしていると認識します。
3. トークンコードが Authentication Manager からユーザーに送信されます。
4. 認証エージェントがユーザーにネクスト トークンコードの入力を求めます。
5. ユーザーは受信した On-Demand トークンコードを入力します。

表示されたプロンプトと実際の処理が異なることをユーザーに通知しておくようにしてください。一部のエージェントでは、誤解を招かないようにプロンプトを変更できます。ただし、この対策が効果的なのはすべてのユーザーが ODA だけを使用する場合のみです。

また、ユーザーがネクスト トークンコードのプロンプトで認証をキャンセルするか、On-Demand トークンコードを入力しないまま長時間経過した場合でも、On-Demand トークンコードの有効期間内であれば、引き続きその On-Demand トークンコードを（PIN とともに）使用して認証することができます。たとえば、ユーザーが再度認証を行うことが可能で、認証エージェントまたは RADIUS クライアントがパスコードの入力をユーザーに求めた時に、ユーザーは PIN と On-Demand トークンコードをパスコードとして入力し、正常に認証を終えることができます。

認証エージェントまたは RADIUS クライアントでの PIN 作成と On-Demand トークンコード

On-Demand トークンコードには常に PIN が必要です。このため、管理者は、On-Demand トークンコードを使用しているユーザーの PIN をクリアする場合にも、必ず一時 PIN を割り当てる必要があります。ユーザーが On-Demand トークンコードの PIN を変更する際の手順は、トークンコードのリクエスト方法によって異なります。

認証エージェントまたは RADIUS クライアントを通じてトークンコードをリクエストする場合：

1. 保護されているリソースにアクセスしようとすると、エージェントからユーザー ID とパスコードの入力を求められます。
2. ユーザーは、パスコード プロンプトに対して、ユーザー ID および現在の PIN（期限切れの PIN か、管理者から割り当てられた一時 PIN）を入力します。
3. エージェントは、ユーザーに新しい PIN の入力と再入力を行うようプロンプトを表示します。
4. ユーザーは新しい PIN を入力します。
5. エージェントからパスコードを入力するようプロンプトが表示されます。
6. 新しい PIN を入力します。
7. On-Demand トークンコードが Authentication Manager からユーザーに送信されます。
8. エージェントがユーザーにネクスト トークンコードの入力を求めたら、ユーザーは受信した On-Demand トークンコードを入力します。

On-Demand トークンコードの制限

On-Demand トークンコードのユーザーには、次の制限が適用されます。

- ユーザーはトラステッド レルム認証を実行できません。
- ユーザーは、認証エージェント経由で On-Demand トークンコードを取得する場合を除き、エイリアスを使用して認証できません。
- On-Demand トークンコードの PIN は、ユーザーに割り当てられる固定パスコードと同じであってはなりません。
- EAP32 対応の認証エージェントは On-Demand トークンコードをサポートしません。

11 RSA セルフサービス

RSA セルフサービスの概要

RSA セルフ サービスは、トークンの導入プロセスを自動化し、Self-service Console を提供します。Self-Service Console は、Authentication Manager ユーザーにさまざまなサービスを提供するために構成する Web ベースのインタフェースです。

RSA セルフ サービスには、以下のコンポーネントが含まれます。

セルフ サービス。ユーザーが、認証、トークン、ユーザー アカウントに関連した多くの日常的なタスクを、ヘルプ デスクに問い合わせることなく管理するための、構成可能なコンソールです。セルフ サービスの使用により、ヘルプ デスクへの問い合わせの量を削減するとともに、ユーザーへの 24 時間サポートの提供を支援します。

プロビジョニング。RSA SecurID トークンの迅速な導入とライフサイクル管理を実現するための、Web ベースのワークフロー システムです。ユーザーがトークン導入プロセスの多くのステップを実行でき、システムによりワークフローが自動化されます。プロビジョニングを使用すると、特に大規模な導入環境において、トークンの導入に関連した管理者のオーバーヘッドを軽減できます。

RSA では、DMZ 内の Web Tier サーバに Self-Service Console をインストールことを推奨しています。Web Tier へのインストールにより、社内リソースを保護しながら、セルフ サービスの利便性をリモート ユーザーに提供します。Self-Service Console の構成メニューは、RSA Security Console に統合されています。ロゴの表示や、表示するセルフサービス機能の選択により、Self-Service Console をカスタマイズできます。

ユーザーが Self-Service Console で実行できるタスクは、インストールされたライセンス、有効化するオプション、ユーザー データが格納されているアイデンティティ ソースが内部か外部かによって異なります。詳細については、287 ページのセルフ サービスのセキュリティ ドメインの選択を参照してください。

Self-Service Console のユーザー操作

構成によって、ユーザーは Self-Service Console から次のタスクを実行できます。

- セルフ サービスユーザーアカウントを登録する
- ユーザー確認用のセキュリティ クエスチョンを構成する
- トークンをリクエストする
- ユーザー プロファイルを更新する
- Self-Service Console パスワードを変更する
- RBA（リスク ベース認証）のデバイス履歴をクリアして、デバイスを登録解除する
- ODA（On-Demand 認証）用のメール アドレスまたは電話番号を変更する
- ODA PIN を管理する
- ユーザー グループ メンバーシップを表示する
- トークンをテストおよび再同期する
- トークンに関連する問題をトラブルシューティングおよび報告する
- トークンを紛失または破損した場合や一時的に使用できない場合、エマージェンシー アクセスをリクエストする
- PIN をロック解除およびリセットする
- On-Demand 認証をリクエストする

ユーザーアカウント登録

新しいユーザーが内部データベースのアカウントをリクエストできるように、システムを構成することができます。この処理をアカウント登録と言います。内部データベースまたは他のいずれかのアイデンティティ ソースにすでにアカウントを持っているユーザーは、アカウント登録する必要ありません。そのようなユーザーは、デフォルトで、管理者が構成したセルフサービス機能にアクセスできます。

アカウント登録時に、ユーザーは、登録を希望するセキュリティ ドメインを選択する必要があります。セルフサービスの構成によって、ユーザーは以下の操作も必要になります。

- ユーザー プロファイルを構成します。
- セキュリティ クエスチョンを構成します。
- ユーザー グループを選択します。

セルフ サービス ユーザーのアイデンティティ ソース

ユーザー アカウントが保存されたアイデンティティ ソースによって、Self-Service Console を使用してユーザーが実行できる操作が異なります。内部データベース、Active Directory、Oracle Directory Server をアイデンティティ ソースとして使用できます。

Active Directory または Oracle Directory Server で［change password during next logon（次回ログオン時にパスワードを変更）］オプションが設定されている場合、ユーザーをセルフサービスに登録できません。

アイデンティティ ソースとしての内部データベースの使用

Authentication Manager は、内部データベースからデータを読み取り、書き込むことができます。内部データベースにアカウントがあるユーザーは、Self-Service Console を使用して、管理者が許可したすべての操作を実行できます。たとえば、パスワードのリセットや、RBA（リスク ベース認証）のユーザー確認方法として On-Demand 認証を使用する場合に、［Identity Confirmation Method configuration（ユーザー確認方法の構成）］ページで、電話番号やメール アドレスを入力するなどの操作が考えられます。

アイデンティティ ソースとしての Active Directory の使用

Active Directory にアカウントがあるユーザーは、Self-Service Console の操作のうち、Authentication Manager から Active Directory へのアクセスが必要となるすべての操作を実行できません。たとえば、Active Directory にアカウントがあるユーザーは、Self-Service Console を使用して、自分のパスワードを変更できません。Authentication Manager は、Active Directory のすべてのユーザーおよびユーザー グループ データへの読み取り専用アクセスができます。

アイデンティティ ソースとしての Oracle Directory Server の使用

Oracle Directory Server にアカウントがあるユーザーは、Self-Service Console の操作のうち、Authentication Manager から Oracle Directory Server へのアクセスが必要となるすべての操作を実行できません。Authentication Manager は、Oracle Directory Server のすべてのユーザーおよびユーザー グループ データへの読み取り専用アクセスができます。

セルフサービスの構成

Self-Service Console ユーザーに機能やサービスを提供するには、セルフサービスを構成する必要があります。Self-Service Console へのアクセスを許可するユーザーと、ログオンに必要なクレデンシャルを指定できます。次のリストは、セルフサービスを構成するためのガイドです。

手順

1. 286 ページのアイデンティティ ソースの選択によるアカウント登録の有効化。
2. 287 ページのセルフ サービスのセキュリティ ドメインの選択。
3. 288 ページのセルフ サービスのユーザー グループの選択。
4. 289 ページのセルフ サービスのユーザー プロファイル構成。
5. 291 ページの Self-Service Console の認証方式の設定。
6. 291 ページのセルフサービス用のセキュリティ クエスチョン。
7. 292 ページのセルフ サービス ユーザー アカウント変更のメール通知の構成。

アイデンティティ ソースの選択によるアカウント登録の有効化

アカウント登録を有効化すると、新しいユーザーは内部データベース上のアカウントをリクエストできるようになります。デフォルトでは、アカウント登録を有効化するために選択できる唯一のアイデンティティ ソースは内部データベースです。ユーザーは、外部アイデンティティ ソースにアカウント登録することはできません。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**Select identity sources（アイデンティティ ソースの選択）**］をクリックします。
3. ［**Display Name for Identity Source Selection Component（アイデンティティ ソース選択コンポーネントの表示名）**］フィールドで、アイデンティティ ソースの選択についてユーザーが理解しやすいテキストを入力します。
4. ［**Allow users to request accounts in this identity source（このアイデンティティ ソースにアカウント登録をリクエストできるようにする）**］を選択し、ユーザーがアカウント登録時に内部データベースを選択できるようにします。
5. ［**Save（保存）**］をクリックします。

セルフ サービスのセキュリティ ドメインの選択

管理者は、ユーザーがセルフ サービスからアカウント登録できるセキュリティ ドメインを選択することができます。ユーザーがアカウント登録するセキュリティ ドメインにより、そのユーザーを管理する管理者、およびそのユーザーに適用されるセキュリティ ポリシーが決まります。

以下の点を考慮してください。

- ヘルプ デスクへの支援依頼が多い場合や、多数のトークンを導入する場合、そのセキュリティ ドメインではセルフ サービスやプロビジョニングを活用することになります。
- セルフ サービスやプロビジョニングを使用してはならないユーザーが含まれているセキュリティ ドメインは選択しないでください。

ユーザーの選択操作を容易にするため、管理者は、Self-Service Console に表示される選択可能なセキュリティ ドメインの名前や説明テキストをカスタマイズすることができます。たとえば、セキュリティ ドメインが社内の部門に相当する場合は、各セキュリティドメインに部門名を示すラベルを付加するとともに、ユーザーに自分の所属部門を選択するように指示するラベルを付加することができます。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**Select Security Domains（セキュリティ ドメインの選択）**］をクリックします。
3. ［**Display Name for Security Domain Selection Component（セキュリティ ドメイン選択コンポーネントの表示名）**］フィールドで、セキュリティ ドメインの選択についてユーザーが理解しやすいテキストを入力します。
   たとえば、社内の部門ごとにセキュリティ ドメインがある場合に、「自分の部門を選択してください。」と入力します。
4. ［**Select More Domains（セキュリティ ドメインの選択）**］をクリックし、下位レベルのセキュリティ ドメインをすべて示すツリーを表示します。
5. 選択可能にするセキュリティ ドメインを選択します。
6. ［**Make Available（選択可能にする）**］をクリックします。
7. ［**Display Name（表示名）**］フィールドで、必要に応じてセキュリティ ドメインのわかりやすい名前を追加します。たとえば、「人事部門」と入力します。
   この表示名が Self-Service Console に表示されるため、ユーザーがセキュリティ ドメインを選択する際に役立ちます。
8. ［**Save（保存）**］をクリックします。

セルフ サービスのユーザー グループの選択

プロビジョニングおよび制限付きエージェントを使用する場合、管理者はユーザーがセルフ サービスからアカウント登録する時に、選択可能なユーザー グループを選択できます。ユーザーがアカウント登録したユーザー グループにより、ユーザーが認証を受けられる制限付きエージェントが決まります。管理者が選択したユーザー グループが、Self-Service Console に表示されます。管理者がユーザー グループを選択しない場合、アカウント登録時に［User Group Selection（ユーザー グループの選択）］ページは表示されません。

セルフ サービス用のユーザー グループを選択するに当たっては、次の点を考慮してください。

- ユーザーがリクエストできるのは、内部データベースのユーザーグループのメンバーシップのみである。Authentication Manager は、外部アイデンティティ ソースのグループにユーザーを追加できない。
- ユーザーが必要とするリソースへのアクセスをどのユーザー グループでユーザーに提供するか。
- ユーザーにアクセスを許可しないユーザー グループがあるか。
- すべてのユーザーにアクセスを許可するユーザー グループがあるか。
- 管理者がデフォルト グループを設定した場合、ユーザーはそのデフォルト グループにのみ属することができる。
- 制限付きエージェントを使用しない場合、プロビジョニングでユーザー グループを選択する必要はない。

注：ユーザーは、内部データベースに存在するユーザー グループであれば、セルフ サービスへのアカウント登録後に追加のユーザー グループ メンバーシップを要求できます。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**Select User Groups（ユーザー グループの選択）**］をクリックします。
3. 内部データベースを選択して、［**Next（次へ）**］をクリックします。内部データベースはアカウント登録時にユーザーが選択可能なユーザー グループを保存する唯一のアイデンティティ ソースです。
4. ［**Display Name for User Group Selection Component（ユーザー グループ選択コンポーネントの表示名）**］フィールドで、ユーザー グループの選択についてユーザーが理解しやすいテキストを入力します。たとえば、リモート アクセスが制限付きエージェントによって保護されている場合は、「アクセス方法を選択してください。」と入力します。
5. ［**Select More Groups（グループを選択）**］をクリックし、選択したアイデンティティ ソース上のユーザー グループのリストを表示します。

6. 目的のユーザー グループを選択し、[**Make Available（選択可能にする）**]をクリックします。
7. （オプション）[**Display Name（表示名）**]フィールドに、ユーザー グループのわかりやすい名前を追加します。たとえば、「VPN」と入力します。
8. （オプション）Self-Service Console からアカウント登録するすべての新しいユーザーにデフォルトで割り当てるユーザー グループがある場合は、それぞれの［Default Group（デフォルト グループ）］チェックボックスをオンにします。
9. [**Save（保存）**]をクリックします。

セルフ サービスのユーザー プロファイル構成

セルフサービスへのアカウント登録には、ユーザー プロファイルが必要です。ユーザー プロファイルには、名前、ユーザー ID、メール アドレス、Self-Service Console パスワード、携帯電話番号などのユーザー属性が含まれます。内部データベースを使用している場合、Self-Service Console のユーザーに対してどのユーザー属性を必須、編集可能、読み取り専用、非表示にするかを指定できます。たとえば、ユーザーに、メール アドレスと携帯電話番号の編集を許可し、ユーザー ID の編集を禁止することができます。外部アイデンティティ ソースに保存されたユーザー属性は、すべて読み取り専用です。ユーザーはこれらの属性を表示し、不一致があれば管理者に報告できます。

ユーザーが自分のユーザー プロファイルを表示または編集できるようにするには、事前にユーザー プロファイルに次のように値が入力済みである必要があります。

新規ユーザー。ユーザーが内部のアイデンティティ ソースにも外部アイデンティティ ソースにも保存されていない場合、ユーザーが必要な情報をユーザー プロファイルに入力する必要があります。

Authentication Manager には登録されていないが、ディレクトリ サーバに保存されたユーザー。ユーザー プロファイルにはディレクトリ サーバに格納された情報が表示されます。

Security Console では、デフォルト ユーザー プロファイルをそのまま使用できるほか、使用するアイデンティティ ソースごとにユーザー プロファイルをカスタマイズすることもできます。ユーザー プロファイルをカスタマイズするかどうかを判断するに当たっては、次の点を検討してください。

- 会社で使用しているフィールド名とデフォルト ユーザー プロファイルのフィールド名の間に違いはないか（たとえば、「User ID」の代わりに「User name」を使用しているなど）。
- フィールドに入力する情報をユーザーに指示するための説明テキストを追加する必要があるか。
- カスタム属性（ユーザーの自宅住所など）を追加する必要があるか。

アイデンティティ ソースに対してカスタム属性を作成すると、ユーザー プロファイルにカスタム属性を追加できます。オプションとして、各属性のラベルをカスタマイズできます。

セルフ サービス ユーザー プロファイルのカスタマイズ

セルフ サービス ユーザー向けに内部データベースを使用している場合は、どのユーザー属性を必須、編集可能、読み取り専用にするか、または Self-Service Console のユーザーに対して非表示にするかを指定できます。各属性の表示ラベルをカスタマイズすることもできます。

次の点に留意してください。

- 外部アイデンティティ ソースに格納されたユーザー属性は、すべて読み取り専用です。ユーザーが Self-Service Console を使用して情報を変更することはできません。
- 必須フィールドは編集可能です。
- アイデンティティ ソースにカスタム属性を作成すると、ユーザー プロファイルに表示するフィールドとして指定できます。
- メール アドレス属性が編集可能で、ユーザー プロファイルの変更時または On-Demand 認証の配信オプション変更時にメール通知を送信するようセルフ サービスが構成されている場合、Authentication Manager は新旧両方のメール アドレスに通知を送信します。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**User Profiles（ユーザー プロファイル**］をクリックします。
3. ［**Choose an Identity Source（アイデンティティ ソースの選択）**］ドロップダウン リストから、アイデンティティ ソースを選択します。
4. ［**Next（次へ）**］をクリックします。
5. ［**Core Attributes（コア属性）**］セクションで、カスタマイズする属性について［**View and manage user profile attribute details（ユーザー プロファイル属性の詳細の表示と管理）**］を選択します。
6. ［**Custom Attributes（カスタム属性）**］セクションで、カスタマイズする属性について［**View and manage user profile attribute details（ユーザー プロファイル属性の詳細の表示と管理）**］を選択します。
7. ［**Save（保存）**］をクリックします。

Self-Service Console の認証方式の設定

ユーザーは、Self-Service Console にアクセスするために必要なクレデンシャルを入力する必要があります。ユーザーがパスワードを使用しない場合は、1 つ以上のその他のクレデンシャルを構成します。次のタイプのクレデンシャルを 1 つ以上構成することができます。

- **RSA パスワード**。アイデンティティ ソースが Authentication Manager の内部データベースであるユーザー向け。このクレデンシャルを使用するには、RSA パスワードがユーザーのアカウントに割り当てられている必要があります。
- **RSA SecurID**。RSA SecurID トークンを使用するユーザー向け。
- **On-Demand**。On-Demand トークンコードを使用するユーザー向け。
- **LDAP パスワード**。アイデンティティ ソースが LDAP ディレクトリ サーバであるユーザー向け。

手順

1. Security Console で、[**Setup（設定）**] > [**Self-Service Settings（セルフ サービスの設定）**] > [**Self-Service Console Authentication（Self-Service Console の認証）**] の順にクリックします。
2. [**Console Authentication Method（コンソールの認証方式）**] フィールドで、ユーザーが Self-Service Console にログオンするときに使用する認証方式を入力します。
   たとえば、On-Demand トークンコードと LDAP パスワードを要求するには、OnDemand+LDAP_Password と入力します。
3. [**Save（保存）**] をクリックします。

次のステップ

認証方式を変更する場合は、Self-Service Console に現在ログオンしているすべてのユーザーが新しい認証方式で再ログオンする必要があるため、ユーザーに通知します。

セルフサービス用のセキュリティ クエスチョン

セルフ サービストラブルシューティング ポリシーでセキュリティ クエスチョンが有効になっている場合、ユーザーがセルフ サービスアカウント登録を行う際、または Self-Service Console にログオンする際に、セキュリティ クエスチョンの回答を作成するよう求めるメッセージが表示されます。アカウント登録されたユーザーがプライマリの認証方式で Self-Service Console にログオンできなくなった場合、本人確認のために質問への回答を求めるプロンプトが表示されます。正しい回答を入力した後、ユーザーは、Self-Service Console のトラブルシューティング画面を使用して、認証の問題を解決することができます。

セキュリティ クエスチョンを Self-Service Console にアクセスするためのプライマリ認証方式として使用することはできません。プライマリ認証方式として使用できるのは、RSA パスワード、LDAP パスワード、On-Demand 認証、SecurID です。

アカウント登録時およびトラブルシューティング時にユーザーが回答するセキュリティ クエスチョンの数を決定します。操作手順については、151 ページのセキュリティ クエスチョンの要件の設定を参照してください。

セルフ サービス ユーザー アカウント変更のメール通知の構成

セルフ サービス アカウントのセキュリティを高めるために、選択したイベントの発生時にユーザーにメール通知を送信するようにセルフ サービスを構成することができます。

次のセルフ サービスイベントでメール通知の送信を有効化できます。

- プロファイルの変更
- パスワードの変更（RSA パスワードまたは LDAP パスワード、ただしユーザーが Self-Service Console から変更した場合のみ）
- PIN の変更および PIN のブロック解除
- On-Demand 認証の配信オプションの変更
- エマージェンシー アクセス リクエスト
- トークン再同期リクエスト

アカウントの変更についての、ユーザーへのメール通知には、Web Tier 上の Self-Service Console へのリンクを含めることができます。ユーザーは、このリンクから直接 Self-Service Console に移動し、自分のアカウントを確認することができます。

導入環境のタイプによって、Self-Service Console にアクセスするために使用される URL が異なる可能性があります。デフォルトでは、Authentication Manager は、プライマリ インスタンス上にインストールされた Self-Service Console にエンド ユーザーが直接接続することを前提としています。使用する導入環境に Web Tier が含まれ、エンド ユーザーがロードバランサまたは仮想ホストを通して Self-Service Console に接続する場合は、適切な URL を使用する必要があります。

メール通知に Self-Service Console へのリンクを含めるには、仮想ホストまたはロードバランサをポイントするように通知のデフォルトの URL を変更します。これにより、Self-Service Console の実際の URL が変更されることはありません。また、指定した URL を使用して Self-Service Console にアクセス可能かの検証は行われません。

このメール通知テンプレートでは、フィールド ラベルやメール本文のカスタマイズ、メール タグの追加 / 削除 / 並べ替えを実行できます。詳細については、294 ページのセルフ サービス用メール テンプレートの例を参照してください。

メール アドレス属性が編集可能で、ユーザー プロファイルの変更時または On-Demand 認証の配信オプション変更時にメール通知を送信するようセルフサービスが構成されている場合、エンドユーザーが Self-Service Console からメール アドレスを変更すると、Authentication Manager は新旧両方のメール アドレスに通知を送信します。

開始する前に

272 ページの SMTP メール サービスの構成

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Self-Service Settings（セルフ サービスの設定）**] の順にクリックします。
2. [**Customization（カスタマイズ）**] で、[**E-Mail Notifications for User Account Changes（ユーザー アカウント変更のメール通知）**] をクリックします。
3. ユーザー アカウント変更に関するメール通知のデフォルトの URL を変更するには、次のいずれかを実行します。
   - Web Tier がない場合。[**Configure Default Self-Service Console URL**（Self-Service Console のデフォルト URL の構成）] で、プライマリ インスタンスの URL とポートを入力します。
     この URL の形式は次のとおりです。
     https://hostname:7004/console-selfservice
     各変数の意味を以下に示します。
     – hostname は、プライマリ インスタンスの完全修飾ホスト名です。
   - Web Tier がある場合。[**Configure Default Self-Service Console URL（Self-Service Console のデフォルト URL の構成）**] で、仮想ホストの URL とポートを入力します。
     この URL の形式は次のとおりです。
     https://virtualhostname:port/console-selfservice
     各変数の意味を以下に示します。
     – virtual-hostname は、仮想ホストの完全修飾ホスト名です。
     – port は、仮想ホストのポートです。
4. [**E-mail Notifications（メール通知）**] セクションで、ユーザーへのメール通知を開始する 1 つ以上のイベントを選択します。
5. [**E-mail Template（メール テンプレート）**] セクションで、[**Subject（件名）**] フィールドと [**Body（本文）**] フィールドを編集します。
   メール テンプレートでは、山括弧（<>）を使用できません。
6. [**Save（保存）**] をクリックします。

セルフ サービス用メール テンプレートの例

次の例は、アカウント変更時のデフォルトのメール テンプレートです。

Recent account change:${MailComposer.NL}${MailComposer.NL}

Account change:${MailComposer.RequestType}${MailComposer.NL}

Performed by:#(${Principal.UserID})${MailComposer.NL}

Date of account change:
${MailComposer.RequestDate}${MailComposer.NL}${MailComposer.NL}

If you have not authorized this change, contact your administrator with the information in this e-mail.

メール テンプレート タグの構文

メール テンプレート タグの構文は、次のとおりです。

${objectname.propertyname}

ここで、

- objectname はセルフサービス オブジェクト名です。
- propertyname はオブジェクトのプロパティ名です。

次に例を挙げます。

```
${Principal.UserID}
```

は、ユーザーのユーザー ID を意味します。

重要：${objectname.propertyname} などのメール タグ構文は変更しないでください。

メール テンプレート タグのデフォルト値

デフォルトのメール テンプレート タグを使用して、メール通知をカスタマイズします。次の表は、デフォルトのメール テンプレート タグの一覧です。

オブジェクト名	プロパティ名	タイプ	説明
Principal	UserID	文字列	ユーザー ID
Principal	E-mail	文字列	ユーザーのメール アドレス
Principal	FirstName	文字列	ユーザーの名前
Principal	LastName	文字列	ユーザーの苗字
MailComposer	RequestType	文字列	リクエスト タイプ
MailComposer	RequestDate	日付	アカウントが変更された日付
MailComposer	NL	文字列	改行する

Self-Service Console のカスタマイズ

ビジネスニーズに合わせて、ユーザー操作を拡張するために、Self-Service Console をカスタマイズすることができます。

295 ページのセルフサービス機能の有効化または無効化。ビジネスニーズのある機能のみ表示します。

296 ページの Self-Service Console の Web ページのカスタマイズ。ロゴを使用して Self-Service Console をブランド化します。ユーザー向けの独自のメッセージを使用して、ヘッダとフッタのテキストをカスタマイズします。

296 ページの Self-Service Console の Web ページのカスタマイズ。Self-Service Console ヘルプ ファイルの内容をカスタマイズして、企業のセルフサービスの使用法を反映させます。

セルフサービス機能の有効化または無効化

セルフ サービスの各機能を有効化または無効化することにより、セルフ サービスの環境をカスタマイズできます。たとえば、ユーザーがパスワードを忘れた場合に、ユーザー自身で復旧できないようにする必要がある場合を考えます。この場合、ユーザーが自分のパスワードを変更できる［**Forgot your password（パスワードを忘れた場合）**］リンクを非表示にすることができます。

次の機能はデフォルトで無効化されています。

- ［**Display Forgot Your Password link**（パスワードを忘れた場合のリンクを表示する）］
- ［**Display Troubleshoot SecurID Token link**（**SecurID** トークンのトラブルシューティングのリンクを表示する）］
- ［**Display I Forgot My PIN option**（**PIN** 忘れオプションを表示する）］

すべての設定はグローバルであり、導入環境全体に適用されます。

開始する前に

これらの機能を有効化する前には、セキュリティ上の影響について慎重に考慮することを推奨します。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［Settings（設定）］ページの［**Customization（カスタマイズ）**］セクションで、［**Enable or Disable Self-Service Features（セルフサービス機能の有効化または無効化）**］をクリックします。

3. ［**Set Display Options for Self-Service Console - Home Page（Self-Service Console ホーム ページの表示オプションの設定）**］で、Self-Service Console のホーム ページで表示または非表示にするリンクとセクションを選択します。

   注：［**Display Log On Section（ログオン セクションを表示する）**］をオフにすると、ユーザーは Self-Service Console のホーム ページからログオンすることも、［My Account（マイ アカウント）］ページに自分のプロファイル情報を表示することもできません。

4. ［**Set Display Options for Self-Service Console - My Account Page（Self-Service Console マイ アカウント ページの表示オプションの設定）**］で、Self-Service Console の［My Account（マイ アカウント）］ページで表示または非表示にするリンクとセクションを選択します。
5. ［**Set Display Options for Troubleshooting（トラブルシューティングの表示オプションの設定）**］で、Self-Service Console で表示または非表示にするリンクを選択します。
6. ［**Save（保存）**］をクリックします。

次のステップ

［**Set Display Options for Troubleshooting（トラブルシューティングの表示オプションの設定）**］で［**Display I Have Forgotten My Smart Card PIN or it is Blocked Option（スマート カードの PIN を忘れたかブロックされた場合のオプションを表示する）**］を有効化した場合、ユーザーがこのオプションを使用できるようにするためには、PIN のロック解除キーをインポートしておく必要があります。操作手順については、163 ページの RSA SecurID PIN のクリアを参照してください。

Self-Service Console の Web ページのカスタマイズ

Self-Service Console の Web ページおよび RBA（リスク ベース認証）ログオン ページで、以下の要素をカスタマイズできます。

手順

1. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Customization（カスタマイズ）**］の順にクリックします。
2. ［Web Tier Customization（Web Tier のカスタマイズ）］ページで、以下を実行します。
   - （Self-Service Console および RBA ログオン ページ）Self-Service Console および RBA ログオン ページの新しいロゴ ファイルを選択します。RSA のロゴを独自のロゴで置き換えることができます。ロゴ ファイルは、5 MB 未満の .gif ファイルである必要あります。イメージは、幅 500 ピクセル、高さ 50 ピクセルに収める必要があります。

- （Self-Service Console）Self-Service Console のヘッダテキストを入力します。たとえば、「○○株式会社のセルフ サービスコンソールへようこそ。On-Demand トークンコードのリクエストや、ユーザー プロファイルの更新を行うことができます。」のようなユーザー向けの情報を入力できます。
- （Self-Service Console）Self-Service Console のフッタ 1 のテキストを入力します。追加できるテキストは最大 3 行までです。
- （Self-Service Console）フッタ 2 のテキストを入力します。
- （Self-Service Console）フッタ 3 のテキストを入力します。

3. ［**Save（保存）**］をクリックします。

次のステップ

215 ページの Web Tier の更新を参照してください。

Self-Service Console ユーザー ヘルプのカスタマイズ

Self-Service Console ヘルプ ファイルの内容をカスタマイズして、企業のセルフサービスの使用法を反映させることができます。

Self-Service Console ヘルプの HTM ファイルを編集して、次のようにカスタマイズできます。

- **properties** ファイルを編集し、Self-Service Console に行った変更を反映します。
- 自社に固有の情報を追加します。例：用語集。
- 自社に当てはまらない情報を削除します。

Authentication Manager アプライアンス上の HTM ファイルの場所は、**/opt/rsa/am/server/apps/rsa-help/eclipse/plugins/com.rsa.ucmuserconsole.help/console-help** です。

Web Tier 上の HTM ファイルの場所は、**RSA_WT_HOME/server/apps/rsa-help/eclipse/plugins/com.rsa.ucmuserconsole.help/console-help です**。

Authentication Manager アプライアンス上の Self-Service Console ヘルプ ファイルを変更しても、Web Tier 上の Self-Service Console ヘルプ ファイルは変更されません。Self-Service Console ヘルプ ファイルを、アプライアンス上の **console-help** ディレクトリから、各 Web Tier サーバの **console-help** ディレクトリにコピーします。

プロビジョニングの概要

セルフ サービスのプロビジョニング機能により、トークンを配布するワークフローが自動化され、ユーザーは Self-Service Console からプロビジョニング タスクの多くを実行できます。

注：プロビジョニング機能は、Authentication Manager Enterprise Server ライセンスに含まれています。Base Server ライセンスを使用している場合にプロビジョニングが必要になった場合は、Enterprise Server ライセンスにアップグレードする必要があります。

ユーザーがトークンの要求、有効化、トラブルシューティングを行うことや、エマージェンシー アクセスを使用することができるように、プロビジョニングを構成できます。プロビジョニングには、トークンの管理、リクエストの承認、トークンの配布を行うために割り当てることができる事前定義の管理者ロールが含まれています。

ユーザーは Self-Service Console から次のプロビジョニング アクションを実行できます。

- アカウント登録要求
- 新しいトークンまたは追加トークンの要求
- トークンの有効化
- On-Demand トークンコード サービスの要求
- 交換用トークンの要求（トークンを紛失または破損した場合、一時的に使用できなくなった場合、まもなく期限切れになる場合）
- 保護されたリソースにアクセスするために必要なユーザー グループ メンバーシップの要求
- On-Demand 認証の要求

プロビジョニングの管理者ロール

プロビジョニングには、次のようなカスタマイズ可能な事前定義の管理者ロールがあります。

Token Administrator（トークン管理者）：トークンをインポートおよび管理し、ユーザーにトークンを割り当てます。

Request Approver（リクエスト承認者）：新しいユーザー アカウント、ユーザー グループ メンバーシップ、トークン要求などのプロビジョニング要求を承認、更新、拒否します。

Token Distributor（トークン配布者）：トークン プロビジョニング要求を管理します。ユーザーに対するトークンの割り当ておよび配布方法を決定します。

事前定義された各ロールについて、管理者ごとに次の表に示されている権限を構成できます。

General Permissions（一般権限）	Authentication Permissions（認証権限）	Self-Service Permissions（セルフ サービス権限）
• ポリシーの管理 • セキュリティ クエスチョンの管理 • 委譲管理 • ユーザーの管理 • ユーザー グループの管理 • レポートの管理	• SecurID トークンの管理 • ユーザー グループの管理 • ユーザー認証属性の管理 • 認証エージェントの管理 • トラステッド レルムの管理 • On-Demand 認証の管理	プロビジョニング要求

各ロールの権限適用範囲をセキュリティ ドメインおよびアイデンティティ ソースに制限できます。また、プロビジョニング管理者がロールの権限を他の管理者に委譲することを許可することもできます。たとえば、企業の事業部のリクエスト承認者は、承認権限を部課レベルの管理者に委譲できます。

また、Authentication Manager でプロビジョニング権限を任意の管理者ロールに割り当てることもできます。管理者ロールを構成するには、Security Console を使用します。

Request Approver および Token Distributor の権限適用範囲

Request Approver は、次の条件を満たす場合にリクエストを承認できます。

リクエスト タイプ	承認条件
トークン	承認者の権限適用範囲に使用可能な未割り当てのトークンがある。
グループ メンバーシップ	ユーザーとグループの両方が承認者の権限適用範囲内にある。
デフォルト グループ	ユーザーが承認者の権限適用範囲にある。グループの権限適用範囲は問わない。
任意のリクエスト	ユーザーが承認者のセキュリティ ドメインに存在する必要があります。

Request Approver 向けのワークフロー手順については、Security Console ヘルプのトピック「Approve and Reject User Requests（ユーザー リクエストの承認および拒否）」を参照してください。

Token Distributor は、自分のセキュリティ ドメインのリクエストのみをレビューしてクローズできます。

Request Approver および Token Distributor の権限

Request Approver および Token Distributor は、ユーザーからリクエストされたトークンのタイプを変更できます。たとえば、キー フォブ トークンのリクエストを USB トークンのリクエストに変更することなどが可能です。

Request Approver および Token Distributor は、次の操作はできません。

- ハードウェア トークンのリクエストからソフトウェア トークンのリクエストへの変更（またはその逆）。
- On-Demand トークンコード サービスのリクエストからハードウェアまたはソフトウェア トークンのリクエストへの変更（またはその逆）。

RSA では、Request Approver および Token Distributor がキー フォブ トークンのリクエストを PIN パッド式トークンのリクエストに変更することを推奨しません。キー フォブ トークンの PIN は PIN パッド式トークンと互換性がなく、ユーザーが使用しようとしても PIN が無効になるためです。

PIN ポリシーを変更する場合は、未処理のトークン リクエストが新しいポリシーの影響を受けないことを確認します。トークンの PIN ポリシーを変更する場合は、未処理のリクエストに対して事前に適切なアクションを行っておくことを推奨します。

Token Distributor 向けのワークフロー手順については、Security Console ヘルプのトピック「Complete User Requests（ユーザー リクエストの完了）」を参照してください。

プロビジョニング リクエストのワークフロー

プロビジョニングでは、ワークフローを使用してトークンの導入を自動化します。ワークフローでは、ユーザーのプロビジョニング リクエストのタイプごとにステップ数および必要なタスクを定義します。ワークフロー内のタスクを実施するユーザーおよび管理者のことをワークフロー参加者と呼びます。

次の表は、ワークフロー参加者のタイプと参加者が実施するタスクを示しています。

ワークフロー参加者	タスク
ユーザー	ユーザーが Self-Service Console からリクエストを送信することによって、ワークフローが開始します。ユーザー リクエストには、次のタイプがあります。 • アカウント登録 • 新規または追加の SecurID トークン • 有効期限が近づいているハードウェア トークンおよびソフトウェア トークンのリプレース • 破損トークンまたは永続的に紛失したトークンのリプレース • On-Demand トークンコード サービス • 追加のユーザー グループ メンバーシップ

ワークフロー参加者	タスク
Request Approver	Request Approver が Security Console で実行するタスク： • すべてのリクエストの表示。 • リクエストの承認、拒否、キャンセル、アクション延期。 • リクエストに対するコメント（必要な場合）。 • トークン タイプの変更（必要な場合）。
Token Distributor	Token Distributor が Security Console で実行するタスク： • 配布が必要なユーザ リクエストの表示。 • ユーザーに対するトークンの割り当ておよび配布方法の決定。 • ユーザーに対するトークン配布の記録。

管理者ロールの割り当て

プロビジョニング リクエストのためにワークフローを使用する場合、Token Administrator、Request Approver、Token Distributor の管理者ロールを割り当てる必要があります。プロビジョニングの管理者ロールの詳細については、298 ページのプロビジョニングの管理者ロールを参照してください。操作手順については、65 ページの管理者ロールの割り当てを参照してください。

ワークフロー ポリシー

セルフ サービスでは、ワークフロー ポリシーを使用してトークンの配布を自動化したり、ODA（On-Demand 認証）の有効化などのユーザーからのリクエストに対応します。ワークフロー ポリシーでは、ユーザー リクエストを処理する方法を決定します。ワークフロー ポリシーは、導入プロセス全体に適用されます。各ユーザー リクエストは、1 つのワークフロー ポリシーで管理されます。ワークフロー ポリシーには、次の機能が用意されています。

- 一般的なワークフロー設定
- ユーザーとグループの設定
- ハードウェア トークン リクエストとソフトウェア トークン リクエストの設定
- On-Demand トークンコード リクエストの設定
- リクエストのタイプごとのステップの数
- プロビジョニング リクエストに関するメール通知受信者のリスト
- リクエストのタイプごとのメール通知の内容

ODA と RBA の詳細については、第 10 章、On-Demand 認証の導入および第 12 章、リスク ベース認証の導入を参照してください。

プロビジョニングの構成

プロビジョニングを有効化し、Self-Service Console ユーザーに提供する機能とサービスを構成する必要があります。ワークフロー ポリシーを指定し、ユーザー リクエストに関するメール通知をカスタマイズできます。次のリストは、プロビジョニングを構成するためのガイドです。

手順

1. 302 ページのプロビジョニングの有効化。
2. 302 ページのデフォルトのワークフロー ポリシーの変更。
3. 303 ページのセキュリティ ドメインへのワークフロー ポリシーの割り当て。
4. 303 ページのワークフロー定義の変更。
5. 305 ページのプロビジョニング リクエストのためのメール通知の使用。
6. 307 ページのセルフ サービス ユーザーのトークンの構成。
7. 308 ページのハードウェア トークンの送付先住所の構成。

プロビジョニングの有効化

ユーザーが Self-Service Console から、アカウント登録、ユーザー グループ、トークン、On-Demand 認証をリクエストするのを許可するには、プロビジョニングを有効化する必要があります。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフサービス設定）**］＞［**Enable or Disable Self-Service Features（セルフサービス機能の有効化 / 無効化）**］を選択します。
2. ［**Enable Provisioning Features（プロビジョニング機能の有効化）**］を選択します。
3. ［**Save（保存）**］をクリックします。

デフォルトのワークフロー ポリシーの変更

ワークフロー定義内のリクエスト承認者の数、メールの受信者、ワークフロー参加者に送信するメールの内容を変更する必要がある場合は、必要に応じて、会社のデフォルトのワークフロー ポリシーを変更できます。

各導入環境には、すべての新規作成されるセキュリティ ドメインに割り当てられるデフォルトのワークフロー ポリシーが存在します。デフォルトのポリシーは変更できます。デフォルトのポリシーは、デフォルトのポリシーを使用するように構成されているすべてのセキュリティ ドメインに適用されます。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Self-Service Settings（セルフ サービスの設定）**] の順にクリックします。
2. [Provisioning（プロビジョニング）] の [**Workflow Policies（ワークフロー ポリシー）**] をクリックします。
3. 検索フィールドを使用して、デフォルトとして設定するポリシーを検索します。
4. 検索結果からデフォルトとして設定するポリシーをクリックし、コンテキスト メニューから [**Edit（編集）**] をクリックします。
5. [Workflow Policy Basics（ワークフロー ポリシーの基本設定）] で、[**Default Policy（デフォルトのポリシー）**] チェックボックスをオンにして、新しいポリシーを導入環境のデフォルトのポリシーとして指定します。
6. [**Save（保存）**] をクリックします。

セキュリティ ドメインへのワークフロー ポリシーの割り当て

Authentication Manager をインストールするか、新しい導入環境を作成すると、デフォルトのワークフロー ポリシーが作成されます。セキュリティ ドメインを作成する際に、デフォルトのポリシーを使用するか、カスタム ポリシーを作成し、そのポリシーをセキュリティ ドメインに割り当てることができます。選択したポリシーは、そのセキュリティ ドメインに属する全ユーザーに適用されます。

手順

1. Security Console で、[**Administration（管理）**] > [**Security Domains（セキュリティ ドメイン）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. セキュリティ ドメインのツリーから編集するセキュリティ ドメインを選択し、コンテキスト メニューから [**Edit（編集）**] をクリックします。
3. [Policies（ポリシー）] の [**Workflow Policy（ワークフロー ポリシー）**] フィールドで、ドロップダウン メニューを使用して、セキュリティ ドメインのポリシーを選択します。
4. [**Save（保存）**] をクリックします。

ワークフロー定義の変更

ユーザー要求には、タイプごとにデフォルトのワークフロー定義が存在します。その定義は、組織のニーズに合わせてカスタマイズできます。ワークフロー定義では、要求のタイプごとにステップ数または作業アイテムを定義します。承認ステップごとに一意のリクエスト承認者が必要です。ワークフロー定義は、以下で構成されます。

- 0 ～ 4 個の承認ステップ：リクエスト承認者はすべての要求を表示し、要求を承認または拒否します。
- 0 ～ 1 個の配布ステップ：トークン配布者がユーザーのトークン要求を表示し、トークンの割り当ておよび配布方法を決定します。

たとえば、ある会社では、すべての新しい従業員がセルフ サービスでアカウント登録し、会社のネットワークにアクセスできるように新しいトークンを要求する必要があるとします。会社のポリシーにより、新しい従業員からのトークン要求は、マネージャとシステム管理者の 2 人の承認が必要な場合、この要件に対応するようにワークフロー定義をカスタマイズできます。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Self-Service Settings（セルフ サービスの設定）**] の順にクリックします。
2. [Provisioning（プロビジョニング）] の [**Workflow Policies（ワークフロー ポリシー）**] をクリックします。
3. 検索フィールドを使用して、編集するポリシーを検索します。
4. 編集するポリシーを選択します。
5. コンテキスト メニューで [**Edit（編集）**] をクリックします。
6. 特定のタイプの要求のワークフロー定義を変更するには、次のいずれかのタブをクリックします。
   - [**User and User Group（ユーザーおよびユーザー グループ）**]：ディレクトリ サーバに登録されているユーザーおよびディレクトリ サーバに登録されていないユーザーからのセルフ サービス アカウント登録要求、ユーザー グループ メンバーシップの要求
   - [**Hardware Token（ハードウェア トークン）**]：ハードウェア トークンの要求。
   - [**Software Token（ソフトウェア トークン）**]：ソフトウェア トークンの要求。
   - [**On-Demand Authentication（On-Demand 認証）**]：On-Demand 認証の有効化の要求。
7. [**Workflow Definitions（ワークフロー定義）**] で、ドロップダウン矢印をクリックして、要求の承認ステップまたは配布ステップの数を変更します。
8. [**Save（保存）**] をクリックします。

注：保存していない場合は、[**Reset（リセット）**] をクリックして、ポリシーを元の設定に戻すことができます。

プロビジョニング リクエストのためのメール通知の使用

プロビジョニング ワークフローの参加者は、リクエストが送信されたとき、承認待ちのとき、承認、キャンセル、拒否されたとき、正常に完了しなかったときに、メール通知を受信できます。次のワークフロー参加者に、メール通知の受信を許可できます。

- すべてのワークフロー参加者。ユーザー、Request Approver、Token Distributor
- スーパー管理者
- 親セキュリティ ドメイン内のワークフロー参加者

リクエストが拒否された理由を説明するなどの目的で、リクエストにコメントを追加した場合は、コメントを含めたメール通知が送信されます。

Authentication Manager からメール通知を送信するには、事前に SMTP を構成する必要があります。詳細については、RSA Security Console ヘルプのトピック「Configure the SMTP Mail Service（SMTP メール サービスの構成）」を参照してください。

親セキュリティ ドメイン内のワークフロー参加者へのメール通知を有効にすると、リクエストが発生したセキュリティ ドメインより上位のセキュリティ ドメイン内のすべての Request Approver と Token Distributor がワークフロー メール通知を受信します。

デフォルト設定では、ワークフローの参加者全員（ユーザー、Request Approver、Token Distributor）に対してワークフローのメール通知が有効ですが、この設定を選択解除できます。参加者のタイプ（スーパー管理者を除く）に応じてワークフローのメール通知を無効化することはできません。

プロビジョニングのワークフロー参加者へのメール通知の構成

セルフ サービスでは、要求の送信時、承認待ち時、キャンセル時、拒否時、送信失敗時などに、ワークフロー参加者が要求に対してアクションを実行する必要があることを通知するメールを自動的に送信できます。ワークフローのメール通知の受信者を指定できます。

セルフ サービスでは、要求を送信したユーザーに自動的にメール通知を送信します。ユーザーに対するメール通知を無効化することはできません。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service（セルフ サービス）**］の順にクリックします。
2. ［**Provisioning（プロビジョニング）**］セクションの［**Workflow Policies（ワークフロー ポリシー）**］をクリックします。
3. 検索フィールドを使用して、変更するポリシーを検索します。
4. 検索結果から変更するポリシーをクリックし、コンテキスト メニューから［**Edit（編集）**］をクリックします。

5. ［**E-mail Notification Settings（メール通知の設定）**］で、次の 1 つ以上のオプションを選択します。
   - ［**Enable e-mail notifications for all workflow participants（すべてのワークフロー参加者へのメール通知を有効化する）**］：すべてのワークフローの参加者（マネージャ、リクエスト承認者またはトークン配布者の権限を持つ管理者）にメール通知が送信されます。
   - ［**Enable e-mail notifications for Super Admin（スーパー管理者へのメール通知を有効化する）**］：スーパー管理者にメール通知が送信されます。
   - ［**Enable e-mail notifications for parent workflow participants（親ワークフロー参加者へのメール通知を有効化する）**］：要求を行ったユーザーの親セキュリティ ドメイン内のすべての承認者と配布者にメール通知が送信されます。
6. ［**Save（保存）**］をクリックします。

セルフ サービス ユーザーのトークンの管理

ユーザーは、Self-Service Console から、トークンとエマージェンシー アクセスを要求できます。管理者は Security Console を使用して、使用可能なトークンのタイプ、エマージェンシー アクセス トークンコード、有効期限切れのトークンの交換リクエストを管理できます。

［**Hardware Token Types Available for Request（リクエスト可能なハードウェア トークン タイプ）**］：リクエスト可能にするトークンのタイプ、認証タイプ、セルフ サービス ユーザー向けのデフォルトのタイプを選択できます。

［**Software Token Profiles Available for Request（リクエスト可能なソフトウェア トークン プロファイル）**］：リクエスト可能にするソフトウェア トークン プロファイルを選択できます。ソフトウェア トークン プロファイルにより、認証タイプとトークン配布方法が決まります。また、ユーザーによるトークン属性の詳細の編集を許可したり、セルフ サービス ユーザー向けのデフォルトのタイプを選択することが可能です。

［**On-Demand Authentication (ODA) Settings（On-Demand 認証の設定）**］：ユーザーが ODA サービスをプライマリ認証方式としてリクエストできるようにすることが可能です。管理者は、プロビジョニング ユーザーがこのサービスを要求できるように ODA 設定を構成しておく必要があります。

［**Token File Password Settings（トークン ファイル パスワードの設定）**］：管理者は、ソフトウェア トークン ファイルを保護するパスワードを指定するようにユーザーに要求できます。

［**Emergency Access Tokencode Settings（エマージェンシー アクセス トークンコードの設定）**］：トークンが一時的または永続的に使用不可になったユーザーがエマージェンシー アクセスを要求することができます。セルフ サービスユーザーは、ヘルプ デスクのサポートなしで、エマージェンシー アクセスを有効化できます。管理者は、ユーザー向けに使用可能とするエマージェンシー アクセスのタイプを構成できます。

［**Expiring Token Parameters（期限切れトークン パラメータ）**］：ユーザーは、トークンの期限切れが近づいたら、Self-Service Console を通じて交換用トークンを要求できます。管理者は、期限切れの何日前からユーザーがこのリクエストを実行できるか日数を構成できます。デフォルトは、有効期限が切れる 30 日前からです。

管理者がトークンの配布と使用に関するレポートを作成する場合は、Authentication Manager 標準のレポートを使用するか、カスタム レポートを作成することができます。レポートの詳細については、386 ページの管理者ロールごとの実行可能なレポートおよび 390 ページのカスタム レポートを参照してください。

セルフ サービス ユーザーのトークンの構成

ユーザーは、Self-Service Console から、トークンとエマージェンシー アクセスをリクエストできます。管理者は、リクエスト可能なトークンのタイプを管理し、エマージェンシー アクセス トークンコードの設定を構成することができます。

開始する前に

232 ページのソフトウェア トークン プロファイルの追加。ソフトウェア トークン プロファイルを追加できるのは、スーパー管理者だけです。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービスの設定）**］の順にクリックします。
2. ［**Provisioning（プロビジョニング）**］セクションで、［**Manage Authenticators（トークンの管理）**］をクリックし、必要に応じて次の操作を実行します。
   - ［**Hardware Token Types Available for Request（リクエスト可能なハードウェア トークン タイプ）**］で、1 つ以上のタイプを選択し、それぞれのタイプの設定を定義します。詳しい手順については、RSA Security Console ヘルプのトピック「プロビジョニング用のハードウェア トークンの選択」を参照してください。
   - ［**Software Token Profiles Available for Request（リクエスト可能なソフトウェア トークン プロファイル）**］で、1 つ以上のソフトウェア トークン プロファイルを選択し、それぞれのタイプの設定を定義します。詳しい手順については、RSA Security Console ヘルプのトピック「プロビジョニング用のソフトウェア トークンの選択」を参照してください。

- ［**On-Demand Authentication Settings（On-Demand 認証の設定）**］で、［**Allow users to request the on-demand tokencode service（On-Demand トークンコード サービスをリクエストできるようにする）**］を選択し、設定を定義します。詳しい手順については、RSA Security Console ヘルプのトピック「プロビジョニング用の On-Demand 認証の選択」を参照してください。
- ［**Token File Password Settings（トークン ファイル パスワードの設定）**］で、［**The user needs to provide the password, to protect the token file（ユーザーはトークン ファイルを保護するパスワードを指定する必要がある）**］を選択し、ファイル形式を選択します。

3. （オプション）エマージェンシー アクセス設定を構成します。詳しい手順については、RSA Security Console ヘルプのトピック「プロビジョニング用のエマージェンシー アクセスの構成」を参照してください。
   - ［**Emergency Access Tokencode Settings（エマージェンシー アクセス トークンコードの設定）**］で、設定を定義します。
   - ［**Emergency Access Tokencode Settings for Permanently Lost or Broken Tokens（トークンを完全に紛失または破損した場合のエマージェンシー アクセス トークンコードの設定）**］で、設定を定義します。
   - ［**Emergency Access Tokencode Settings for Temporarily Unavailable Tokens（トークンが一時的に使用できなくなった場合のエマージェンシー アクセス トークンコードの設定）**］で、設定を定義します。
   - ［**Expiring Token Parameters（期限切れトークン パラメータ）**］で、ユーザーが交換用トークンをリクエストできるのは期限切れの何日前からかを設定します。
4. ［**Save（保存）**］をクリックします。

ハードウェア トークンの送付先住所の構成

プロビジョニングを構成するときに、各ユーザーのハードウェア トークンの送付先となる送付先住所を構成できます。各ユーザーが個別の送付先住所を持つことができます。送付先住所は、ユーザー プロファイル上に表示されます。

管理者が送付先データを内部データベースに格納した場合、配布ステップを必要とするトークンのリクエストのたびに、ユーザーは、送付先住所を入力する必要があります。

ディレクトリ サーバをアイデンティティ ソースとして使用する場合は、送付先住所を既存のアイデンティティ属性にマッピングすることができます。これにより、アイデンティティ ソースがユーザーの住所情報を自動的に追加するようになります。ユーザーは送付先住所を表示できますが、変更することはできません。

送付先住所の変更は、現在のトークン リクエストにのみ適用されます。送付先住所を変更しても、アイデンティティ ソース上のユーザーレコードが変更されることはありません。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**Self-Service Settings（セルフ サービスの設定）**] の順にクリックします。
2. [**Provisioning（プロビジョニング）**] で、[**Set Shipping Addresses（送付先住所の設定）**] をクリックします。
3. （オプション）[**Shipping Address Mapping and Display Options（送付先住所のマッピングおよび表示オプション）**] で、送付先住所のフィールドを [**Required（必須）**]、[**Optional（オプション）**]、[**Read-only（読み取り専用）**]、[**Hidden（非表示）**] のいずれにするかを指定します。
4. （オプション）それぞれのフィールドについて、次のいずれかを実行します。
   - データを内部データベースに格納する場合は、[**Map to（マッピング）**] で、[**Unmapped（マッピングしない）**] を選択します。
   - 送付先住所についてアイデンティティ ソースからの情報を使用するには、[**Map To（マッピング）**] で、使用可能なアイデンティティ属性のいずれかを選択します。
5. [**Save（保存）**] をクリックします。

セルフ サービス トラブルシューティング

セルフ サービス トラブルシューティング機能を使用すると、Self-Service Console のユーザーは、パスワードやパスコードなどのプライマリ認証方式で保護されたリソースにアクセスできないときに、定型的な認証のトラブルシューティングを行うことができます。

ユーザーのレコードが内部データベースに格納されている場合、ユーザーは次のようなトラブルシューティングを行うことができます。

- パスワードのリセット
- トークン PIN のリセット
- トークンの再同期
- 新しいトークンのリクエスト（古いトークンを紛失した場合）
- エマージェンシー アクセス トークンコードのリクエスト

管理者は、セルフ サービス トラブルシューティング ポリシーをセキュリティ ドメインに割り当てます。デフォルトのポリシーは、新規作成したセキュリティ ドメインに自動的に割り当てられます。デフォルトのポリシーは、カスタム ポリシーを選択することによって割り当てを解除されます。

セルフ サービス トラブルシューティング ポリシーの追加

レプリケーション導入環境では、ポリシーの変更はレプリカ インスタンス上ですぐに確認できない可能性があります。この遅延はキャッシュ更新間隔が原因です。変更は 10 分以内にレプリケーションされます。レプリカ インスタンスに変更が反映されるまでの時間を短縮する手順については、423 ページのキャッシュのフラッシュを参照してください。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Self-Service Troubleshooting Policies（セルフ サービス トラブルシューティング ポリシー）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Self-Service Troubleshooting Policy Name（セルフ サービス トラブルシューティング ポリシー名）**］フィールドで、ポリシー名を入力します。128 文字以内の一意の名前を使用してください。
3. （オプション）新しいポリシーをシステムのデフォルト ポリシーとして指定するには、［**Default Policy（デフォルト ポリシー）**］を選択します。このオプションを選択すると、新規作成されるセキュリティ ドメインはこのポリシーを使用します。
4. （オプション）［**Authentication Method（認証方式）**］で、ユーザーがプライマリ認証方式を使用できない場合に使用する認証方式を選択します。
5. ［**Lock User Accounts（ユーザー アカウントのロック）**］フィールドは、ユーザーがセルフ サービス トラブルシューティング機能にアクセスする際に許可される認証失敗回数を制御します。失敗は無制限に許可することも、一定の日数、時間、分、秒の範囲内で指定した回数許可することもできます。指定した回数を超えると、このポリシーによってそのユーザーのアカウントはトラブルシューティング機能からロック アウトされます。
6. ［**Unlock（ロック解除）**］フィールドでは、［**Lock User Accounts（ユーザー アカウントのロック）**］フィールドで指定された認証失敗回数の上限を超えたためロックされたユーザーのアカウントを管理者が手動でロック解除するように構成できるほか、システムによってロック解除を自動的に行うように構成することもできます。自動でロック解除する場合は、何日後、何時間後、何分後、何秒後にロック解除するかを指定できます。
7. ［**Save（保存）**］をクリックします。

12 リスク ベース認証の導入

リスクベース認証

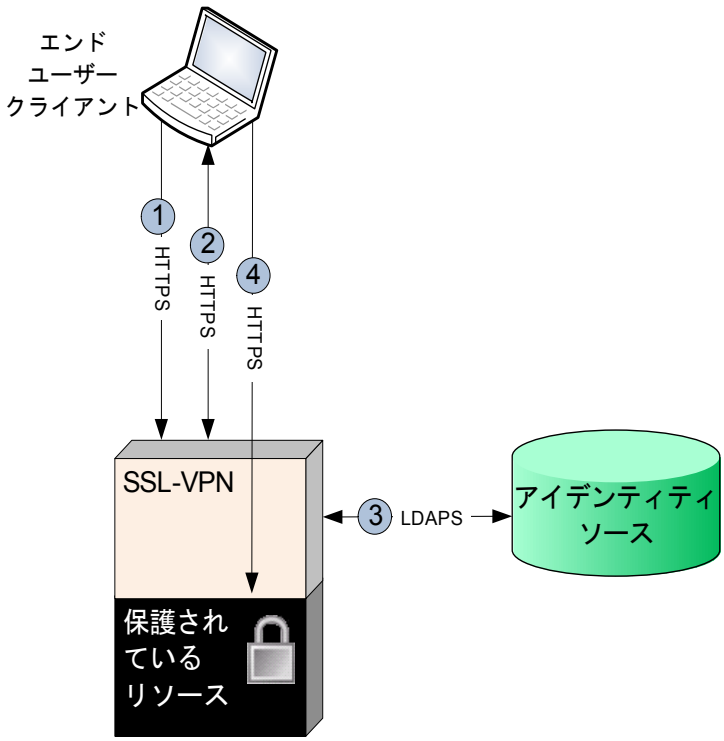
RBA（リスク ベース認証）は、ユーザーの行動パターンやアクセスに使用するデバイスをユーザーに気づかせることなく分析することにより、潜在的なリスクや不正な認証試行を識別します。RBA は、RSA SecurID 認証および従来のパスワード ベースの認証を強化します。評価リスクが許容できない場合、ユーザーは次のいずれかの方法によってユーザー本人であることを証明するよう要求されます。

- ODA（On-Demand 認証）。ユーザーは、PIN、および、事前に設定した携帯電話番号またはメール アカウントに送信されたワンタイム トークン コードを正確に入力する必要があります。
- セキュリティ クエスチョン。ユーザーは、1 つ以上のセキュリティ クエスチョンに正しく回答する必要があります。質問の正解は、Self-Service Console で構成するか、またはサイレント収集期間に認証を行う時に構成します。

Authentication Manager には、各ユーザーのデバイスと行動パターンに関する情報をインテリジェントに収集して分析するリスクエンジンが含まれています。ユーザーが認証を試行すると、リスクエンジンは収集したデータを参照してそのリスクを評価します。その後、リスクエンジンはユーザーの認証試行に高、中、低などの保証レベルを割り当てます。RBA は、この保証レベルを、あらかじめ構成された許容可能な最低保証レベルと比較します。保証レベルが最低保証レベルに満たない場合、このユーザーにはセキュリティ クエスチョンまたは ODA を使用したユーザー確認が求められます。

リスク ベース認証のデータ フロー

次の図は、RBA（リスク ベース認証）を構成する前の Web ベース アプリケーションを表します。この例では、ネットワーク リソースは SSL-VPN で保護されており、SSL-VPN はユーザーのログオン クレデンシャルの検証に LDAP ディレクトリを使用するよう構成されています。



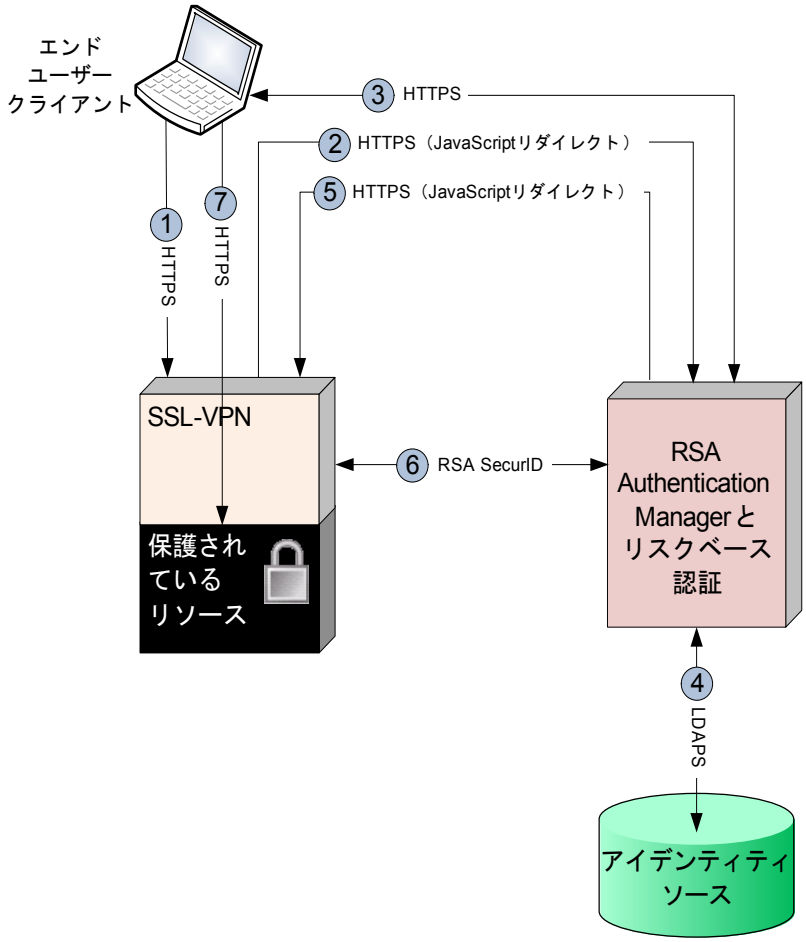
データ フローは、次の順序で発生します。

1. ユーザーは HTTPS 接続で SSL-VPN のログオン ページにアクセスします。
2. ユーザーはユーザー名とパスワードを入力します。
3. SSL-VPN は、アイデンティティ ソースとして使用する LDAP ディレクトリに LDAPS 接続し、ユーザーの ID を検証します。
4. SSL-VPN からユーザーに、保護リソースへのアクセス権が付与されます。

RBA が有効な場合、ユーザーは Web ベース アプリケーションのログオン ページから、Authentication Manager のログオン ページにリダイレクトされます。ユーザーがログオン クレデンシャルを入力すると、Authentication Manager が、アイデンティティ ソースとして使用する LDAP ディレクトリでユーザーのクレデンシャルを検証します。

ユーザーがこのワークフローを意識することのないように、RBA を導入することができます。リダイレクトは即時実行されます。また、Authentication Manager のログオン ページをカスタマイズできます。

次の図は、RBA が SSL-VPN と統合された図です。



データ フローは、次の順序で発生します。

1. ユーザーは HTTPS 接続で SSL-VPN のログオン ページにアクセスします。
2. SSL-VPN によってユーザーのブラウザが Authentication Manager のログオン ページにリダイレクトされます。
3. ユーザーはユーザー名とパスワードを入力します。
4. Authentication Manager は、アイデンティティ ソースとして使用する LDAP ディレクトリに LDAPS 接続し、ユーザーの ID を検証します。

また、Authentication Manager では認証試行の保証レベル（ユーザーにユーザー確認を求めるか否かを決定する信頼度）も評価されます。次のいずれかの状況が発生します。

- 保証レベルが RBA ポリシーの最低レベルを満たす場合、データフローはステップ 5 に続きます。
- 保証レベルが RBA ポリシーの最低レベルに満たない場合、ユーザーにはユーザー確認が求められます。次のいずれかの状況が発生します。
  - ユーザー確認が成功すると、データフローはステップ 5 に続きます。
  - ユーザー確認ができない場合は、Authentication Manager からユーザーのブラウザにアクセス拒否のメッセージが送られ、データフローが終了します。

5. Authentication Manager は、ユーザーのブラウザを、ユーザーのクレデンシャルが検証できたことを示す認証アーティファクトとともに SSL-VPN にリダイレクトします。
6. SSL-VPN は、Authentication Manager の固有の認証プロトコルである RSA SecurID プロトコルを使用して、認証アーティファクトを検証します。
7. SSL-VPN からユーザーに、保護リソースへのアクセス権が付与されます。

リスク ベース認証の導入に関する検討事項

RBA（リスク ベース認証）を導入する前に、RBA 導入戦略を計画し、RBA ポリシーを策定するために、次の点を検討します。

- セキュリティ ドメイン内の全ユーザーが RBA を使用しますか。「はい」の場合は、全ユーザーを自動的に有効化するよう Authentication Manager を構成します。「いいえ」の場合は、管理者がユーザーを個別に有効化します。
- Web Tier を使用していますか。RSA では、RBA を使用する場合は、Web Tier の導入を推奨します。複数の Web Tier を導入し、RBA トラフィックを処理することができます。
- RBA の優先インスタンスとして選択するインスタンスはどちらですか。RBA の優先インスタンスを指定する必要があります。RBA トラフィックを処理する Web Tier ごとに、優先インスタンスを選択する必要があります。
- RBA を Web ベースの認証エージェントと統合しますか。RSA は、特定の Web ベース エージェントと RBA の統合をサポートしています。その他の Web ベース エージェントは、SecurID プロトコルまたは RADIUS プロトコルのどちらかをサポートしていれば RBA に統合できます。
- サイレント収集を使用しますか。サイレント収集のデータ蓄積期間中に、システムによって各ユーザーのベースライン認証履歴の作成と認証デバイスの自動登録が行われます。

- ユーザーはどのくらいの頻度で、パブリックのコンピュータまたはデバイスから保護対象リソースにアクセスしますか。これは、最低保証レベルの選択、サイレント収集の有効化 / 無効化、デバイス設定の構成を選択する際に考慮します。ユーザーが頻繁にパブリックのコンピュータまたはデバイスを使用する場合は、より高い保証レベルを選択します。
- ユーザーが通常保護対象リソースにアクセスする際、複数のデバイスを使用しますか、または場所を変えてアクセスしますか。ユーザーの場所、デバイス、行動の変化を、Authentication Manager はどのくらい敏感に感知する必要がありますか。これは、最低保証レベルを選択し、デバイス設定を構成する際に考慮します。
- どのユーザー確認方法を使用しますか。たとえば、組織が業務用として承認した携帯電話をユーザーが携帯する場合、On-Demand 認証を選択できます。ラップトップまたはデスクトップ ユーザーの場合は、セキュリティ クエスチョンを選択できます。
- 各ユーザーに関連づけるデバイスはいくつですか。各デバイスをユーザーに登録しておく期間はどのくらいですか。これは、デバイス設定を構成する際に考慮します。
- RBA のログオン ページに自社のロゴが必要ですか。詳細については、296 ページの Self-Service Console の Web ページのカスタマイズを参照してください。
- ユーザーは RSA SecurID 認証を使用しますか。RBA が有効な場合、次のトークン関連のイベントによってリスク レベルが上昇する可能性があります。
  - ユーザーのログオン失敗回数が閾値を超える
  - ユーザーが一時トークンコードまたは固定パスコードを使用する
  - 管理者がユーザーの PIN をクリアする
  - 管理者がユーザーの PIN を変更する
  - 管理者がトークンの紛失処理をした後、ユーザーがそのトークンを使用してログオンを試行する

  システムが SecurID ユーザーにユーザー確認を求める理由を理解できるように、これらの追加のリスク要因について SecurID ユーザーを教育します。

リスク ベース認証のリスクエンジンに関する検討事項

RBA（リスク ベース認証）のリスクエンジンは、クライアント デバイスおよびユーザーの行動パターンに基づいて、各ユーザーのプロファイルを作成します。RBA を導入する前に、RBA リスクエンジンに関する以下の要素を検討します。

- RBA リスクエンジンには、ユーザーとそのデバイス、および一般的な構成ユーザーの行動パターンに関するプロファイルを構築するため、必要なデータを取得する学習期間が必要です。この学習期間中、プロファイルを構築してベースラインの保証レベルを確立するまでは、ユーザーは頻繁にユーザー確認を求められる可能性があります。ユーザーの利便性のため、サイレント収集オプションを構成し、ベースラインの保証レベルを確立するまでの間はユーザーにユーザー確認を求めないようにすることができます。319 ページのサイレント収集を参照してください。
- RBA リスクエンジンは、統計的確率に基づいたソフト マッチング技術を採用しています。デバイスの一致を判断するだけの十分なデータがない場合、リスクエンジンはフォレンジック分析ツールを使用して一致率を評価し、保証レベルを調整します。
- RBA リスクエンジンは自動調整機能を備えており、導入環境に応じて、ほとんどの認証に共通しているパラメータ値を無視する方法を学習します。自動調整によりセキュリティが向上し、全体的なユーザー確認の頻度が下がります。

最低保証レベル

最低保証レベルは、それぞれの認証試行が満たす必要のある信頼性の閾値です。これに満たない場合、ユーザーは本人確認を求められます。この設定は、各ユーザーのセキュリティ ドメイン別に RBA（リスク ベース認証）ポリシーで設定します。

ユーザーの認証試行が行われるとき、その都度リスクエンジンによってデバイスの一致とユーザーの行動パターンがリアルタイムに評価され、保証レベルが割り当てられます。リスクエンジンはユーザーの保証レベルを、RBA ポリシー内の最低保証レベルと比較します。ユーザーのレベルが最低レベルに満たない場合、そのユーザーにはプロンプトが表示され、本人確認が求められます。

認証試行の保証レベルが高いと見なされるには、ほとんどまたはすべてのデバイス特性が以前の認証試行時に記録されたものと一致する必要があります。デバイス特性としては、IP アドレス、ブラウザのタイプとバージョン、デバイスを特定する HTTP および Flash クッキーがありますが、これらに限定されません。

デバイスがユーザーのデバイス履歴に含まれていない場合（加えて、サイレント収集の期間が終了しているか、無効化されている場合）、認証試行の保証レベルは低いと見なされ、ユーザーは RBA で保護されたリソースにアクセスするために本人確認を行う必要があります。ユーザーの保証レベルが閾値を下回っており、ユーザーが本人確認の方法を構成していない場合、ユーザーは保護されたリソースにアクセスできません。

最低保証レベルを決定するための推奨事項

RBA（リスク ベース認証）を導入する前に、最低保証レベルに関する次の要素を考慮してください。

- リスク レベルの算出には、多くの要素が考慮されます。結果は使用するネットワーク、ユーザー、個別の状況によって異なります。
- 導入環境に最適な最低保証レベルは、以下によって異なります。
  - 保護するリソースの機密性
  - ユーザーの本人確認が発生する割合が許容可能なレベルか
- 認証の強度を主眼とする場合、より高い保証レベルから開始し、ユーザー確認が頻繁に行われるようであればより低いレベルに調整します。
- 使いやすさを主眼とする場合、より低い保証レベルから開始し、セキュリティを強化する必要があればより高いレベルに調整します。
- RSA では、Medium-High（高）保証レベルから開始することを推奨します。

デバイスが既知でユーザーの行動が予想可能な場合は保証レベルが高くなるため、一部のユーザーは、より高い最低保証レベルを設定しても適応できます。たとえば、同じデバイスと場所から定期的に認証する従業員は、頻繁に出張する従業員よりも常に高い保証レベルを割り当てられます。最低保証レベルはユーザー構成の多数派に合わせて調整してください。

リスク ベース認証に対するユーザーの行動パターンの影響

ユーザーの行動パターンは、ユーザーが本人確認を求められる頻度に影響を与えます。システムは、ユーザーが導入環境の既知のユーザーであるという信頼度を示す行動パターン リスク レベルを計算し、ユーザーに割り当てます。行動パターン リスク レベルは、ユーザーの通常の行動パターンに基づきます。ユーザーが間違ったパスワードを使用して連続で複数回認証を行おうとするなど、通常と異なる行動をすると、行動パターンリスクレベルが上がり、認証試行の評価リスクが高くなります。

また、システムは、デバイスが導入環境の既知のデバイスであるという信頼度を示すデバイス保証レベルを計算し、クライアント デバイスに割り当てます。デバイス保証レベルは、固有のデバイス マッチング 技術に基づきます。

低リスクの行動パターンには、ほとんどの状況で完全に正当な一般的行動であるものの、不正行為と関連する恐れのある行動が含まれます。次に例を挙げます。

- ユーザーのアカウントが最近変更された。
- ユーザーが以前使用したことのない IP アドレスから認証しようとしている。

中リスクの行動パターンには、複数の行動の組み合わせにより疑わしいと判断される行動パターンが含まれます。次に例を挙げます。

- ユーザー確認に失敗した直後、未知の IP アドレスからユーザー認証を試みる。
- Self-Service Console からユーザー プロファイルを変更した後、未知の IP アドレスからユーザー認証を試みる。

最高リスクの行動パターンには、明確に不正行為とみなされる行動が含まれます。たとえば、無効または改ざんされた Cookie を持つマシンから認証を試みることは、リスクの高い行動です。

次の表に、ユーザーの行動パターンリスクレベルとデバイス保証レベルが最終的な保証レベルに与える影響を示します。

デバイス マッチング 技術	デバイス 保証レベル	行動パターン リスク レベル			
		Low（低）	Medium（中）	Medium-High（高）	High（最高）
2 つ以上の固有属性および統計データが一致	High（最高）	High（最高）	High（最高）	Medium-High（高）	Very Low（最低）
1 つ以上の固有属性および統計データが一致	Medium-High（高）	Medium-High（高）	Medium（中）	Low（低）	Very Low（最低）
1 つの固有属性が一致	Medium（中）	Medium（中）	Medium（中）	Low（低）	Very Low（最低）
統計データが一致	Low（低）	Very Low（最低）	Very Low（最低）	Very Low（最低）	Very Low（最低）
未登録デバイス	Very Low（最低）	Very Low（最低）	Very Low（最低）	Very Low（最低）	Very Low（最低）

サイレント収集

サイレント収集は、新規ユーザーのプロファイルと行動パターンデータを収集するプロセスを、ユーザーや管理者の介入なしに実施することができるオプション機能です。

サイレント収集を有効化すると、リスクエンジンは、定義された期間、リスク判定に基づいた本人確認要求をすることなく、ユーザーの行動パターンの監視を行います。この期間中、リスクエンジンは自動的にユーザー デバイスを登録し、行動パターンを観察します。リスクエンジンが十分な情報を収集して特定ユーザーについて高い保証レベルを確保できるようになったら、そのユーザーには、必要な情報を入力するようプロンプトが表示されます。たとえば、ユーザーはセキュリティ クエスチョンや On-Demand 認証を構成することが必要になる場合があります。

管理者は、同じセキュリティ ドメインに属するすべてのユーザーのサイレント収集の期間を RBA（リスク ベース認証）ポリシーで有効化できます。サイレント収集は、リスクエンジンによる各ユーザーのベースライン プロファイルの構成を支援します。

サイレント収集は、導入環境に次のような影響を与えます。

- サイレント収集の実行中、認証には、エージェントが要求する認証方式のみが使用されます。ユーザーに本人確認が求められることはありません。
- すべてのデバイスがユーザーの RBA プロファイルに登録されます。このとき、キオスク端末など、不要なデバイスの情報が含まれる可能性があります。

構成手順については、RSA Security Console ヘルプのトピック「リスクベース認証ポリシーのサイレント収集の構成」を参照してください。

リスク ベース認証の実装

RBA（リスク ベース認証）を実装するには、次のタスクを完了します。

開始する前に

Authentication Manager が使用不可の場合、またはユーザー認証が成功しない場合、ユーザーが引き続きネットワーク リソースにアクセスできるようにバックアップ認証方式を選択します。320 ページのリスク ベース認証のバックアップ認証方式を参照してください。

処理手順

1. DNS（ドメイン名システム）で、Authentication Manager のエントリーを更新します。操作手順については、47 ページの DNS（ドメイン ネーム システム）の更新計画を参照してください。
2. 導入環境に適した RBA ポリシーを指定します。操作手順については、108 ページのリスク ベース認証ポリシーの追加を参照してください。

3. RBA の高可用性を確保します。320 ページのリスク ベース認証のバックアップ認証方式を参照してください。
4. RSA Authentication Agent ソフトウェアまたはサード パーティ製品を入手します。321 ページの RSA Authentication Agent の取得を参照してください。
5. RSA Authentication Agent ソフトウェアまたはサード パーティ製品を導入します。70 ページの認証エージェントの導入を参照してください。
6. 322 ページの RBA 統合スクリプト テンプレートのインストールを実行します。
7. 322 ページのリスク ベース認証用の認証エージェントの構成を実行します。
8. エージェントを取得したときにダウンロードした導入ガイドを使用して、Authentication Manager との間で認証リクエストを処理するようエージェントを構成します。
9. RBA の統合をテストします。324 ページのリスク ベース認証の統合のテストを参照してください。

リスク ベース認証のバックアップ認証方式

RSA は、Authentication Manager のレプリケーション導入環境をセットアップすることを推奨します。レプリカ インスタンスにより、RBA（リスク ベース認証）の高可用性が確保されます。レプリカ インスタンスを使用しない場合は、バックアップ認証方式を使用するよう、Web ベース アプリケーションを構成します。Authentication Manager が使用不可になった場合、またはユーザー認証が成功しない場合、バックアップ認証方式により、ユーザーは引き続きネットワーク リソースにアクセスできます。

Web ベース アプリケーションに RBA を構成する場合、Authentication Manager はディレクトリ サーバおよび内部データベースを使用してユーザーを認証します。有効なバックアップ認証方式として、ディレクトリ サーバを使用して直接ユーザーを認証できるように Web ベース アプリケーションの認証構成を復元する計画を立てます。

使用するバックアップ認証方式は、それぞれの導入環境の Web ベースアプリケーションおよびユーザー認証フローに関与するその他の製品によって決まります。次の方式を検討します。

- Web ベース アプリケーションの元のログオン ページを使用する。
  ユーザーを元のログオン ページにリダイレクトするか、変更したログオン ページを元のログオンページで置き換えます。
- Web ベース アプリケーションを使用して、RBA を使用するユーザ集団に固有のバックアップ認証方式を作成する。
  RBA を使用するユーザーのグループ、ドメインのみ、認証ワークフローを変更します。

- Web ベース アプリケーションを使用して、RBA で保護しているネットワーク リソースに固有のバックアップ認証方式を作成する。

  RBA で保護しているネットワーク リソースのプロファイルまたはポリシーを変更します。

詳細については、お使いのエージェントのドキュメントを参照してください。

RSA Authentication Agent の取得

必要となるエージェントは、保護するリソースのタイプによって異なります。たとえば、Apache Web サーバを保護するには、RSA Authentication Agent for Apache をダウンロードする必要があります。

ダウンロード パッケージには、「Installation and Administration Guide」と「Readme」も含まれています。エージェントをインストールする前に、これらのドキュメントを一読してください。エージェント ソフトウェアのインストール手順については、お使いのエージェントのマニュアルを参照してください。

RSA Authentication Agent ソフトウェアが組み込まれた製品を購入することも可能です。たとえば、リモート アクセス サーバ、ファイアウォールなどの製品があります。

手順

次のいずれかの操作を実行します。

- RSA エージェントおよび RSA エージェントが必要なサード パーティ エージェントの場合は、**http://japan.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings** にアクセスします。

  お使いのプラットフォーム用のエージェント ソフトウェアを探し、エージェント ソフトウェアと RBA Integration Script（RBA 統合スクリプト）テンプレートをダウンロードします。
- RSA エージェントが組み込まれているサード パーティ エージェントの場合は、RSA Secured の Web サイト（**https://gallery.emc.com/community/marketplace/rsa?view=overview**）にアクセスし、お使いのエージェントに対応した Authentication Manager 用の導入ガイドのリストを探します。

  お使いのエージェントに対応した Authentication Manager 用の導入ガイドをダウンロードします。導入プロセスの間にアクセスできる、デスクトップまたはローカル ドライブに保存します。

  注：導入ガイドは、認定されたパートナー ソリューションにのみ発行されます。

次のステップ

70 ページの認証エージェントの導入を参照してください。

RBA 統合スクリプト テンプレートのインストール

RSA SecurCare Online からダウンロードした RBA 統合スクリプト テンプレートが、Authentication Manager にインストールされている統合スクリプト テンプレートよりも新しい場合、新しい方のテンプレートを使用します。導入環境のバージョン番号を調べる場合にも、この手順を実行する必要があります。バージョン番号は、統合スクリプト テンプレートのヘッダに含まれています（例：<Version>1.0</Version>）。

開始する前に

SSH を使用する場合は、Authentication Manager アプライアンスで SSH 接続を有効化する。操作手順については、455 ページのアプライアンスの SSH の有効化を参照してください。

手順

1. SSH クライアントまたは SCP クライアントで、オペレーティング システム アカウントのユーザー ID「**rsaadmin**」とパスワードを使用してアプライアンスにログオンします。
2. ダウンロードした統合スクリプト テンプレートを、アプライアンスの **/opt/rsa/am/utils/rba-agents** ディレクトリにコピーします。

   Authentication Manager によって統合スクリプト テンプレートのリストが更新されるまで数分待ちます。
3. 生成された統合スクリプト（.js ファイル）のヘッダにあるバージョン番号が、ダウンロードした統合スクリプト テンプレート（.xml ファイル）のヘッダにあるバージョン番号と同じことを確認します。たとえば、生成された .js ファイルと .xml テンプレートの先頭付近で <Version>1.0</Version> を探します。
4. エージェントごとにステップ 1 ～ 3 を繰り返します。

次のステップ

322 ページのリスク ベース認証用の認証エージェントの構成

リスク ベース認証用の認証エージェントの構成

RBA（リスク ベース認証）を使用して Web ベース アプリケーションを保護するには、RBA 用の認証エージェントを構成し、Web ベース アプリケーションのデフォルトのログオン ページに導入する統合スクリプトを生成する必要があります。統合スクリプトは、Web ベース アプリケーションのデフォルトのログオン ページから、Authentication Manager が提供する RBA 用のカスタマイズされたログオン ページにユーザーをリダイレクトします。

手順

1. プライマリ インスタンスの Security Console で、[**Access（アクセス）**] > [**Authentication Agents（認証エージェント）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 適切なエージェントをクリックして、[**Edit（編集）**] をクリックします。
3. [**Risk-Based Authentication（RBA）（RBA 認証）**] セクションで [**Enable this agent for risk-based authentication（リスク ベース認証を有効化する）**] をクリックします。
4. このエージェントの唯一の認証方式として RBA を有効化するには、[**Allow access only to users who are enabled for risk-based authentication（リスク ベース認証が有効なユーザーのみにアクセスを許可する）**] を選択します。ユーザーの RBA が有効化されていない場合、エージェントはリソースへのアクセスを拒否します。
5. [**Authentication Method（認証方式）**] ドロップダウン リストから [**Password（パスワード）**] または [**SecurID**] を選択します。このフィールドにより、RBA を使用する場合にエージェントが必要とする認証方式が決定されます。
6. [**Save Agent & Go to Download Page（エージェントを保存してダウンロード ページに移動）**] をクリックします。
7. [**Agent Type（エージェントのタイプ）**] ドロップダウン リストから適切なエージェントを選択して、[**Download File（ファイルのダウンロード）**] をクリックします。

   Authentication Manager に格納されている .xml 統合スクリプト テンプレートに基づいた JavaScript 統合ファイルがシステムによって生成されます。
8. プロンプトに従って、ローカルに JavaScript ファイルを保存します。

次のステップ

- Web Tier やロードバランサなどのコンポーネントが正しくインストールされ、構成されていることを確認します。詳細については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
- ダウンロードしたエージェント用の導入ガイドを参照します。生成されたスクリプトをエージェントにアップロードし、Authentication Manager との間で認証要求の受け渡しを行うようにエージェントを構成します。
- RBA の統合の状態をテストします。

リスク ベース認証の統合のテスト

Authentication Manager がエージェントでユーザーを認証できることを確認するため、RBA（リスク ベース認証）の統合をテストします。テストが成功しない場合、構成をトラブルシューティングして、成功するまでテストを繰り返します。

テストが成功しない場合、Authentication Activity Monitor のログを確認してトラブルシューティングします。

処理手順

1. Security Console を使用して、内部データベース上に、テストユーザとして、デフォルトのセキュリティ ドメイン（SystemDomain）に属する新しいユーザーを追加します。
   操作手順については、141 ページの内部データベースへのユーザーの追加を参照してください。
2. デフォルトのセキュリティ ドメイン（SystemDomain）に関連づけられた RBA ポリシーに次の構成があるかどうかを確認し、必要に応じてポリシーを編集します。
   - 自動有効化が許可されている。
   - サイレント収集が許可されている。

   RBA ポリシーを編集する手順については、Security Console ヘルプのトピック「Edit a Risk-Based Authentication Policy（リスクベース認証ポリシーの編集）」を参照してください。
3. Security Console で Authentication Activity Monitor を開始します。
   ［**Start Monitor（モニタ開始）**］をクリックして、認証アクティビティをリアルタイムで表示します。
4. 以下のいずれかの操作を実行します。
   - 同じネットワーク上の別のコンピュータに移動して、ブラウザを起動し、使用する Web ベース アプリケーションのログオン ページにアクセスします。
   - 同じマシンに複数のブラウザ アプリケーションがインストールされている場合は、別のブラウザ アプリケーションを起動します。たとえば、Firefox で Security Console にアクセスしている場合は、Internet Explorer を使用して Web ベース アプリケーションのログオン ページにアクセスできます。

   Web ベース アプリケーションのログオン ページは、自動的に Authentication Manager のログオン ページにリダイレクトされます。このページにリダイレクトしない場合は、トラブルシューティングを行います。詳細については、325 ページの認証テストのトラブルシューティングを参照してください。

5. テスト ユーザーのログオン クレデンシャルを入力します。
6. ブラウザに、アクセス先のネットワーク リソースのランディング ページが正しくロードされていることを確認します。
7. Authentication Activity Monitor の認証ログを確認します。テストに成功したら、認証成功が記録されたエントリーをよく理解します。テストに失敗した場合は、エントリーと 325 ページの認証テストのトラブルシューティングを確認してください。

認証テストのトラブルシューティング

認証テストに失敗したら、次の表の推奨方法に従って、テスト中に観察したシステムの動作をトラブルシューティングします。

システムの動作	アクション
ブラウザに Authentication Manager のログオン ページではなく、Web ベース アプリケーションのデフォルトのログオン ページが表示される。	• RBA 統合スクリプトを適切に生成し、導入したことを確認します。詳細については、お使いの Web ベース アプリケーションの導入ガイドを参照してください。 • Web ベース アプリケーションの統合スクリプト ファイルが、ISO-8859-1（Latin-1 と呼ばれることもある）または ASCII でエンコードされていることを確認します。これ以外のファイル エンコーディング形式はサポートされていません。

システムの動作	アクション
Web ベース アプリケーションからリダイレクトされたログオン ページがロードされない。	• ブラウザで JavaScript が許可されていることを確認します。詳細については、お使いのブラウザのドキュメントを参照してください。 • ブラウザで Cookie が有効化されていることを確認します。詳細については、お使いのブラウザのドキュメントを参照してください。 • サポートされているブラウザを使用していることを確認します。サポートされているブラウザのリストについては、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。 • 以下のいずれかの操作を実行します。 – 導入環境に Web Tier がある場合、URL が仮想ホストおよび仮想ホスト ポートに解決されることを確認します。 – 導入環境に Web Tier がなく、ロードバランサがある場合、URL がロードバランサおよびロードバランサのポートに解決されることを確認します。 – 導入環境に Web Tier もロードバランサもない場合、URL がプライマリ インスタンスおよびプライマリ インスタンスのポートに解決されることを確認します。 • すべてのファイアウォールの構成で、URL で指定するホストとポートへの着信トラフィックが許可されていることを確認します。 • DNS（ドメイン名システム）サーバに RBA の適切なホスト名と IP アドレスが登録されているか確認します。47 ページの DNS（ドメイン ネーム システム）の更新計画を参照してください。 • NAT（ネットワーク アドレス変換）またはロードバランサが、Authentication Manager ホスト（Web Tier または Authentication Manager インスタンスのいずれか）にルーティングしなければならないリクエストに干渉していないか、導入シナリオに応じて確認します。 こうしたアクションによってブラウザがリダイレクト ループに入る問題を解決できます。 • Web Tier がプライマリ インスタンスおよびレプリカ インスタンスと通信できることを確認します。また、導入環境にロードバランサが含まれる場合は、ロードバランサが Web Tier と通信できることを確認します。 これらの方法では問題を解決できない場合、RSA では、次の操作を推奨しています。 統合スクリプトを生成して、Web ベース アプリケーションのログオン ページに再配置します。詳細については、お使いの Web ベース アプリケーションの導入ガイドを参照してください。

システムの動作	アクション
Web ベース アプリケーションによってリダイレクトされたページにエラー メッセージ「Agent Integration Error（エージェントの統合エラー）」が表示されます。	• Authentication Manager でエージェント レコードを作成したことを確認します。詳細については、72 ページの認証エージェントの追加を参照してください。 • 統合スクリプトを生成して、Web ベース アプリケーションのログオン ページに再配置します。詳細については、お使いの Web ベース アプリケーションの導入ガイドを参照してください。 • 導入環境にロードバランサが含まれる場合、そのロードバランサにセッション維持機能が構成されていることを確認します。セッション維持機能（「セッション親和性」または「持続性セッション」とも呼ばれる）は、セッション中にロードバランサがクライアントのリクエストを同じサーバに送信する機能です。Authentication Manager の場合、ロードバランサは認証セッションの間、クライアントのリクエストを同じ Authentication Manager インスタンスまたは Web Tier に送信する必要があります。詳細については、お使いのロードバランサのドキュメントを参照してください。 • より詳細なエラー メッセージは **rsa-console.log** にあります。操作手順については、Operations Console ヘルプのトピック「Download Troubleshooting Files（トラブルシューティング ファイルのダウンロード）」を参照してください。
テスト ユーザーとしてログオンした後ページ エラーが発生する。	サポートされる RBA 導入シナリオに沿って導入したことを確認します。サポートされる導入シナリオについては、「RSA Authentication Manager 8.0 設計ガイド」を参照してください。

システムの動作	アクション
テスト ユーザーのログオン クレデンシャルを入力した後、再度ログオンを求められる。	次の操作を実行します。 • Authentication Manager のアカウント設定でテスト ユーザーのログオンが許可されていることを確認します。ユーザーが存在し、デフォルトのセキュリティ ドメイン（SystemDomain）に属している必要があり、アカウントが有効化されている必要があります。アカウントの有効期限は終了しておらず、ユーザーがロックアウトされていないことを確認します。詳細については、145 ページのユーザー アカウントの有効化を参照してください。 • デフォルトのセキュリティ ドメイン（SystemDomain）の RBA ポリシーによって、自動有効化とサイレント収集が許可されていることを確認します。詳細については、107 ページのリスク ベース認証ポリシーを参照してください。 • 自動有効化が許可されていない場合、ユーザーの RBA を有効化します。 • Authentication Activity Monitor に必要なログ エントリーがすべて表示されていることを確認します。必要なエントリー タイプは、authentication method success with password and SecurID、authentication method success with RBA、artifact generation success、artifact delivery success です。 これで問題が解決されない場合、Authentication Manager とお使いの Web ベース アプリケーションのノード シークレットをクリアしてください。Authentication Manager のノード シークレットをクリアする詳細については、76 ページのノード シークレットの管理を参照してください。Web ベース アプリケーションのノード シークレットをクリアする詳細については、お使いの Web ベース アプリケーションのドキュメントを参照してください。

ユーザーのリスク ベース認証の有効化

次の方法のいずれかを使用して、ユーザーの RBA（リスク ベース認証）を有効化します。

自動。ユーザーが RBA で保護されたリソースにアクセスすると、最初に認証に成功した後、RBA は自動的に有効になります。手順については、Security Console ヘルプのトピック「Enable Users Automatically for Risk-Based Authentication（ユーザーのリスクベース認証を自動的に有効化する）」を参照してください。

手動。指定したユーザーのみが RBA で保護されたリソースにアクセスできます。管理者は、これらのユーザーに対する RBA の有効化を手動で設定する必要があります。手順については、Security Console ヘルプのトピック「Enable Users Manually for Risk-Based Authentication（ユーザーのリスクベース認証を手動で有効化する）」を参照してください。

リスク ベース認証ポリシーのユーザー確認方法の有効化

導入環境で RBA（リスク ベース認証）を使用する場合は、少なくとも 1 つのユーザー確認方法を有効化する必要があります。RBA は、クライアント デバイスとユーザーの行動パターンに関する情報の蓄積を利用して、認証要求の潜在的なリスクを評価することで、従来のパスワード ベースのシステムを強化する多要素認証ソリューションです。評価リスクが高い場合、ユーザーは次のいずれかの方法によってユーザー本人であることを証明することを要求されます。

- **ODA（On-Demand 認証）**。ユーザーは、PIN と事前構成された携帯電話番号またはメール アカウントに送信されたワン タイム トークン コードを正確に入力する必要があります。
- **セキュリティ クエスチョン**。ユーザーは、事前に登録した 1 つ以上のセキュリティ クエスチョンに正しく回答する必要があります。

セキュリティ クエスチョンと ODA の両方を有効化すると、構成する方法の数はユーザーが選択できます。ユーザーが両方の方法を構成した場合、ユーザー確認時にどちらの方法を使用するかを選択できます。

ユーザーによるユーザー確認方法の構成方法

ユーザー確認方法を構成するには、ユーザーは、次のいずれかを実行する必要があります。

- サイレント収集期間中にインラインで構成プロセスを完了します。
  サイレント収集期間中に、ユーザーの保証レベルが必要な保証レベルを満たしている場合、そのユーザーはユーザー確認方法を構成するよう求められます。
- 管理者の指示により、Self-Service Console を使用した構成プロセスを完了します。
  管理者が構成手順と Self-Service Console へのリンクをユーザーに送信し、ユーザーが Self-Service Console にログオンして、ユーザー確認方法を構成します。

リスク ベース認証のデバイス設定

RBA（リスク ベース認証）の場合、システムはリスクを判断する際の要素としてデバイス履歴を使用します。デバイス履歴とは、それまでのログオン成功時にユーザーが使用したデバイスのリストです。システムが各ユーザーのデバイス履歴を保存しています。リストに追加されると、デバイスは登録済みとみなされます。ユーザーが登録済みのデバイスを使用して RBA で保護されたリソースにアクセスしようとする場合、認証試行はより高い保証レベルを持つと考えられます。ユーザーが不明なデバイスでログオンしようとする場合、ユーザーはシステムによりユーザー確認を求められます。ログオンに成功した場合、新しいデバイスがユーザーのデバイス履歴のリストに追加されます。

システムが RBA のユーザーのデバイスを登録および管理する方法を指定します。次のクライアント デバイス設定を構成できます。

設定	説明
新規デバイス登録	Authentication Manager は、新しいデバイスを自動的に登録できます。または、ユーザーにデバイスを登録するか否か確認することができます。ユーザーがパブリックのデバイスまたは共有デバイスから RBA で保護されたリソースにアクセスすることが予想される場合は、登録するデバイスの選択をユーザーに許可します。
登録デバイスの合計数	各ユーザーのデバイス履歴に保存する登録デバイスの最大数を設定できます。登録デバイスの数が制限を超えると、夜間のクリーンアップ ジョブにより最も長く使用されていないデバイスから順に削除されます。
デバイスの登録解除	ユーザーのデバイス履歴から非アクティブなデバイスを削除するタイミングを指定できます。この指定によって、たとえば 60 日間使用されていないデバイスを履歴から削除することができます。全ユーザーのニーズを考慮します。ほとんどのユーザーは同じクライアント デバイスを頻繁に使用して RBA で保護されたリソースにアクセスしますが、まれにパブリックのクライアント デバイスのみを使用するユーザーもいます。

リスク ベース認証ポリシーのデバイス登録の構成

デバイス登録とは、ユーザーのデバイス履歴リストにユーザーの認証デバイスを保存する処理のことです。リスト内の各デバイスは、以前に成功したログオン時に使用されたものです。ユーザーが登録済みデバイスを使用して RBA で保護されたリソースにアクセスしようとすると、認証試行の保証レベルが高くなる可能性が大きくなります。

システムは、新しいデバイスを自動的に登録できます。また、ユーザーがデバイスの登録を選択することもできます。ユーザーが公共のデバイスまたは共有デバイスから RBA 保護リソースにアクセスすることが予想される場合は、登録するデバイスの選択をユーザーに許可できます。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Risk-Based Authentication Policies（リスク ベース認証ポリシー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 構成するポリシーをクリックして、［**Edit（編集）**］を選択します。
3. ［**Device Registration and Identity Confirmation Settings（デバイス登録およびユーザー確認の設定）**］セクションの［**New Device Registration（新規デバイス登録）**］で次のいずれかを選択します。
   - 認証後にユーザーのデバイス履歴にデバイスを自動的に追加するには、［**Register the user authentication device automatically after successful authentication（認証成功後、ユーザーが使用したデバイスを自動的に登録する）**］を選択します。
   - デバイスをデバイス履歴に追加するかどうか選択するようユーザーにプロンプトを表示するには、［**Prompt the user to choose whether the system registers the device after successful authentication（認証成功後、デバイスを登録するか否かをユーザーが選択する）**］を選択します。
4. ［**Save（保存）**］をクリックします。

リスク ベース認証ポリシーのデバイス履歴の設定の構成

RBA（リスク ベース認証）の場合、システムが各ユーザーのデバイス履歴を保持します。デバイス履歴とは、以前に成功したログオンの時にユーザーが使用した認証デバイスのリストです。リストに追加されたデバイスは、登録済みデバイスと見なされます。ユーザーが登録済みデバイスを使用して RBA で保護されたリソースにアクセスしようとすると、認証試行の保証レベルが高くなる可能性が大きくなります。

各ユーザーのデバイス履歴に保持される登録済みデバイスの最大数を設定できます。登録済みデバイスの数が制限を超えた場合、毎晩実行されるクリーンアップ ジョブによって、最も長く使用されていないデバイスが削除されます。

また、ユーザーのデバイス履歴から非アクティブなデバイスが削除されるタイミングを指定することもできます。この指定によって、たとえば 30 日間非アクティブなデバイスを履歴から削除することができます。

手順

1. Security Console で、［**Authentication（認証）**］＞［**Policies（ポリシー）**］＞［**Risk-Based Authentication Policies（リスク ベース認証ポリシー）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. 構成するポリシーをクリックして、［**Edit（編集）**］を選択します。
3. ［**Device Administration Settings（デバイス管理の設定）**］で、次のフィールドに数値を入力します。
   - ［**Total Registered Devices（登録デバイスの合計数）**］フィールドに、各ユーザーのデバイス履歴に保持される登録済みデバイスの最大数を入力します。
   - ［**Unregister Devices（デバイスの登録解除）**］フィールドに、システムが非アクティブ状態のデバイスをユーザーのデバイス履歴から削除する場合に、連続何日間使用しなかったら削除するか日数を入力します。
4. ［**Save（保存）**］をクリックします。

リスク ベース認証を使用する Web ベース アプリケーション向けのカスタム ソリューション

RSA SecurID Ready の認定を受けているが、RSA Authentication Manager の RBA（リスク ベース認証）のサポート対象になっていない Web ベース アプリケーションについては、独自のカスタム ソリューションを作成できます。カスタム ソリューションを作成するには、RSA が提供する XML テンプレートを使用して独自の RBA 統合スクリプトを作成する必要があります。RSA SecurID Ready 製品の完全なリストについては、**https://gallery.emc.com/community/marketplace/rsa?view=overview** にアクセスしてください。

RSA SecurID Ready アプリケーション用の RBA 統合スクリプトを作成する手順については、「RSA Authentication Manager Custom Implementation Guide」を参照してください。ISO イメージは、RSA SecurCare Online（**https://knowledge.rsasecurity.com**）からダウンロードできます（このサイトへのアクセスには RSA SecurCare Online のログオン アカウントが必要です）。

13 RSA RADIUS の管理

RSA RADIUS の概要

RSA RADIUS と RSA Authentication Manager を共に使用すると、RADIUS 対応デバイスを通じてネットワーク リソースにアクセスしようとするユーザーを直接認証できます。RADIUS サーバは、VPN などの RADIUS クライアントからユーザー アクセス リクエストを受信します。RADIUS サーバが受信したアクセス リクエストは RSA Authentication Manager に転送され、検証されます。Authentication Manager が許可または拒否メッセージを RADIUS サーバに送信し、RADIUS サーバがそのメッセージをリクエスト送信元の RADIUS クライアントに転送します。

RADIUS は、Authentication Manager のインストール中に自動的にインストールされて構成されます。インストール後、RADIUS は Authentication Manager と同じインスタンス上で稼働するように構成されます。

RSA RADIUS の構成と、RSA RADIUS が稼働する個々のインスタンスに必要な設定の管理は、Operations Console を使用して行います。

RADIUS の日常的な運用管理に関連するほとんどのタスクは、Security Console から実行できます。

RSA RADIUS 認証プロセス

RADIUS で保護されるネットワークでは、認証プロセスは次のようになります。

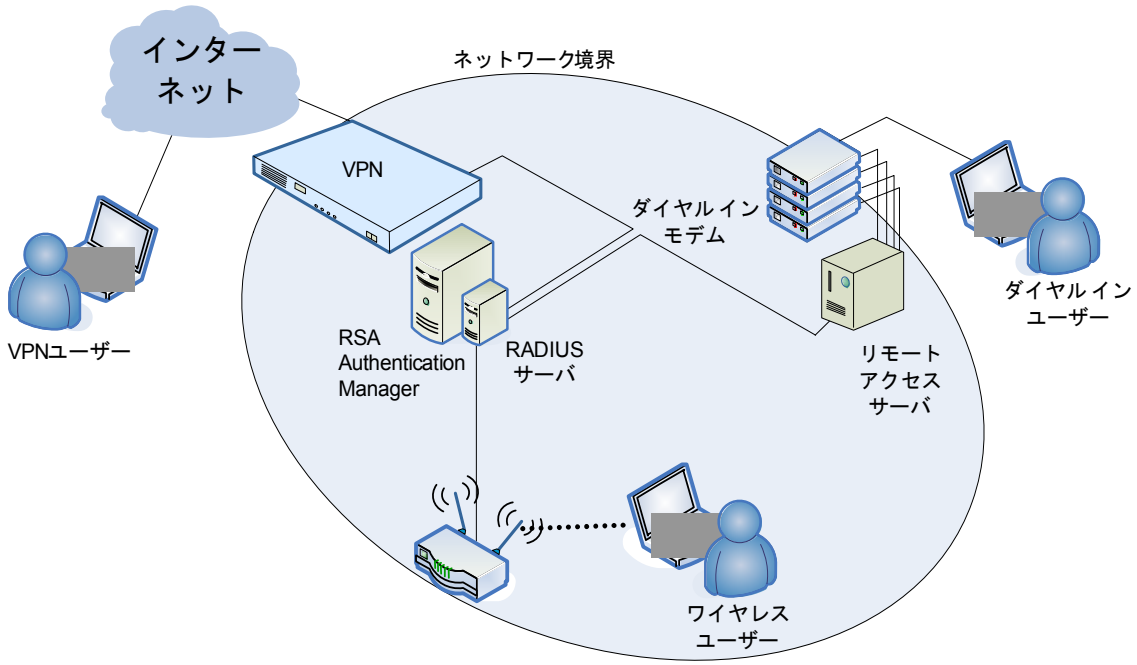
1. ユーザーは認証情報を RADIUS クライアントに提示します。
2. RADIUS クライアントは「Access-Request」を RADIUS サーバに送信します。このリクエストには、次の情報が含まれます。
   - ユーザー ID
   - ユーザー パスワード（暗号化済み）
   - クライアント ID
   - ポート ID
3. RSA RADIUS は、共有シークレットを使用してクライアントを検証します。シークレットが存在しない場合、リクエストは無視されます。
4. RSA RADIUS は、ユーザーがリソースにアクセスするために満たさなければならない要件をチェックします。これらの要件は RADIUS 属性と呼ばれ、次のものが含まれます。

- パスワード
- ユーザーがリソースへのアクセスに使用できるクライアント
- ユーザーがアクセスできるポート

5. RSA RADIUS はリクエストを Authentication Manager に転送します。
6. Authentication Manager はリクエストを許可または拒否します。
7. RSA RADIUS は、次の 3 つのうちのいずれかの応答を送信します。
   - Access-Accept。RSA RADIUS はアクセスを許可し、RADIUS 属性のセットをクライアントに返します。
   - Access-Challenge。RSA RADIUS は、チャレンジを送信し、ユーザーはそれに対してパスコードなどを返信する必要があります。
   - Access-Reject。条件が満たされなかったため、アクセスは拒否されます。

RADIUS クライアントはネットワーク境界でユーザー アクセスを制御します。RADIUS クライアント（VPN サーバ、ワイヤレス アクセス ポイント、ダイヤル イン モデムに接続されたネットワーク アクセス サーバ）が RSA RADIUS と通信することにより、ユーザー認証が実行され、適切なアクセス制御パラメータが確立されます。認証が成功すると、RSA RADIUS はセッション制御用の属性のセットを RADIUS クライアントに返します。

次の図は、RSA RADIUS サーバが Authentication Manager インスタンス上のサービスとして実行されることを示しています。RADIUS サービスは、クライアントからのリクエストを処理し、Authentication Manager と通信します。Authentication Manager は認証を処理し、ユーザーのアクセスを許可または拒否します。



RADIUS のネットワーク トポロジー

通常 VPN サーバは、ファイアウォールによって RADIUS サーバおよびインターネットから分離されます。ほとんどの場合、ロード バランシングおよびフェイルオーバーのために、RADIUS プライマリ サーバに加えて複数の RADIUS レプリカ サーバを構成します。サイト全体にわたって戦略的に有効な場所に複数のワイヤレス アクセス ポイントを配置するなど、追加の RADIUS クライアントを構成することもあります。管理者がこのような詳細をあまり意識する必要はありません。日常的な管理操作のほとんどはプライマリ サーバで実行され、管理操作による変更の一部はプライマリ サーバからレプリカ サーバにレプリケーションされるからです。

実行頻度の低い一部の管理操作では、フェイルオーバー、災害復旧、その他のシステム保守のために、管理者にレプリカ サーバに関する知識が必要になります。

インターネットに直接接続しているリモート ユーザーは、RADIUS 対応の VPN サーバを使用してネットワーク リソースにアクセスできます。インターネットに直接接続していないリモート ユーザーは、RADIUS 対応のネットワーク アクセス サーバに接続されているダイヤル イン モデムと電話回線を使用して接続できます。ワイヤレス ユーザーは、RADIUS 対応のワイヤレス アクセス ポイントを通じてネットワークにアクセスできます。

RADIUS では、これらのアクセス方式のいずれについても、次の機能を提供します。

- 詳細なアクセス制御：管理者は、ユーザーが使用できるネットワーク アクセス デバイス、ユーザーのセッションの長さ、ユーザーが使用できる IP アドレスまたは範囲などを制限することによって個々のユーザーのアクセスを厳密に管理できます。
- 包括的かつ柔軟なアカウンティング：Sarbanes-Oxley（米国企業改革法）やその他の監査要件に対応するため、管理者が実際のニーズに応じてイベント ログ データをカスタマイズできます。ログ データはフラット ファイルに保存できます。

RADIUS サーバとクライアント間の通信

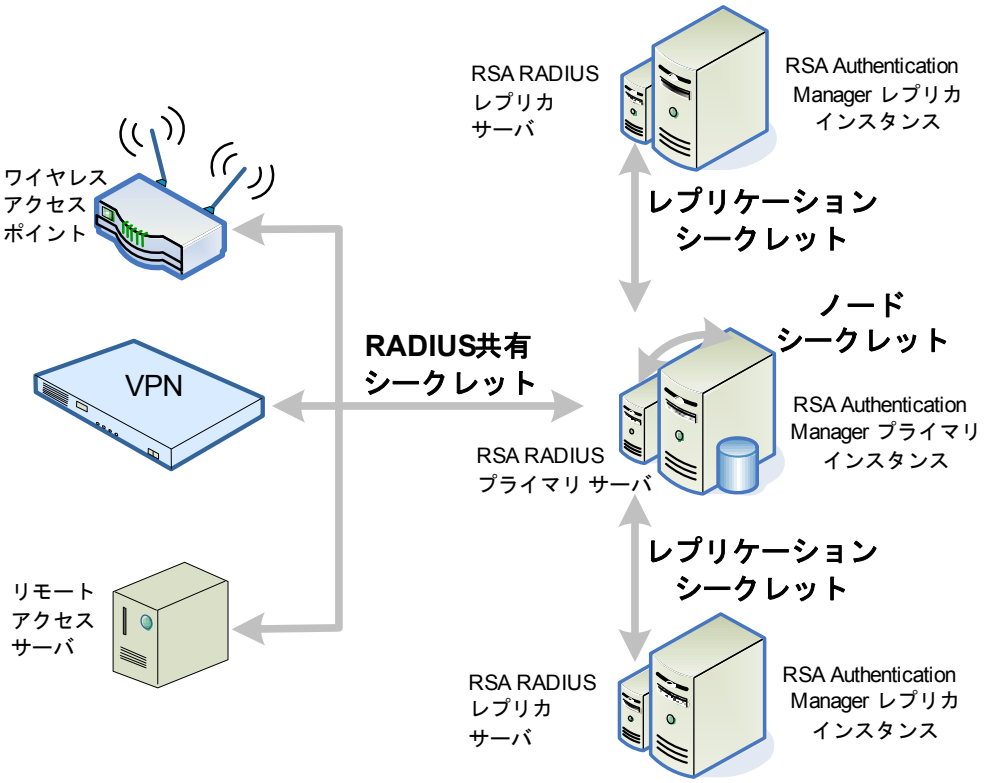
RADIUS サーバと Authentication Manager の間の通信では、HTTPS が常に使用されます。RADIUS サーバとクライアントの間の通信では、RADIUS プロトコルが常に使用されます。Authentication Manager は、RADIUS プロトコルで使用可能なセキュリティ機能を使用します。たとえば、機密情報を扱うフィールドに対しては、共有シークレットを使用して暗号化します。

共有シークレットは、ホスト間のパスワードとして機能するテキスト文字列です。RADIUS サーバで使用される共有シークレットには、次のタイプがあります。

- **RADIUS 共有シークレット：**RADIUS サーバと RADIUS クライアントの間の通信をセキュリティ保護するために使用されます。
- **アカウンティング シークレット：**（次の図には示されていません）RADIUS プライマリ サーバと RADIUS クライアントの間のアカウンティング トラフィックのセキュリティ保護に使用されます。RADIUS サーバは RADIUS クライアントのアカウンティング シークレットを使用します。クライアントにアカウンティング シークレットが存在しない場合、RADIUS サーバはクライアントの RADIUS 共有シークレットを使用します。
- **レプリケーション シークレット：**RADIUS プライマリ サーバと RADIUS レプリカ サーバの間の通信をセキュリティ保護するために使用されます。このシークレットは Authentication Manager のインストール時に生成されます。このシークレットを管理することはできません。

- **ノード シークレット：**RADIUS サーバと Authentication Manager サーバの間の通信をセキュリティ保護するために使用されます。RADIUS プライマリ サーバとすべてのレプリカ サーバがノード シークレットを使用します。このシークレットは Authentication Manager のインストール時に生成されます。このシークレットを管理することはできません。

RADIUS 共有シークレットとアカウンティング共有シークレットは、Security Console を通じて構成できます。RADIUS 共有シークレットを作成した後で、RADIUS クライアントの管理インタフェースを使用して RADIUS クライアントにこの共有シークレットを設定する必要があります。



RSA RADIUS サーバの管理

このトピックでは、RSA RADIUS サーバをライフサイクル全体にわたって管理する方法について説明します。次のトピックが含まれます。

- RSA RADIUS 管理用の管理コンソール
- RADIUS サーバの表示
- RADIUS データ レプリケーション
- システム生成 PIN を使用するための RSA RADIUS の構成
- RADIUS サーバの再起動
- RSA RADIUS サーバの保守

RSA RADIUS 管理用の管理コンソール

RSA RADIUS の管理には Security Console と Operations Console を使用します。

Security Console は、次の日常的な RADIUS 管理タスクを実行するために使用します。

- 導入環境内の RADIUS サーバのリスト、各 RADIUS サーバの IP アドレスとレプリケーション ステータスを表示します。
- RADIUS クライアントと RADIUS クライアント エージェントを管理します。
- RADIUS プロファイルを管理します。これには、ユーザー、ユーザー グループ、エージェントへのプロファイルの割り当て、デフォルト プロファイルの指定が含まれます。
- RADIUS ユーザー属性とカスタム属性を管理します。
- RADIUS サーバと RADIUS クライアントの統計情報を表示します。
- レプリカ RADIUS サーバへのレプリケーションを手動で開始します。
- レプリカ RADIUS サーバへの定期的なレプリケーションを構成します。

RADIUS サーバの非日常的な保守を行うには、Operations Console を使用します。Operations Console で次のタスクを実行します。

- 導入環境内の RADIUS サーバのリスト、各 RADIUS サーバの IP アドレスとレプリケーション ステータスを表示します。
- RSA RADIUS が使用する証明書を管理します。これには、RADIUS サーバ証明書と、EAP-TTLS（Extensible Authentication Protocol-Tunneled Transport Layer Security）認証用の信頼するルート証明書が含まれます。
- RADIUS サーバ ファイルを管理します。これには、RADIUS ディクショナリファイルと構成ファイルが含まれます。

Operations Console を使用して RADIUS サーバを変更する際は、次の制限が適用されます。

- 1 つの RADIUS サーバに対して行われた変更は、次の変更を除き、導入環境内の別のサーバにレプリケーションされません。
  - ルート証明書
  - peapauth.aut
  - ttlsauth.aut
- 変更内容を反映するためには、RADIUS サーバの再起動が必要になります。

RADIUS サーバの表示

RSA Authentication Manager では、すべての RADIUS サーバのリストを表示できます。たとえば、Authentication Manager ですべてのサーバのリストを表示して、RADIUS レプリカ サーバの数を迅速に確認することができます。

すべての RADIUS サーバと、それぞれのサーバに関する次のプロパティを表示できます。

- [**Type（タイプ）**]：プライマリまたはレプリカ。
- [**IP Address（IP アドレス）**]：RADIUS クライアントおよび他の RADIUS サーバがこのサーバとの通信に使用する IP アドレス。これは Authentication Manager と同じ IP アドレスです。
- [**Replication Status（レプリケーション ステータス）**]：RADIUS サーバの RADIUS データの状態。詳細については、341 ページの RADIUS レプリケーション ステータスを参照してください。

手順

Security Console で、[**RADIUS**] > [**RADIUS Servers（RADIUS サーバ）**] の順にクリックします。

RADIUS データ レプリケーション

RADIUS は、RADIUS プライマリ サーバのデータと RADIUS レプリカ サーバのデータを同期します。管理者が Security Console で RADIUS データを変更すると、プライマリ サーバが変更を検出し、レプリケーション可能なすべての RADIUS データをレプリカ サーバに送信します。変更がない場合、データはレプリケーションされません。

RADIUS プライマリ サーバは、RADIUS 構成ファイルや RADIUS ディクショナリファイルをレプリケーションしません。各 RADIUS サーバにはこれらのファイルの独自のセットがあります。RADIUS プライマリ サーバのファイルを変更した場合、同じ変更を導入環境内の各 RADIUS レプリカ サーバのファイルに加える必要があります。

RADIUS 構成ファイルを表示して編集するには、変更を行う RADIUS サーバの Operations Console にログオンする必要があります。構成ファイルの詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。ディクショナリファイルの詳細については、RADIUS デバイスのドキュメントを参照してください。

RADIUS データをレプリケーションするには、次の 2 つの方法のいずれかを使用します。

- 定期的なレプリケーションの構成
- レプリケーションの手動実行

デフォルトでは、定期的なレプリケーションを行うよう構成されています。

定期的なレプリケーションの構成方法

定期的なレプリケーションがデフォルトの方法です。これが有効化されていると、RADIUS プライマリ サーバは、次のステップを実行します。

1. プライマリ サーバ上の RADIUS データに加えられた変更を 15 分ごとに検索します。
2. すべての変更を各 RADIUS レプリカ サーバにレプリケーションします。
3. 各 RSA RADIUS レプリカ サーバが最新のデータを保持していることを検証します。

RSA RADIUS レプリカ サーバがレプリケーション後の更新に失敗した場合、RADIUS プライマリ サーバはシステム ログと Authentication Manager 重大システムイベント通知システム（指定したユーザーにメール送信するように構成できます）にメッセージを記録します。失敗をログに記録し、通知を送信するまでに、最大で 15 分かかります。

重要：定期的なレプリケーションを無効化した場合、失敗は通知されません。

レプリケーションの手動実行

レプリケーションの手動実行では、管理者が Security Console を使用して RADIUS レプリカ サーバへの RADIUS データのレプリケーションを開始する必要があります。この方法は、定期的なレプリケーションが有効化されているかどうか、RADIUS データが変更されたかどうかに関係なく使用できます。RADIUS レプリカ サーバが一定期間オフラインになっていたために最新の状態でない場合、RADIUS サーバが使用可能になった後でレプリケーションを手動で実行すると、最新の RADIUS データが導入環境のすべての RADIUS レプリカ サーバに送信されます。

最新の状態でない RADIUS レプリカ サーバ

RADIUS レプリカ サーバ上のデータは、RADIUS レプリカ サーバが一定期間使用不可になる（たとえば、オフラインになるか、ネットワークの問題が原因で RADIUS プライマリ サーバがレプリカに接続できない）と、最新の状態でなくなります。

使用不可のレプリカ サーバは、RADIUS プライマリ サーバからデータを受信できません。ただし、RADIUS レプリカ サーバが使用可能になると、1 時間ごとに未適用の更新をチェックし、より新しいデータを見つけた場合にはレプリケーションを開始します。

1 時間のインターバルの前に RADIUS データ が変更された場合には、RADIUS レプリカ サーバは導入環境に構成されたレプリケーション方法を通じて更新を受信できます。

RADIUS レプリケーション ステータス

RADIUS レプリケーションでは、RADIUS レプリカ サーバ上のデータを RADIUS プライマリ サーバ上のデータに同期します。プライマリ サーバは、管理者が Security Console を使用して RADIUS データを変更したことを検出し、レプリケーション可能なすべての RADIUS データをレプリカ サーバに送信します。変更が行われていない場合は、データをレプリケーションしません。

次の表に、RADIUS サーバのステータスの有効値を示します。

サーバ	ステータス	説明	アクション
プライマリ	Cannot determine status（ステータス不明）	RADIUS プライマリ サーバがダウンしている可能性があります。	RSA RADIUS サービスを実行しているプライマリ インスタンスが起動していることを確認します。 343 ページの RSA RADIUS レプリケーションの検証
	Out-of-Sync（同期ずれ）	RADIUS プライマリ サーバ上のデータが変更され、RADIUS レプリカ サーバにレプリケーションする必要があります。	定期的レプリケーションが有効化されている場合は、なし。定期的レプリケーションが有効化されていない場合は、レプリケーションを手動で実施します。
	Synchronized（同期）	導入環境に RADIUS レプリカが存在する場合、RADIUS プライマリからレプリケーションする変更はありません。 注：導入環境が RADIUS プライマリのみの場合、レプリケーションする必要のある変更が発生することはありません。	なし。

サーバ	ステータス	説明	アクション
レプリカ	Cannot determine status（ステータス不明）	RADIUS プライマリ サーバと RADIUS レプリカ サーバが通信できていません。。	RSA RADIUS サービスを実行しているプライマリ インスタンスが起動していることを確認します。 RSA RADIUS サービスを実行しているレプリカ インスタンスが起動しており、プライマリ インスタンスに接続できることを確認します。 詳細については、343 ページの RSA RADIUS レプリケーションの検証を参照してください。
	Initiating Data Transfer（データ転送を開始中）	RADIUS プライマリがレプリカへのデータのレプリケーションを開始しようとしています。	なし。
	Out-of-Sync（同期ずれ）	RADIUS プライマリサーバ上のデータの変更をレプリカ サーバにレプリケーションする必要があります。	定期的レプリケーションが有効化されている場合は、なし。定期的レプリケーションが有効化されていない場合は、レプリケーションを手動で実施します。
	Synchronized（同期）	RADIUS プライマリ サーバとレプリカ サーバ上のデータが同じです。レプリカの RADIUS データは最新のものです。	なし。
	Unreachable（到達不能）	RADIUS プライマリ サーバがレプリカ サーバに接続できません。	プライマリ インスタンスとレプリカ インスタンスが通信できることを確認します。詳細については、343 ページの RSA RADIUS レプリケーションの検証を参照してください。

RSA RADIUS レプリケーションの検証

RADIUS プライマリと RADIUS レプリカの間の適切な通信を確保するには、次の事項を確認します。

- Authentication Manager のインスタンスがネットワークに接続されている。
- すべてのホスト名と IP アドレスが正しく構成されている。したがって、プライマリ インスタンスでレプリカ インスタンスをホスト名と IP アドレスによって解決でき、レプリカ インスタンスでプライマリ インスタンスをホスト名と IP アドレスによって解決できる。
- プライマリ インスタンスとレプリカ インスタンスの間のファイアウォールで、ポート 1812 および 1813 での通信が可能である。
- プライマリ インスタンスとレプリカ インスタンスのシステム時刻のずれが、10 分以内に収まっている。時刻のずれが 10 分を超えている場合、RADIUS プライマリは RADIUS レプリカにデータをレプリケーションできない。

Security Console の［RADIUS Servers（RADIUS サーバ）］ページで、RADIUS サーバのレプリケーションのステータスを確認できます。

定期的 RADIUS レプリケーションの有効化

定期的なレプリケーションを有効化した場合、RADIUS プライマリ サーバは RADIUS データへの変更を 15 分ごとにチェックします。変更が検出された場合、導入環境内の利用可能なすべての RADIUS レプリカ サーバに RADIUS データをレプリケーションします。データをレプリケーションした後、プライマリ サーバは各 RADIUS レプリカ サーバが最新の状態であることを検証します。RADIUS レプリカ サーバが更新に失敗した場合、RADIUS プライマリ サーバはシステム ログおよび重大システム イベントの通知システムにメッセージを記録します。指定した担当者にメール メッセージを送信するように構成できます。

手順

1. Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。
2. ［**Advanced Settings（詳細設定）**］セクションで、［**RADIUS**］をクリックします。
3. ［**RADIUS Replication Configuration（RADIUS レプリケーション構成）**］の［**Periodic RADIUS Replication（定期的 RADIUS レプリケーション）**］で、［**Enable periodic RADIUS Replication every 15 minutes（15 分ごとの定期的 RADIUS レプリケーションを有効化する）**］を選択します。
4. ［**Save（保存）**］をクリックします。

RADIUS レプリカ サーバへのレプリケーションの手動開始

RADIUS プライマリ サーバから導入環境のすべての RADIUS レプリカ サーバへの RADIUS データベースのレプリケーションを手動で開始できます。たとえば、重要な RADIUS クライアントをネットワークに追加した場合、すべての RADIUS レプリカ サーバへのレプリケーションを開始します。

手順

1. Security Console で、[**RADIUS**] > [**RADIUS Servers（RADIUS サーバ）**] の順にクリックします。
2. [**Initiate Replication（レプリケーションの開始）**] をクリックします。

システム生成 PIN を使用するための RSA RADIUS の構成

RSA RADIUS は、デフォルトではシステム生成 PIN を使用できません。システム生成 PIN を使用する場合、各 RADIUS サーバで、RADIUS 構成ファイル **securid.ini** の変更と、RADIUS サーバの再起動を実施する必要があります。そうしないとシステム生成 PIN を使用した認証は失敗します。

開始する前に

スーパー管理者である必要があります。

手順

1. RADIUS サーバをホストする RSA Authentication Manager インスタンスで Operations Console にログオンします。
2. [**Deployment Configuration（導入環境の構成）**] > [**RADIUS Servers（RADIUS サーバ）**] の順にクリックします。
3. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。
4. このインスタンスの RADIUS サーバを選択し、コンテキスト メニューから [**Manage Server Files（サーバ ファイルの管理）**] をクリックします。
5. [**Configuration Files（構成ファイル）**] タブで、**securid.ini** ファイル選択し、コンテキスト メニューから [**Edit（編集）**] をクリックします。
6. 次の行を探します。

   ```
   AllowSytemPins = 0
   ```

   0 はシステム生成 PIN の使用を許可しないことを意味します。システム生成 PIN の使用を許可するには、この行を次のように変更します。

   ```
   AllowSystemPins = 1
   ```

   1 はシステム生成 PIN の使用を許可することを意味します。
7. [**Save and Restart RADIUS（保存と RADIUS の再起動）**] をクリックします。
8. 変更を有効にするには、RADIUS サーバを再起動します。

RADIUS サーバの再起動

RSA Authentication Manager が開始されると、RSA RADIUS サーバは自動的に開始されます。次の状況で、RADIUS サーバを再起動する必要があります。

- RADIUS サーバのポートの割り当てを変更した後。
- RADIUS サーバ ファイル（.ini、.dct、.aut）を変更した後。
- RADIUS サーバ証明書を置き換えた後。
- RADIUS サーバが停止した場合。

開始する前に

スーパー管理者である必要があります。

手順

1. RADIUS サーバをホストしている RSA Authentication Manager インスタンス上の Operations Console で、**［Deployment Configuration（導入環境の構成）＞［RADIUS Servers（RADIUS サーバ）］**の順にクリックします。
2. プロンプトが表示された場合は、Security Console のユーザー ID とパスワードを入力し、［**OK**］をクリックします。
3. 再起動する RADIUS サーバをクリックし、コンテキスト メニューの［**Restart Server（サーバの再起動）**］をクリックします。
4. ［Restart RADIUS Server（RADIUS サーバの再起動）］ページの［Confirmation（確認）］で、［**Yes, restart RADIUS Server（はい、RADIUS サーバを再起動します）**］を選択して［**Restart Server（サーバの再起動）**］をクリックします。

RSA RADIUS サーバの保守

ホスト システムを整備する、認証レスポンス タイムを向上させる、使用不可になった RADIUS サーバをリカバリするなどの目的で、RSA RADIUS サーバに対して保守および変更を行うことができます。このセクションで取り上げる保守タスクは、次のとおりです。

- RSA RADIUS サーバ ファイルのカスタマイズ
- RADIUS サーバ ファイルの編集

RADIUS はプライマリ インスタンスまたはレプリカ インスタンスにインストールされ、Authentication Manager と同じインスタンス上で実行されるように構成されます。プライマリ インスタンスまたはレプリカ インスタンス上の Operations Console を使用して、RADIUS サーバ構成を変更できます。

RSA RADIUS は、RSA Authentication Manager と同じホスト名と IP アドレスを使用します。RADIUS サーバのホスト名や IP アドレスを変更するには、RSA Authentication Manager のホスト名や IP アドレスを変更する必要があります。

詳細については付録 A、インスタンス ネットワーク設定の変更。を参照してください。

RSA RADIUS サーバ ファイルのカスタマイズ

各 RSA RADIUS サーバには、サーバを稼働環境内でカスタマイズするための構成ファイル、初期設定ファイル、ディクショナリファイルが保存されます。多くの場合は、これらのファイルを変更せずにデフォルトのまま使用するのみで十分です。ただし、次のいずれかに該当する場合は、これらのファイルを必要に応じて変更することになります。

- アカウンティング属性などのログ オプションを変更する場合。
- RADIUS プロファイルに含める必要のある特別な属性名を使用する RADIUS クライアントを構成する場合。このクライアントからのリクエストを処理する各 RADIUS サーバに、RADIUS クライアントに付属しているディクショナリファイルを追加する必要があります。異なる RADIUS クライアントの間で属性名を適切に関連づけるには、**mapping.ini** ファイルの編集が必要になることがあります。

Operations Console を使用して、RADIUS サーバ ファイル（構成ファイル、初期設定ファイル、ディクショナリファイル）を表示し、編集のために開きます。構成ファイルで使用される構文の詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

RADIUS サーバ ファイルの編集

RSA RADIUS サーバ ファイルの変更が必要となる場合があります。たとえば、ログ オプションを変更する場合や、特別な属性名を使用する RADIUS クライアントを構成するために、RADIUS プロファイルにそれらの属性を追加する場合などです。

変更は、編集を行った RADIUS サーバにのみ適用されます。

重要：構成ファイルの編集は慎重に行ってください。ユーザーが加えた変更は検証されることなく、既存ファイルが新しい内容で上書きされます。構成ファイルで使用する構文の詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

開始する前に

スーパー管理者および Operations Console 管理者のクレデンシャルを持っている必要があります。

手順

1. RADIUS サーバをホストしている RSA Authentication Manager インスタンスの Operations Console にログオンします。
2. ［**Deployment Configuration（導入環境の構成）**］＞［**RADIUS Servers（RADIUS サーバ）**］の順にクリックします。
3. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力し、［**OK**］をクリックします。

4. このインスタンスでホストされている RADIUS サーバを選択し、コンテキスト メニューから［**Manage Server Files（サーバ ファイルの管理）**］を選びます。
5. ［Manage Server Files（サーバ ファイルの管理）］ページで、次のいずれかを実行します。
   - ［**Configuration Files（構成ファイル）**］タブをクリックして、.conf、.aut、.ini などの構成ファイルを表示します。
   - ［**Dictionary Files（ディクショナリファイル）**］タブをクリックして、RADIUS ディクショナリファイルを表示します。
6. 編集するファイルを選択して、コンテキスト メニューから［**Edit（編集）**］を選択します。
7. テキスト ファイルを編集して、［**Save（保存）**］をクリックします。
8. 変更を適用するには、［**Save & Restart RADIUS Server（保存して RADIUS サーバを再起動する）**］をクリックします。

次のステップ

編集内容を導入環境全体で同期する必要がある場合（.dct ファイルを編集した場合など）は、編集内容を他の RADIUS サーバにコピーする必要があります。編集内容を導入環境の他の RADIUS サーバにコピーするには、［ RADIUS Server（RADIUS サーバ）］ページから適切な RADIUS サーバを選択し、コピーまたは編集を行います。

RADIUS クライアント

RADIUS クライアントは、ネットワーク境界に配置された RADIUS 対応デバイスです。ネットワーク リソースにアクセスするユーザーにアクセス制御を適用します。

RADIUS クライアントには、次のような種類があります。

- VPN サーバ
- ワイヤレス アクセス ポイント
- ダイヤル イン モデムをサポートするネットワーク アクセス サーバ
- ダイヤル イン モデム

RADIUS クライアントは、ユーザーのアクセス要求を RADIUS サーバに送信します。RADIUS サーバが受け取った要求は、RSA Authentication Manager に転送して検証されます。

Authentication Manager でアクセス要求が許可された場合、RADIUS クライアントはユーザーのネットワーク アクセス要求を受け入れます。それ以外の場合は、ユーザーのネットワーク アクセス要求を拒否します。

RADIUS クライアントは、認証エージェントを割り当てて構成することも、割り当てずに構成することもできます。2 つの方法では、アクセス制御とログのレベルが異なります。

エージェントありの RADIUS クライアント：エージェントを RADIUS クライアントに追加すると、どの RADIUS クライアントが認証に使用されるかを Authentication Manager が判断することができ、その情報がログファイルに保存されます。詳細については、RADIUS クライアントの追加を参照してください。

エージェントなしの RADIUS クライアント：エージェントを割り当てない RADIUS クライアントの場合、Authentication Manager は認証要求を送信した RADIUS クライアントをトラッキングできず、クライアントにプロファイルを割り当てることができません。RADIUS サーバは、単純に、RADIUS クライアントからの共有シークレットが RSA RADIUS に格納されている共有シークレットと一致することを検証し、クライアント情報を含まない要求を Authentication Manager に転送します。

すべての認証要求は、RADIUS サーバから、RADIUS サーバに割り当てられた認証エージェントを介して送信されたように見えます。この方法を使用している場合、Security Console で RADIUS クライアントのエージェントを追加しても、Authentication Manager はクライアントとエージェントを関連づけないため、エージェントに指定したプロパティはどれもクライアントに適用されません。

システムが、エージェントの割り当てがないクライアントからのユーザー認証を受け付けるようにするには、**securid.ini** ファイルの CheckUserAllowedByClient パラメータを 0 に設定する必要があります。デフォルトでは、このパラメータは 1 に設定されています。1 に設定した場合、システムはエージェントが割り当てられたクライアントからのユーザー認証を受け付けます。詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

Authentication Manager に RADIUS クライアントを大量に追加する必要がある場合は、RADIUS クライアントにエージェントを割り当てないことを推奨します。たとえば、ISP 管理者が、1,000 台のネットワーク アクセス サーバを追加し、RSA RADIUS サーバに構成する場合を考えます。各 RADIUS クライアントのエージェントを追加する代わりに、［**ANY Client**］を選択し、各 RADIUS クライアントに対して同じ共有シークレットを入力します。いずれかのクライアントが、関連づけられている RADIUS サーバにネットワーク アクセス要求を送信すると、RADIUS サーバは共有シークレットを確認し、クライアント情報を含まない認証要求を Authentication Manager に転送します。

RADIUS クライアントの追加

認証方式として RSA SecurID を使用するよう構成されている RADIUS デバイスごとに、RADIUS クライアントを導入環境に追加する必要があります。RADIUS クライアントが認証要求を RSA RADIUS サーバに送信すると、RSA RADIUS サーバが要求を Authentication Manager に転送します。

RBA（リスク ベース認証）を使用する場合、RADIUS クライアントに関連づけたエージェントで、RBA を有効化する必要があります。

手順

1. Security Console で、[**RADIUS**] > [**RADIUS Clients（RADIUS クライアント）**] > [**Add New（新規追加）**] の順にクリックします。

   [**Client Name（クライアント名）**] フィールドに、クライアントの名前（たとえば、VPN-London）を入力します。英字、数字、ハイフン（-）、下線（_）を入力できます。スペース、タブ、@ 記号、ほとんどの特殊文字、印刷不可能な文字は使用できません。このフィールドは、50 文字に制限されています。

   （たとえば、多くの RADIUS クライアントを迅速に追加するために）認証要求を送信した RADIUS クライアントを RSA Authentication Manager で追跡しないようにする場合、名前を入力する必要はありません。

2. （オプション）[**ANY Client**] フィールドで、[Accept authentication requests from any RADIUS client using the shared secret specified for this client（このクライアントに指定された共有シークレットを使用する任意の RADIUS クライアントからの認証要求を許可する）] を選択します。

   このオプションを選択した場合は、この RADIUS クライアントのために RADIUS サーバが認証を行わないように、プロキシ認証も無効化する必要があります。詳細については、347 ページの RADIUS クライアント を参照してください。

   クライアントを保存した後でその名前を変更することはできません。クライアントの名前を変更するには、そのクライアントを削除してから、新しいクライアントを新しい名前で追加する必要があります。

3. [**IP Address（IP アドレス）**] フィールドに、RADIUS クライアントの IP アドレス（たとえば、111.222.33.44）を入力します。

   前のステップで [**ANY Client（ANY クライアント）**] を選択した場合は IP アドレスが適用されないため、IP アドレスを入力することはできません。

4. [**Make/Model（製造元 / モデル）**] ドロップダウン リストで、RADIUS クライアントのタイプを選択します。RADIUS クライアントの製造元およびモデルが不明な場合は、[**Standard Radius（標準 Radius）**] を選択します。

   RADIUS サーバは、製造元およびモデルを使用して、このクライアントと通信を行うときに使用する RADIUS 属性のディクショナリを決定します。

5. ［**Shared Secret（共有シークレット）**］フィールドに、RADIUS クライアントのインストールおよび構成時に指定した認証共有シークレット（大文字と小文字が区別されるパスワード）を入力します。
   RADIUS クライアントは、RADIUS プライマリ サーバまたは RADIUS レプリカ サーバと通信を行うときに同じ共有シークレットを使用します。
6. RADIUS クライアントと RADIUS サーバとの間のアカウンティング トランザクション用に（ステップ 5 で指定した共有シークレット以外の）別の共有シークレットを使用するには、［**Accounting（アカウンティング）**］を選択します。
   ［**Accounting Shared Secret（アカウンティング共有シークレット）**］フィールドに、RADIUS クライアントのインストールおよび構成時に指定したアカウンティング共有シークレットを入力します。RADIUS クライアントは、RADIUS プライマリ サーバまたは RADIUS レプリカ サーバと通信を行うときに同じ共有シークレットを使用します。
7. ［**Client Status（クライアント ステータス）**］を選択し、RADIUS サーバが RADIUS クライアントからキープアライブ パケットを受け取ることなくクライアント接続を保持する秒数を指定します。
   ［**Inactivity Time（非アクティブ時間）**］フィールドに、秒数を入力します。RADIUS クライアント構成で指定したキープアライブ値より少し大きい値を入力します。選択した時間が短すぎる場合、サーバが有効な接続を閉じる可能性があります。詳細については、RADIUS クライアントのマニュアルを参照してください。
8. ［**Notes（メモ）**］フィールドに、このクライアントに関するメモを入力します（たとえば、「ロンドンのサイトに配置」）。
9. 変更を保存するには、次のいずれかを実行します。
   - ［**Save and Create Associated RSA Agent（保存と関連する RSA エージェントの作成）**］をクリックします。これにより、Authentication Manager は、認証に使用される RADIUS エージェントを判別し、この情報をログに記録できます。このオプションは、RBA（リスク ベース認証）を使用する場合は必須です。
   - （**securid.ini** ファイルの CheckUserAllowed ByClient パラメータを 0 に設定して）プロキシ認証を無効化している場合にのみ、［**Save（保存）**］をクリックします。このオプションを選択した場合は、このクライアントにプロファイルを割り当てることができません。Authentication Manager では、すべての認証要求が RADIUS サーバから送信されたものとして扱われます。

次のステップ

- この RADIUS クライアントに対して RSA エージェントを作成した場合は、エージェントを構成する必要があります。操作手順については、RSA Security Console ヘルプのトピック「RADIUS クライアント エージェントの追加」を参照し、ステップ 8 から開始してください。

- 構成が完了すると、レプリケーションが 15 分ごとに実行されます。レプリケーションを手動で開始してこの新しいクライアントを RADIUS レプリカ サーバに認識させる方法については、344 ページの RADIUS レプリカ サーバへのレプリケーションの手動開始を参照してください。

EAP-POTP 設定

EAP（Extensible Authentication Protocol）は、複数の認証方式をサポートする認証フレームワークです。EAP により、RADIUS プロトコルや RADIUS サーバに対する変更を必要とすることなく新しい認証方式をサポートできます。EAP-POTP は、ワンタイム パスワード（RSA SecurID）認証の方法を定義し、RSA RADIUS 内に次の機能を提供します。

- ワンタイム パスワードのエンド ツー エンドの保護
- 相互認証
- 802.1x（ワイヤレス）用のセッション キーの導出
- トークン例外ケースのサポート（New PIN またはネクスト トークンコードなど）
- ワイヤレス接続が失われた場合のセッションの迅速な再開

EAP-POTP 設定は、認証に使用するワンタイム パスワードを保護するためのキー生成要素（およびキー）の基本パラメータを定義します。

デフォルト値は、セキュリティ（暗号強度）とシステムの応答性のバランスが取れた設定になっているため、ほとんどの環境で良好に使用できます。EAP-POTP のデフォルト値は増減できます。ただし、キー生成に使用される値をごくわずかに変更しただけでも認証時のレスポンス タイムが大きく変わる可能性があります。EAP-POTP 設定は、導入環境全体に影響を与えます。

注：RSA RADIUS では、EAP 認証方式を使用した場合、Filter-ID 属性はサポートされません。

EAP-TTLS の構成

RSA RADIUS サーバは、EAP-TTLS（Extensible Authentication Protocol-Tunneled Transport Layer Security）認証を処理するように構成できます。EAP-TTLS プロトコルを使用して行われた認証リクエストを RSA RADIUS で処理するには、次の証明書が必要です。

- 各 RADIUS サーバのサーバ証明書。RADIUS クライアントが RADIUS サーバを認証するために使用します。デフォルトで、各 RADIUS サーバにサーバ証明書がインストールされます。
- 信頼するルート証明書。RADIUS サーバが RADIUS クライアントを認証するために使用します。デフォルトでは、RADIUS サーバにルート証明書はインストールされません。

RADIUS サーバ証明書の置換

クライアントが RADIUS サーバを認証できるように、RSA RADIUS は RADIUS サーバ証明書を RADIUS クライアントに提示します。Operations Console を使用して、RADIUS サーバの既存のサーバ証明書を別の証明書で置き換えることができます。たとえば、自分の組織が信頼するルート認証局が発行した証明書を割り当てます。RSA RADIUS は、サーバ証明書をレプリケーションしません。各 RADIUS サーバに直接アクセスし、次の手順を実行する必要があります。

開始する前に

- スーパー管理者である必要があります。
- キーストア（.pfx）ファイルがあることを確認します。このファイルには、新しいサーバ証明書および関連づけられた秘密鍵が含まれています。このファイルは PKCS #12 ファイル形式で、置換用の新しいサーバ証明書および秘密鍵のみを格納しています。キーストアに複数の証明書が含まれていると、不適切な証明書が置換用のサーバ証明書として使用される可能性があります。
- システムへの信頼するルート証明書の追加を行います。置換用のサーバ証明書の署名に使用した証明書を追加します。署名証明書は、DER 形式で、.der 拡張子を使用している必要があります。置換用のサーバ証明書が自己署名証明書である場合は、署名証明書を追加する必要はありません。

手順

1. プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**RADIUS Servers（RADIUS サーバ）**］の順にクリックします。
2. プロンプトが表示された場合は、Security Console のユーザー ID とパスワードを入力し、［**OK**］をクリックします。
3. 証明書を置き換える RADIUS サーバをクリックし、コンテキスト メニューの［**Manage EAP Certificates（EAP 証明書の管理）**］をクリックします。
4. ［Manage EAP Certificates（EAP 証明書の管理）］ページで、［**Server Certificate（サーバ証明書）**］タブをクリックします。
5. ［**Replace Server Certificate（サーバ証明書の置換）**］セクションの［**Browse（参照）**］をクリックし、置換用の証明書および秘密鍵を含むキーストア ファイルを選択します。

   PKCS #12 形式のキーストアファイル（拡張子は .pfx）を選択する必要があります。
6. **Keystore Password（キーストア パスワード）**］フィールドに、置換用の証明書が含まれたキーストア ファイルのパスワードを入力します。

7. ［**Save & Restart RADIUS Server（保存と RADIUS サーバの再起動）**］をクリックします。
   変更を有効にするためには、RADIUS サーバを再起動する必要があります。
8. 導入環境にある各 RSA RADIUS サーバに対して、この手順を繰り返します。

信頼するルート証明書の追加

信頼するルート証明書は、RADIUS サーバが RADIUS クライアントを認証するために使用します。Operations Console を使用して、RSA RADIUS の信頼するルート証明書を追加します。デフォルトでは、RSA RADIUS には信頼するルート証明書は含まれていません。必要な数の証明書を追加できます。信頼するルート証明書は、プライマリ インスタンスにのみ追加する必要があります。RSA RADIUS は、信頼するルート証明書を導入環境内のすべての RSA RADIUS サーバにレプリケーションします。

開始する前に

- スーパー管理者である必要があります。
- 証明書が次の要件を満たしていることを確認します。
  - 証明書が DER 形式である。
  - 証明書ファイルの拡張子が .der である。

手順

1. Authentication Manager プライマリ インスタンスで Operations Console にログオンします。
2. ［**Deployment Configuration（導入環境の構成）**］＞［**RADIUS Servers（RADIUS サーバ）**］の順にクリックします。
3. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。
4. プライマリ RADIUS サーバを選択し、コンテキスト メニューから［**Manage EAP Certificates（EAP 証明書の管理）**］をクリックします。
5. ［Manage EAP Certificates（EAP 証明書の管理）］ページで、［**Trusted Root Certificates（信頼するルート証明書）**］タブをクリックします。
6. ［**Browse（参照）**］をクリックし、追加する証明書ファイルを選択します。
7. ［**Add（追加）**］をクリックし、証明書をサーバに追加します。
8. 信頼するルート証明書の追加が完了したら、［**Done（完了）**］をクリックします。

ユーザー アクセスの管理

RSA RADIUS 管理者は、属性と値のペアを使用して RADIUS ユーザー アクセスを管理します。RADIUS の認証試行の間、RADIUS クライアントおよび RADIUS サーバは属性と値のリストを交換します。クライアントはチェック リストを送信し、サーバはリターン リストを返します。

属性は 2 つの方法で割り当てることができます。

- 属性を RADIUS プロファイルに追加し、プロファイルをユーザーまたはエージェントに割り当てます。
  詳細については、357 ページの RADIUS プロファイルの追加および358 ページの RADIUS プロファイル関連づけを参照してください。
- ユーザー属性（標準ユーザー属性またはカスタム ユーザー属性）をユーザーに直接割り当てます。
  詳細については、363 ページの RADIUS ユーザー属性を参照してください。

本セクションには、以下のトピックが含まれています。

- RADIUS プロファイル
- RADIUS プロファイルの追加
- RADIUS プロファイル関連づけ
- デフォルトの RADIUS プロファイルの指定
- RADIUS ユーザー属性

RADIUS プロファイル

RADIUS プロファイルは、RADIUS によるユーザー認証のセッション要件を指定する、属性の名前付きの集合です。プロファイルの作成または更新時に、チェックリストおよびリターン リスト内の属性および属性値を追加、削除、変更できます。

プロファイルにより、ユーザー グループの管理が容易になります。管理者は、特定のユーザー グループ向けに属性のチェックリストおよびリターン リストを持つプロファイルを作成し、そのプロファイルを Authentication Manager 内で定義されている特定のユーザー ID に割り当てます。Security Console では、プロファイルの作成および更新用の管理ページ、チェックリストとリターンリストに使用可能な属性がドロップダウンリストで表示されます。

プロファイルは、導入環境のすべての RSA RADIUS サーバに同期されます。プロファイル名は Authentication Manager に保存されるため、Security Console から一元的に管理できます。RSA RADIUS の初期状態では、プロファイルは存在しません。プロファイルは、管理者が Security Console を通じて作成します。

RADIUS 属性

RSA RADIUS では、単一値属性、複数値属性、順序指定可能な複数値属性を使用することにより、認証時のシステムの動作をより柔軟に制御できます。

- 単一値属性と複数値属性

  属性には、単一値属性と複数値属性があります。単一値属性はチェックリストまたはリターン リスト内に 1 つだけ含まれます。複数値属性は複数含めることができます。チェックリスト内に属性が複数回現れる場合は、それらの値がいずれも有効であることを意味します。たとえば、チェックリストにそれぞれ異なる電話番号を設定した複数の Calling-Station-ID 属性を含めることができます。指定されている電話番号のいずれもが有効であるため、ネットワークにダイヤル インしようとするユーザーはどの電話番号から発信した場合でも認証を受けることができます。

  リターン リスト内に属性が複数含まれている場合は、その属性の値すべてが応答パケットの一部として送信されます。たとえば、あるユーザーに対して IP ヘッダ圧縮と IPX ヘッダ圧縮の両方を有効化するには、リターン リストに Framed-Compression 属性を 2 つ追加し、一方の値を VJ-TCP-IP-header-compression に設定し、もう一方の値を IPX-header-compression に設定する必要があります。

- 順序指定可能な複数値属性

  リターン リストの複数値属性には、順序を指定できるものがあります。これらの属性は、RADIUS 応答内に複数含めることができ、属性を含める順序が重要な意味を持ちます。たとえば、Reply-Message 属性を使用すると、ユーザーに対して表示するテキスト メッセージを返すことができます。複数行のメッセージを送信するには、この属性をリターン リストに複数追加し、メッセージの各行を正しい順序で指定します。

RADIUS チェックリスト

RADIUS チェックリストは、認証要求の一部として RADIUS クライアントから RADIUS サーバへ送信する必要のある属性のセットです。必須の属性が含まれていない場合、要求は拒否されます。たとえば、チェックリスト属性の一例である NAS-IP-Address 属性は、ユーザーに使用を許可する RADIUS クライアントの IP アドレスを指定します。この属性がアクセス要求に含まれていない場合、要求は拒否されます。

RADIUS サーバは RADIUS クライアントからの認証要求を検証して、プロファイル内でチェックリスト属性として定義されている属性および属性値が認証要求に含まれていることを検証します。

RADIUS クライアントから送信される認証要求には、すべての使用可能な属性および属性値がデフォルトで含まれています。RADIUS クライアントが特定の属性を送信しない構成になっている場合に、その属性がチェックリスト属性として定義されていると、認証要求は失敗します。RADIUS クライアントの構成手順については、RADIUS クライアント デバイスのマニュアルを参照してください。

属性をチェックリストに割り当てるには、属性を RADIUS プロファイルに追加し、そのプロファイルをユーザーまたはエージェントに割り当てます。

RADIUS リターン リスト

RADIUS リターン リストとは、ユーザー認証時に RADIUS サーバから RADIUS クライアントへ返される属性のセットです。リターン リスト属性は、RADIUS クライアントがユーザーを接続するときに必要となる追加パラメータ（VLAN の割り当てや IP アドレスの割り当てなど）を指定します。認証が成功すると、そのユーザーのセッション パラメータを設定するため、Access-Accept メッセージとともにリターン リスト属性が RADIUS サーバから RADIUS クライアントへ送信されます。

次の 2 つの方法で、属性をリターン リストに追加できます。

- 属性をプロファイル内のリターン リストに追加し、そのプロファイルをユーザーまたはエージェントに割り当てる。詳細については、357 ページの RADIUS プロファイルの追加および 358 ページの RADIUS プロファイル関連づけを参照してください。
- ユーザー属性（標準またはカスタムのユーザー属性）をユーザーに直接割り当てる。詳細については、363 ページの RADIUS ユーザー属性を参照してください。

注：このガイドでは、特定の属性の目的と使用方法については説明しません。各 RADIUS クライアント デバイスのマニュアルを参照してください。

デフォルト プロファイル

RSA RADIUS では、デフォルト プロファイルがサポートされています。デフォルト プロファイルが指定されていれば、プロファイルを割り当てられていない RADIUS ユーザーが認証を受けたときに、そのデフォルト プロファイルで定義されている属性と値がそのユーザーに適用されます。

インストール時に、デフォルトの RADIUS プロファイルを指定することはできません。デフォルト プロファイルは、管理者が作成し、デフォルトとして指定する必要があります。Authentication Manager に 1 つ以上の RADIUS プロファイルがすでに追加されている場合は、Security Console の［System Settings（システム設定）］ページでデフォルト プロファイルを指定できます。また、RADIUS 構成ファイルの **securid.ini** で指定することもできます。Authentication Manager で指定したデフォルト プロファイルは、**securid.ini** ファイルで指定されたデフォルト プロファイルよりも常に優先されます。

デフォルト プロファイルに対しても、通常のプロファイルの場合と同様に、チェックリストおよびリターン リスト内の属性と属性値を管理者が追加、削除、変更できます。

デフォルトの RADIUS プロファイルの設定の詳細については、RSA Security Console ヘルプのトピック「RADIUS 設定の構成」を参照してください。

ディクショナリファイルによる属性のカスタマイズ

RSA RADIUS では、サーバに付属しているディクショナリファイルに標準の RADIUS 属性が定義されています。これらの標準属性のみでも RADIUS クライアント デバイスの主要ブランドのほとんどをサポートできます。新しい RADIUS クライアント デバイスや特別な RADIUS クライアント デバイスを購入した場合、クライアント固有の属性を含むディクショナリファイルがそのデバイスに付属していることがあります。そのディクショナリファイルを各 RADIUS サーバにインストールすれば、RADIUS クライアント用の新しい属性や変更された属性をプロファイルに含めて使用することが可能になります。

ごくまれに、RADIUS 内の属性名が特定の RADIUS クライアントで使用される属性名と異なっていることがあります。管理者は Operations Console を通じて、ディクショナリファイルで定義されている属性を変更できます。

RADIUS プロファイルの追加

RADIUS プロファイルは、リモート ネットワーク アクセスを要求するユーザーのセッション要件を指定する属性の、名前付きの集合です。属性はチェックリストまたはリターン リストに格納されます。

プロファイルを追加することによって、ユーザー、ユーザー エイリアス、トラステッド ユーザー、エージェントに割り当てる、チェックリスト属性およびリターン リスト属性の集合を作成できます。

手順

1. Security Console で、[**RADIUS**] > [**RADIUS Profiles（RADIUS プロファイル）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**Profile Name（プロファイル名）**] フィールドに、このプロファイルの目的を識別する一意の名前（たとえば、SALES）を入力します。

   プロファイルを保存した後でその名前を変更することはできません。プロファイルの名前を変更するには、そのプロファイルを削除してから、新しいプロファイルを新しい名前で追加する必要があります。
3. [**Notes（メモ）**] フィールドに、このプロファイルに関するメモ（たとえば、「このプロファイルは Sales に所属するすべての従業員に使用する」）を入力します。
4. [**Return List Attributes（リターン リスト属性）**] で、次のいずれかを実行します。
   - 属性を追加するには、それぞれのリターン リスト属性を選択し、このプロファイルの対応する値を入力して、[**Add（追加）**] をクリックします。属性と属性値の詳細については、RADIUS クライアントのマニュアルを参照してください。
   - 属性を削除するには、リスト ボックスで属性を選択し、[**Remove（削除）**] をクリックします。

- 属性を更新するには、リストで属性を選択した後、更新した値をフィールドに入力し、[**Update（更新）**] をクリックします。並べ替え可能（O のマークで示されます）な複数値（M のマークで示されます）のリターン リスト属性を入力した場合は、[**Up（上）**] または [**Down（下）**] をクリックすることにより、属性とその値の順序を指定できます。
- 特定の値を指定せず、RADIUS 要求内の属性値を RADIUS 応答でクライアントにエコーするようにするには、属性に [**Echo**] を選択します。

5. [**Checklist Attributes（チェックリスト属性）**] で、次のいずれかを実行します。
   - 属性を追加するには、それぞれのチェックリスト属性を選択し、このプロファイルの対応する値を入力して、[**Add（追加）**] をクリックします。属性と属性値の詳細については、RADIUS クライアントのマニュアルを参照してください。
   - 属性を削除するには、リスト ボックスで属性を選択し、[**Remove（削除）**] をクリックします。
   - 属性を更新するには、リストで属性を選択した後、更新した値をフィールドに入力し、[**Update（更新）**] をクリックします。
   - RADIUS クライアントがこれらの属性のいずれか（たとえば、Port-Limit）を送信しないときでも、その属性に対して [**Default（デフォルト）**] が選択されていれば、RADIUS サーバは認証要求を処理します。RADIUS クライアントがこれらの属性のいずれかを送信せず、その属性に対して [**Default（デフォルト）**] が選択されていない場合、RADIUS サーバは認証要求を拒否します。
6. [**Save（保存）**] をクリックします。
7. RADIUS レプリカ サーバにこの新しいプロファイルを認識させるには、レプリカ サーバへのレプリケーションを手動で開始します。定期的レプリケーションを構成している場合は、レプリケーションが 15 分ごとに実行されます。操作手順については、344 ページの RADIUS レプリカ サーバへのレプリケーションの手動開始を参照してください。

RADIUS プロファイル関連づけ

RADIUS プロファイルを導入環境内のユーザーおよびエージェントに割り当てることによって、RADIUS プロファイルをユーザーおよびエージェントに関連づけることができます。ユーザーまたはエージェントにプロファイルを割り当てると、ユーザーまたはエージェントが RADIUS 認証を試行するたびに、RADIUS サーバはプロファイルに含まれるチェックリストとリターン リストを使用します。

管理者は、次のオブジェクトにプロファイルを割り当てることや割り当て解除することができます。

- **ユーザー：**システムによって管理されるアカウント。通常は人ですが、コンピュータや Web サービスの場合もあります。
- **ユーザー エイリアス：**ユーザーがが自分以外のユーザー ID を使用して RSA SecurID トークンをで認証できるようにします。たとえば、特定のユーザーにエイリアス「root」を割り当てたとします。そのユーザーは、ユーザー ID「root」と自身のトークンを使用してログオンできます。
- **トラステッド ユーザー：**信頼する別の RSA Authentication Manager 8.0 導入環境のユーザー。
- **エージェント：**ネットワーク上の Authentication Manager と通信して認証を行うため、RADIUS クライアントまたはサーバにインストールされたソフトウェア アプリケーション。

ユーザーおよびエージェント（ユーザーのネットワーク要求の送信先）に RADIUS プロファイルが割り当てられていない場合は、ユーザーのネットワーク要求にデフォルトの RADIUS プロファイルを割り当てることができます。

ユーザーへの割り当て

ユーザーは、Authentication Manager 内で定義されます。ユーザーと正しい RSA SecurID トークン レコードの関連づけが定義とともに維持されます。管理者は、Security Console の RADIUS 用ページでユーザー ID をプロファイルに関連づけることができます。このアクションを実行すると、プロファイルの属性がユーザーに適用されます。

ユーザー エイリアスへの割り当て

ユーザー エイリアスにより、ユーザーが必要に応じて複数のロールを持つことができます。たとえば、ユーザー Alice にユーザー ID として Alice_User、ユーザー エイリアス ID として Alice_Admin が割り当てられているとします。Alice のユーザー ID はユーザー用に設定されたプロファイルに関連づけられているため、Alice が Alice_User としてログオンすると、ユーザーに関連づけられているすべての属性が Alice に適用されます。一方、Alice のユーザー エイリアス ID は管理者用に設定されたプロファイルに関連づけられているため、Alice が Alice_Admin としてログオンした場合は、より管理者に適した属性が Alice に適用されます。たとえば、ルータおよび VPN サーバの管理に必要な IP アドレスにアクセスできます。

トラステッド ユーザーへの割り当て

トラステッド レルムを構成している場合、他のバージョン 8.0 レルムのユーザーが RSA RADIUS を使用してリソースにアクセスしようとすることがあります。このようなユーザーに RADIUS プロファイルをどのように関連づけるかは、それらのリモートの「トラステッド ユーザー」がローカル レルム内でどのように定義されているかに依存します。

注：RSA_RADIUS を使用して、トラステッド ユーザーを認証するには、トラステッド レルムで Authentication Manager 7.1 以降が実行されている必要があります。Authentication Manager 8.0 と 6.1 のレルム間認証では、RSA RADIUS を使用した認証はサポートされません。

トラステッド ユーザー ID を事前に Authentication Manager 内で定義し、そのトラステッド ユーザー ID に RADIUS プロファイルを関連づけることができます。このプロファイルは、トラステッド ユーザーに適した属性を定義することで、トラステッド ユーザー専用のプロファイルとして設定できます。そのトラステッド ユーザーのアクセス要求が成功すると、関連づけられているプロファイル属性が RADIUS サーバから RADIUS クライアント デバイスへ返されます。RADIUS ユーザー属性が割り当てられている場合は、それらも返されます。

トラステッド ユーザー ID が事前に設定されていない場合は、RADIUS サーバ上の認証エージェントが Authentication Manager にトラステッド ユーザー アカウントを動的に作成します。その後、Authentication Manager が認証要求を他のトラステッド レルムに転送します。この転送は、認証の成功メッセージまたは失敗メッセージが返されるまで行われます。認証が成功した場合は、Authentication Manager がトラステッド ユーザーのホーム レルムをトラステッド ユーザー ID に追加し（今後の認証要求の処理を高速化するため）、パスコード受け付けのメッセージを RADIUS に返します。

トラステッド ユーザーが使用する RADIUS クライアント（VPN サーバ、ワイヤレス アクセス ポイント、ダイヤル イン モデムをサポートするネットワーク アクセス サーバ）にエージェント プロファイルが関連づけられている場合は、トラステッド ユーザーがそのプロファイルの属性を取得します。エージェント プロファイルが関連づけられていない場合、デフォルト プロファイルが指定されていれば、ユーザーはそのプロファイルを取得します。

認証エージェントへの割り当て

認証エージェントにプロファイルを割り当てると、プロファイル内の属性が、対応する特定の RADIUS クライアント デバイスを認証に使用するすべてのユーザーに割り当てられます。

たとえば、VPN サーバを通じて認証するリモート ユーザーに対してリソースのセットへのアクセスを許可すると同時に、同じユーザーがワイヤレス アクセス ポイントから認証した場合にはアクセス可能なサービスのセットを制限することなどができます。RSA RADIUS では、エージェント プロファイルとユーザー プロファイルのどちらを優先して適用するかを管理者が選択できます。これによってユーザー用プロファイルとエージェント用プロファイルの両方が同じユーザーに適用される場合に競合が回避されます。操作手順については、RSA Security Console ヘルプのトピック「RADIUS 設定の構成」を参照してください。

プロファイルの優先度

ユーザー用プロファイルとエージェント用プロファイルの両方がユーザーに適用される場合、たとえば、RADIUS プロファイルをユーザーに割り当て、ユーザーが別のプロファイルが割り当てられているエージェントを使用して RADIUS クライアントからネットワーク アクセスを要求すると、競合が発生します。プロファイルの競合を防止するには、プロファイルの優先順位を指定します。

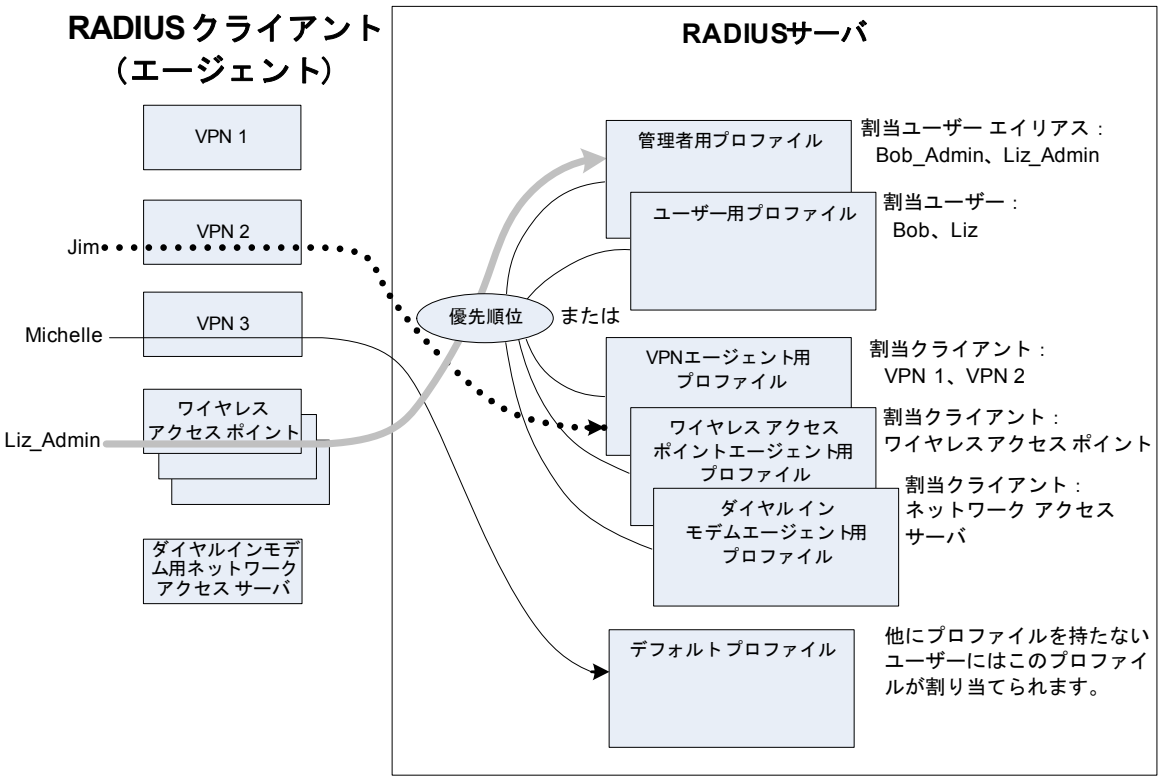
操作手順については、RSA Security Console ヘルプのトピック「RADIUS プロファイルの優先順位の選択」を参照してください。

プロファイルの割り当ての例

次の図は、ユーザーおよびエージェント（RADIUS クライアント）に割り当てられたプロファイルに基づいて RADIUS がどのようにユーザーにプロファイルを適用するかを示しています。

- Jim には明示的にプロファイルが割り当てられていません。Jim が認証に使用する VPN2 にはプロファイルが明示的に割り当てられているため、VPN エージェント用のプロファイルが Jim に適用されます。
- Liz_Admin には、管理者用プロファイルが明示的に割り当てられています。Liz_Admin が認証に使用するワイヤレス アクセス ポイントにもプロファイルが明示的に割り当てられています。Liz_Admin に適用可能なプロファイルが 2 つ存在していることになりますが、優先メカニズムによって、どちらのプロファイルを適用するかが決定されます。

- Michelle にはプロファイルが割り当てられていません。Michelle が認証に使用する VPN3 にもエージェント用のプロファイルが明示的に割り当てられていません。Michelle に適用するプロファイルが他に存在しないため、デフォルト プロファイルが Michelle に適用されます。



デフォルトの RADIUS プロファイルの指定

ユーザーおよびエージェント（ユーザーのネットワーク リクエストの送信先）に RADIUS プロファイルが割り当てられていない場合に、RADIUS サーバがユーザーのネットワーク リクエストに割り当てるデフォルトの RADIUS プロファイルを指定します。

開始する前に

スーパー管理者である必要があります。

手順

1. Security Console で、**［Setup（セットアップ）］＞［System Settings（システム設定）］**の順にクリックします。
2. ［Advanced Settings（詳細設定）］セクションで、**［RADIUS］**をクリックします。
3. **［Default RADIUS Profile（デフォルトの RADIUS プロファイル）］**の**［Selected RADIUS Profile（RADIUS プロファイルの選択）］**ドロップダウン メニューからプロファイルを選択します。
4. **［Save（保存）］**をクリックします。

RADIUS ユーザー属性

RSA RADIUS では、標準およびカスタムの RADIUS 属性をサポートしています。

- **標準：**RADIUS プロトコル標準仕様で指定された固定名と ID 番号が割り当てられた属性。詳細については、RADIUS クライアント デバイスのマニュアルを参照してください。
- **カスタム：**RADIUS クライアントのメーカーによって定義された、RADIUS プロトコルに含まれていない属性。これらのカスタム属性を使用する場合は、Security Console を使用して属性を定義し、ユーザーまたはトラステッド ユーザーに割り当てます。ユーザーのユーザー エイリアスにも、これらのカスタム属性を割り当てることができます。詳細については、RSA Security Console ヘルプのトピック「RADIUS カスタムユーザー属性定義の編集」を参照してください。

複数のユーザー、ユーザー エイリアス、トラステッド ユーザー、エージェントに属性を割り当てる場合は、属性を含むプロファイルを作成し、そのプロファイルをオブジェクトに割り当てることができます。

1 人のユーザーまたはトラステッド ユーザーにのみ標準またはカスタムの特定の属性を割り当てる場合は、RADIUS プロファイルを使用せず、ユーザーまたはトラステッド ユーザーに直接これらの RADIUS 属性を割り当てることができます。プロファイルを使用しないでユーザーまたはトラステッド ユーザーに割り当てた RADIUS 属性は、RADIUS ユーザー属性と呼びます。ユーザーに RADIUS ユーザー属性を割り当てた場合、そのユーザーのすべてのユーザー エイリアスにも属性が割り当てられます。エージェントにユーザー属性を割り当てることはできません。RSA Authentication Manager は、ユーザー のユーザー エイリアスにも属性と値を自動的に割り当てます。

次の 2 つの方法で RADIUS ユーザー属性を定義できます。

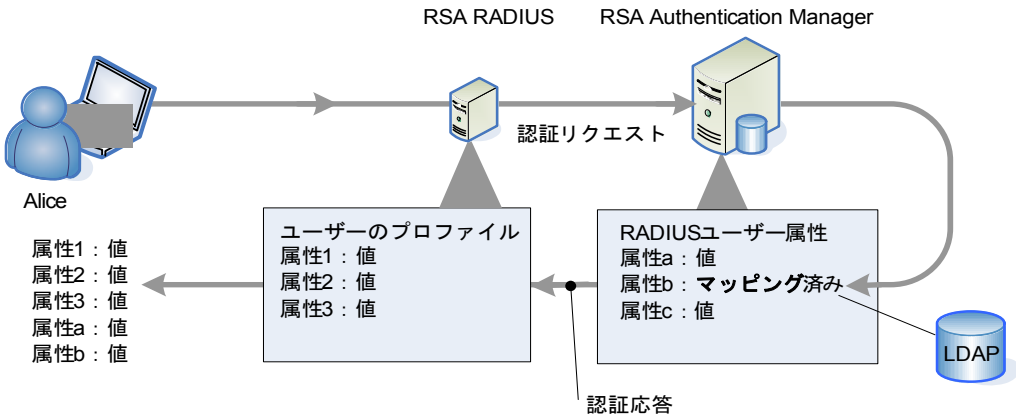
- 実際の値を指定しない
  値を指定しないで定義した属性については、管理者がユーザーに属性を割り当てる時にそのユーザーに適した値を入力できます。たとえば、RADIUS ユーザー属性が Callback Number の場合、ユーザーに割り当てる時に、管理者がユーザーのコールバック電話番号を入力します（RADIUS では、ユーザーが特定の電話番号から通話していることを確認する目的でコールバック番号を使用できます）。RADIUS ユーザー属性は、プロファイルに含まれる同一名の属性より優先して適用されます。
- アイデンティティ ソースに格納されたデータにマッピングする
  会社の LDAP ディレクトリなどのアイデンティティ ソースにすでに格納されている情報を使用します。したがって、属性値を複数の場所に維持する必要がありません。

RADIUS サーバは RADIUS クライアントにプロファイルのリターン リストの属性とともに RADIUS ユーザー属性を送信します。RADIUS ユーザー属性は、プロファイルを使用してユーザーまたはトラステッド ユーザーに割り当てられた属性より優先されます。

また、RADIUS ユーザー属性定義をアイデンティティ ソース属性にマッピングすることもできます。RADIUS サーバは、アイデンティティ ソース属性の値を RADIUS ユーザー属性定義に適用します。たとえば、RADIUS Callback-ID 属性を会社の LDAP データベースの Phone Number 属性にマッピングすることができます。RADIUS ユーザー属性定義をアイデンティティ ソース属性にマップしない場合は、RADIUS ユーザー属性をユーザーまたはトラステッド ユーザーに割り当てるときに、属性値を入力する必要があります。

ユーザー属性の割り当ての例

次の図は、ユーザー Alice が RADIUS を通じて認証を受ける場合のプロファイル リターン リスト属性と RADIUS ユーザー属性の関係を示しています。Alice には、RADIUS ユーザー属性 a および b が割り当てられています（属性 c は別のユーザーに割り当てられています）。Alice が認証に成功すると、すべてのプロファイル属性と RADIUS ユーザー属性 a および b が Alice に適用されます。RADIUS ユーザー属性 b の値は、LDAP アイデンティティ ソースから取得されます。



カスタム RADIUS ユーザー属性定義の追加

RADIUS ユーザー属性は、ユーザーに割り当てられている RADIUS プロファイルとは別に、そのユーザーに割り当てることができます。たとえば、コールバック用の電話番号属性を追加し、自分の電話番号を持つユーザーに個々に割り当てることができます。

カスタム RADIUS ユーザー属性は、以下のいずれかにすることができます。

- RADIUS ディクショナリに新たに追加する非標準の RADIUS 属性（64 ～ 255 の値）。
- RADIUS ディクショナリの既存の非標準の RADIUS 属性。

カスタム ユーザー属性定義は、値を指定してもしなくてもよく、LDAP ディレクトリの属性にマッピングすることもできます。

開始する前に

- カスタム RADIUS 属性が新しい属性である場合は、ディクショナリにある既存の属性と競合しないようにしてください。追加する属性と同じ名前または番号の属性がディクショナリに含まれている場合は、競合する属性をコメント アウトします。
- 新しいカスタム属性を作成する場合は、その属性を使用する各 RADIUS クライアント タイプの RADIUS ディクショナリに、RADIUS 属性定義を追加します。属性は、各 RSA RADIUS サーバのディクショナリに追加する必要があります。手順については、RSA Operations Console ヘルプのトピック「RADIUS 属性定義のディクショナリへの追加」を参照してください。

手順

1. Security Console で、［**RADIUS**］＞［**RADIUS User Attribute Definitions（RADIUS ユーザー属性定義）**］＞［**Add New（新規追加）**］の順にクリックします。
2. ［**Number（数字）**］フィールドに、64 ～ 225 の数字を入力します。
3. ［**Attribute Name（属性名）**］フィールドに、属性の機能を説明する名前を入力します。
   標準の RADIUS 属性名とは異なる名前を入力します。
4. ［**Map to Identity Attribute（アイデンティティ属性へのマッピング）**］セクションで、カスタム属性をアイデンティティ ソース属性にマッピングするか、手動で属性値を入力するかを選択し、以下のいずれかを行います。
   - ［**Yes（はい）**］を選択した場合は、RADIUS 属性をマップするアイデンティティ属性を選択し、この属性マッピングについてのメモを入力します。たとえば「人事データベースの電話番号にマップ」のように入力します。
   - ［**No（いいえ）**］を選択した場合は、デフォルト値とこの属性についてのメモを入力します。たとえば「2012 年 10 月 1 日現在のユーザーの社内電話番号」のように入力します。
5. ［**Save（保存）**］をクリックします。

次のステップ

定義を追加するときに値を入力しない場合は、ユーザーまたはトラステッド ユーザーに属性を割り当てるときに、属性値を入力する必要があります。詳細については、366 ページの RADIUS ユーザー属性のユーザーへの割り当てを参照してください。

RADIUS ユーザー属性のユーザーへの割り当て

標準またはカスタムの RADIUS 属性をユーザーに割り当てることができます。たとえば、[Callback-Number] 属性をユーザーに割り当て、ユーザーのオフィスの電話番号を値として設定できます。RSA Authentication Manager は、ユーザーのユーザー エイリアスにも属性と値を自動的に割り当てます。

RADIUS プロファイルと RADIUS ユーザー属性の両方でユーザーに RADIUS 属性を割り当てた場合、RADIUS サーバは、RADIUS ユーザー属性定義に指定された値を適用します。

開始する前に

RADIUS ユーザー属性を有効化します。詳細については、RSA Security Console ヘルプのトピック「RADIUS ユーザー属性の有効化と無効化」を参照してください。

手順

1. Security Console で、[**Identity（アイデンティティ）**] > [**Users（ユーザー）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 属性を割り当てるユーザーをクリックします。
3. コンテキスト メニューで [**Authentication Settings（認証設定）**] をクリックします。
4. [**RADIUS User Attributes（RADIUS ユーザー属性）**] で、次のいずれかを実行します。
   - 属性を追加するには、ユーザーに割り当てる属性を選択した後、属性の値を [**Value（値）**] フィールドに入力し、[**Add（追加）**] をクリックします。
   - 属性を削除するには、リストで属性を選択し、[**Remove（削除）**] をクリックします。
   - 属性を更新するには、リストで属性を選択した後、値をフィールドに入力し、[**Update（更新）**] をクリックします。

     RADIUS ユーザー属性はアイデンティティ ソース属性にマッピングできます。詳細については、アイデンティティ ソース属性への RADIUS ユーザー属性定義のマッピングを参照してください。
5. [**Save（保存）**] をクリックします。

アイデンティティ ソース属性への RADIUS ユーザー属性定義のマッピング

RADIUS ユーザー属性定義は、アイデンティティ ソース属性にマッピングできます。たとえば、RADIUS Callback-ID 属性を企業の LDAP ディレクトリ内の Phone Number 属性にマッピングすることができます。

RADIUS ユーザー属性定義をアイデンティティ ソース属性にマッピングしない場合は、RADIUS 属性をユーザーに割り当てるときに、属性値を入力する必要があります。

手順

1. Security Console で、［**RADIUS**］＞［**RADIUS User Attribute Definitions（RADIUS ユーザー属性定義）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
2. ［**Standard Attributes（標準属性）**］または［**Custom Attributes（カスタム属性）**］をクリックします。
3. マッピングする属性をクリックします。
4. コンテキスト メニューで［**Edit（編集）**］をクリックします。
5. ［**Map to an Identity Attribute（アイデンティティ属性へのマッピング）**］で、［**Yes（はい）**］を選択します。
6. ［**Select an Identity Attribute（アイデンティティ属性の選択）**］リストから、RADIUS 属性をマッピングするアイデンティティ属性を選択します。
7. ［**Save（保存）**］をクリックします。

システム使用状況の監視と解析

導入環境を初期インストールして構成した後、攻撃の検出、監査、トラブルシューティングの目的で RSA RADIUS のシステム使用状況を積極的に監視する必要が生じるかもしれません。

このセクションでは、RSA RADIUS のシステム使用状況の解析について詳しく説明します。次のタスクについて説明します。

- RADIUS サーバ統計情報の表示
- RADIUS クライアント統計情報の表示

RADIUS サーバの認証統計情報

認証に関する統計情報には、ACCEPT の数と REJECT の数の集計、REJECT のタイプごとの集計や再試行の集計などが含まれます。

次の表は、認証に関する統計情報フィールドの一覧です。この表では、認証が拒否された場合に考えられる原因についても示しています。

認証に関する統計情報	意味
[Transactions（トランザクション）]	
[Accepts]	ACCEPT 応答が返された RADIUS トランザクションの現在数、平均数、ピーク数。
[Rejects]	REJECT 応答が返された RADIUS トランザクションの現在数、平均数、ピーク数。[Reject Details（REJECT の詳細）] セクションに詳細が示される。
[Overall（全般）]	
[Total Transactions（合計トランザクション）]	[Accepts]、[Rejects]、[Silent Discards（廃棄）] の合計値。
[Silent Discards（廃棄）]	クライアントを識別できなかった要求の数。認証サービスを要求しているデバイスの名前または IP アドレス、あるいは両方に一致する RADIUS クライアント エントリーが見つからなかった場合に発生する可能性がある。
[Challenges]	RADIUS クライアントから受信した CHALLENGE の数。
[Reject Details（REJECT の詳細）]	
[Dropped Packet（パケットのドロップ）]	サーバで処理できるパケット数の上限を超過したため RADIUS によって破棄された RADIUS 認証パケットの数。
[Invalid Request（無効な要求）]	無効な RADIUS 要求の数 **考えられる原因：**デバイスから RADIUS に送信されるパケットが正しい形式になっていない。構成エラーが存在するか、またはデバイスが RADIUS 標準に準拠していないため。

認証に関する統計情報	意味
［Failed Authentication（認証失敗）］	ユーザー名またはパスワードが無効なため失敗した認証要求の数 **考えられる原因：**すべてのトランザクションの認証が失敗する場合は、RADIUS に入力された共有シークレットがクライアント デバイスで入力された共有シークレットに一致していない可能性がある。
［Failed on Checklist（チェックリストの失敗）］	認証に成功した要求のうち、チェックリスト要件を満たせなかった要求の数。
［Insufficient Resources（リソース不足）］	サーバ リソースに問題があるため発生した REJECT の数。
［Rejects Sent（REJECT の送信）］	
［Transactions Retried（再試行したトランザクション）］	重複する要求を 1 回以上受信した要求の数。
［Total Retry Packets（再試行パケットの合計）］	重複するパケットの受信数。

RADIUS サーバ統計情報の表示

Security Console は、RADIUS サーバの起動後に、統計情報のトラッキングを開始します。管理者が RADIUS サーバを再起動すると、Security Console は統計情報をクリアし、トラッキングを再度開始します。RADIUS ログ ファイルに統計情報を記録できます。

手順

1. Security Console で、［**RADIUS**］＞［**RADIUS Statistics（RADIUS 統計情報）**］＞［**RADIUS Server Statistics（RADIUS サーバ統計情報）**］の順にクリックします。
2. ［**Select a RADIUS Server（RADIUS サーバの選択）**］ドロップダウン リストから、統計情報を表示するサーバを選択します。
3. トランザクション タイプを選択します。
   - ［**Authentication（認証）**］：ACCEPT の数、REJECT の数、廃棄の数、CHALLENGE の数、REJECT と CHALLENGE の詳細。
   - ［**Accounting（アカウンティング）**］：START の数、STOP の数、ON の数、OFF の数、INTERIM の数、失敗と再試行の詳細。

RADIUS クライアントの統計情報

RSA Authentication Manager の Security Console には、RSA RADIUS クライアントの統計情報が表示されます。統計情報には、RADIUS クライアントの認証およびアカウンティングに関するデータが含まれています。

管理者が RADIUS クライアントに関連づけられている RADIUS サーバを起動すると、Security Console は統計情報のトラッキングを開始します。管理者が RADIUS サーバを再起動すると、Security Console は統計情報をクリアし、トラッキングを再度開始します。RADIUS ログ ファイルに統計情報を記録できます。

Security Console では、RADIUS クライアントの統計情報を表示する際に、次の 4 つのタイプから選択できます。

- ［Accounting Request Diagnostics（アカウンティング要求の診断）］
- ［Account Request Types（アカウンティング要求のタイプ）］
- ［Authentication Request Diagnostics（認証要求の診断）］
- ［Summary（サマリー）］

RADIUS クライアントの統計情報を表示するには、Security Console ヘルプのトピック「RADIUS クライアントの認証およびアカウンティング統計情報の表示」を参照してください。

認証の統計情報

認証では、有効なユーザーがネットワーク サービスを要求していることを検証します。認証の統計情報には、次のものがあります。

統計情報	説明
［Authentication Request Diagnostics（認証要求の診断）］	
［Retry Packets（再試行パケット）］	クライアントから関連づけられている RADIUS サーバに送信された重複メッセージの数。
［Invalid secrets（無効なシークレット）］	クライアントから関連づけられている RADIUS サーバに送信された無効なシークレットを含むメッセージの数。
［Challenges（チャレンジ）］	クライアントから関連づけられている RADIUS サーバに送信された CHALLENGE の数。
［Invalid requests（無効な要求）］	この RADIUS クライアントによって行われた無効な RADIUS 要求の数。たとえば、構成エラーが存在するか、またはデバイスが RADIUS 標準に準拠していないために、クライアントが RADIUS サーバに正しくない形式のパケットを送信しています。

統計情報	説明
[Invalid types (無効なタイプ)]	クライアントから関連づけられている RADIUS サーバに送信された無効な認証タイプの数。たとえば、クライアントが RADIUS 認証要求パケット以外の RADIUS パケットをサーバ の認証ポートに送信しました。
[Dropped Packets (パケットのドロップ)]	RADIUS クライアントが受信したパケットが処理できるパケット数の上限を超過したためにドロップされた RADIUS 認証パケットの数。

アカウンティングの統計情報

アカウンティングでは、ユーザーが使用するネットワーク リソースをトラッキングします。アカウンティングの統計情報には、次のものがあります。

統計情報	説明
[Accounting Request Diagnostics（アカウンティング要求の診断)]	
[Retry Packets (再試行パケット)]	クライアントから関連づけられている RADIUS サーバに送信された重複パケットの数。
[Invalid secrets (無効なシークレット)]	このクライアントから送信され、無効なシークレットを使用したため失敗したアカウンティング要求の数。
[Invalid requests (無効な要求)]	このクライアントから関連づけられているサーバに送信された無効な RADIUS 要求の数。たとえば、クライアントが正しく解析できない要求を送信しました。
[Invalid types (無効なタイプ)]	クライアントから関連づけられている RADIUS サーバに送信された無効なアカウンティング タイプの数。たとえば、クライアントがサーバの間違ったポートに要求を送信しました。
[Dropped Packets (パケットのドロップ)]	クライアントから関連づけられている RADIUS サーバに送信され、サーバがさまざまな理由（リソース エラーなど）でドロップした RADIUS アカウンティング パケットの数。
[Accounting Request Types（アカウンティング要求のタイプ)]	
[Starts]	クライアントから関連づけられている RADIUS サーバに送信された Accounting-Start メッセージの数。
[Stops]	クライアントから関連づけられている RADIUS サーバに送信された Accounting-Stop メッセージの数。
[Interim requests (Interim 要求)]	クライアントから関連づけられている RADIUS サーバに送信された Interim アカウンティング パケットの数。

統計情報	説明
［Ons］	RADIUS クライアントのリスタート時に、クライアントから関連づけられている RADIUS サーバに送信された Accounting-On メッセージの数。
［Offs］	RADIUS クライアントのシャットダウン時に、クライアントから関連づけられている RADIUS サーバに送信された Accounting-Off メッセージの数。
［Acks］	関連づけられている RADIUS サーバからクライアントに送信された ACK メッセージの数。

サマリー統計情報

サマリー統計情報には、認証およびアカウンティングの要求、ACCEPT、REJECT に関する情報が含まれます。

統計情報	説明
［Auth reqs（認証要求）］	このクライアントから関連づけられている RADIUS サーバに送信された認証要求の合計数。
［Accepts］	関連づけられている RADIUS サーバからクライアントに送信された ACCEPTッセージの数。
［Rejects］	関連づけられている RADIUS サーバからクライアントに送信された REJECT メッセージの数。
［Acct Reqs（アカウンティング要求）］	このクライアントから関連づけられている RADIUS サーバに送信されたアカウンティング要求の合計数。
［Starts］	このクライアントによって処理されたトランザクションのうち認証成功後にダイヤルイン接続が開始された数。
［Stops］	このクライアントによって処理されたトランザクションのうち RADIUS クライアントによってダイヤルイン接続が終了された数。

RADIUS クライアント統計情報の表示

RSA Authentication Manager では、RSA RADIUS クライアントの認証統計情報およびアカウンティング統計情報が表示されます。

手順

1. Security Console で、［**RADIUS**］＞［**RADIUS Statistics（RADIUS 統計情報）**］＞［**RADIUS Client Statistics（RADIUS クライアント統計情報）**］の順にクリックします。
2. ［**Select RADIUS Client（RADIUS クライアントの選択）**］ドロップダウンリストから、統計情報を表示するクライアントを選択し、そのクライアントが関連づけられている RADIUS サーバを選択します。
3. トランザクション タイプを選択します。
   - ［**Accounting Request Diagnostics（アカウンティング要求の診断）**］：重複するメッセージ、無効なシークレットが含まれているメッセージ、不正なメッセージ、不正なタイプが含まれているメッセージ、破棄された要求の数を RADIUS クライアントごとに示します。
   - ［**Accounting Request Types（アカウンティング要求のタイプ）**］：Accounting-Start メッセージ、Accounting-Stop メッセージ、Interim メッセージ、Accounting-On メッセージ、Accounting-Off メッセージ、Ack メッセージの数を RADIUS クライアントごとに示します。
   - ［**Authentication RequestDiagnostics（認証要求の診断）**］：重複するメッセージ、チャレンジ、無効な認証情報が含まれているメッセージ、無効な認証要求、無効なタイプ、廃棄された要求の数を、RADIUS クライアントごとに示します。
   - ［**Summary（サマリー）**］：認証要求の数、Access-Accept メッセージの数、Access-Reject メッセージの数、アカウンティング要求の数、, Accounting-Start メッセージの数、Accounting-Stop メッセージの数を RADIUS クライアントごとに示します。

アカウンティング属性および管理操作の記録

ユーザー認証時には、ユーザーが認証を試行するたびに RADIUS クライアントが属性を送信します。これらの情報は、RADIUS サーバによって収集されます。RADIUS サーバでは、これらの情報のうち課金目的または監視目的で必要になるものだけを保存できます。サーバでは、これらの情報がコンマ区切りファイルに書き込まれるため、スプレッドシートやその他のアプリケーションで読み取ることができます。

RADIUS ログ ファイルには、管理者の操作について、認証および Security Console または Operations Console を通じて行った変更が記録されます。

次の表は、アカウンティングおよびログ記録を設定するための構成ファイルについて示します。構成ファイルの変更の詳細については、346 ページの RADIUS サーバ ファイルの編集、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

ファイル名	機能
account.ini	RADIUS アカウンティング属性をログに記録する方法を制御します。
radius.ini	RADIUS がサーバ ログ ファイルに記録するメッセージのタイプやログ ディレクトリの場所などの設定を制御します。

RADIUS サーバ ログ ファイル

サーバ ログ ファイルには、サーバの起動やシャットダウン、ユーザーの認証や拒否などの RADIUS イベントが、一連のメッセージとして ASCII テキスト ファイルに記録されます。サーバ ログ ファイル内では、各行に RADIUS イベントの日時と詳細が示されます。RADIUS の稼働中に現在のログ ファイルを開くことができます。

サーバ ログ ファイルの最大サイズを指定することもできます。最大サイズを指定するには、**radius.ini** ファイルの［Configuration（構成）］セクションで LogfileMaxMBytes 設定にゼロ以外の値を入力します。

- 最大ファイル サイズを設定した場合は、サーバ ログ ファイルを開いた日時がサーバ ログ ファイルの名前に追加されます（YYYYMMDD_HHMM.log）。現在のサーバ ログ ファイルがメガバイト（1024×1024 バイト）単位の指定サイズにほぼ等しくなると、現在のログ ファイルが閉じられ、新しいログ ファイルが開かれます。閉じられたファイルのサイズは、最大サイズの指定値より若干小さくなります。
- 最大ファイル サイズを 0 に設定した場合（または LogfileMaxMBytes の設定を省略した場合）、サーバ ログ ファイルのサイズは無視され、ログ ファイルを開いた日付がログ ファイル名に使用されます（YYYYMMDD.log）。

注：ログ ファイルのサイズは、1 分おきにチェックされます。1 分に 2 回以上の頻度でログ ファイルをロール オーバーすることはできません。ログ ファイルのサイズは、サイズ チェック時に LogfileMaxMBytes の閾値を超えていなくても、前回のチェックが行われてから次回のチェックが行われるまでの間のタイミングで一時的に（1 分未満の時間内で）最大サイズの指定値を超える可能性があります。

サーバ ログ ファイルへの記録の詳細レベルは、LogLevel、LogAccept、LogReject、TraceLevel の各設定を通じて制御できます。

LogLevel 設定では、サーバ ログ ファイルの詳細レベルを決定します。LogLevel に設定できる値は、0、1、2 のいずれかです。0 の場合は情報量が最も少なくなり、1 の場合は中間的な詳細レベル、2 の場合は最も詳細なレベルになります。LogLevel 設定は、**radius.ini** ファイルの［Configuration（構成）］セクションおよび .aut ファイルの［Settings（設定）］セクションで指定します。

LogAccept フラグと LogReject フラグでは、サーバ ログ ファイルへの Access-Accept メッセージおよび Access-Reject メッセージの記録をオンまたはオフにできます。これらのフラグは **radius.ini** ファイルの［Configuration（構成）］セクションで指定します。値を 1 に設定すると対応するメッセージの記録がオンになり、0 に設定すると対応するメッセージの記録がオフになります。Access-Accept メッセージが記録されるのは LogAccept が 1 に設定されている場合のみで、Access-Reject メッセージが記録されるのは LogReject が 1 に設定されている場合のみです。さらに、どちらのメッセージについても、これらのメッセージの記録が可能な詳細レベルが LogLevel で指定されていることが前提となります。

TraceLevel 設定では、パケットを受信して処理しているときにパケットを記録するかどうか、記録する場合は、どの詳細レベルでログに記録するかを指定します。

アカウンティング ログ ファイルの使用

RADIUS アカウンティング イベントは、アカウンティング ログ ファイルに記録されます。アカウンティング イベントには、接続の開始を示す START（開始）メッセージ、接続の終了を示す STOP（停止）メッセージ、接続が継続中であることを示す INTERIM（処理中）メッセージがあります。

アカウンティング ログ ファイルでは、スプレッドシートやデータベース プログラムにインポートできるように、コンマ区切りの ASCII 形式が使用されています。デフォルトでは、アカウンティング ログ ファイルは RADIUS の database ディレクトリに保存されます。アカウンティング ログ ファイルは、yyyymmdd.ACT の形式のファイル名で保存されます。ここで、yyyy は 4 桁の年、mm は月、dd はログ ファイルの作成日です。

RADIUS の稼働中に現在のログ ファイルを開くことができます。

アカウンティング ログ ファイルの形式

各アカウンティング ログ エントリーの最初の 6 つのフィールドは、RADIUS が提供するフィールドです。ファイルの閲覧とソートに役立ちます。

- **Date**：イベントの発生日
- **Time**：イベントの発生時刻
- **RAS-Client**：アカウンティング レコード送信元の RADIUS クライアントの名前または IP アドレス

- **Record-Type**：RADIUS の標準アカウンティング パケット タイプ（START、STOP、INTERIM、ON、OFF のいずれか）
- **Full-Name**：RADIUS サーバによって実行される認証に基づくユーザーの完全識別名
- **Auth-Type**：実行された認証のクラスを示す番号：

  10：SecurID ユーザー

  11：SecurID プレフィックス

  12：SecurID サフィックス

デフォルトでは、Auth-Type 識別子の後ろに RADIUS の標準属性が続きます。詳細については、377 ページの RADIUS アカウンティング属性を参照してください。

記録される RADIUS の標準属性またはベンダー固有の属性の追加、削除、並べ替えを行うには、**account.ini** 初期設定ファイルを編集します。詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

アカウンティング ログ ファイルのヘッダとプレースホルダ

アカウンティング ログ ファイルの 1 行目は、ログに記録する属性の名前を、記録する順番に列挙したファイル ヘッダです。1 行目のサンプルを次に示します。このサンプルでは、必須フィールドを斜体の太字で示し、RADIUS の標準属性を太字で、ベンダー固有の属性を標準書式で示しています。

```
"Date","Time", "RAS-Client", "Record-Type", "Full-Name",
"Auth-Type", "User-Name", "NAS-Port", "Acct-Status-Type",
"Acct-Delay-Time", "Acct-Input-Octets", "Acct-Output-Octets",
"Acct-Session-Id", "Acct-Authentic","Acct-Session-Time",
"Acct-Input-Packets", "Acct-Output-Packets",
"Acct-Termination-Cause", "Acct-Multi-Session-Id",
"Acct-Link-Count","Acc-Err-Message",
"Nautica-Acct-SessionId","Nautica-Acct-Direction",
"Nautica-Acct-CauseProtocol","Nautica-Acct-CauseSource",
"Telebit-Accounting-Info","Last-Number-Dialed-Out",
"Last-Number-Dialed-In-DNIS","Last-Callers-Number-ANI",
"Channel","Event-Id","Event-Date-Time",
"Call-Start-Date-Time","Call-End-Date-Time",
"Default-DTE-Data-Rate","Initial-Rx-Link-Data-Rate",
"Final-Rx-Link-Data-Rate","Initial-Tx-Link-Data-Rate",
"Final-Tx-Link-Data-Rate","Sync-Async-Mode",
"Originate-Answer-Mode","Modulation-Type",
"Equalization-Type","Fallback-Enabled","Characters-Sent",
"Characters-Received","Blocks-Sent","Blocks-Received",
"Blocks-Resent","Retrains-Requested","Retrains-Granted",
"Line-Reversals","Number-Of-Characters-Lost",
"Number-of-Blers","Number-of-Link-Timeouts",
"Number-of-Fallbacks","Number-of-Upshifts",
"Number-of-Link-NAKs","Back-Channel-Data-Rate",
"Simplified-MNP-Levels","Simplified-V42bis-Usage", "PW_VPN_ID"
```

RSA RADIUS は、アカウンティング ログ ファイルにアカウンティング イベントを書き込みます。アカウンティング ログ ファイルに記録するイベントにデータのない属性がある場合は、コンマのプレースホルダによりエントリーが空であることが示されます。これにより、すべてのエントリーとヘッダの整合性が正しく維持されます。1 行目のヘッダが前出のサンプルのように定義されている場合のログ エントリーの例を次に示します。この例では、Acct-Status-Type 属性の値が 7 に設定されています。

```
"12/23/1997","12:11:55","RRAS","Accounting-On",
,,,,7,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,
```

RADIUS アカウンティング属性

次の表は、RFC 2866「RADIUS Accounting」で定義されている RADIUS の標準アカウンティング属性を示しています。

RADIUS のアカウンティング属性	説明
User-Name	クライアントが受信したユーザー名。
NAS-Port	クライアント デバイス上のポート番号。
Acct-Status-Type	ユーザー サービスの開始または終了を示す番号： 1：Start 2：Stop 3：Interim-Acct 7：Accounting-On 8：Accounting-Off
Acct-Delay-Time	クライアントがこのレコードの送信を試行している間に経過した秒数。サーバへの到着時刻からこの値を減算することにより、このリクエストを生成したイベントのおおよその発生時刻を求めることができる。
Acct-Input-Octets	接続先からポートが受信したオクテット（バイト）の数。STOP レコードの場合にのみ書き込まれる。
Acct-Output-Octets	ポートから接続先へ送信したオクテット（バイト）の数。STOP レコードの場合にのみ書き込まれる。
Acct-Session-Id	ログ ファイル内で START レコードと STOP レコードを照合するために使用される識別子。

RADIUS のアカウンティング属性	説明
Acct-Authentic	ユーザーの認証が RADIUS、ネットワーク アクセス デバイス（ローカル）、その他のリモート認証プロトコルのいずれによって行われたかを示す。 1：RADIUS 2：Local 3：Remote
Acct-Session-Time	接続の経過時間（秒単位）。STOP レコードの場合にのみ書き込まれる。
Acct-Input-Packets	接続先からポートが受信したパケット数。STOP レコードの場合にのみ書き込まれる。
Acct-Output-Packets	ポートから接続先へ送信したパケット数。STOP レコードの場合にのみ書き込まれる。
Acct-Termination-Cause	セッションの終了方法を示す番号。STOP レコードの場合にのみ書き込まれる。 1：User Request 2：Lost Carrier 3：Lost Service 4：Idle Timeout 5：Session Timeout 6：Admin Reset 7：Admin Reboot 8：Port Error 9：NAS Error 10：NAS Request 11：NAS Reboot 12：Port Unneeded 13：Port Preempted 14：Port Suspended 15：Service Unavailable 16：Callback 17：User Error 18：Host Request

RADIUS のアカウンティング属性	説明
Acct-Multi-Session-Id	複数の関連するセッションをログ ファイル内でまとめてリンクしやすくするための一意なアカウンティング識別子。
Acct-Link-Count	アカウンティング レコードの生成時に特定のマルチリンク セッション内で認識されていたリンクのカウント。

14 ログとレポート

ログ メッセージの概要

RSA Authentication Manager では、すべてのイベントに対してログ メッセージが生成されます。これらのメッセージは、メッセージの送信元に応じて、ログ ファイルおよびデータベース ファイルに格納されます。これらのログ ファイルを使用して、導入環境内のアクティビティを監視し、ユーザーのログオン要求や管理操作などのイベントの記録を生成できます。

ログ構成の変更をレプリケーションするように選択した場合を除き、ほとんどのログの設定はインスタンスごとに行われます。例外は、ログ ローテーションの設定です。これは、インスタンスごとに Operations Console で構成します。

システムでは、ほとんどの正常な読み取りアクションをログに記録しません。

ログのタイプ

Authentication Manager は次のタイプのログを保持します。

- **Administrative Audit（管理監査）**：ユーザーの追加や編集などの管理アクションを記録するログ メッセージ。このカテゴリーには、管理アクションのシステム レベルの障害は含まれません。これらのメッセージは、システム ログに記録されます。
- **Runtime Audit（ランタイム監査）**：ユーザーの認証や許可などのランタイム アクティビティをすべて記録するログ メッセージ。
- **System（システム）**：「Server started」や「Connection Manager lost db connection」などのシステム レベルのメッセージ。このカテゴリーには、管理アクションのシステム レベルの障害が含まれます。

ログ レベル

ログのタイプごとに、Security Console を使用して、ログ ファイルに書き込む詳細のレベルを構成できます。たとえば、Administrative Audit（管理監査）ログでは致命的エラーのみを記録し、System（システム）ログではすべてのメッセージを記録するよう選択できます。操作手順については、397 ページのアプライアンス ログ設定の構成を参照してください。

ログ レベルを変更してデフォルト値に戻すには、次の表に示した値を選択します。

ログ	デフォルト設定
Administrative Audit（管理監査）ログ	Success（成功）
Runtime Audit（ランタイム監査）ログ	Success（成功）
System（システム）ログ	Warning（警告）

トラブルシューティング ファイルのダウンロード

Operations Console を使用すると、ログとレポートをダウンロードして、トラブルシューティングに使用できます。これらのログ ファイルは製品バックアップには含まれないため、定期的にダウンロードすることでアーカイブできます。また、トラブルシューティング ファイルをダウンロードして、移行レポートを含む移行のログ ファイルにアクセスすることもできます。

ログ ファイルは、ダウンロードできるように .zip ファイルに圧縮されています。RSA カスタマー サポートでは、トラブルシューティングのためにこの .zip ファイルの提供をお願いする場合があります。この .zip ファイルには、hosts ファイル、IP アドレス、データベース スキーマなどの機密情報が格納されています。この .zip ファイルはパスワードで保護されています。.zip ファイルの内容を表示するには、Winzip バージョン 9 以上を使用します。

注：RSA カスタマー サポートに機密情報を知らせたくない場合は、RSA カスタマー サポートに提供する前に、.zip ファイルから機密情報を削除してください。RSA カスタマー サポート以外とは、.zip ファイルを共有しないでください。

開始する前に

スーパー管理者である必要があります。ただし、RSA Runtime Server がダウンした場合は、Operations Console のクレデンシャルを使用してこのページにアクセスできます。

手順

1. Operations Console で、**［Administration（管理）］＞［Download Troubleshooting Files（トラブルシューティング ファイルのダウンロード）］**の順にクリックします。
2. プロンプトが表示されたら、スーパー管理者のクレデンシャルを入力して、**［OK］**をクリックします。
3. ダウンロードするログを選択します。インスタンスがプライマリであるかレプリカであるかによって、表示されるオプションが異なります。

次の表に、使用可能なすべてのオプションを示します。

オプション	説明
Product Information（製品情報）	ライセンス関連情報、Authentication Manager およびオペレーティング システムのバージョン、構成済みのアイデンティティ ソースなど、Authentication Manager の構成の詳細を格納したファイル。
Authentication Manager Log Files（Authentication Manager のログ ファイル）	管理操作やユーザーのアクションなど、導入環境のアクティビティの詳細を格納したログ。ログ ファイルには、次のものが含まれます。 Authentication Manager インスタンスのログ Quick Setup のログ オペレーティング システム ファイル レプリケーション ログ ファイル 移行ログ ファイル
System Log Report（システム ログ レポート）（プライマリ インスタンスのみ）	導入環境のアクティビティ、管理操作、すべてのアクティビティの結果を CSV（コンマ区切り）ファイルに保存したレポート。

注：RSA Runtime Server、または内部データベースがダウンした場合、ダウンロードされるのは、［Product Information（製品情報）］オプションで取得できるファイルのサブセットのみです。またこの場合、［System Log Report（システム ログ レポート）］オプションは、プライマリ インスタンスではグレー表示になります。

4. ［**Create Password（パスワードの作成）**］フィールドに、有効なパスワードを入力します。
5. 確認のためパスワードを再入力します。
   パスワードを間違いのないようにメモします。.zip アーカイブ ファイルの内容を表示するには、このパスワードが必要です。また、.zip アーカイブ ファイルを RSA カスタマー サポートに提供する場合は、このパスワードも提供する必要があります。
6. ［**Generate and Download Zip File（Zip ファイルの生成とダウンロード）**］をクリックします。
   進行状況が、［**Progress Monitor（進行状況）**］ページに表示されます。完了まで数分かかる場合があります。
7. ［**Progress Monitor（進行状況）**］ページで、［**Download Zip File（Zip ファイルのダウンロード）**］をクリックします。

リアルタイム監視

導入環境をリアルタイムで監視するには、次のいずれかのツールを使用します。

ツール	詳細情報
Activity Monitor	384 ページのリアルタイム監視
リモートおよびローカルの Syslog	397 ページのアプライアンス ログ設定の構成 412 ページのリアルタイム ログ監視用のリモート Syslog ホストの構成
SNMP（Simple Network Management Protocol）	405 ページの SNMP の概要
ユーザー ダッシュボードの Runtime Activity Monitor	Security Console ヘルプのトピック「User Dashboard（ユーザー ダッシュボード）」

複数のアクティビティ モニタを使用したリアルタイム モニタリング

複数のアクティビティ モニタを使用し、ログ エントリーなど、Authentication Manager のアクティビティをリアルタイムに表示できます。アクティビティ モニタは 4 種類あり、それぞれが別々のブラウザ ウィンドウで開きます。また、表示される情報のタイプも異なります。

モニタ	表示情報
認証アクティビティ	• 認証を行うユーザー • 認証リクエストのソース • 認証に使用されたサーバ
システム アクティビティ	• アクティビティの発生時刻 • アクティビティの説明 • アクティビティの成否 • アクティビティの発生したサーバ
管理アクティビティ	ユーザーの追加や削除などの変更。
ユーザー ダッシュボードのランタイム アクティビティ モニタ	• 特定の 1 ユーザの過去 7 日間のリアルタイム認証アクティビティ ログ • アクティビティの発生時刻、アクティビティの結果、アクティビティの説明

表示情報はカスタマイズできます。たとえば、管理アクティビティ モニタを使用して特定の管理者、ユーザー ID、認証エージェント、セキュリティ ドメインのアクティビティを表示できます。

複数のアクティビティ モニタのウィンドウを同時に開くことができます。たとえば、特定の管理者、ユーザー グループ全体、セキュリティ ドメイン全体を同時に監視できます。

アクティビティ モニタを一時停止して、特定のログ メッセージをレビューできます。モニタを再開すると、アクティビティ モニタの一時停止中に生成されたログ メッセージがすべて、アクティビティ モニタの表示の一番上に追加されます。

新しいメッセージの数が、表示用に指定したメッセージ数を上回る場合は、最新のメッセージのみが表示されます。たとえば、100 個のメッセージを表示するようにモニタを構成し、新規メッセージが 150 個ある場合には、100 個の最新のメッセージのみが表示されます。

Security Console の［User Dashboard（ユーザー ダッシュボード）］ページでも、ユーザーの認証アクティビティを表示できます。詳細については、RSA Security Console ヘルプのトピック「ユーザー ダッシュボード」を参照してください。

アクティビティ モニタでのメッセージ表示

この処理手順を使用し、アクティビティ モニタにメッセージを表示して問題を解決します。

手順

1. Security Console で、［**Reporting（レポート）**］＞［**Real-time Activity Monitors（リアルタイム アクティビティ モニタ）**］の順にクリックし、使用可能なアクティビティ モニタを選択します。
2. アクティビティ モニタに表示するログ メッセージの条件を指定します。すべてのアクティビティを表示する場合は、これらのフィールドを空白のままにします。
3. ［**Start Monitor（モニタ開始）**］をクリックします。
4. 確認したいメッセージが表示されたら、［**Pause Monitor（モニタ一時停止）**］をクリックします。
5. 確認したいメッセージの日時をクリックします。

レポート

レポートでは、導入環境のユーザー、管理者、システム アクティビティに関して、ログに記録された情報およびリアルタイムの情報にアクセスできます。この情報は、トラブルシューティング、セキュリティ上の問題の監査、さまざまなポリシーへのコンプライアンス対応に役立ちます。

用意されているいずれかのテンプレートを使用してレポートを作成できます。各テンプレートでは、報告する情報のタイプを選択することや、情報を絞り込むために適用するパラメータを選択することができます。たとえば、All Users（すべてのユーザー）テンプレートを使用して、導入環境でリスクベース認証が有効化されたすべてのユーザーの苗字および名前をリストするレポートを作成できます。

レポートを作成して保存したら、管理者はいつでも手動でそのレポートを実行できます。操作手順については、RSA Security Console ヘルプのトピック「レポート ジョブの実行」を参照してください。指定した日時にレポートを自動的に実行するようにスケジュールを設定することもできます。操作手順については、RSA Security Console ヘルプのトピック「反復レポート ジョブのスケジュール」を参照してください。

レポート出力は、Security Console で表示するか、CSV ファイル、XML ファイル、HTML ファイルとしてダウンロードすることもできます。

管理者ロールごとの実行可能なレポート

それぞれの管理者が実行できるレポートは管理者権限によって決まります。事前定義された管理者ロールには、デフォルトのレポート作成権限が割り当てられています。次の表に、事前定義された管理者ロールと、それぞれのロールに実行権限があるレポートを示します。権限を拡張する場合は、事前定義されたロールを変更することができます。

注：セキュリティ ドメインの表示権限を持たない管理者が実行できるレポート作成機能には制限があります。管理者がセキュリティ ドメインを表示できるようにすることを推奨します。

管理者ロール					
レポート名	**Help Desk Admin（ヘルプデスク管理者）**	**User Admin（ユーザー管理者）**	**Agent Admin（エージェント管理者）**	**Security Domain Admin（セキュリティドメイン管理者）**	**Super Admin（スーパー管理者）**
Administrator Activity（管理者アクティビティ）					○
Administrators of a Security Domain（セキュリティ ドメインの管理者）		○	○	○	○
Administrators with a Specified Role（指定したロールの管理者）				○	○
Administrators with Fixed Passcode（固定パスコードを持つ管理者）		○	○	○	○
Agent Not Updated By Auto-registration More than Given Number of Days（指定された日数を超えて自動登録で更新されないエージェント）		○	○	○	○
Agents with Unassigned IP Address（IP アドレスが未割り当てのエージェント）		○	○	○	○
All User Groups（すべてのユーザー グループ）		○	○	○	○
All Users（すべてのユーザー）		○	○	○	○
Authentication Activity（認証アクティビティ）					○
Distributed Token Requests（配布済みのトークン リクエスト）					○
Expired User Accounts（期限切れのユーザー アカウント）		○	○	○	○

管理者ロール					
レポート名	**Help Desk Admin（ヘルプデスク管理者）**	**User Admin（ユーザー管理者）**	**Agent Admin（エージェント管理者）**	**Security Domain Admin（セキュリティドメイン管理者）**	**Super Admin（スーパー管理者）**
List all RSA Agent with assigned RADIUS client/RADIUS server（RADIUS クライアント /RADIUS サーバが割り当てれたすべての RSA エージェントのリスト）		○	○	○	○
List all RSA Agents with assigned RADIUS profile（RADIUS プロファイルが割り当てられたすべての RSA エージェントのリスト）		○	○	○	○
List all Users with assigned RADIUS profile（RADIUS プロファイルが割り当てられたすべてのユーザーのリスト）		○	○	○	○
Object Lifecycle Activity（Non User/User Group）（オブジェクトのライフサイクル アクティビティ（ユーザー / ユーザー グループ以外））					○
Risk-Based Authentication（RBA）Activity（RBA アクティビティ）					○
Risk-Based Authentication（RBA）Activity Users（RBA アクティビティ ユーザー）		○	○	○	○
Software Token（ソフトウェア トークン）		○	○	○	○
System Log Report（システム ログ レポート）					○
Token Expiration Report（トークン期限切れレポート）		○	○	○	○

管理者ロール					
レポート名	**Help Desk Admin（ヘルプデスク管理者）**	**User Admin（ユーザー管理者）**	**Agent Admin（エージェント管理者）**	**Security Domain Admin（セキュリティ ドメイン管理者）**	**Super Admin（スーパー管理者）**
User and User Group Lifecycle Activity（ユーザーおよびユーザー グループのライフサイクル アクティビティ）					○
User and User Groups Missing from Identity Source（アイデンティティ ソースから消えたユーザーおよびユーザー グループ）		○	○	○	○
Users Enabled for On-Demand Authentication（On-Demand 認証が有効なユーザー）		○	○	○	○
Users Enabled for On-Demand Tokencode Service Who Have Never Logged In（On-Demand トークンコード サービスが有効な未ログインユーザー）		○	○	○	○
User Never Logged On with Token（トークンを使用して一度もログオンしていないユーザー）		○	○	○	○
"Users with Days Since Last Login Using Specific Token（特定のトークンタイプの最終ログイン日が指定期間に含まれるユーザー）		○	○	○	○
Users with Disabled Accounts（無効なアカウントのユーザー）		○	○	○	○
Users with Tokens（トークン所有ユーザー）		○	○	○	○
Users with Tokens Set Online Emergency Access Tokencode（オンライン エマージェンシー アクセス トークンコードが設定されたトークンを持つユーザー）		○	○	○	○

スケジュール レポート ジョブ

スケジュール レポート ジョブでは、指定したスケジュールに従ってレポートを作成します。スケジュール レポート ジョブを作成する場合は、次のパラメータを構成できます。

［**Job Starts（ジョブの開始）**］：反復レポート ジョブの最初のインスタンスを実行する日付。

［**Frequency（頻度）**］：反復レポートの頻度。

- ［Daily（毎日）］または［Weekly（毎週）］：レポートを毎日実行するか、特定の日（複数日も可）に実行することができます。
- ［Monthly（毎月）］：レポートを毎月実行するか、特定の月に実行することができます。レポートを実行する日を指定することもできます。

［**Run Time（実行時間）**］：レポートを実行する時刻。

［**Job Expires（ジョブの有効期限）**］：反復レポート ジョブが終了する日付。有効期限なしを選択するか、特定の日付を入力できます。

［**Input Parameter（入力パラメータ）**］：レポート結果のフィルタを指定します。使用可能な値は、レポートによって異なります。たとえば、無効なユーザー アカウントに関するレポートの場合、特定の名前を持つ無効なアカウントのみをレポートに表示できます。

カスタム レポート

システムのイベントとオブジェクトに関するカスタム レポートを作成して実行できます。

たとえば、無効なユーザー アカウントをすべて表示するレポートを作成できます。ユーザー ID、名前、アイデンティティ ソース、セキュリティ ドメインなどの関連情報を含むレポートを設計することができます。

管理者アクティビティを表示するレポートを作成することができます。たとえば、すべての管理者のアクティビティのレポートを作成したり、1 人の管理者の詳細な情報を表示したりできます。

カスタム レポートは、Authentication Manager の事前定義のレポートテンプレートを使用して作成できます。各テンプレートには、定義済みの変数セット、列見出し、その他のレポート情報が含まれています。テンプレートのリストについては、386 ページの管理者ロールごとの実行可能なレポートを参照してください。

カスタム レポートはテンプレートを基盤として作成します。テンプレートには、入力パラメータや出力列など、一連のデータの起点が定義されています。表示する列、データ フィルタの適用、実行オプションの変更などを決定できます。

レポートの追加

導入環境に関する情報を生成するためのレポートを追加します。追加するタイプのレポートのレポート テンプレートを選択し、レポートで提供する特定の情報に合わせてテンプレートをカスタマイズします。

手順

1. Security Console で、[**Reporting（レポート作成）**] > [**Reports（レポート）**] > [**Add New（新規追加）**] の順にクリックします。
2. [(Select Template) テンプレートの選択] ページで、レポートのテンプレートを選択します。
   それぞれのテンプレートには異なる入力パラメータと出力列が含まれています。[**Description（説明）**] 列には、各テンプレートのサマリーが表示されます。
3. [**Next（次へ）**] をクリックします。
4. [**Security Domain（セキュリティ ドメイン）**] メニューから、レポートを管理するセキュリティ ドメインを選択します。
   セキュリティ ドメインによって、レポートを管理できる管理者が決まります。
5. [**Report Name（レポート名）**] フィールドに、レポートの一意の名前を入力します。
   最大文字数は 64 文字です。&、%、>、< の各文字は使用できません。
6. [**Run As**（実行ユーザー）] で、次のいずれかのオプションを選択します。
   - [**The administrator running the report job（レポート ジョブを実行する管理者）**]。レポート データは、レポートを実行した管理者の権限適用範囲に制限されます。
   - [**The report creator（レポート作成者）**]。レポート データは、レポートを作成した管理者の権限適用範囲に制限されます。レポートを実行する管理者の権限適用範囲がレポート作成者の権限適用範囲より狭い場合、レポートにはレポート作成者の広い権限適用範囲のデータが含まれます。

   レポートを作成した管理者のみが [**Run As（実行ユーザー）**] オプションを変更できます。
7. [Output Columns（出力列）] セクションで、レポートに表示する項目を [**Available（選択可能）**] から、[**Show in Report（レポートに表示）**] に移動します。
8. [Input Parameter Values（入力パラメータ値）] セクションで、値を入力するか、またはフィールドを空白のままにしておきます。
   フィールドを空白のままにした場合、管理者は、レポートを実行するときに値を設定できます。値を入力した場合、管理者は、レポートを実行するときにこれらの値を使用する必要があります。特定のロールを持つ管理者をレポートに含めるには、ロール名を指定する必要があります。この名前の大文字と小文字は区別されます。
9. [**Save（保存）**] をクリックします。

次のステップ

レポートは手動で実行することも、指定した時間に実行するようにスケジュール設定することもできます。

完了したレポート

Security Console では、実行中のレポートやレポート キューで実行を待機しているレポートの一覧を表示できます。また、完了したレポートを表示したり、ダウンロードすることができます。[Report Output（レポート出力）] ページでは、レポート ジョブが、[Completed（完了）] タブと [In Progress（実行中）] タブに分かれて表示されます。ステータスに基づいてレポート ジョブを表示したり、検索条件を使用して特定のレポート ジョブを検索したりできます。

完了したレポートは、次の方法で表示できます。

- 個別のブラウザ ウィンドウに表示し、表示後に保存できます。
- ダウンロードして CSV ファイルに保存します。
- ダウンロードして XML ファイルに保存します。
- ダウンロードして HTML ファイルに保存します。

操作手順については、RSA Security Console ヘルプのトピック「View In Progress Report Jobs and Completed Reports（実行中のレポート ジョブと完了したレポートの表示）」を参照してください。

サンプル レポート

このセクションでは、次のレポート テンプレートを使用したサンプル レポートを紹介します。

- All Users（すべてのユーザー）
- Users with Tokens（トークン所有ユーザー）
- Authentication Activity（認証アクティビティ）
- System Log（システム ログ）

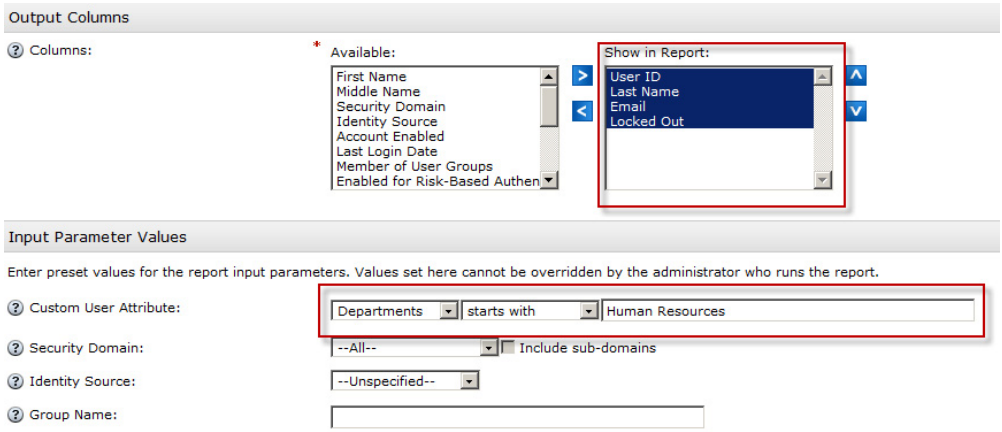
All Users（すべてのユーザー）レポートのサンプル

All Users（すべてのユーザー）レポートは、導入環境内のユーザーに関する情報を提供します。カスタム ユーザー属性、セキュリティ ドメイン、グループなどの入力値に基づいて結果をフィルタできます。

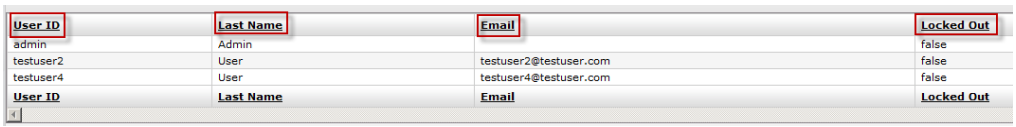
たとえば、部門がカスタム ユーザー属性として定義されている場合は、特定の部門内の全ユーザーを列挙したレポートを生成できます。

次の例では、Departments（部門）というカスタム ユーザー属性があり、Human Resources（人事）、Finance（財務）、IT という値が事前に定義されています。

たとえば、Human Resources（人事）部門に所属する全ユーザーを、その User ID（ユーザー ID）、Last Name（苗字）、Email（メール）、Lockout Status（ロックアウト ステータス）とともに列挙するレポートを生成するとします。［Add a New Report（新しいレポートの追加）］ページの［Custom User Attribute（カスタム ユーザー属性）］フィールドで、［Departments（部門）］を選択します。検索文字列として Human Resources（人事）と入力します。［Show in Report（レポートに表示）］に次の列を追加します。



次の図にレポートの出力を示します。赤色でハイライト表示されている列ヘッダは、［Add a New Report（新しいレポートの追加）］ページで定義されているものと同じです。

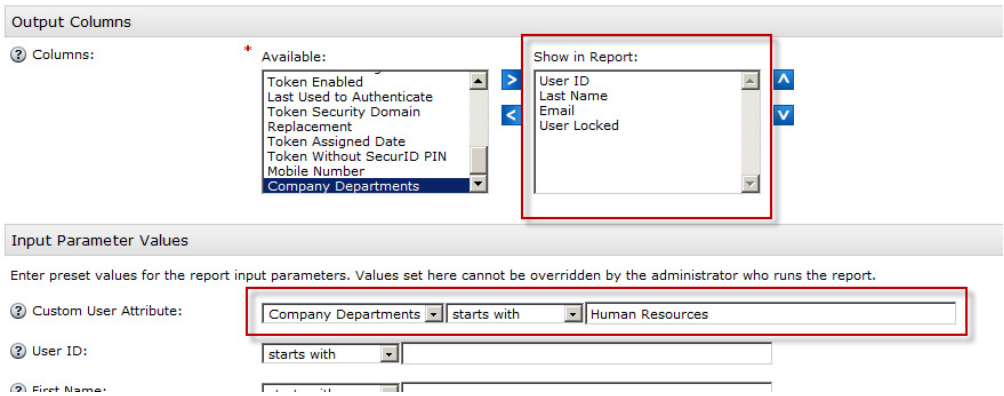


User ID	Last Name	Email	Locked Out
admin	Admin		false
testuser2	User	testuser2@testuser.com	false
testuser4	User	testuser4@testuser.com	false
User ID	Last Name	Email	Locked Out

Users with Tokens（トークン所有ユーザー）レポートのサンプル

Users with Tokens（トークン所有ユーザー）レポートには、トークンが割り当てられているユーザーが列挙されます。カスタム ユーザー属性などの入力パラメータ値を使用して、結果を絞り込むことができます。

たとえば、Human Resources（人事）部門に所属するユーザーの User ID（ユーザー ID）、First Name（名前）、Last Name（苗字）と、各アカウントのロックアウト ステータスを列挙するレポートを生成するとします。次の図に示すように、出力列と入力パラメータを指定します。



次の図にレポートの出力を示します。赤色でハイライト表示されている列ヘッダは、[Add a New Report（新しいレポートの追加）] ページで定義されているものと同じです。

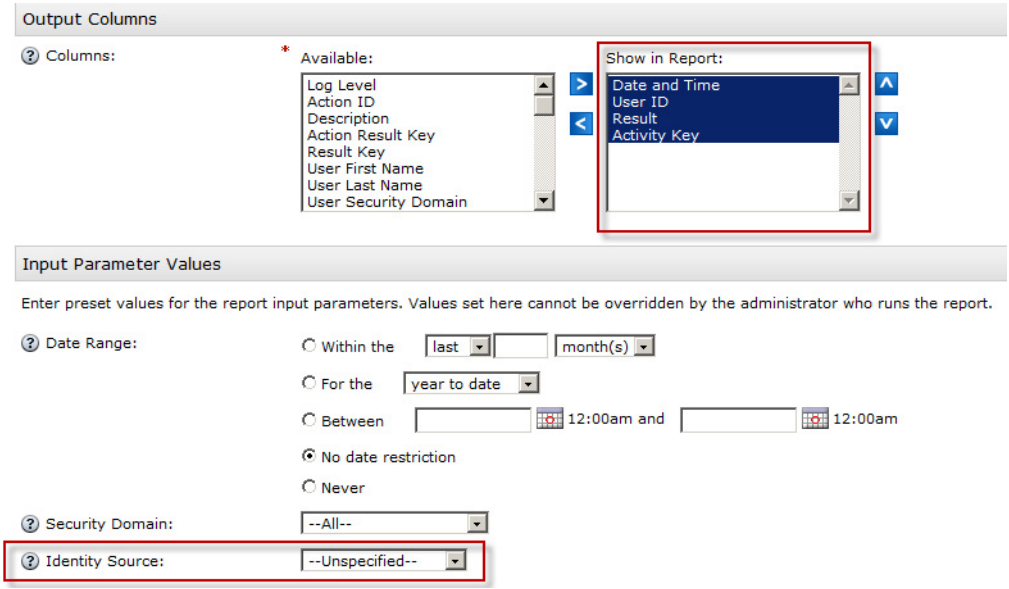
User ID	Last Name	Email	User Locked
admin	Admin		FALSE
testuser2	User	testuser2@testuser.com	FALSE
testuser2	User	testuser2@testuser.com	FALSE
testuser9	User	testuser9@testuser.com	FALSE
User ID	Last Name	Email	User Locked

Authentication Activity（認証アクティビティ）レポートのサンプル

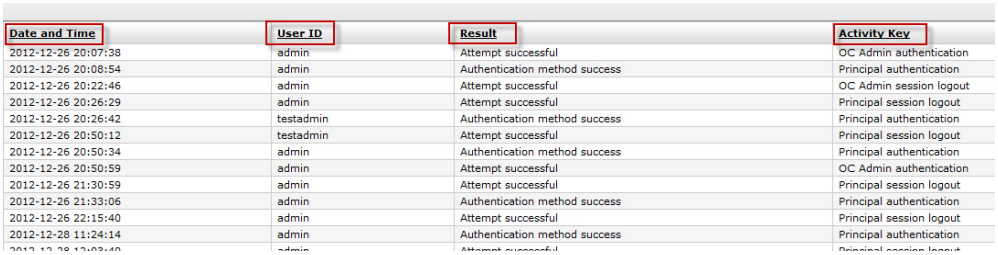
Authentication Activity（認証アクティビティ）レポートは、次のタイプの認証アクティビティをトラッキングするのに役立ちます。

- Security Console と Operations Console へのログイン
- トークン所有ユーザーによる認証
- サーバ上のエージェントでの認証

たとえば、複数のアイデンティティ ソースを対象として、ユーザー ID、認証の日時、試行の結果、発生したアクティビティのタイプを列挙する Authentication Activity（認証アクティビティ）レポートを生成するとします。次の図に示すように、出力列と入力パラメータ値を指定します。



次の図にレポートの出力を示します。赤色でハイライト表示されている列ヘッダは、[Add New Report（新しいレポートの追加）] ページで定義されているものと同じです。

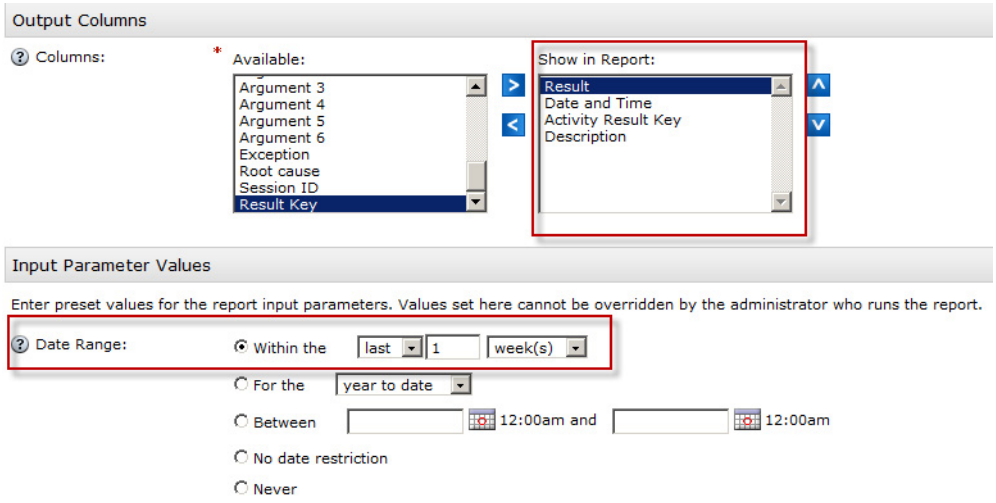


Date and Time	User ID	Result	Activity Key
2012-12-26 20:07:38	admin	Attempt successful	OC Admin authentication
2012-12-26 20:08:54	admin	Authentication method success	Principal authentication
2012-12-26 20:22:46	admin	Attempt successful	OC Admin session logout
2012-12-26 20:26:29	admin	Attempt successful	Principal session logout
2012-12-26 20:26:42	testadmin	Authentication method success	Principal authentication
2012-12-26 20:50:12	testadmin	Attempt successful	Principal session logout
2012-12-26 20:50:34	admin	Authentication method success	Principal authentication
2012-12-26 20:50:59	admin	Attempt successful	OC Admin authentication
2012-12-26 21:30:59	admin	Attempt successful	Principal session logout
2012-12-26 21:33:06	admin	Authentication method success	Principal authentication
2012-12-26 22:15:40	admin	Attempt successful	Principal session logout
2012-12-28 11:24:14	admin	Authentication method success	Principal authentication

System Log Report（システム ログ レポート）のサンプル

System Log Report（システム ログ レポート）には、システム ログのログ エントリーが列挙されます。入力パラメータ値を使用すると、結果を特定の期間に絞り込むことができます。

たとえば、システム ログ内のイベントの Result（結果）、Activity Result Key（アクティビティ結果キー）、Date and Time（日時）、Description（説明）を過去 1 週間分列挙するレポートを生成するとします。次の図に示すように、出力列と入力パラメータを指定します。



次の図にレポートの出力を示します。赤色でハイライト表示されている列ヘッダは、[Add New Report（新しいレポートの追加）] ページで定義されているものと同じです。

Result	Date and Time	Activity Result Key	Description
Adjudicator detected clock set forward	2013-01-28 13:54:19	Warning	Detected clock setforward, current:"1/28/13 8:24 AM" expected:"1/25/13 2:17 PM"
Adjudicator detected clock set forward	2013-01-30 00:22:44	Warning	Detected clock setforward, current:"1/29/13 6:52 PM" expected:"1/29/13 6:52 PM"
Adjudicator detected clock set forward	2013-01-30 02:14:52	Warning	Detected clock setforward, current:"1/29/13 8:44 PM" expected:"1/29/13 8:44 PM"
Attempt successful	2013-01-24 13:33:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 13:43:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 13:53:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:03:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:13:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:23:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".

アプライアンス ログのローテーション ポリシー

アプライアンス ログ ファイルには、仮想アプライアンスのオペレーティング システムのメッセージが含まれます。アプライアンス では、ログ データの管理を簡略化するために、ログ ローテーション ポリシーに従いアプライアンス ログを複数のファイルに保存します。このポリシーを定義できます。

アプライアンスは、アプライアンス ログごとに 1 つの初期ファイルを作成します。このファイルが指定されたサイズまたは時間制限（毎日、毎週、毎月）に達した場合、アプライアンスはファイル名に日付を追加して名前を変更し、その後新しいログファイルへの記録を開始します。たとえば、システムログ ファイルの初期ファイル名は messages ですが、2012/06/30 のローテーション時に messages-20120630 という名前に変更されます。ローテーション後、messages という名前の新しいファイルがシステムによって作成され、最新のログ メッセージが記録されます。

ログ ファイルを圧縮して、必要なストレージ領域を減らすことができます。たとえば、ローテーションされたログ ファイルを bzip2 で圧縮する場合、前の例のファイルの名前は **messages-20120630.bz2** になります。

削除するアプライアンス ログ ファイルをシュレッダ処理で上書きし、機密情報を復元できないようにできます。たとえば、削除するファイルを 7 回上書きするようにシステムに指定できます。回数が多いほど安全性が高まりますが、回数を少なくすることにより必要なシステム リソースも少なくなります。

アプライアンスでは、作成したログ ファイルが最大数に達すると、最も古いローテーション済みログ ファイルを削除してから、現在のファイルをローテーションさせます。たとえば、ファイルの最大数が 5 個に設定されている場合は、5 個のローテーション済み **messages** ファイルが作成されると、アプライアンスは最も古いファイルを削除してから現在の **messages** ファイルをローテーションさせます。

アプライアンス ログ設定の構成

ログ ローテーション設定により、アプライアンスのオペレーティング システムのログが無制限に増大するのを防ぐことができます。管理者は、アプライアンス ログのローテーションの方法とタイミングを構成できます。

アプライアンス ログでは、syslog エントリー、アプライアンスの SNMP メッセージ、NTP（Network Time Protocol）サーバの更新などの項目を追跡できます。Authentication Manager のログでは、レプリカ インスタンスの追加やユーザーの認証など、製品固有のアクティビティを追跡します。

Authentication Manager のログ設定は、Security Console で構成します。

手順

1. Operations Console で、［**Administration（管理）**］＞［**Log Rotation Settings（ログ ローテーション設定）**］の順にクリックします。
2. ［**Log Rotation Options（ログ ローテーション オプション）**］フィールドで、次のいずれかを実行します。
   - ［**Rotate when the maximum file size reached is** <n> **KB（ファイル サイズが指定した最大値になったらローテーションする：＜数値＞ KB）**］を選択し、サイズに基づいてログ ファイルをローテーションさせます。最大ファイル サイズを入力します。
   - ［**Rotate（ローテーション）**］を選択し、ログ ファイルを毎日、毎週、毎月のいずれの間隔に基づいてローテーションさせます。

   ログ ファイルが指定したサイズに達するか、指定した期間が経過すると、アプライアンスはローテーションする ファイルの名前を、月、日、年を付加して変更します。アプライアンスは、新しいログ ファイルへの書き込みを開始します。

3. ［**Compression Options（圧縮オプション）**］フィールドで、［**Compress rotated log files（ローテーションしたログ ファイルを圧縮する）**］を選択すると、ローテーションしたファイルの保存に必要なディスク領域を削減できます。
4. ［**Shred Options（シュレッダ オプション）**］フィールドでは、削除したログファイルの復元をより困難にするため、上書きすることを選択できます。
5. ［**Maximum Number of Files Allowed（ファイルの最大数）**］フィールドで、システムに保持するローテーションされたログファイルの最大数を指定します。
   ローテーションされたログファイルが最大数に達すると、アプライアンスは、現在のログ ファイルをローテーションさせる前に最も古いログ ファイルを削除します。ファイルの最大数には、アクティブなログ ファイルは含まれません。
6. ［**Save（保存）**］をクリックします。

変更を保存していない場合は、［**Reset（リセット）**］をクリックすると、ログのローテーション設定を編集開始前の状態にリセットできます。

ログ ファイルの使用

ログ ファイルに対して次のような操作を実行できます。

- ログ アーカイブ
- アーカイブされたログ ファイルの完全性の検証
- ログ メッセージのローカルファイルへの保存
- ローカル ログ ファイルの最大ログ ファイル数の設定
- ローカル ログ ファイルの最大サイズの設定
- ログ内のトークン シリアル番号のマスク

ログ アーカイブ

ログ ファイルをアーカイブすることで、ログオン試行や Security Console の管理操作など、導入環境内のすべてのアクティビティの履歴を保持できます。アーカイブされたログ ファイルを調べて、問題をトラブルシューティングすることや、セキュリティ上の問題を監査することができます。

Security Console を使用して、次の方法でログ ファイルをアーカイブします。

- ワン タイム ログ アーカイブ ジョブのスケジュール。操作手順については、RSA Security Console ヘルプのトピック「今すぐアーカイブを使用したログのアーカイブ」を参照してください。

- 定期的ログ アーカイブ ジョブのスケジュール。定期的アーカイブ ジョブは、指定された日、週、月に自動的に実行されます。操作手順については、RSA Security Console ヘルプのトピック「スケジュール ログ アーカイブによるログのアーカイブ」を参照してください。

ログ アーカイブを管理する次の操作を実行できます。

- 指定した日数以上格納されているオンライン ログ データをパージしてエクスポートする
- 指定した日数以上格納されているオンライン ログ データをエクスポートする
- 指定した日数以上格納されているオンライン ログ データをパージする
- オンライン ログ データをパージおよびエクスポートしない

アーカイブされたログ ファイルの完全性の検証

Verify Archive Log ユーティリティ（verify-archive-log）を使用すると、ログ ファイルが改ざんされていないことを検証できます。

開始する前に

一連のログ イベントが変更されていないことを保証するために、システムはログ ファイルの完全性を検証する必要があります。ログ ファイルの完全性が検証済みかどうかを判断するには、ログ ファイルを保存したディレクトリを確認します。完全性を検証済みのログ ファイルには、同じ名前の *.log ファイルと *.sig ファイルがあります。

処理手順

1. アプライアンスにログオンします。
2. ユーザーを rsaadmin ユーザーに切り換えます。
   a. 次のように入力し、Enter キーを押します。

      ```
      sudo su rsaadmin
      ```

   b. プロンプトに従って、オペレーティング システムのアカウント パスワードを入力して Enter キーを押します。
3. ディレクトリを Authentication Manager ユーティリティのディレクトリに変更します。次のように入力し、Enter キーを押します。

   `cd /opt/rsa/am/utils`
4. 次のように入力し、Enter キーを押します。

   ```
   ./rsautil verify-archive-log -f log_filename
   ```

   log_filename は、検証するログファイルの名前と拡張子です。
5. プロンプトに従って、Operations Console 管理者ユーザー名とパスワードを入力します。

Operations Console 管理者パスワードを入力した後、ユーティリティからログ ファイルの検証ステータスが返されます。ステータスは、検証が成功したら［VERIFIED（正常）］、失敗したら［TAMPERED（改ざん）］になります。

ユーティリティからファイルの完全性を検証できないというエラーが返された場合、そのファイルがシステムによって検証済みであるかを確認します。

ログ メッセージのローカルファイルへの保存

すべてのログオン リクエストと Security Console を使用して実行されるすべての操作の監査証跡を維持するため、ログメッセージを収集することができます。ローカル ファイルにログメッセージを送信するよう、Authentication Manager を構成する必要があります。

ローカル ログ ファイルは、次の場所にあります。

- 管理：**RSA_AM_HOME/server/logs/imsAdminAudit.log**
- ランタイム：**RSA_AM_HOME/server/logs/imsRuntimeAudit.log**
- システム：**RSA_AM_HOME/server/logs/imsSystem.log**

これらの場所は変更できません。

すべてのインスタンスでログメッセージをローカルファイルに送信するよう構成

導入環境のすべてのインスタンスで、ローカル ファイルにログメッセージを送信するよう構成するには、この処理手順を実行します。

開始する前に

この処理手順は、Linux オペレーティング システムの知識があることを前提としています。必要な知識がない場合は、この処理手順を実行しないでください。

処理手順

1. プライマリ インスタンスにログオンし、ユーザーを rsaadmin に変更します。
2. ディレクトリを **RSA_AM_HOME\utils** に変更します。次のコマンドの 1 つを入力し、Enter キーを押します。

   管理ログ：

   ```
   ./rsautil store -a config_all
   ims.logging.audit.admin.datastore database,file
   ```

   ランタイム ログ：

   ```
   ./rsautil store -a config_all
   ims.logging.audit.runtime.datastore database,file
   ```

   システム ログ：

   ```
   ./rsautil store -a config_all
   ims.logging.system.datastore database,file
   ```

3. プロンプトに従って、Operations Console 管理者パスワードを入力して Enter キーを押します。

1 つのインスタンスでログメッセージをローカルファイルに送信するよう構成

導入環境の 1 つのインスタンスで、ローカル ファイルにログメッセージを送信するよう構成するには、この処理手順を実行します。

開始する前に

この処理手順は、Linux オペレーティング システムの知識があることを前提としています。必要な知識がない場合は、この処理手順を実行しないでください。

処理手順

1. プライマリ インスタンスにログオンし、ユーザーを rsaadmin に変更します。
2. 完全修飾ホスト名を確認するため、Security Console にログオンし、［Setup（セットアップ）］＞［**System Settings（システム設定）**］＞［**Basic Settings（基本設定）**］＞［**Logging（ログ）**］の順にクリックします。
3. ディレクトリを **RSA_AM_HOME\utils** に変更します。次のコマンドの 1 つを入力し、Enter キーを押します。

   管理ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.audit.admin.datastore database,file host_name
   ```

   host_name には、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名を指定します。

   ランタイム ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.audit.runtime.datastore database,file
   host_name
   ```

   host_name には、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名を指定します。

   システム ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.system.datastore database,file host_name
   ```

   host_name には、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名を指定します。
4. プロンプトに従って、Operations Console 管理者パスワードを入力して Enter キーを押します。

ローカル ログ ファイルの最大ログ ファイル数の設定

保存するローカル ログ ファイルの数を構成できます。最大数に達すると、最も古いファイルが自動的に削除され、新しいログ ファイルが保存されます。この制限を設定するには、max_backup_index パラメータを変更します。デフォルトは 100 ファイルです。

開始する前に

次の処理手順は、Linux オペレーティング システムの知識があることを前提としています。必要な知識がない場合は、この処理手順を実行しないでください。

処理手順

1. プライマリ インスタンス ホストにログオンし、ユーザーを rsaadmin に変更します。
2. 完全修飾ホスト名を確認するため、Security Console にログオンし、**[Setup（セットアップ）] > [System Settings（システム設定）] > [Basic Settings（基本設定）] > [Logging（ログ）]** の順にクリックします。
3. ディレクトリを **RSA_AM_HOME\utils** に変更します。次のコマンドの 1 つを入力し、Enter キーを押します。

   管理ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.audit.admin.file.max_backup_index n host_name
   ```

   ここで、

   - n は、ローカル ログ ファイルの最大数
   - host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名

   ランタイム ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.audit.runtime.file.max_backup_index n
   host_name
   ```

   ここで、

   - n は、ローカル ログ ファイルの最大数
   - host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名

   システム ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.system.file.max_backup_index n host_name
   ```

ここで、

- n は、ローカル ログ ファイルの最大数
- host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名

すべてのインスタンスの設定を変更する場合、update_config ではなく config_all オプションを使用し、host_name は省略します。たとえば、すべてのインスタンスでシステム ログファイルの最大数を 5 個に変更するには、次のように入力します。

```
./rsautil store -a config_all
ims.logging.system.file.rotation_size 5
```

ローカル ログ ファイルの最大サイズの設定

デフォルトでは、ローカル ログ ファイルの最大サイズは 10 MB です。この制限を増減できます。

開始する前に

この処理手順は、Linux オペレーティング システムの知識があることを前提としています。必要な知識がない場合は、この処理手順を実行しないでください。

処理手順

1. プライマリ インスタンスにログオンし、ユーザーを rsaadmin に変更します。
2. ディレクトリを **RSA_AM_HOME\utils** に変更します。次のコマンドの 1 つを入力し、Enter キーを押します。

   管理ログ：

   ```
   rsautil store -a update_config
   ims.logging.audit.admin.file.rotation_size n host_name
   ```

   ここで、

   - n は、ローカル ログ ファイルの最大サイズ（MB）
   - host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名。

   ランタイム ログ：

   ```
   ./rsautil store -a update_config
   ims.logging.audit.runtime.file.rotation_size n host_name
   ```

   ここで、

   - n は、ローカル ログ ファイルの最大サイズ（MB）
   - host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名。

システム ログ：

```
./rsautil store -a update_config
ims.logging.system.file.rotation_size n host_name
```

ここで、

- n は、ローカル ログ ファイルの最大サイズ（MB）
- host_name は、プライマリ インスタンスまたはレプリカ インスタンスの完全修飾ホスト名。

すべてのインスタンスの設定を変更する場合、update_config ではなく config_all オプションを使用し、host_name は省略します。たとえば、すべてのインスタンスでシステム ログの最大サイズを 5 MB に変更するには、次のように入力します。

```
./rsautil store -a config_all
ims.logging.system.file.rotation_size 5
```

ログ内のトークン シリアル番号のマスク

RSA Authentication Manager インスタンスの外部にあるアプリケーションに送信されるログ データにトークンのシリアル番号の一部だけを含めるように Authentication Manager を構成できます。たとえば、ログ データを Syslog、ローカル ファイル、SNMP（Simple Network Management Protocol）を使用してネットワーク管理サーバに記録する際に、これを行います。

0 ～ 12 桁のトークンのシリアル番号を含めるように Authentication Manager を構成できます。デフォルト値は 12 桁です。この場合、トークンのシリアル番号全体が含まれます。

手順

1. プライマリ インスタンスで、RSA Security Console にログオンします。
2. **［Setup（セットアップ）］＞［System Settings（システム設定）］＞［Basic Settings（基本設定）］＞［Logging（ログ）］**の順にクリックします。
3. **［Select Instance（インスタンスの選択）］**で、プライマリ インスタンスを選択し、**［Next（次へ）］**をクリックします。
4. **［Configure Settings（設定の構成）］**で、**［Log Data Masking（ログ データ マスキング）］**の下にある**［Number of digits of the token serial number to display（トークンのシリアル番号の表示桁数）］**ボックスに、桁数を入力します。
5. **［Save（保存）］**をクリックします。
   設定は、導入環境内のすべてのインスタンスに適用されます。

高度なログとトラブルシューティング

このセクションでは、ログとトラブルシューティングの高度なタスクについて説明します。

- SNMP の概要
- SNMP の構成
- トラブルシューティング用のログ ファイル
- トレース ログ
- リアルタイム ログ監視用のリモート Syslog ホストの構成
- 重大システム イベントの通知の構成
- 重大システム イベントのタイプ

SNMP の概要

RSA Authentication Manager は、SNMP（Simple Network Management Protocol）を使用して、サード パーティの NMS（ネットワーク管理システム）をサポートします。NMS は、Authentication Manager が本番環境でどのように機能しているかを明らかにし、パフォーマンス最適化のための導入環境の構成をより簡単にします。

GET とトラップを指定することによって NMS で取得する情報を定義できます。NMS は、GET を使用して情報を要求し、トラップによってトリガーされたメッセージを受け取ります。また、NMS は MIB（管理情報ベース）からネットワーク情報を取得します。

GET とトラップは、次の 2 つの点で異なります。

- GET が情報を要求するのに対し、トラップは情報を自動的に送信します。
- GET が集積されたデータで構成されているのに対し、トラップは個別のデータです。

たとえば、認証に成功するたびに通知を送信するように Authentication Manager を構成しているとします。認証に 100 回成功すると、100 のトラップ メッセージが送信されます。成功した認証数に関して GET を行った場合は、100 の値を示すメッセージを 1 つ受け取ります。

Authentication Manager のエラー通知、警告通知、成功通知を受け取るように NMS を構成することができます。通知は、トラップ メッセージで送信されたデータ（メッセージ ID など）に基づいてインターセプトおよびフィルタ処理することができます。

ディスク使用量、メモリ使用量、CPU システム負荷を監視するようにトラップを設定することもできます。使用されるリソースが多すぎないかインスタンスをチェックし NMS に通知する間隔を指定できます。

SNMP の設定はインスタンスごとに行います。あるインスタンスへの変更が他のインスタンスに影響を与えることはありません。

Authentication Manager では、SNMP は、外部アイデンティティ ソースからではなく、内部データベースからのみ値を取得します。たとえば、外部アイデンティティ ソースには 2,000 人のユーザーがいる一方、Authentication Manager の内部データベースには 1,000 人しかユーザーがいないとします。ユーザーの総数を GET した場合、返される値は 1000 です。

NMS でフィルタ処理できる Authentication Manager のメッセージ ID とメッセージの原因を表示する方法については、「RSA Authentication Manager 8.0 SNMP Reference Guide」を参照してください。

SNMP の構成

RSA Authentication Manager に対して SNMP（Simple Network Management Protocol）GET およびトラップを構成できます。

管理者はプライマリ インスタンスにログオンして、各インスタンスの SNMP 設定を構成する必要があります。レプリカ インスタンスの Security Console では、SNMP 設定の表示のみできます。プライマリ インスタンスの設定をすべてのインスタンスに適用することができます。

開始する前に

スーパー管理者である必要があります。

手順

1. プライマリ インスタンスの Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [Advanced Settings（詳細設定）] で、[**Network Monitoring (SNMP)（ネットワーク監視（SNMP））**] をクリックします。
3. インスタンスを選択します。
4. [**Next（次へ）**] をクリックします。
5. [**Network Monitoring using SNMP v3（SNMP v3 を使用したネットワーク監視）**] で、[**On（オン）**] を選択します。これで、SNMP エージェントが有効化されます。[**On（オン）**] を選択しない場合は、この処理手順の残りをスキップしてください。
   この設定を変更して、SNMP を一時的に無効化することもできます。[**Off**（オフ）] を選択しても、このページのその他の SNMP 設定がクリアされることはありません。
6. [**Request Port（リクエスト ポート）**] フィールドで、SNMP エージェントが GET リクエストをリスンするポート番号を入力します。デフォルトのポート番号は 161 です。

注：ポート番号 8002 は指定しないでください。仮想アプライアンスの内部 SNMP エージェントがポート 8002 を使用します。

7. ［**Security Name（セキュリティ名）**］フィールドで、アプライアンス SNMP エージェントのユーザー名を定義します。SNMP エージェントは、このユーザー名を使用して、GET リクエストを認証し、トラップを送信します。
8. ［**Security Level（セキュリティレベル）**］フィールドで、SNMP 通信のセキュリティのレベルを選択します。
   - ［**No Authentication（認証なし）**］の場合は、認証は行わず、SNMP 通信は暗号化されません。ステップ 11 に進みます。
   - ［**Authentication, No Privacy（認証、プライバシーなし）**］の場合は、GET またはトラップの送信側を認証しますが、SNMP データ通信は暗号化されません。
   - ［**Authentication and Privacy（認証とプライバシー）**］の場合は、GET またはトラップの送信側を認証し、SNMP データ通信を暗号化します。
9. 認証を行う場合は、次の操作を実行します。
   a. ［**Authentication Password（認証パスワード）**］フィールドで、GET またはトラップの送信側を認証するためのパスワードを入力します。一部の SNMP クライアントでは「パスフレーズ」という用語を使用します。
   b. 「**Authentication Protocol（認証プロトコル）**］リストから、GET またはトラップの送信側を認証するためのプロトコルを選択します。
10. 暗号化する場合は、次の操作を実行します。
    a. ［**Privacy Password（プライバシー パスワード）**］フィールドで、SNMP データ通信を暗号化するためのパスワードを入力します。一部の SNMP クライアントでは「パスフレーズ」という用語を使用します。
    b. ［**Privacy Protocol（プライバシー プロトコル）**］フィールドで、SNMP データ通信を暗号化するためのアルゴリズムを選択します。
11. ［**Download（ダウンロード）**］をクリックし、MIB（管理情報ベース）.zip ファイルを保存します。

    この .zip ファイルには、Authentication Manager とアプライアンス オペレーティング システムの両方の MIB ファイルが含まれています。
12. ［**Trap Settings（トラップの設定）**］セクションで、トラップするログ イベントのタイプと重大度を指定します。

ログ イベントのタイプ	説明	重大度
Administrator Activity（管理者アクティビティ）	導入環境の管理者アクション。Console を使用した場合と API を使用した場合の両方を含みます。	重大度レベルは累積的です。 • ［**Success（成功）**］の場合は、成功、警告、エラーのすべてのイベントをトラップする。 • ［**Warning（警告）**］の場合は、警告イベントとエラー イベントの両方をトラップする。 • ［**Error（エラー）**］の場合は、エラーのみをトラップする。
Authentication Activity（認証アクティビティ）	ユーザー ID、認証時間、認証エージェント、アカウント ロックアウトなどのユーザー認証に関連するすべてのイベント。	
System Log Report（システム ログ レポート）	導入環境、内部プロセス、状態やイベント（起動、接続の確立 / 切断、更新イベント）などの Authentication Manager に関する情報。	

13. ［**Send Traps for Operating Systems Events（オペレーティング システム イベントのトラップ送信）**］で、仮想アプライアンスのリソース使用率を監視するかどうかを選択します。

    すべての OS 属性に対して、システムがトラップを送信する閾値を入力します。すべての属性に値が必要ですが、トラップを送信する必要がない属性に対しては高い閾値を設定することができます。

14. ［**Traps Receiver Settings（トラップ受信者の設定）**］で、SNMP トラップ通知を受信するマシンの IP アドレスまたはホスト名を追加します。デフォルトのポート番号 162 を維持することも変更することもできます。

    また、複数のトラップ受信者を入力すること、既存のトラップ受信者を更新すること、トラップ受信者をリストから削除することができます。

15. プライマリ インスタンスを構成し、同じ設定をレプリカ インスタンスにも適用する場合は、［**Apply the above settings to the replica instance(s) upon save（保存時に上記の設定をレプリカ インスタンスに適用）**］をクリックします。

16. ［**Save（保存）**］をクリックします。

次のステップ

SNMP 構成の変更がレプリカ インスタンスに反映されるまで最大 10 分かかる可能性があります。SNMP 構成の変更が反映されるまでの時間を短縮するために、管理者はレプリカ インスタンスの Operations Console にログオンして、キャッシュをフラッシュすることができます。詳細については、423 ページのキャッシュのフラッシュを参照してください。

トラブルシューティング用のログ ファイル

Security Console に表示されるログ メッセージは、Authentication Manager ディレクトリ内のファイルにも書き込まれます。このディレクトリには、Authentication Manager の トラブルシューティングに役立つアプライアンスのその他のログも含まれています。

セキュア シェル（SSH）クライアントを使用してアプライアンス オペレーティング システムにログオンした後、ログ ファイルにアクセスできます。Operations Console を使用して、これらのログをダウンロードすることもできます。詳細については、382 ページのトラブルシューティング ファイルのダウンロードを参照してください。

Authentication Manager ログ

以下の表は、使用可能なログ ファイルを示しています。

ログ ファイル名	内容
imsAdminAudit.log	管理監査ログに書き込まれたメッセージ。これらのメッセージは、ユーザーの追加や編集などの管理アクションを記録します。 **注：**内部データベースに保存される管理監査ログに書き込まれないデータのみ含まれます。
imsRuntimeAudit.log	ランタイム監査ログに書き込まれたメッセージ。これらのメッセージは、認証や制限付きエージェント アクセスのチェックなどのランタイム アクティビティを記録します。 **注：**内部データベースに保存されるランタイム監査ログに書き込まれないデータのみ含まれます。
imsSystem.log	システム ログに書き込まれたメッセージ。これらのメッセージは、システムの起動やレプリカの追加などのシステム レベルのアクティビティを記録します。 **注：**内部データベースに保存されるシステム ログに書き込まれないデータのみ含まれます。
imsTrace.log	トレース ログに書き込まれたメッセージ。これらのメッセージは、システムのデバッグに使用します。
AdminServer.log	管理サーバ（Operations Console をホストするアプリケーションサーバ）に関するメッセージ。

ログ ファイル名	内容
AdminServer_access.log	管理サーバ（Operations Console をホストするアプリケーションサーバ）の送受信 HTTP トラフィックに関するメッセージ。
biztier.log	プライマリ インスタンスに関するメッセージ。サーバの起動、環境、実行中のサーバ コンポーネント、ネットワーク サービス、サーバ エラーについての情報が含まれます。
biztier_access.log	プライマリ Authentication Manager HTTP インタフェースに関するメッセージ。
console.log	Console Server に関するメッセージ。サーバの起動、環境、実行中のサーバ コンポーネント、ネットワーク サービス、サーバ エラーについての情報が含まれます。
console_access.log	Console Server の送受信 HTTP トラフィックに関するメッセージ。この中には、Security Console が含まれます。Web Tier が構成されていない場合は、Self-Service Console も含まれます。
rsa-console.log	Security Console に関するメッセージ。
BiztierServerWrapper.log	Biz Tier の Authentication Manager サーバ サービス起動に関するメッセージ。
AdminServerWrapper.log	管理サーバのサービス起動情報に関するメッセージ。
ConsoleServerWrapper.log	Console Server のサービス起動情報に関するメッセージ。
imsOCAdminAudit.log	Operations Console 内の管理監査ログに書き込まれた情報に関するメッセージ。これらのメッセージは、ユーザーの追加や編集などの管理アクションを記録します。
imsOCRuntimeAudit.log	Operations Console 内のランタイム監査ログに書き込まれた情報に関するメッセージ。これらのメッセージは、ユーザーの認証や許可などのランタイム アクティビティを記録します。

ログ ファイル名	内容
imsOCSystem.log	Operations Console 内のシステム ログに書き込まれた情報に関するメッセージ。「Authentication Manager Server started」や「Connection Manager lost db connection」などのシステム レベルのメッセージを記録します。
imsOCTrace.log	Operations Console 内のトレース ログに書き込まれた情報に関するメッセージ。これらのメッセージは、デバッグに使用します。
ops-console.log	Operations Console に関するメッセージ。
radius-console.log	RADIUS サーバに関するメッセージ。
radiusoc.log	システムのデバッグに使用できる Operations Console 内の RADIUS サーバ関連ログ メッセージを収集します。
radiusoc-access.log	RADIUS サーバの送受信 HTTP トラフィックに関するメッセージ。
radiusOCServerWrapper.log	RADIUS サーバの HTTP インタフェースに関するメッセージ。
rsa-runtime.log	RADIUS サーバのサービス起動情報に関するメッセージ。
imsRadiusTrace	トレース ログに書き込まれたメッセージ。これらのメッセージは、RADIUS サーバのデバッグに使用します。

内部データベース関連ログ ファイル

以下の表は、**/opt/rsa/am/rsapgdata/pg_log** に保存されるデータベース関連ログ ファイルを示しています。

ログ ファイル名	内容
postgresql-yyyy-mm-dd_064308.log **注：**ログ ファイル名には、yyyy-mm-dd 形式で、現在の日付が含まれています。	「out of disk space（ディスク領域不足）」や「disk hardware error（ディスク ハードウェア エラー）」など、下位レベルのデータベース故障の継続的なログです。データベースに書き込まれるすべての Authentication Manager 関連アクティビティも収集します。

トレース ログ

トレース ログは、アプリケーションの問題をデバッグするのに役立ちます。Security Console の［Log Configuration（ログの構成）］ページで、トレース ログ ファイルに書き込まれる詳細レベルを構成できます。トレース ログでは、次のログ レベルを指定できます。

Fatal（致命的）。アプリケーションまたは関連するサブコンポーネントが近い将来にクラッシュする恐れがあることを示すログ メッセージのみを収集します。致命的なメッセージには、迅速な注意を払う必要があります。

Error（エラー）。致命的なメッセージに加え、対処が必要であってもアプリケーションがクラッシュするとは限らないエラー状態をすべて収集します。

Warning（警告）。致命的なメッセージとエラー メッセージに加え、アプリケーションの実行中の軽微な問題に関するログ メッセージもすべて収集します。

Information（情報）。致命的なメッセージ、エラー メッセージ、警告メッセージに加え、アプリケーションの通常のライフサイクル中の重要なイベントに関するログ メッセージもすべて収集します。

Verbose（詳細）。致命的なメッセージ、エラー メッセージ、警告メッセージ、情報メッセージに加え、頻繁に発生する小さなイベントに関するログ メッセージもすべて収集します。

重要：RSA カスタマー サポートから指示があった場合を除き、トレース ログ レベルを［Verbose（詳細）］に長期間設定しないでください。トレース ログにより大量のディスク領域が使用され、システム パフォーマンスに影響する恐れがあります。

一部の日常的なシステム アクティビティは、ログ レベルが［Information（情報）］または［Verbose（詳細）］に設定されている場合にのみシステム ログに書き込まれます。この情報を内部データベースに書き込んで表示したい場合、これらのいずれかのログ レベルを使用します。システム起動イベントのように、あまり頻繁に発生しない、重要なシステム ログ メッセージは、ログ レベルに関係なく記録されます。

リアルタイム ログ監視用のリモート Syslog ホストの構成

リモート Syslog ホストを構成して、Authentication Manager からのログ メッセージを記録できます。リモート ホストは、Syslog 機能を備えた有効な UNIX または Linux マシンでなければなりません。リモート Syslog は、RSA Authentication Manager を含むネットワーク内の複数のシステムからのログを管理します。Authentication Manager からのメッセージを記録するよう、リモート ホストを構成します。構成で使用されるファイルと IP テーブルの場所は、リモート ホストに応じて異なる場合があります。手順については、UNIX または Linux のドキュメントを参照してください。

リモート Syslog ホストを構成した後、Security Console でログの宛先となるリモート ホストを指定する必要があります。手順については、RSA Security Console ヘルプのトピック「Configure Logging（ログの構成）」を参照してください。

重大システム イベントの通知の構成

RSA Authentication Manager は、重大システム イベントが発生した場合（たとえば、レプリカ インスタンスのレプリケーション ステータスが Out-of-Sync（同期ずれ）に変更された場合）にメールで管理者に通知する機能を備えています。

RSA では、Authentication Manager を構成して、重大システム イベントの通知を主要な管理者に送信することをお勧めします。これにより、管理者はその状況が問題となる前に解決できます。

開始する前に

- スーパー管理者である必要があります。
- Security Console で SMTP メール サービスが構成されている必要があります。手順については、RSA Security Console ヘルプのトピック「SMTP メール サービスの構成」を参照してください。

手順

1. Security Console で、[**Set Up（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [**Basic Settings（基本設定）**] セクションで、[**Critical System Event Notification（重大システム イベントの通知）**] をクリックします。
3. [**Enable Notifications（通知を有効化する）**] で、[**On（オン）**] を選択します。
4. [**Send Notifications for（通知の対象）**] で、次の中から 1 つ以上の項目を選択します。
   - [**Backup Events（バックアップ イベント）**]。バックアップが過去 7 日間作成されていないか、スケジュール バックアップが失敗したため、新しいバックアップが必要です。
   - [**Identity Source Connection Events（アイデンティティ ソース接続イベント）**]。アイデンティティ ソース ディレクトリに接続できません。
   - [**Low Disk Space Events（ディスク領域不足イベント）**]。ディスク領域が 5 GB を下回っています。
   - [**RADIUS Configuration Events（RADIUS 構成イベント）**]。Quick Setup、アタッチ、リバランス、ホスト名の変更、IP アドレスの変更の実行中に RADIUS の構成が失敗しました。
   - [**RADIUS Replication Events（RADIUS レプリケーション イベント）**]。RADIUS レプリケーションが失敗しました。

- ［**Realm Certificate Removal Events（レルム証明書の削除イベント）**］。ホスト名の変更時にレルム証明書の削除に失敗しました。
- ［**Replication Events（レプリケーション イベント）**］。レプリケーション ステータスが変更されました。たとえば、レプリカ インスタンスのレプリケーション ステータスが Out-of-Sync（同期ずれ）に変更されました。

5. ［**Send Notifications to（通知の送信先）**］で、次のいずれか、または両方の項目を選択します。
   - ［**Super Administrators（スーパー管理者）**］
   - ［**Individual Email Addresses（個人メール アドレス）**］

     ［**Individual Email Addresses（個人メール アドレス）**］を選択した場合は、各受信者のメール アドレスを対応するフィールドに入力します。複数のメール アドレスはセミコロンで区切ります。
6. ［**Save（保存）**］をクリックします。

重大システム イベントのタイプ

重大システム イベントの通知は、導入環境内の望ましくない状況を管理者に警告します。これにより、管理者はその状況が問題となる前に解決できます。次のイベントが発生した場合のメール通知を有効化するには、Security Console を使用します。

イベント タイプ	通知の原因
Backup Events（バックアップ イベント）	バックアップが過去 7 日間作成されていないか、スケジュール バックアップが失敗したため、新しいバックアップが必要です。 バックアップの詳細については、423 ページの導入環境のバックアップを参照してください。
Identity Source Connection Events（アイデンティティ ソース接続イベント）	アイデンティティ ソース ディレクトリに接続できません。 アイデンティティ ソースの詳細については、RSA Operations Console ヘルプのトピック「アイデンティティ ソースの追加」を参照してください。
Low Disk Space Events（ディスク領域不足イベント）	ディスク領域が 5 GB を下回っています。 ディスク領域の問題については、第 15 章、災害復旧を参照してください。
RADIUS Configuration Events（RADIUS 構成イベント）	Quick Setup、アタッチ、リバランス、ホスト名の変更、IP アドレスの変更の実行中に RADIUS の構成が失敗しました。 RADIUS については、第 13 章、RSA RADIUS の管理を参照してください。

イベント タイプ	通知の原因
RADIUS Replication Events（RADIUS レプリケーション イベント）	RADIUS レプリケーションが失敗しました。 RADIUS については、管理者ガイドの「RSA RADIUS の管理」の章を参照してください。
Realm Certificate Removal Events（レルム証明書の削除イベント）	ホスト名の変更時にレルム証明書の削除に失敗しました。
Replication Events（レプリケーション イベント）	レプリケーション ステータスが変更されました。たとえば、レプリカ インスタンスのレプリケーション ステータスが Out-of-Sync（同期ずれ）に変更されました。レプリケーション ステータスについては、419 ページのレプリケーション ステータスの確認を参照してください。

15 災害復旧

導入環境の問題のトラブルシューティング

導入環境が正常に動作していない場合、発生する現象によって問題を判別することができます。問題を判別したら、適切なソリューションを選択して導入環境をリストアできます。

プライマリ インスタンスまたはレプリカ インスタンスのデータを紛失した時の現象

RSA Authentication Manager データが誤って削除されると、次のイベントが発生します。

- レコードがないため、一部のユーザーが認証を受けることができない。
- ポリシー設定が正常に機能しない。
- 制限付きエージェントが正常に機能しない。
- トラステッド レルムの認証が正常に機能しない。

導入環境にデータ紛失の現象が見られる場合、バックアップからデータをリストアすることにより、問題を解決することができます。詳細については、433 ページのプライマリ インスタンスのリストアを参照してください。

プライマリ インスタンスが応答しなくなった時の現象

プライマリ インスタンスが応答を停止すると、次のイベントが発生します。

- レプリカ インスタンスは認証リクエスト処理を継続するが、システム全体の認証リクエストの処理に通常よりも時間がかかる。
- 導入環境の管理ができない。
- 別の DN（識別名）に移動したか、Authentication Manager で認証または編集を一度も行ったことのない LDAP ディレクトリのユーザーが、認証またはユーザーデータの編集を行うことができない。
- 導入環境にレプリカ インスタンスが含まれ、ロードバランサを使用している場合、RBA（リスク ベース認証）は認証を継続する。そうでない場合、レプリカ インスタンスを昇格するまで、RBA は使用不可となる。
- 導入環境にレプリカ インスタンスがない場合、認証が停止する。
- ヘルプ デスク ソリューションが機能しなくなる。
- ロックアウトされているユーザーをロック解除できない。
- プライマリ インスタンス上のデータベースが使用不可となる。

- Self-Service Console が使用不可となる。
- プライマリ インスタンスがログ ファイルを生成していない。

プライマリ インスタンスが応答しない場合、プライマリ インスタンスをリストアすることにより、問題を解決することができます。詳細については、433 ページのプライマリ インスタンスのリストアを参照してください。

レプリカ インスタンスが応答しなくなった時の現象

レプリカ インスタンスが応答を停止すると、次のイベントが発生します。

- プライマリ インスタンスおよびその他のレプリカ インスタンスが認証リクエスト処理を継続するが、認証に通常よりも時間がかかる。
- プライマリで行われたデータベース更新のうち、レプリカにまだ反映されていないものは、プライマリ インスタンス データベースのディスクが一杯になるかレプリカが削除または復旧されるまでキューイングされる。プライマリ インスタンスにキューイングされたトランザクション数に応じて、ディスク領域不足を避けるため、システムがレプリカ インスタンスを **Out of Sync** に設定する。
- レプリカ インスタンスがログ ファイルを生成していない。

レプリカ インスタンスが応答しない場合、レプリカ インスタンスを置換することにより、問題を解決することができます。詳細については、433 ページのプライマリ インスタンスの置換を参照してください。

Web Tier が応答しなくなった時の現象

Web Tier が応答を停止すると、次のイベントが発生します。

- プライマリ インスタンスの Web Tier の場合、Self-Service Console が使用不可となる。
- プライマリインスタンス単独の導入環境では、RBA（リスク ベース認証）が停止する。

Web Tier が応答しない場合、現在の Web Tier を削除し、新しい Web Tier を追加することにより、問題を解決することができます。詳細については、446 ページの Web Tier のリストアを参照してください。

レプリケーションの問題が発生した時の現象

プライマリ インスタンスとレプリカ インスタンス間のデータ レプリケーション機能が停止した場合、割り当てられたディスク領域が一杯になってしまうため、インスタンスがユーザーの認証を停止する可能性があります。重大システムイベントの通知を有効化している場合、レプリケーション機能が停止した時に、メッセージを受信できます。

レプリカ インスタンスをプライマリ インスタンスと同期することにより、問題を解決することができます。詳細については、422 ページのレプリカ インスタンスの同期を参照してください。

導入環境の問題の解決

導入環境の問題は、多くの場合、次の 1 つ以上のタスクを実行することで解決できます。

- アプライアンスのリブート
- レプリケーション ステータスの確認
- レプリカ インスタンスの同期
- キャッシュのフラッシュ

アプライアンスのリブート

ソフトウェア アップデートの一環としてアプライアンスのリブートが必要となる場合があります。

リブート処理は約 10 分かかります。リブートが完了すると、Operations Console のログオン ページにリダイレクトされます。

開始する前に

Operations Console 管理者である必要があります。

手順

1. リブートするアプライアンスで、RSA Operations Console にログオンします。
2. [**Maintenance（保守）**] > [**Reboot Appliance（アプライアンスのリブート）**] の順にクリックします。
3. [Reboot Appliance Confirmation（アプライアンスリブートの確認）] ページで、[**Yes, reboot the appliance（はい、アプライアンスをリブートします）**] を選択し、[**Reboot（リブート）**] をクリックします。
4. [Reboot Appliance Progress（アプライアンスのリブート中）] ページで、リブートが完了するまで待機します。
5. RSA Operations Console のログオン ページが表示されたら、RSA Operations Console にログオンします。

レプリケーション ステータスの確認

導入環境の各レプリカ インスタンスのレプリケーション ステータス レポートを表示することができ、必要に応じてレプリカ インスタンスの削除や同期ができます。

レプリケーション ステータスを表示するには、導入環境に 1 つ以上のレプリカ インスタンスが存在する必要があります。

プライマリ インスタンスでは、レプリケーション ステータス レポートに次の情報が表示されます。

- ［**Disk Space Available（使用可能なディスク領域）**］：プライマリ インスタンスの使用可能な空きディスク領域。空きディスク領域が不足している場合、レプリケーションは停止します。
- ［**Minimum Disk Space for Replication（レプリケーションに必要な最小ディスク領域）**］：レプリケーションに必要なプライマリ インスタンスの空きディスク領域。
- ［**Replication Status（レプリケーション ステータス）**］：導入環境のプライマリ インスタンスと各レプリカ インスタンスの間のレプリケーションのステータス。

  レプリカ インスタンスで表示するレプリケーション ステータス レポートには、そのレプリカ インスタンスとプライマリ インスタンスの間のレプリケーションのステータスのみが表示されます。各ステータスの詳細については、420 ページのレプリケーション ステータスを参照してください。

レプリカ インスタンスをシャットダウンした場合、およそ 3 分間待ってから再起動してください。そうでない場合には、レプリケーション ステータスを確認できません。即座に再起動し、再起動が 3 分未満で完了すると、システム アクティビティ モニタにメッセージが何も表示されないことがあります。ただし、レポートを実行すれば、イベントを確認することができます。

レプリケーション エラーが発生した場合は、ログ ファイルをダウンロードしてトラブルシューティングに役立てることができます。詳細については、382 ページのトラブルシューティング ファイルのダウンロードを参照してください。

手順

プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Instances（インスタンス）**］＞［**Status Report（ステータス レポート）**］の順にクリックします。

レプリケーション ステータス

レプリケーション ステータス レポートには、導入環境内の各レプリカ インスタンスのレプリケーション ステータスが表示されます。

次の表に、レプリケーション ステータスの説明を示します。重大システムイベントの通知で、レプリケーション ステータスを有効化した場合は、レプリケーション ステータスが変更されたときにメール通知を受信します。各ステータスの説明には、重大システムイベント通知メッセージに使用されるステータスの用語が示されています。

ステータス	説明
Attachment in Progress （アタッチが進行中） （プライマリ インスタンスのみ）	レプリカ インスタンスは現在プライマリ インスタンスにアタッチ中です。 重大システム イベント通知：ATTACHING
Attachment Unsuccessful （アタッチの失敗）	レプリカ インスタンスのアタッチが失敗しました。 重大システム イベント通知：FAILED
Instance Offline （インスタンス オフライン） （プライマリ インスタンスのみ）	レプリカ インスタンスは、ステータスの更新を停止しました。シャットダウンされたか、ネットワークが切断された可能性があります。 重大システム イベント通知：OFFLINE
Internal Replication Error （内部レプリケーション エラー）	エラーが発生しました。 重大システム イベント通知：UNHEALTHY
Normal（正常）	レプリケーションが正常に行われています。 重大システム イベント通知：HEALTHY
Out of Sync（同期ずれ）	レプリカ インスタンスは、プライマリ インスタンスと同期していません。手動で同期する必要があります。 重大システム イベント通知：OUT_OF_SYNC
Synchronization in Progress（同期中）	レプリカ インスタンスは、プライマリ インスタンスとの同期の処理中です。 重大システム イベント通知：SYNCHRONIZING

レプリカ インスタンスをシャットダウンした場合、およそ 3 分間待ってレプリケーション ステータスを確認してから、再起動してください。即座に再起動し、再起動が 3 分未満で完了すると、システム アクティビティ モニタにメッセージが何も表示されない可能性があります。ただし、レポートを実行すれば、イベントを確認することができます。

レプリケーション エラーが発生した場合は、ログ ファイルをダウンロードしてトラブルシューティングに役立てることができます。詳細については、382 ページのトラブルシューティング ファイルのダウンロードを参照してください。

レプリカ インスタンスの同期

プライマリ インスタンスのデータは、導入環境内の各レプリカ インスタンスに頻繁にレプリケーションされます。Operations Console の［Replication Status Report（レプリケーション ステータス レポート）］ページで、各レプリカ インスタンスのレプリケーション ステータスを表示できます。レプリカ インスタンスのステータスが［**Out of Sync（同期ずれ）**］と表示された場合は、このレプリカ インスタンスを手動で同期する必要があります。同期処理により、レプリカ インスタンスのデータとプライマリ インスタンスのデータの同期が回復します。

次の手順を実行して、同期ずれが発生したレプリカ インスタンスをプライマリ インスタンスと同期します。

開始する前に

Operations Console 管理者である必要があります。

手順

1. プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Instances（インスタンス）**］＞［**Status Report（ステータス レポート）**］の順にクリックします。
2. ［**Out of Sync（同期ずれ）**］ステータスのレプリカ インスタンスで、［**Sync（同期）**］をクリックします。

   注：一度に同期できるレプリカ インスタンスは 1 個だけです。

   同期の進行状況が表示されます。
   30 分経過しても同期処理が完了しない場合、または同期の進行状況にエラーが表示された場合は、レプリカ インスタンスのトラブルシューティング ファイルをダウンロードして問題を解決します。操作手順については、382 ページのトラブルシューティング ファイルのダウンロードを参照してください。
3. 同期タスクが完了した後で、［**Done（完了）**］をクリックします。

キャッシュのフラッシュ

キャッシュをフラッシュして、メモリから古い情報を削除します。キャッシュをフラッシュすると、次にアクセスしたときに、選択したオブジェクトについてはデータベースから最新の情報を取得します。

キャッシュの内容は 10 分ごとに自動更新されます。キャッシュ設定に応じて、プライマリで発生した変更がデータベースのレプリケーションによってレプリカに反映され、すべてのインスタンスで正しく表示されるようになるまでに最大で 10 分かかります。また、10 分ごとの自動更新を待たずに、個々のインスタンスでキャッシュをフラッシュできます。

開始する前に

Operations Console 管理者およびスーパー管理者である必要があります。

手順

1. キャッシュをフラッシュするインスタンスの Operations Console で、［**Maintenance（保守）**］＞［**Flush Cache（キャッシュのフラッシュ）**］をクリックします。
2. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力し、［**OK**］をクリックします。
3. ［**Flush Cache（キャッシュのフラッシュ）**］で、以下のいずれかを実行します。
   - すべてのキャッシュをフラッシュする場合は、［**Flush all cache objects（すべてのキャッシュ オブジェクトをフラッシュ）**］を選択し、［**Flush（フラッシュ）**］をクリックします。
   - ［**Flush specific cache objects（特定のキャッシュ オブジェクトをフラッシュ）**］を選択し、フラッシュするキャッシュを選択して、［**Flush（フラッシュ）**］をクリックします。

導入環境のバックアップ

導入環境データのバックアップを作成するには、Operations Console を使用します。このバックアップを使用して、以下の方法で導入環境を修復できます。

- 誤って削除されたデータのリストア
- 障害が発生したプライマリ インスタンスのリストア

次のいずれかの方法を使用して導入環境のデータをバックアップできます。

- **Back Up Now（今すぐバックアップ）**。手動による、導入環境の一回限りのバックアップです。操作手順については、425 ページの今すぐバックアップ機能によるバックアップの作成を参照してください。
- **Schedule Backups（スケジュール バックアップ）**。指定したスケジュールに従って実行する導入環境の定期的バックアップです。操作手順については、426 ページのスケジュール バックアップによるバックアップの作成を参照してください。

RSA は、最新のバックアップを保持するよう推奨します。過去 7 日間正常なバックアップを作成していない場合、重大システム イベント通知を構成していれば、導入環境から通知が送信されます。

バックアップの作成中、認証は継続します。ただし、バックアップ操作により認証プロセスが遅くなることがあります。RSA では、認証トラフィックが少ないときやバッチ ジョブが実行中でないときに導入環境データをバックアップするよう推奨します。

バックアップには機密情報が含まれるため、バックアップは暗号化されます。バックアップを実行する時に、暗号化に使用するパスワードを指定する必要があります。リストアを実行する時に、このパスワードを入力して、バックアップを復号化し、内容の完全性をチェックできます。

内部データベースのサイズにより、バックアップの作成に必要な時間が決定されます。内部データベースのサイズが大きい場合、処理に時間がかかる場合があります。

アプライアンス上、またはリモートの場所にバックアップを保存できます。RSA では、導入環境をリストアして災害から復旧できるように、リモートの場所に最新のバックアップを保存することを推奨します。

バックアップ ファイルの内容

バックアップ ファイル（.RSAbackup）には、次のデータが含まれます。

- **内部データベース**。構成、ポリシー、ユーザー、グループなどが含まれます。
- **Authentication Manager のファイル**。データおよび構成ファイル。例えば、更新ログ、ブートローダ設定、キー、内部データベースなどの内部サービスにアクセスするために使用するパスワードなど。
- **RADIUS**。RADIUS プライマリのリストアに必要なすべてのデータおよび構成ファイル。インポートされた EAP-TTLS（Extensible Authentication Protocol-Tunneled Transport Layer Security）クライアントの信頼するルート証明書を含む。すべての RADIUS データがバックアップに含まれます。RADIUS データは個別にバックアップまたはリストアできません。
- **内部データベースのログ ファイル データ**。管理監査ログ、ランタイム監査ログ、システム ログ。
- **コンソールの SSL 証明書**。ブラウザと Operations Console、Security Console、Self-Service Console 間の通信を保護する証明書。

バックアップにはアプライアンスの導入に使用するファイルが含まれません。バックアップにはアプライアンスの導入後に追加または変更したデータのみが含まれます。

バックアップには、ユーザーおよびトークンを別の導入環境に移行するため、エクスポートにより生成されたファイルは含まれません。エクスポートが完了したら、ファイルをローカルにダウンロードしてエクスポート ジョブを削除します。

今すぐバックアップ機能によるバックアップの作成

今すぐバックアップ機能では、導入環境の 1 回限りのバックアップを手動で作成します。

導入環境に重要な変更が生じる保守タスクを実行する前に、今すぐバックアップ機能を実行し、必要に応じて導入環境をリストアできるようにしておきます。たとえば、今すぐバックアップ機能を実行する必要があるのは、次のような場合です。

- プライマリ インスタンスの導入直後
- 移行の完了後
- 更新の適用前と適用直後
- レプリカ インスタンスの追加や削除など、導入環境のトポロジーを変更した後

手順

1. Operations Console で、［**Maintenance（保守）**］＞［**Backup and Restore（バックアップとリストア）**］＞［**Backup Now（今すぐバックアップ）**］の順にクリックします。
2. ［**Backup Name（バックアップ名）**］フィールドで、デフォルトの名前を受け入れるか、自分で指定したバックアップ名に置き換えます。
   デフォルトの名前には、タイム スタンプおよび .RSAbackup という拡張子が含まれています。タイム スタンプには、YYYYMMDDHHMM という形式が使用されます。
   たとえば、デフォルトの名前が 201208251230.RSAbackup である場合、2012 はバックアップ作成時の年、08 は月、25 は日、12 は時間、30 は分をそれぞれ示しています。
   デフォルトの名前を変更する場合、新しい名前には .RSAbackup という拡張子を使用する必要があります。この拡張子では、大文字と小文字が区別されます。
3. ［**Backup Password（バックアップ パスワード）**］フィールドに、有効なパスワードを入力し、同じパスワードを［**Confirm Backup Password（バックアップ パスワードの確認）**］フィールドに入力します。
   指定したバックアップ パスワードを間違いのないようにメモします。導入環境をリストアするときに、このパスワードが必要です。
4. ［**Backup Location（バックアップ場所）**］で、以下のいずれかを実行します。
   - ［**Local Authentication Manager Server（ローカル Authentication Manager サーバ）**］を選択します。バックアップはこのアプライアンスに保存されます。

- ［**Windows Shared Folder（Windows 共有フォルダ）**］を選択します。
  - ［**Windows Shared Folder（Windows 共有フォルダ）**］フィールドに、既存の Windows 共有フォルダへのパス（たとえば、「**¥primary.company.net¥backup_path**」）を入力します。
  - 共有フォルダにユーザー名が必要な場合は、［**Folder User Name（フォルダ ユーザー名）**］フィールドにユーザー名（たとえば、「Domain1¥User1」）を入力します。
  - 共有フォルダにパスワードが必要な場合は、［**Folder Password（フォルダ パスワード）**］フィールドにパスワード（たとえば、「password1」）を入力します。
- ［**NFS (Network File System) Shared Folder（NFS 共有フォルダ）**］を選択します。［**NFS Shared Folder（NFS 共有フォルダ）**］フィールドに、NFS サーバおよびファイル ディレクトリへのパス（たとえば「**fileserver.company.net:/backup_path**」）を入力します。

5. ［**Backup（バックアップ）**］をクリックします。
   ［Progress Monitor（進行状況）］ページにバックアップの進行状況が表示されます。
6. バックアップ プロセスが完了したら、［**Done（完了）**］をクリックします。

スケジュール バックアップによるバックアップの作成

［Schedule Backups（スケジュール バックアップ）］では、指定された日時に従い、導入環境データのバックアップを定期的に作成します。［Schedule Backups（スケジュール バックアップ）］を使用して、常に最新のバックアップを保持するようにします。これにより、最小限のデータ損失で導入環境をリストアできます。

バックアップ処理の間も認証要求は処理されます。しかし、バックアップ操作により全体的なシステム パフォーマンスは遅くなります。低負荷時間帯にバックアップが実行されるようにバックアップのスケジュールを設定することを推奨します。

レプリカ インスタンスをプライマリ インスタンスに昇格させた場合は、新しいプライマリ インスタンスで［Schedule Backups（スケジュール バックアップ）］を構成する必要があります。

また、スケジュール設定されたバックアップが失敗した場合にも重大システム イベント通知が送信されます。

手順

1. Operations Console で、［**Maintenance（保守）**］＞［**Backup and Restore（バックアップとリストア）**］＞［**Schedule Backups（スケジュール バックアップ）**］の順にクリックします。
2. ［**Schedule Backup Status（スケジュール バックアップのステータス）**］で、［**On（オン）**］を選択します。

3. ［**Backup Configuration（バックアップ構成）**］で、次の手順を実行します。
   a. ［**Backup Password（バックアップ パスワード）**］フィールドに、有効なパスワードを入力します。［**Confirm Backup Password（バックアップ パスワードの確認）**］フィールドに、同じパスワードを入力します。
      指定したバックアップ パスワードを慎重にメモします。導入環境をリストアするときに、このパスワードが必要です。
   b. ［**Maximum Number of Archived Backups（バックアップ アーカイブの最大数）**］では、デフォルトで 4 が選択されますが、ドロップダウンリストから新しい数を選択することもできます。
      RSA では、4 個以上のバックアップをアーカイブに保存することを推奨します。スケジュール バックアップの合計が最大数に達した場合は、次回スケジュール バックアップを実行する時に、最も古いバックアップが削除されます。
4. ［**Backup Location（バックアップ場所）**］で、以下のいずれかを実行します。
   - ［**LocalAuthentication ManagerServer（ローカル Authentication Manager サーバ）**］を選択します。バックアップは、アプライアンスに格納されます。
   - ［**Windows Shared Folder（Windows 共有フォルダ）**］を選択します。
     – ［**Windows Shared Folder（Windows 共有フォルダ）**］フィールドに、既存の Windows 共有フォルダへのパス（たとえば、「¥primary.company.net•ackup_path」）を入力します。
     – 共有フォルダにユーザー名が必要な場合は、［**Folder User Name（フォルダ ユーザー名）**］フィールドにユーザー名（たとえば、「Domain1¥User1」）を入力します。
     – 共有フォルダにパスワードが必要な場合は、［**Folder Password（フォルダ パスワード）**］フィールドにパスワード（たとえば、「password1」）を入力します。
   - ［**NFS (Network File System) Shared Folder（NFS 共有フォルダ）**］を選択します。［**NFS Shared Folder（NFS 共有フォルダ）**］フィールドに、NFS サーバおよびファイル ディレクトリへのパス（たとえば「**fileserver.company.net:/backup_path**」）を入力します。
5. ［**Schedule（スケジュール）**］で、デフォルト設定を受け入れるか、別のバックアップ スケジュールを指定します。
   たとえば、月曜日と水曜日の午前 2 時にバックアップを作成するようスケジュールできます。
6. ［**Save（保存）**］をクリックします。

プライマリ インスタンスまたはレプリカ インスタンスのスナップショット

VMware スナップショットを作成すると、RSA Authentication Manager のプライマリ インスタンスまたはレプリカ インスタンスの特定の時点の状態を保存できます。ただし、スナップショットは Operations Console のバックアップ機能に代わるものではありません。スナップショットはテスト環境で極めて便利です。導入環境に加えた変更をすばやく元に戻せるためです。本番の導入環境をリストアする目的であれば、Operations Console を使用して Authentication Manager の最新のバックアップを管理することを推奨します。

Authentication Manager インスタンスのスナップショットを作成する際には、次の設定を指定する必要があります。

- 仮想マシンのメモリは保存しない。
- 静止ゲスト ファイル システムを選択する。このオプションにより、Authentication Manager インスタンスで実行中のプロセスが一時停止します。

詳細な手順については、VMware vSphere Client のドキュメントを参照してください。

Authentication Manager インスタンスをスナップショットで復元する場合は、追加のタスクを実行する必要があります。詳細については、428 ページのプライマリ インスタンスまたはレプリカ インスタンスのスナップショットおよび 445 ページのスナップショットによるレプリカ インスタンスの復元を参照してください。

プライマリ インスタンス データのリストア

プライマリ インスタンスのデータを誤って削除してしまったが、プライマリ インスタンスが正常に機能している場合、Operations Console の［Restore from Backup（バックアップからのリストア）］を使用して削除されたデータをリストアできます。

重要：プライマリ インスタンスに障害が発生している場合は、削除されたデータをリストアしても復旧させることはできません。逆に更なる問題を引き起こす可能性があります。障害が発生したプライマリ インスタンスをリストアするには、433 ページのプライマリ インスタンスのリストアを参照してください。

［Restore from Backup（バックアップからのリストア）］を使用する場合、次のアクティビティが実行されます。

- RSA Authentication Manager サービスが停止するため、他のプロセスがデータベースに接続できなくなる。リストア処理中は、プライマリ インスタンスでの管理操作および認証操作を実行できない。
- リモートの保存場所に保存されているバックアップ データがプライマリ インスタンスにコピーされる。
- バックアップ データによって、既存のすべてのデータが上書きされる。
- システム パスワードやデータベース パスワードなどの一部の保護されたデータがリストアされる。

［Restore from Backup（バックアップからのリストア）］の操作では、バックアップ作成後に変更されたデータはリストアされません。それらの変更は失われます。このため、ユーザーはバックアップを作成する前に使用したクレデンシャルを入力する必要があります。同様に、バックアップが作成された後に収集した行動パターンデータおよびデバイス データは使用できなくなるため、リスク ベース認証ユーザーはユーザー確認を求められる場合があります。バックアップに含まれるサード パーティ CA（認証局）から発行されたすべてのコンソール証明書はリストアされますが、これらのコンソール証明書はどれもアクティブになりません。リストア処理では導入環境のアクティブな証明書は変更されません。リストア処理が完了すると、導入環境のアクティブな証明書はアクティブな状態を維持します。

バックアップから導入環境データをリストアした後、リストアされた証明書のいずれかをアクティブ化する場合は、Operations Console を使用します。たとえば、古い導入環境のデフォルトの証明書を、サード パーティ CA（認証局）が署名した証明書に置換した場合、この証明書はリストアされますが、アクティブではありません。Operations Console を使用して、リストアされた導入環境でこの証明書をアクティブ化できます。操作手順については、201 ページのコンソール証明書の置換を参照してください。

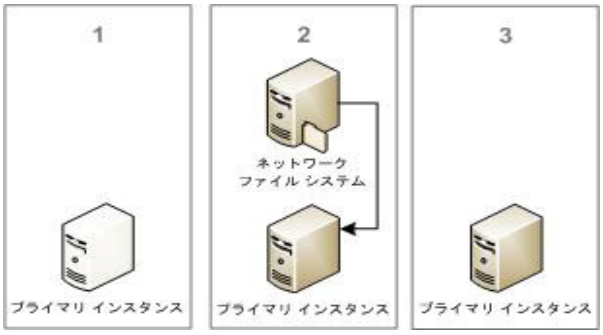
スタンドアロン導入環境でのプライマリ インスタンス データのリストア

スタンドアロン導入環境で誤って削除したデータをリストアするには、次のタスクを完了します。

処理手順

1. プライマリ インスタンスをトラブルシューティングして、データは失われているがプライマリ インスタンスはまだ正常に機能していることを判定します。操作手順については、417 ページの導入環境の問題のトラブルシューティングを参照してください。
2. ［Restore from Backup（バックアップからのリストア）］の処理手順を実行します。操作手順については、431 ページのバックアップからのリストアを参照してください。

次の図は、この処理を示しています。



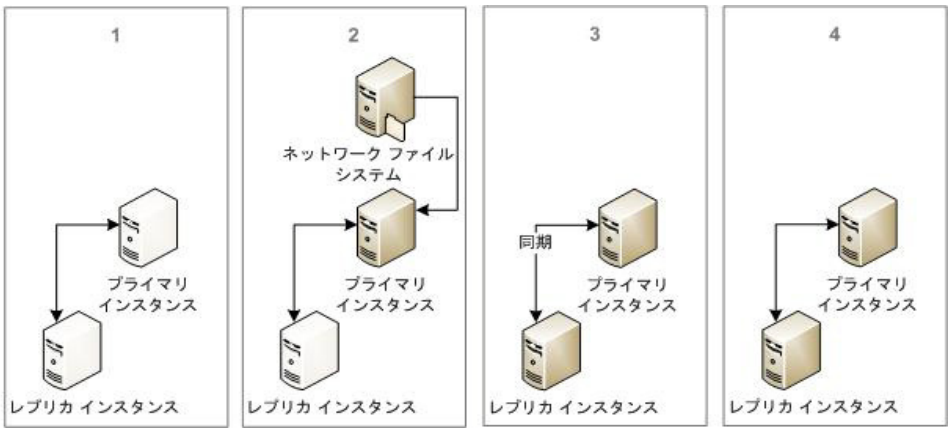
レプリケーション導入環境でのプライマリ インスタンス データのリストア

データがプライマリ インスタンスで誤って削除され、失われたデータがレプリカ インスタンスにレプリケーションされている場合、以下のタスクを完了することによりプライマリ インスタンスのデータをリストアできます。

処理手順

1. プライマリ インスタンスをトラブルシューティングして、データは失われているがプライマリ インスタンスはまだ正常に機能していることを判定します。操作手順については、417 ページの導入環境の問題のトラブルシューティングを参照してください。
2. ［Restore from Backup（バックアップからのリストア）］の処理手順を実行します。操作手順については、431 ページのバックアップからのリストアを参照してください。
3. 各レプリカ インスタンスを手動で同期します。操作手順については、422 ページのレプリカ インスタンスの同期を参照してください。

次の図は、この処理を示しています。



バックアップからのリストア

この手順では、バックアップから環境導入データをリストアします。

データのリストアの実行中は、管理操作および認証操作を実行できません。認証サービスの停止と起動が行われるため、リストア プロセスはバックアップ プロセスよりも時間がかかります。データのリストアにかかる時間の長さは、内部データベースのサイズによっても異なります。内部データベースが大きい場合は、プロセスの完了に時間がかかります。

開始する前に

- バックアップを作成しておく必要があります。
- Operations Console 管理者である必要があります。

手順

1. Operations Console で、［**Maintenance（保守）**］＞［**Backup and Restore（バックアップとリストア）**］＞［**Restore from Backup（バックアップからのリストア）**］の順にクリックします。
2. ［**Backup Location（バックアップ場所）**］で、以下のいずれかを実行します。
   - ［**Local Authentication Manager Server（ローカル Authentication Manager サーバ）**］を選択します。
   - ［**Windows Shared Folder（Windows 共有フォルダ）**］を選択します。
     - ［**Windows Shared Folder（Windows 共有フォルダ）**］フィールドに、既存の Windows 共有フォルダへのパス（たとえば、「**¥primary.company.net¥backup_path**」）を入力します。
     - 共有フォルダにユーザー名が必要な場合は、［**Folder User Name（フォルダ ユーザー名）**］フィールドにユーザー名（たとえば、「Domain1¥User1」）を入力します。
     - 共有フォルダにパスワードが必要な場合は、［**Folder Password（フォルダ パスワード）**］フィールドにパスワード（たとえば、「password1」）を入力します。
   - ［**NFS (Network File System) Shared Folder（NFS 共有フォルダ）**］を選択します。
     ［**NFS Shared Folder（NFS 共有フォルダ）**］フィールドに、NFS サーバ ホスト名および NFS 共有フォルダへのパスを入力します（たとえば、「**fileserver.company.net:/backup_path**」）。

3. ［**Restore Options（リストアのオプション）**］で、以下のいずれかを実行します。
   - ［**All Data（すべてのデータ）**］を選択して、導入環境データをリストアします。
     ［All Data（すべてのデータ）］オプションを選択した場合、導入環境のリストア中は管理または認証操作を実行できません。
   - ［**Log Data Only（ログ データのみ）**］を選択して、管理監査ログ、ランタイム監査ログ、システムログのデータをリストアします。
     レプリカ インスタンスを昇格させて、前のプライマリ インスタンスから新しいプライマリ インスタンスへ履歴ログ データを転送する場合は、このオプションを選択します。
4. ［**Next（次へ）**］をクリックします。
   バックアップのリストが表示されます。［**Log Data Only（ログ データのみ）**］を選択した場合、現在の導入環境で作成されたバックアップのみが表示されます。
5. 使用するバックアップ（.RSAbackup）を選択し、［**Next（次へ）**］をクリックします。
   現在の導入環境で作成された最新の正常なバックアップを使用する必要があります。
6. ［Restore from Backup（バックアップからのリストア）］ページで、適切なバックアップを選択したことを確認し、以下のいずれかを実行します。
   - 別のバックアップを選択するには、［**Back（戻る）**］をクリックします。
   - 選択したバックアップをリストアするには、このバックアップのパスワードを入力し、［**Restore（リストア）**］をクリックします。
     ［Progress Monitor（進行状況）］ページが表示されます。
7. リストア プロセスが完了したら、［**Done（完了）**］をクリックします。

次のステップ

- レプリケーション導入環境では、各レプリカ インスタンスをリストアされたプライマリ インスタンスと同期します。操作手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの同期」を参照してください。
- レプリカ インスタンスに Web Tier が関連づけられている場合は、Web Tier パッケージを作成し、Web Tier インストーラを実行します。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「Web Tier のインストール」の章を参照してください。

プライマリ インスタンスのリストア

プライマリ インスタンスに障害が発生した原因がデータベース スキーマの変更または重要なアプリケーション ファイルの削除のどちらかである場合、プライマリ インスタンスが使用不可になる可能性があります。

プライマリ インスタンスが使用不可になると、導入環境を管理できません。たとえば、プライマリ インスタンスがないとユーザーを追加することはできません。

プライマリ インスタンスに障害が発生していると思われる場合は、次のいずれかの方法を使用してプライマリ インスタンスをリストアできます。

- プライマリ インスタンスの置換
- レプリカ インスタンスの昇格
- プライマリ インスタンスまたはレプリカ インスタンスのスナップショット

プライマリ インスタンスの置換

プライマリ インスタンスを新しいアプライアンスに置換し、[Restore from Backup（バックアップからのリストア）] を使用してプライマリ インスタンス データをリストアすることで、障害が発生したプライマリ インスタンスをリストアできます。

バックアップを使用して、障害が発生したプライマリ インスタンスと異なる IP アドレスまたはホスト名を持つプライマリ インスタンスをリストアする場合、アプライアンスを置換した後で **Authentication Manager** 構成ファイル（**sdconf.rec**）を生成し、このファイルを各認証エージェントにインストールする必要があります。

障害が発生したプライマリ インスタンスを置換するには時間がかかる場合があります。レプリケーション導入環境で、データをプライマリ インスタンスに送信できないためにレプリカ インスタンスのストレージ領域が不足している場合は、レプリカ インスタンスも応答しなくなる可能性があります。このような状況が発生した場合、レプリカ インスタンスはユーザーを認証できません。

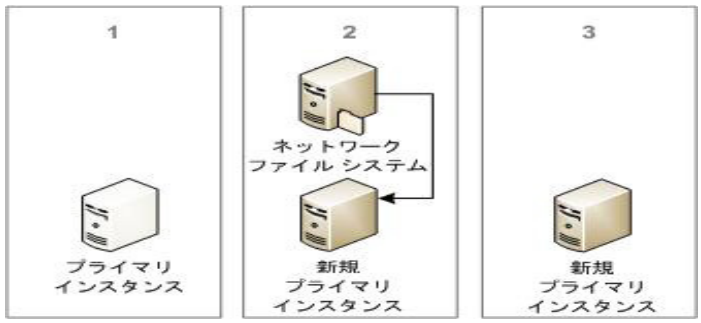
スタンドアロン導入環境でのプライマリ インスタンスの置換

スタンドアロン導入環境で障害が発生したプライマリ インスタンスを置換するには、次のタスクを実行します。

処理手順

1. 新しいプライマリ アプライアンスを導入および構成し、障害が発生したプライマリ インスタンスと置換します。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
2. ［Restore from Backup（バックアップからのリストア）］を使用して、新しいアプライアンス上に古いプライマリ インスタンスのバックアップをリストアします。操作手順については、431 ページのバックアップからのリストアを参照してください。
3. （オプション）別の IP アドレスまたはホスト名を持つプライマリ インスタンスにバックアップをリストアする場合は、Authentication Manager 構成ファイル（**sdconf.rec**）を生成して各認証エージェントにインストールします。
   構成ファイルの生成手順については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。
   構成ファイルのインストール手順については、エージェントのドキュメントを参照してください。
4. （オプション）導入環境が別のレルムと信頼関係を構築しており、新しいホスト名で仮想マシンのプライマリ インスタンスをリストアした場合、信頼関係を修復する必要があります。操作手順については、447 ページの信頼関係の修復を参照してください。
5. vSphere Client を使用して、ディスクから古いプライマリ インスタンスの仮想マシンを削除します。操作手順については、vSphere のドキュメントを参照してください。

次の図は、この処理を示しています。



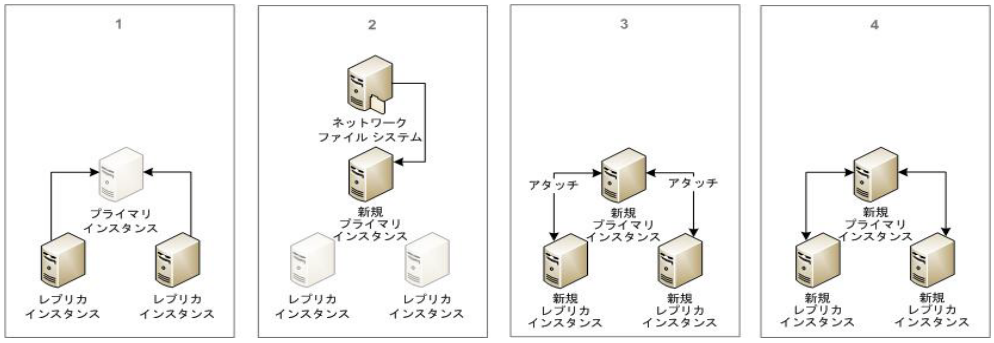
レプリケーション導入環境でのプライマリ インスタンスの置換

レプリケーション導入環境で障害が発生したプライマリ インスタンスを置換するには、次のタスクを実行します。

処理手順

1. vSphere Client を使用して、各レプリカ インスタンスの仮想マシンを一時停止します。操作手順については、vSphere のドキュメントを参照してください。
2. 新しいプライマリ アプライアンスを導入および構成し、障害が発生したプライマリ インスタンスと置換します。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
3. [Restore from Backup（バックアップからのリストア）]を使用して、新しいアプライアンス上に古いプライマリ インスタンスのバックアップをリストアします。操作手順については、431 ページのバックアップからのリストアを参照してください。
   リストア作業により、各レプリカ インスタンスが自動的に導入環境から削除されます。
4. 新しいレプリカ インスタンスを導入および構成して、削除された各レプリカ インスタンスを置換します。また、各レプリカ インスタンスをプライマリ インスタンスにアタッチします。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
5. （オプション）別の IP アドレスまたはホスト名を持つプライマリ インスタンスにバックアップをリストアした場合は、Authentication Manager 構成ファイル（**sdconf.rec**）を生成して各認証エージェントにインストールします。
   構成ファイルの生成手順については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。
   構成ファイルのインストール手順については、エージェントのドキュメントを参照してください。
6. （オプション）導入環境が別のレルムと信頼関係を構築しており、新しいホスト名で仮想マシンのプライマリ インスタンスをリストアした場合、信頼関係を修復する必要があります。操作手順については、447 ページの信頼関係の修復を参照してください。
7. vSphere Client を使用して、ディスクから古いプライマリ インスタンスの仮想マシンおよび古いレプリカ インスタンスの仮想マシンをすべて削除します。操作手順については、vSphere のドキュメントを参照してください。

次の図は、この処理を示しています。



レプリカ インスタンスの昇格

障害のあるプライマリ インスタンスを復旧するため、レプリカインスタンスをプライマリ インスタンスに昇格させることができます。

プライマリ インスタンスを新しいアプライアンスで置き換えるよりも、レプリカ インスタンスを昇格させてプライマリ インスタンスを復旧する方が、短時間で処理できます。ただし、昇格させるレプリカ インスタンスに対して、Operations Console 管理者が物理的にアクセスできる必要があります。これにより、進行中の管理が容易になります。

レプリカ インスタンスをプライマリ インスタンスに昇格させると、導入環境のトポロジーが次のように変更されます。

- 障害が発生しているプライマリ インスタンスは、導入環境から削除される。
- 昇格されたレプリカ インスタンスが、新しいプライマリ インスタンスになる。
- 新しいプライマリ インスタンスの RADIUS サーバが、RADIUS プライマリになる。別のレプリカ RADIUS サーバを個別に昇格させることはできません。
- Web Tier が古いプライマリ インスタンスに関連づけられている場合は、古い プライマリ インスタンスに関連づけられた Web Tier を再起動する必要がある。
- 導入環境内のいずれかのレプリカ インスタンスに関連づけられている Web Tier がある場合は、それらの Web Tier を再起動する必要がある。

1 つのレプリカ インスタンスを持つ導入環境でのレプリカ インスタンスの昇格

レプリカ インスタンスをプライマリ インスタンスに昇格させるには、次のタスクを実行します。

開始する前に

レプリカ インスタンスを昇格させる前に、プライマリ インスタンスが応答しないことを確認してください。

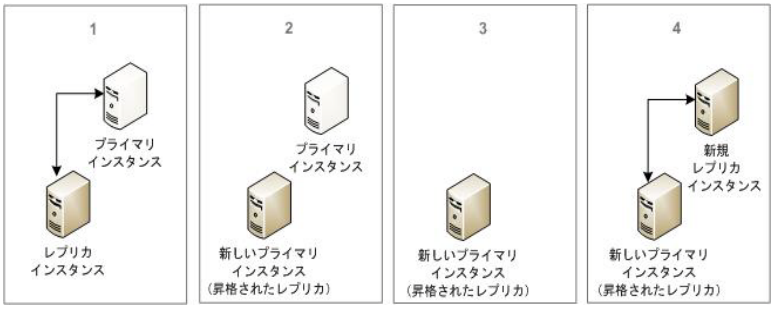
プライマリ インスタンスが部分的に機能している場合、vSphere Client を使用してプライマリ インスタンスの仮想マシンをシャットダウンします。操作手順については、vSphere のドキュメントを参照してください。

処理手順

1. レプリカ インスタンスをプライマリ インスタンスに昇格します。
   操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。
2. 導入環境で Web Tier を使用している場合は、次の操作を実行します。
   a. Web Tier が古いプライマリ インスタンスと関連づけられている場合は、すべての Web Tier を再起動します。
      操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。
   b. Web Tier がレプリカ インスタンスと関連づけられている場合は、Web Tier のステータスが［**Offline（オフライン）**］と表示されるまで待ちます。これには 30 分ほどかかる場合があります。各 Web Tier の Bootstrapper Server および Web Tier サービスを再起動し、Web Tier のステータスが［**Online（オンライン）**］と表示されるまで待ってから Web Tier サービスにアクセスします。
      操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。
3. （オプション）古いプライマリ インスタンスの履歴ログ データを新しいプライマリ インスタンス上で使用可能にするためには、古いプライマリ インスタンスの最後の良好な状態のバックアップからログ データをリストアします。
   操作手順については、431 ページのバックアップからのリストアを参照してください。
4. 新しいレプリカ アプライアンスを導入および構成して、昇格したレプリカ インスタンスを置換します。また、新しいレプリカ インスタンスを新しいプライマリ インスタンスにアタッチします。
   操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「Deploying a Replica Appliance（レプリカ アプライアンスの導入）」の章を参照してください。
5. 新しいプライマリ インスタンスをバックアップします。
   操作手順については、425 ページの今すぐバックアップ機能によるバックアップの作成を参照してください。

6. vSphere Client を使用して、ディスクから古いプライマリ インスタンスの仮想マシンを削除します。
   操作手順については、vSphere のドキュメントを参照してください。

次の図は、この処理を示しています。



複数のレプリカ インスタンスを持つ導入環境でのレプリカ インスタンスの昇格

レプリカ インスタンスをプライマリ インスタンスに昇格させるには、次のタスクを実行します。

開始する前に

レプリカ インスタンスを昇格させる前に、プライマリ インスタンスが応答しないことを確認してください。

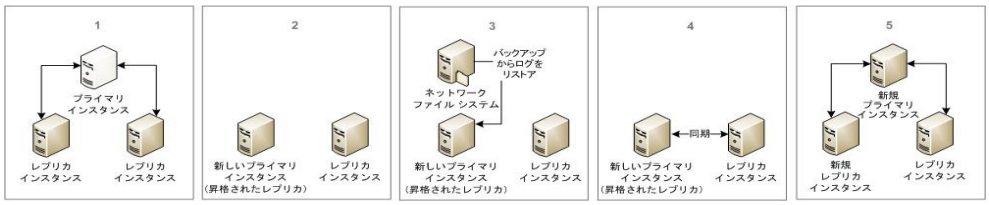
プライマリ インスタンスが部分的に機能している場合、vSphere Client を使用してプライマリ インスタンスの仮想マシンをシャットダウンします。操作手順については、vSphere のドキュメントを参照してください。

処理手順

1. レプリカ インスタンスを、プライマリ インスタンスに昇格させます。
   操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。
2. 導入環境で Web Tier を使用している場合は、次の操作を実行します。
   a. Web Tier が古いプライマリ インスタンスと関連づけられている場合は、すべての Web Tier を再起動します。
      操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。
   b. Web Tier がレプリカ インスタンスと関連づけられている場合は、Web Tier のステータスが［**Offline（オフライン）**］と表示されるまで待ちます。これには 30 分ほどかかる場合があります。各 Web Tier の Bootstrapper Server および Web Tier サービスを再起動し、Web Tier のステータスが［**Online（オンライン）**］と表示されるまで待ってから Web Tier サービスにアクセスします。
      操作手順については、439 ページのレプリカ インスタンスの昇格を参照してください。

3. （オプション）古いプライマリ インスタンスの履歴ログ データを新しいプライマリ インスタンス上で使用可能にするためには、古いプライマリ インスタンスの最後の良好な状態のバックアップからログ データをリストアします。
   操作手順については、431 ページのバックアップからのリストアを参照してください。
4. 新しいレプリカ インスタンスを導入および構成して、昇格したレプリカ インスタンスを置換します。また、新しいレプリカ インスタンスを新しいプライマリ インスタンスにアタッチします。
   操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「Deploying a Replica Appliance（レプリカ アプライアンスの導入）」の章を参照してください。
5. 新しいプライマリ インスタンスをバックアップします。
   操作手順については、425 ページの今すぐバックアップ機能によるバックアップの作成を参照してください。
6. vSphere Client を使用して、ディスクから古いプライマリ インスタンスの仮想マシンを削除します。
   操作手順については、vSphere のドキュメントを参照してください。

次の図は、この処理を示しています。



レプリカ インスタンスの昇格

この手順では、正常に機能しないプライマリ インスタンスを導入環境から削除し、レプリカ インスタンスを新しいプライマリ インスタンスに昇格させます。レプリカ インスタンスを昇格させると、導入環境を管理する機能が復旧します。

レプリカ インスタンスの昇格処理の間は、レプリカでの認証や、ユーザーの追加などの管理機能を実行できません。

開始する前に

Operations Console 管理者である必要があります。

手順

1. 昇格させるレプリカ インスタンスの Operations Console にログオンし、［**Deployment Configuration（導入環境の構成）**］＞［**Instances（インスタンス）**］＞［**Promote to Primary（プライマリへの昇格）**］の順にクリックします。
2. ［Promote Replica to Primary（レプリカをプライマリに昇格）］ページの［**Current Replica Instance Details（現在のレプリカ インスタンスの詳細）**］で情報を参照し、これが昇格させるレプリカ インスタンスであることを確認します。
3. ［**Confirmation（確認）**］で、［**Yes, promote the replica（はい、レプリカを昇格します）**］を選択して、［**Promote（昇格）**］をクリックします。
   昇格の進行状況が表示されます。このプロセスの詳細を確認するには、［**Advanced Status View（詳細ステータス ビュー）**］をクリックします。
4. すべての昇格タスクが完了したら、［**Next（次へ）**］をクリックします。
5. ［**Summary/Results（サマリー / 結果）**］および［**Proposed Next Steps（次のステップの提案）**］の情報を確認し、［**Done（終了）**］をクリックします。

次のステップ

- 昇格プロセスが完了した後で、新しいプライマリ インスタンスの次の項目をチェックし、必要な変更を行います。

項目	手順
プライマリ インスタンス Web Tier： Web Tier が古いプライマリ インスタンスに関連づけられている場合は、次のステップを実行します。 1. 各レプリカ インスタンスのレプリケーション ステータスをチェックします。レプリケーション ステータスが［**Normal（正常）**］と表示されていることを確認します。 2. すべてのレプリカ インスタンスのステータスが［**Normal（正常）**］と表示された後、サーバ リストのチェックが開始されるまで 5 分間待ちます。 3. 各 Web Tier で Bootstrapper Server および Web Tier サービスを再起動します。	RSA Operations Console ヘルプのトピック「レプリケーション ステータスの確認」を参照してください。 217 ページの Web Tier サービスの管理を参照してください。

項目	手順
レプリカ インスタンス Web Tier： Web Tier がレプリカ インスタンスに関連づけられている場合は、次のステップを実行します。 1. Web Tier ステータスが［**Offline（オフライン）**］と表示されるまで待ちます。 30 分ほどかかる場合があります。 2. 各 Web Tier で Bootstrapper Server および Web Tier サービスを再起動します。 3. Web Tier サービスにアクセスする前に、Web Tier ステータスが［**Online（オンライン）**］と表示されるまで待ちます。	RSA Operations Console ヘルプのトピック「Web Tier 導入環境の表示」を参照してください。 217 ページの Web Tier サービスの管理を参照してください。
アイデンティティ ソース：使用するアイデンティティ ソースが新しいプライマリ インスタンスに接続されていることを確認します。	RSA Operations Console ヘルプのトピック「導入環境のアイデンティティ ソースの表示」を参照してください。
スケジュール バックアップ：プライマリ インスタンスのバックアップ スケジュールを確認します。新しいプライマリ インスタンスがバックアップの保存場所に接続できることを確認します。	426 ページのスケジュール バックアップによるバックアップの作成を参照してください。
Self-Service Console URL：セルフ サービス ユーザー アカウントの変更を通知するメールに含まれる Self-Service Console の URL が正しいことを確認します。	RSA Security Console ヘルプのトピック「セルフ サービス ユーザー アカウント変更のメール通知の構成」を参照してください。
重大イベント通知：重大システム イベントの通知およびその他の目的（動的シード配布など）のメール通知が正しく送信されるよう SMTP 構成を確認します。	RSA Security Console ヘルプのトピック「SNMP の構成」を参照してください。

- 旧プライマリ インスタンスの履歴ログ データを新しいプライマリ インスタンスで利用するには、Operations Console を使用し、古いプライマリ インスタンスの最後の正常なバックアップからログ データをリストアします。操作手順については、431 ページのバックアップからのリストアを参照してください。

スナップショットによるプライマリ インスタンスの復元

不具合のあるプライマリ インスタンスをリストアするには、そのプライマリ インスタンスを以前の仮想マシンの状態のスナップショットに復元します。

スナップショットへの復元中にレプリカ インスタンスのアタッチまたは同期を試みると、レプリカ インスタンスのステータスは［**Attachment Unsuccessful (アタッチ失敗)**］になります。このステータスは、Operations Console の［Replication Status Report（レプリケーション ステータス レポート）］ページに表示されます。このような状態になった場合は、このレプリカ インスタンスを削除し、新しいレプリカ インスタンスをアタッチする必要があります。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。

プライマリ インスタンスのスナップショットを復元するときは、レプリカ インスタンスを復元する必要はありません。

スタンドアロン導入環境におけるスナップショットによるプライマリ インスタンスの復元

スタンドアロン導入環境では、プライマリ インスタンスのスナップショットを作成し、プライマリ インスタンスのスナップショットをいつでも復元できます。スナップショットの作成については、428 ページのプライマリ インスタンスまたはレプリカ インスタンスのスナップショットを参照してください。

レプリケーション導入環境におけるスナップショットによるプライマリ インスタンスの復元

レプリケーション導入環境では、プライマリ インスタンスのスナップショットを作成し、プライマリ インスタンスのスナップショットをいつでも復元できます。スナップショットの作成については、428 ページのプライマリ インスタンスまたはレプリカ インスタンスのスナップショットを参照してください。

スナップショットの復元後、アタッチされた稼働中のレプリカ インスタンスはいずれもプライマリ インスタンスと同期ずれの状態になるため、同期する必要があります。操作手順については、422 ページのレプリカ インスタンスの同期を参照してください。

その他のスナップショット タスク

スナップショットに保持される仮想マシンの状態は特定の時点の状態であるため、必要に応じて追加のタスクを実行してください。

- プライマリ インスタンスのホスト名を変更する前に作成したスナップショットでプライマリ インスタンスを復元した場合、プライマリ インスタンスはどのレプリカ インスタンスとも通信できなくなります。通信を回復するには、プライマリ インスタンスの Operations Console ですべてのレプリカ インスタンスを削除し、導入環境から各レプリカ インスタンス仮想マシンを削除します。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。削除したレプリカ インスタンスは、新しいレプリカ インスタンスに置き換え可能です。
- レプリカ インスタンスのホスト名を変更する前に作成したスナップショットでプライマリ インスタンスを復元した場合、プライマリ インスタンスはそのレプリカ インスタンスと通信できなくなります。通信を回復するには、プライマリ インスタンスの Operations Console でそのレプリカ インスタンスを削除し、導入環境からそのレプリカ インスタンス仮想マシンを削除します。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。削除したレプリカ インスタンスは、新しいレプリカ インスタンスに置き換え可能です。
- プライマリ インスタンスに昇格する前にレプリカ インスタンスのスナップショットを作成した場合、昇格後に不具合があっても、そのスナップショットを使用して新しいプライマリ インスタンスを復元することはできません。新しいプライマリ インスタンスに不具合がある場合は、別のレプリカ インスタンスをプライマリ インスタンスに昇格するか、新しいプライマリ インスタンスを導入し、プライマリ インスタンスのバックアップをリストアしてください。不具合のあるプライマリ インスタンス仮想マシンは、必要に応じて削除します。操作手順については、433 ページのプライマリ インスタンスのリストアを参照してください。
- スナップショットの作成後に削除したレプリカ インスタンスを含むスナップショットでプライマリ インスタンスを復元すると、プライマリ インスタンスの Operations Console には、これらのレプリカ インスタンスがアタッチされたままの状態で表示されます。導入環境の実際の状態を表示するには、これらのレプリカ インスタンスを Operations Console から削除し、必要に応じて各レプリカ インスタンス仮想マシンを削除します。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。
- レプリカ インスタンスをアタッチする前の導入環境でプライマリ インスタンスのスナップショットを作成し、作成後にレプリカ インスタンスをアタッチした場合、プライマリ インスタンスをスナップショットで復元しても、プライマリ インスタンスの Operations Console にそのレプリカ インスタンスは表示されません。導入環境の実際の状態を復元するには、このレプリカ インスタンスの仮想マシンを削除します。

レプリカ インスタンスのリストア

レプリカ インスタンスに障害が発生した原因が、データベース スキーマの変更または重要なアプリケーション ファイルの削除のいずれかである場合、レプリカ インスタンスが不安定になったり、応答しなくなる可能性があります。レプリカ インスタンスが使用不可になると、認証のフェイルオーバーができなくなり、プライマリ インスタンスが使用不可になった場合にすばやく管理をリストアすることもできなくなります。

レプリカ インスタンスに障害が発生していると思われる場合は、次のいずれかの方法を使用して障害が発生したレプリカ インスタンスをリストアできます。

- レプリカ インスタンスの置換
- スナップショットによるレプリカ インスタンスの復元

レプリカ インスタンスの置換

応答しないレプリカ インスタンスを置換するには、次のタスクを実行します。

開始する前に

レプリカ インスタンスを昇格させる前に、レプリカ インスタンスが応答しないことを確認してください。

レプリカ インスタンスが部分的に機能している場合、vSphere Client を使用してレプリカ インスタンスの仮想マシンをシャットダウンします。操作手順については、vSphere のドキュメントを参照してください。

処理手順

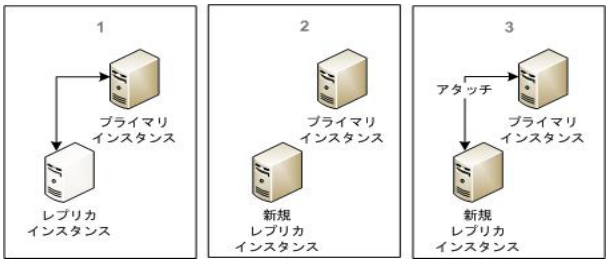
1. 応答しないレプリカ インスタンスを導入環境から削除します。操作手順については、Operations Console ヘルプのトピック「Delete a Replica Instance（レプリカ インスタンスの削除）」を参照してください。
2. 新しいレプリカ インスタンスを導入して、削除したレプリカ インスタンスと置換し、プライマリ インスタンスにアタッチします。

   操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「Deploying a Replica Appliance（レプリカ アプライアンスの導入）」の章を参照してください。
3. プライマリ インスタンスをバックアップします。

   操作手順については、425 ページの今すぐバックアップ機能によるバックアップの作成を参照してください。
4. vSphere Client を使用して、ディスクから古いレプリカ インスタンスの仮想マシンを削除します。

   操作手順については、vSphere のドキュメントを参照してください。

次の図は、この処理を示しています。



スナップショットによるレプリカ インスタンスの復元

不具合のあるレプリカ インスタンスをリストアするには、そのレプリカ インスタンスを以前の仮想マシンの状態のスナップショットで復元します。

レプリカ インスタンスをスナップショットで復元すると、プライマリ インスタンスに送信されていなかったレプリカ データは失われます。スナップショットの作成後にプライマリ インスタンスに送信されたレプリカ データは保持されます。

レプリカ インスタンスをスナップショットで復元するときは、プライマリ インスタンスを復元する必要はありません。

スナップショットによるレプリカ インスタンスの復元

レプリケーション導入環境では、レプリカ インスタンスのスナップショットを作成し、そのレプリカ インスタンスのスナップショットをいつでも復元できます。スナップショットの作成については、428 ページのプライマリ インスタンスまたはレプリカ インスタンスのスナップショットを参照してください。

スナップショットの復元後、レプリカ インスタンスはプライマリ インスタンスと同期ずれの状態になるので、同期する必要があります。操作手順については、422 ページのレプリカ インスタンスの同期を参照してください。

その他のスナップショット タスク

スナップショットには特定の時点の仮想マシンの状態が保持されるため、レプリカ インスタンスを特定のスナップショットで復元した後、プライマリ インスタンスがレプリカ インスタンスと通信できなくなる可能性があります。このような状態が発生するのは、次の変更を行う前に作成されたスナップショットでレプリカを復元する場合です。

- プライマリ インスタンスまたはレプリカ インスタンスに新しいホスト名を設定する。
- レプリカ インスタンスを昇格して、プライマリ インスタンスを置き換える。

プライマリ インスタンスとレプリカ インスタンスの通信を回復するには、プライマリ インスタンスの Operations Console でレプリカ インスタンスを削除し、導入環境からレプリカ インスタンス仮想マシンを削除します。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。削除したレプリカ インスタンスを新しいレプリカ インスタンスに置き換えます。

Web Tier のリストア

Web Tier が応答を停止した場合、リストアするには、次の処理手順を実行します。これらの処理手順は、プライマリ インスタンスとレプリカ インスタンスが正常に機能しており、Web Tier のみリストアする必要がある場合に適用されます。

処理手順

1. Web Tier サーバで、お使いのプラットフォームに応じた RSA Authentication Web Tier アンインストーラを実行します。操作手順については、以下のいずれかを参照してください。
   - 215 ページの Windows での Web Tier のアンインストール。
   - 216 ページの Linux での Web Tier のアンインストール。
2. Web Tier 導入レコードを削除するには
   a. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
   b. ［Web-Tier］ページで、削除する Web Tier を選択し、［**Delete（削除）**］をクリックします。

   詳細な操作手順については、Operations Console ヘルプのトピック「Delete a Web-Tier Deployment Record（Web Tier 導入レコードの削除）」を参照してください。
3. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Add New（新規追加）**］の順にクリックして、新しい Web Tier 導入レコードを追加します。操作手順については、Operations Console ヘルプのトピック「Add a Web-Tier Deployment Record（Web Tier 導入レコードの追加）」を参照してください。
4. プライマリ インスタンスで、Web Tier 導入パッケージを作成するには
   a. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
   b. ［Web-Tier Deployments（Web Tier の導入）］ページで、Web Tier パッケージを作成する Web Tier を選択してください。

c. ［Generate Web-Tier Deployment Package（Web Tier 導入パッケージの作成）］ページで、Web Tier パッケージ ファイルのパスワードを入力してください。

d. ［**Generate Web-Tier Package（Web Tier パッケージの作成）**］をクリックします。

e. ［**Download（ダウンロード）**］をクリックします。

5. お使いのプラットフォームに応じた RSA Authentication Web Tier インストーラを実行します。操作手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「Installing Web Tiers（Web Tier のインストール）」の章を参照してください。

信頼関係の修復

新しいホスト名のマシンに RSA Authentication Manager 8.0 プライマリ インスタンスをリストアするか、移行を実行する場合に、以前に別のレルムと信頼関係を構築していた場合は、次の信頼関係を修復する必要があります。

- **トラステッド レルム**。2 つの Authentication Manager 8.0 導入環境の間、または Authentication Manager 8.0 導入環境と Authentication Manager 7.1 導入環境の間の信頼関係です。操作手順については、448 ページのバージョン 8.0 レルムとの信頼関係の修復または 450 ページのバージョン 7.1 レルムとの信頼関係の修復を参照してください。

  トラステッド レルムの場合、修復プロセスにより、トラステッド ユーザーやグループなど、元のトラステッド レルムの情報が保持されます。このプロセスは、トラステッド レルムを追加するプロセスと似ています。移行またはリストアされるバージョン 8.0 導入環境の管理者と、相手のバージョン 8.0 または 7.1 導入環境の管理者の両方がこの修復プロセスに参加します。ただし、信頼パッケージをインポートするのは、トラステッド レルムの相手側の管理者だけです。移行またはリストアする導入環境の管理者は、信頼を修復する相手側の導入環境の管理者に信頼パッケージを提供します。このパッケージは、トラステッド レルムを修復するために使用されます。

- **クロス トラスト**。バージョン 8.0 とバージョン 6.1 の導入環境の間のレガシー信頼関係です。操作手順については、454 ページのレガシー トラステッド レルムの修復を参照してください。

  レガシー信頼関係の場合、修復プロセスでは、Authentication Manager 6.1 導入環境でレルム レコードのホスト名と IP アドレスを更新する必要があります。

バージョン 8.0 レルムとの信頼関係の修復

新しいホスト名のマシンに、バージョン 8.0 プライマリ インスタンスをリストアし、別のバージョン 8.0 レルムとの信頼関係を確立済みであった場合は、次の処理手順を実行して、2 つの RSA Authentication Manager 8.0 導入環境間の信頼を修復します。

開始する前に

リストアした導入環境の管理者および信頼を修復する導入環境の管理者は、この処理手順の実行中に直接コミュニケーションできる必要があります。

手順

1. リストアした導入環境の管理者は、次のステップを実行して信頼パッケージを生成します。
   a. Security Console で、［**Administration（管理）**］＞［**Trusted Realms（トラステッド レルム）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
   b. ［**Trusted Realm Name（トラステッド レルム名）**］で、修復するトラステッド レルム名をクリックします。
   c. コンテキスト メニューから［**Generate Trust Package（信頼パッケージの生成）**］をクリックし、ファイル（**TrustPackage.xml**）を保存します。
   d. 信頼パッケージを保存したら、安全性の高い方法で、信頼を修復する導入環境の管理者に送信します。
2. 信頼を修復する導入環境の管理者は、次のステップを実行して信頼パッケージをインポートします。
   a. 信頼パッケージを受け取ったら、［**Administration（管理）**］＞［**Trusted Realms（トラステッド レルム）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
   b. ［**Trusted Realm Name（トラステッド レルム名）**］で、修復するトラステッド レルム名をクリックします。
   c. コンテキスト メニューから［**Repair Trust（信頼の修復）**］をクリックします。
   d. ［**Trust Package from Trusted Realm（トラステッド レルムの信頼パッケージ）**］フィールドで、新しい信頼パッケージを参照してそのパッケージ ファイルへのパスを入力し、［**Open（開く）**］をクリックします。
   e. ［**Next（次へ）**］をクリックし、リストアした導入環境の管理者に連絡します。

3. リストアした導入環境の管理者は、次のステップを実行して、信頼を修復する導入環境の管理者との間で確認コードを共有します。
   a. Security Console で、[**Administration（管理）**] > [**Trusted Realms（トラステッド レルム）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
   b. [**Trusted Realm Name（トラステッド レルム名）**] で、修復するトラステッド レルム名をクリックします。
   c. コンテキスト メニューから [**View（表示）**] をクリックし、[**Current Realm Confirmation Code（現在のレルム確認コード）**] に表示された確認コードを読み取り、信頼を修復する導入環境の管理者にそのコードを伝え、信頼パッケージが有効であることを検証します。
      現在のレルム確認コードは、関係を修復する管理者側のトラステッド レルム確認コードと一致している必要があります。
4. 信頼を修復する導入環境の管理者は、次のステップを実行して信頼を修復します。
   a. [Update Trusted Realm（トラステッド レルムの更新）] ページの [**Trusted Realm Confirmation Code（トラステッド レルム確認コード）**] で、[**Trust Package Confirmation Code（信頼パッケージ確認コード）**] を読み取ってリストアした導入環境の管理者に伝え、信頼パッケージが有効であることを検証します。
      トラステッド レルム確認コードは、リストアした導入環境の管理者の現在のレルム確認コードと一致している必要があります。
      確認コードが一致しない場合は、リストアしたレルムの管理者に対して、新しい信頼パッケージを生成して送信するように依頼します。
   b. [**Confirm and Next（確認して次へ）**] をクリックします。
   c. （オプション）[**Authentication Status（認証ステータス）**] で、トラステッド レルムのユーザーをレルムで認証する場合は、[**Authenticate Trusted Users（トラステッド ユーザーを認証する）**] を選択します。
   d. [**Create Trusted Users in Security Domain（セキュリティ ドメインにトラステッド ユーザーを作成）**] では、トラステッド レルムのユーザーが属するセキュリティ ドメインを選択します。
      トラステッド レルムのユーザーを認証したら、そのユーザーはレルム内のセキュリティ ドメインに属する必要があります。選択するセキュリティ ドメインは、内部データベースをアイデンティティ ソースとして使用するように構成する必要があります。

e. （オプション）［**Trusted User Name Identifier（トラステッド ユーザーの名前識別子）**］フィールドで、トラステッド ユーザーであることを認識するための一意の識別子を入力し、［**Add（追加）**］をクリックします。一意の識別子として使用できるのは、ユーザーのドメイン名や、jsmith@company.com などのメール アドレスです。この値は、すべてのトラステッド レルムを通じて一意でなければなりません。

   たとえば、レルム A の John Smith がローカル レルムでは jsmith であるとします。あなたのレルムは、jsmith という ID を知りません。このフィールドに yourcompany.com と入力した場合、John Smith はあなたのレルム内では、jsmith@yourcompany.com として認識されます。

f. ［**Save（保存）**］をクリックします。

バージョン 7.1 レルムとの信頼関係の修復

新しいホスト名のマシンにバージョン 8.0 プライマリ インスタンスをリストアし、バージョン 7.1 レルムとの信頼関係を確立済みであった場合は、次の処理手順を実行して、RSA Authentication Manager 8.0 導入環境と RSA Authentication Manager 7.1 導入環境の間の信頼を修復します。

開始する前に

バージョン 8.0 の管理者とバージョン 7.1 の管理者は、この処理手順の実行中に直接コミュニケーションできる必要があります。

手順

1. バージョン 8.0 で、信頼パッケージを生成し、安全性の高い方法でそのパッケージをバージョン 7.1 の管理者に送信します。信頼パッケージを生成するには、次の操作を実行します。
   a. バージョン 8.0 の Security Console で、［**Administration（管理）**］＞［**Trusted Realms（トラステッド レルム）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。
   b. ［**Trusted Realm Name（トラステッド レルム名）**］で、修復するバージョン 7.1 のトラステッド レルムをクリックします。
   c. コンテキスト メニューから［**Generate Trust Package（信頼パッケージの生成）**］をクリックし、ファイル（**TrustPackage.xml**）を保存します。
2. バージョン 7.1 の管理者に対して、バージョン 8.0 の信頼パッケージをインポートして［**Current Realm Confirmation Code（現在のレルム確認コード）**］を記録するように依頼します。操作手順については、RSA Security Console ヘルプのトピック「信頼パッケージの再インポート」を参照するようにバージョン 7.1 の管理者にアドバイスします。

3. インポートの一環として、バージョン 7.1 の管理者は［**Trusted Realm Confirmation Code（トラステッド レルム確認コード）**］を確認する必要があります。バージョン 8.0 の管理者は、次の操作を実行し、レルムの確認コードを読み取り、バージョン 7.1 の管理者との間で共有します。

   a. バージョン 8.0 の Security Console で、［**Administration（管理）**］＞［**Trusted Realms（トラステッド レルム）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。

   b. ［**Trusted Realm Name（トラステッド レルム名）**］で、修復するバージョン 7.1 のレルムをクリックします。

   c. コンテキスト メニューから［**View（表示）**］をクリックし、［**Current Realm Confirmation Code（現在のレルム確認コード）**］で確認コードを探します。確認コードを読み取り、バージョン 7.1 の管理者にそのコードを伝え、信頼パッケージが有効であることを検証します。

      バージョン 8.0 の［**Current Realm Confirmation Code（現在のレルム確認コード）**］とバージョン 7.1 の［**Trusted Realm Confirmation Code（トラステッド レルム確認コード）**］は一致している必要があります。確認コードが一致しない場合は、新しい信頼パッケージを生成し、安全性の高い方法でそのパッケージをバージョン 7.1 の管理者に送信する必要があります。

不完全なバックアップを使用した場合のトラステッド レルムの不一致の修復

バックアップを使用して新しい仮想アプライアンスにプライマリ インスタンスをリストアする場合、トラステッド レルムの接続情報がバックアップに含まれます。導入環境と一致しないバックアップでプライマリ インスタンスをリストアする場合、不一致を修復する必要があります。たとえば、バックアップの作成後にトラステッド レルムを追加した場合、バックアップにはトラステッド レルムの接続情報は含まれません。このバックアップでプライマリ インスタンスをリストアする場合、追加のタスクを実行して不一致をなくす必要があります。

次の表は、バックアップが導入環境の現在の状態を反映していない場合、導入環境の不一致をリストアするために必要なタスクを示しています。

導入環境の関係	バックアップ	リストアのタイプ	必要なタスク
導入環境 A（バージョン 8.0 またはバージョン 7.1）が導入環境 B（バージョン 8.0）と信頼関係を構築している。	バックアップには信頼関係のデータが含まれていない。	導入環境 B を同じ仮想マシンのバックアップでリストアする。	1. 導入環境 A で信頼パッケージを再生成する。 2. 導入環境 B で、導入環境 A との新しい信頼を追加する。

導入環境の関係	バックアップ	リストアのタイプ	必要なタスク
導入環境 A（バージョン 8.0 またはバージョン 7.1）が導入環境 B（バージョン 8.0）と信頼関係を構築している。	バックアップには信頼関係のデータが含まれていない。	導入環境 B を別の仮想マシンのバックアップでリストアする。	1. 導入環境 A で信頼パッケージを再生成する。 2. 導入環境 B で信頼パッケージを生成する。 3. 導入環境 A がバージョン 7.1 の場合、導入環境 B の信頼を削除後、新規追加する。導入環境 A がバージョン 8.0 の場合、導入環境 B の信頼を修復する。 4. 導入環境 B で、導入環境 A の信頼を修復する。
導入環境 A（バージョン 6.1）が導入環境 B（バージョン 8.0）と信頼関係を構築している。	バックアップには信頼関係のデータが含まれていない。	導入環境 B を同じ仮想マシンのバックアップでリストアする。	導入環境 A で、レルム（導入環境 B）を削除する。
導入環境 A（バージョン 6.1）が導入環境 B（バージョン 8.0）と信頼関係を構築している。	バックアップには信頼関係のデータが含まれていない。	導入環境 B を別の仮想マシンのバックアップでリストアする。	導入環境 A で、レルム（導入環境 B）を削除する。
導入環境 A（バージョン 8.0 またはバージョン 7.1）が導入環境 B（バージョン 8.0）と信頼関係を構築していない。	バックアップに信頼関係のデータが含まれている。	導入環境 B を同じ仮想マシンのバックアップでリストアする。	1. 導入環境 A で信頼パッケージを生成する。 2. 導入環境 B で信頼パッケージを再生成する。 3. 導入環境 A で、新しい信頼を追加する。 4. 導入環境 B で、導入環境 A との新しい信頼を修復する。

導入環境の関係	バックアップ	リストアのタイプ	必要なタスク
導入環境 A（バージョン 8.0 またはバージョン 7.1）が導入環境 B（バージョン 8.0）と信頼関係を構築していない。	バックアップに信頼関係のデータが含まれている。	導入環境 B を別の仮想マシンのバックアップでリストアする。	1. 導入環境 A で信頼パッケージを生成する。 2. 導入環境 B で信頼パッケージを再生成する。 3. 導入環境 A で、導入環境 B の新しい信頼を追加する。 4. 導入環境 B で、導入環境 A の新しい信頼を修復する。
導入環境 A（バージョン 6.1）が導入環境 B（バージョン 8.0）と信頼関係を構築していない。	バックアップに信頼関係のデータが含まれている。	導入環境 B を同じ仮想マシンのバックアップでリストアする。	1. 導入環境 B で、導入環境 A との古いレルム間認証を削除する。 2. 導入環境 A で、導入環境 B とのレルム間認証を有効化する。
導入環境 A（バージョン 6.1）が導入環境 B（バージョン 8.0）と信頼関係を構築していない。	バックアップに信頼関係のデータが含まれている。	導入環境 B を別の仮想マシンのバックアップでリストアする。	1. 導入環境 B で、導入環境 A との古いレルム間認証を削除する。 2. 導入環境 A で、導入環境 B とのレルム間認証を有効化する。

レルム間認証の有効化の詳細については、「RSA Authentication Manager 6.1 管理者ガイド」の「Realm Administration（レルム管理）」の章を参照してください。トラステッド レルムの作成の詳細については、465 ページのトラステッド レルムの管理を参照してください。

レガシー トラステッド レルムの修復

バックアップを使用して新しい仮想アプライアンス上にプライマリ インスタンスをリストアすると、内部データベースに保存されたレルム間認証の接続情報は使用できなくなります。レルム間認証をリストアするには、接続情報を修復する必要があります。

新しい仮想アプライアンス上にプライマリ インスタンスをリストアする場合、Progress Monitor にはトラステッド レルムも修復する必要があるかどうかを確認するメッセージが表示されます。Authentication Manager 6.1 のレガシー レルム側でレルム間認証がすでに有効化されている場合は、Authentication Manager 6.1 導入環境で、レルム レコードのホスト名と IP アドレスを更新して、信頼関係を修復します。

詳細については、RSA Authentication Manager 6.1 Host Mode Console ヘルプのトピック「Edit a Trusted Realm」を参照してください。

16 高度な管理

アプライアンスのオペレーティング システム上でのトラブルシューティングと高度な管理

Authentication Manager の管理には、Operations Console および Security Console を使用しますが、アプライアンスのオペレーティング システムにアクセスして次のような高度な管理タスクを実行する必要が生じる場合があります。

- RSA Authentication Manager CLU（コマンド ライン ユーティリティ）の実行。
- Authentication Manager サービスの停止と開始。
- アプライアンスの問題のトラブルシューティング。

アプライアンスのオペレーティング システムには、SSH（セキュア シェル）クライアントを使用してアクセスします。SSH クライアントは、SSH を使用してリモート コンピュータに接続するソフトウェア アプリケーションです。このクライアントは、アプライアンスにネットワーク接続可能なローカル コンピュータにインストールします。SSH クライアントを使用してアプライアンスのオペレーティング システムにアクセスするには、アプライアンスの SSH を有効化する必要があります。

VMware vSphere Client を使用して仮想アプライアンスのオペレーティング システムにアクセスすることもできます。

アプライアンスの SSH の有効化

SSH クライアントを使用してアプライアンスのオペレーティング システムにログオンするには、アプライアンスの SSH を有効化する必要があります。

アプライアンスのオペレーティング システムへのログオンに関しては、セッション有効期間を設定できます。管理者がセッションを無期限に開かれたままにすると、不正アクセスの危険がありますが、セッション有効期間によりこれを防ぐことができるため、重要なセキュリティ機能と言えます。セッション有効期間の設定は、SSH クライアントまたは VMware vSphere Client を使用してオペレーティング システムにアクセスするときに適用されます。

手順

1. Operations Console で、［**Administration（管理）**］＞［**Operating System Access（オペレーティング システム アクセス）**］の順にクリックします。
2. ［**Enable SSH（SSH の有効化）**］を選択します。

3. アイドル状態が続いたときにセッションをタイムアウトさせる場合は、［**Session Lifetime Settings（セッション有効期間の設定）**］で［**Time out idle sessions（アイドル セッションのタイムアウト）**］を選択し、タイムアウトまでの時間を入力します。
4. ［**Save（保存）**］をクリックします。

アプライアンスのオペレーティング システムへのログオン

SSH クライアントを使用して仮想アプライアンスのオペレーティング システムにログオンするには、次の手順を実行します。

開始する前に

- rsaadmin オペレーティング システム パスワードを入手する。
- アプライアンス仮想マシンのホスト名を入手する。
- アプライアンスの SSH を有効化する。

手順

1. SSH クライアントを起動し、IP アドレスまたは完全装飾ホスト名を使用してアプライアンスに接続します。
2. ユーザー名の入力を要求するプロンプトが表示されたら、オペレーティング システムのユーザー ID「**rsaadmin**」を入力して Enter キーを押します。
3. パスワードの入力を要求するプロンプトが表示されたら、rsaadmin オペレーティング システム アカウントのパスワードを入力し、Enter キーを押します。

Clam Antivirus ソフトウェアの実行

各 RSA Authentication Manager インスタンスには、ClamAV（Clam Antivirus）ソフトウェアが含まれています。ClamAV は、侵入や悪意のあるコードによるシステムまたはデータへのアクセスに対するリスクを低減することを目的としたオープン ソース ソフトウェア ツールキットです。ClamAV に対するソフトウェア アップデートは、RSA が提供するアップデートの一環としてのみ適用するようにしてください。ウイルス定義ファイルの更新、および Authentication Manager インスタンスに既知のマルウェアがないか ClamAV によるスキャンの実行は、お客様にて実施いただく必要があります。

開始する前に

- 以下の手順は、Linux のコマンドに関する知識があることを前提にしています。
- オペレーティング システム アカウントのユーザー ID **rsaadmin** のパスワードを入手してください。

- SSH（セキュア シェル）クライアントでオペレーティング システムにアクセスできるように、SSH を有効化する。または、VMware vSphere Client の OS コンソールからオペレーティング システムにアクセスすることもできます。SSH の使用手順については、455 ページのアプライアンスの SSH の有効化を参照してください。

手順

1. 導入環境の各インスタンスで、VMware vSphere Client または SSH（セキュア シェル）クライアントを使用してオペレーティング システムにアクセスします。
2. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用してアプライアンスのオペレーティング システムにログオンします。
3. ウイルス定義ファイルを更新します。以下のいずれかの手順を選択します。
   - Authentication Manager インスタンスがインターネットにアクセスできる場合は、最新のウイルス定義ファイルを自動的にダウンロードして適用できます。以下のコマンドを入力します。

     ```
     sudo /usr/bin/freshclam
     ```
   - Authentication Manager インスタンスがインターネットにアクセスできない場合は、**main.cvd** および **daily.cvd** ウイルス定義ファイルを ClamAV Web サイト（**http://www.clamav.net/**）から手動でダウンロードします。
     ファイルをインスタンスの **/var/lib/clamav/** ディレクトリにコピーします。
4. ファイルとディレクトリのウイルス スキャンを手動で実行するには、次のコマンドを入力します。

   ```
   sudo clamscan -r / --exclude-dir=/proc --exclude-dir=/sys
   --exclude-dir=/opt/rsa/am/rsapgdata
   --follow-dir-symlinks=0 --follow-file-symlinks=0
   --log=/var/log/clamav.log
   ```

   自動ウイルス スキャンをスケジュールするには、これと同じコマンドを実行する **cron** ジョブを作成します。
5. **/var/log/clamav.log** でスキャン結果をチェックします。

RSA Authentication Manager のサービス

製品の機能に必要な RSA Authentication Manager サービスは、すべて自動的に開始されます。これらのサービスは、手動で管理することもできます。

自動的に開始される RSA Authentication Manager サービス

自動的に開始される Authentication Manager サービスを次の表に示します。

サービス名	説明	詳細
console	RSA Console Server	Security Console と Self-Service Console をホストします。
biztier	RSA Runtime Server	
admin	RSA Administration Server と Operations Console	Operations Console をホストします。
db	RSA Database Server	
primary_replication	RSA Replication（プライマリ）	プライマリ インスタンスのみで実行されます。
replica_replication	RSA Replication（レプリカ）	レプリカ インスタンスのみで実行されます。
radius	RSA RADIUS Server	
radiusoc	RSA RADIUS Server Operations Console	

セキュリティ上の理由により、アプライアンスの SSH サービスは自動的に開始されません。SSH クライアントを使用してアプライアンスのオペレーティング システムにログオンするには、Operations Console で SSH を有効化する必要があります。詳細については、456 ページのアプライアンスのオペレーティング システムへのログオンを参照してください。

RSA Authentication Manager サービスの手動での管理

次の処理手順を使用して、RSA Authentication Manager のサービスを手動で管理します。選択したサービスまたはすべてのサービスに対して同時に次のアクションを実行できます。

- 停止
- 開始
- 現在のステータスの表示
- 再起動

処理手順

1. SSH クライアントまたは VMware vSphere Client を使用して、ユーザー ID **rsaadmin** と現在のオペレーティング システムのパスワードで、アプライアンスにログオンします。操作手順については、456 ページのアプライアンスのオペレーティング システムへのログオンを参照してください。
2. ディレクトリを変更します。次のように入力します。

   ```
   cd /opt/rsa/am/server
   ```

   Enter キーを押します。
3. コマンドを実行します。次のように入力し、Enter キーを押します。

   ```
   ./rsaserv stop|start|status|restart [service name]
   [nodep] [exclude service name]
   ```

   ここで、

   - stop、start、status、restart、nodep は、RSA サービスを管理するオプションです。依存関係のあるサービスを開始しない場合は、nodep を指定します。特定のサービスをコマンドから除外するには、exclude と service name を指定します。
   - service name は、管理する Authentication Manager サービスの名前です。

   サービス名：

   all（すべての RSA サービス）

   console（RSA Console Server）

   biztier（RSA Runtime Server）

   admin（RSA Administration Server と Operations Console）

   db（RSA Database Server）

   primary_replication（RSA Replication Primary）

   replica_replication（RSA Replication Replica）

   radiusoc（RSA RADIUS Server Operations Console）

   radius（RSA RADIUS Server）

   例：

   すべてのサービスを開始するには、次のコマンドを使用します。

   ```
   ./rsaserv start all
   ```

   依存関係のあるサービスを再起動せずにデータベース サーバを再起動するには、次のコマンドを使用します。

   ```
   ./rsaserv restart db nodep
   ```

   RSA Administration サービス以外のすべての RSA サービスを停止するには、次のコマンドを使用します。

   ```
   ./rsaserv stop all exclude admin
   ```

4. 終了したら、次のように入力します。

```
exit
```

Enter キーを押します。

スーパー管理者のリストア

スーパー管理者ロールは、あらかじめ定義されている管理者ロールで、導入環境全体における完全な管理者権限を備えた唯一のロールです。スーパー管理者は、次の操作を実行できます。

- 他のすべての管理者へのロールの委譲。
- セキュリティ ドメイン階層の作成。

スーパー管理者は導入時に作成されます。特定の重要なタスクを実行できるのはスーパー管理者のみです。導入環境には少なくとも 1 人のスーパー管理者が必要です。

スーパー管理者が削除された場合は、Super Admin Restoration ユーティリティ（restore-admin）を使用して新しいスーパー管理者を作成してください。RSA では、非常に信頼する管理者にスーパー管理者ロールを割り当てることを推奨します。

スーパー管理者のリストアが必要になるのは、次のような状況です。

- 唯一のスーパー管理者が導入環境から削除されたとき。
- ユーザーの誰にもスーパー管理者ロールが割り当てられていないとき。
- 唯一のスーパー管理者がロックアウトされているとき。

スーパー管理者がロックアウトされた場合には、次のいずれかの方法で回復できます。

- 別のスーパー管理者が手動でスーパー管理者をロック解除する。
- スーパー管理者に適用されているロックアウト ポリシーで自動ロック解除が可能な場合は、ロックアウトが期限切れになるまで待機する。
- これらの方法が使用できない場合に、Super Admin Restoration ユーティリティを使用します。操作手順については、461 ページのスーパー管理者のリストアを参照してください。

スーパー管理者のリストア

この処理手順を使用すると、Super Admin Restoration ユーティリティ（restore-admin）を使用して、スーパー管理者ユーザーを導入環境にリストアできます。

Super Admin Restoration ユーティリティは、緊急時に導入環境へのアクセスを回復するために使用されます。このユーティリティを使用して作成したスーパー管理者の有効期間は、デフォルトでは 24 時間です。スーパー管理者を作成するときに指定するパスワードに対しては、デフォルト パスワード ポリシーによる妥当性検査は行われません。RSA では、このユーティリティを使用する際には、デフォルト パスワード ポリシーを満たすパスワードを作成することをベスト プラクティスとして推奨しています。

コマンドラインに、他のオプションと同時に、Operations Console 管理者のクレデンシャルを入力することができますが、これによってセキュリティの脆弱性が生じる可能性があります。パスワードは、ユーティリティのプロンプトが表示されたときにのみ入力することを推奨します。

開始する前に

- Linux オペレーティング システムの操作に関する知識を持っている必要があります。
- この処理手順はレプリカ インスタンスでは実行しないでください。
- Operations Console を使用して SSH を有効化する必要があります。これにより、オペレーティング システムのシェル コマンド プロンプトにアクセスできるようになります。
- OS ログイン クレデンシャル（rsaadmin ログイン ID とパスワード）が必要です。これらのクレデンシャルにより、OS にログインして OS シェル コマンド プロンプトにアクセスできるようになります。
- Operations Console 管理者のクレデンシャルが必要です。restore-admin コマンドを実行するために必須です。

処理手順

1. SSH クライアントまたは VMware vSphere Client を使用して、ユーザー ID **rsaadmin** と現在のオペレーティング システムのパスワードで、アプライアンスにログオンします。操作手順については、456 ページのアプライアンスのオペレーティング システムへのログオンを参照してください。
2. ディレクトリを **/opt/rsa/am/utils** に変更します。
3. 次のように入力します。

   ```
   ./rsautil restore-admin -u newadmin -p adminpassword
   ```

   ここで、

   - newadmin は新しいスーパー管理者のユーザー ID です。

- adminpassword は新しいスーパー管理者のパスワードです。

Enter キーを押します。

4. Operations Console 管理者のユーザー名の入力を求めるプロンプトが表示されたら、Operations Console 管理者のユーザー ID を入力して、ENTER キーを押します。
5. プロンプトが表示されたら、Operations Console 管理者のパスワードを入力して、ENTER キーを押します。
6. 「**Are you sure you want to continue?(Y/N)**（続行しますか？（Y/N））」とプロンプトが表示されたら、**Y** を入力して、ENTER キーを押します。

次のステップ

Super Admin Restoration ユーティリティは、Security Console の認証ポリシーを LDAP_Password/RSA Password にリセットします。この変更を有効にするため、Operations Console を使用して、キャッシュをフラッシュしてください。操作手順については、423 ページのキャッシュのフラッシュを参照してください。

RSA Authentication Manager のアップデート

RSA は、Authentication Manager に対する製品アップデートをパッチおよびサービス パックの形式で定期的に発行します。RSA では、安全で効率的な導入環境を維持するために、利用可能になった製品アップデートはただちに適用することを推奨しています。各製品アップデートに対して、RSA では、アップデートの適用に関する重要な情報が含まれたリリース ノートを提供しています。問題を回避するには、アップデートを適用する前に、リリース ノートの情報をすべて読む必要があります。

新しい製品アップデートのメール通知を受信するには、**RSA SecurCare Online** にログオンし、Authentication Manager の「RSA SecurCare Notes & Security Advisories」に登録します。

製品アップデートは、**RSA SecurCare Online** からダウンロードします。アップデートは、ISO イメージの形式で提供されます。RSA では、ISO イメージを物理 DVD または CD-ROM に焼くことは推奨していません。代わりに、導入環境からアクセスできるディレクトリに ISO イメージを保存してください。

Operations Console を使用して、各プライマリおよびレプリカ インスタンスで製品アップデートを適用します。製品アップデートをダウンロードした後で、ISO イメージの場所を指定します。ローカル ブラウザから個々のアップデートをアップロードして適用することができます。また、NFS 共有、Windows 共有フォルダ、DVD/CD-ROM に格納されたアップデートをスキャンできます。スキャンの後で、適用するアップデートを個別に選択できます。

注：仮想アプライアンスに組み込まれたサード パーティ製品へのアップデートの適用は、RSA が提供するパッチの一部としてのみ実行してください。たとえば、仮想アプライアンス オペレーティング システムに対する必要なアップレーは RSA から提供します。

導入環境に Web Tier が含まれている場合は、Authentication Manager のバージョンを更新するときに Web Tier を更新する必要があります。Authentication Manager の Operations Console には、最新ではない Web Tier に対して、更新ボタンが表示されます。操作手順については、215 ページの Web Tier の更新を参照してください。

ソフトウェア バージョンの表示

処理手順

Security Console で［**Software Version Information**（ソフトウェア バージョンの表示）］をクリックします。

IP アドレスまたはホスト名の検証

Operations Console を使用してオペレーティング システムのコマンドを実行し、IP アドレスまたはホスト名を検証します。

処理手順

Operations Console ホーム ページで、［**Administration**（管理）］＞［**Network**（ネットワーク）］＞［**Network Tools**（ネットワーク ツール）］の順にクリックします。

詳細については、RSA Security Console ヘルプのトピック「Verify an IP Address or Hostname （IP アドレスまたはホスト名の検証）」を参照してください

17 トラステッド レルムの管理

トラステッド レルム

導入環境とは、プライマリ インスタンスと必要に応じて追加された 1 つ以上のレプリカ インスタンスで構成される RSA Authentication Manager インストール環境のことです。

レルムは 1 つの組織単位であり、ユーザーとユーザー グループ、トークン、パスワード ポリシー、エージェントなど、1 つの導入環境で管理されるすべてのオブジェクトが含まれます。各導入環境にはレルムが 1 つだけあります。

たとえば、ロンドンに本部がある会社がニューヨークにオフィスを持っているとします。ロンドンのオフィスとニューヨークのオフィスのそれぞれに Authentication Manager の導入環境があります。各導入環境で管理されるオブジェクトがレルムを構成します。ロンドン レルムとニューヨーク レルムです。

複数のレルム間で、信頼関係を持つことができます。これにより、あるレルムのユーザーが、別のレルムで認証し、その別のレルムのリソースにアクセスすることができるようになります。

たとえば、ロンドン レルムがニューヨーク レルムとの信頼関係を持っているとします。これは、ニューヨーク レルムがロンドン レルムのユーザーを「信頼」し、ニューヨーク レルムのユーザーと同じ権限を与えることを意味します。ロンドン オフィスのユーザーは、ニューヨークに滞在中、他のすべてのニューヨーク オフィスの ユーザーと同様にニューヨーク オフィスで認証を受けられます。

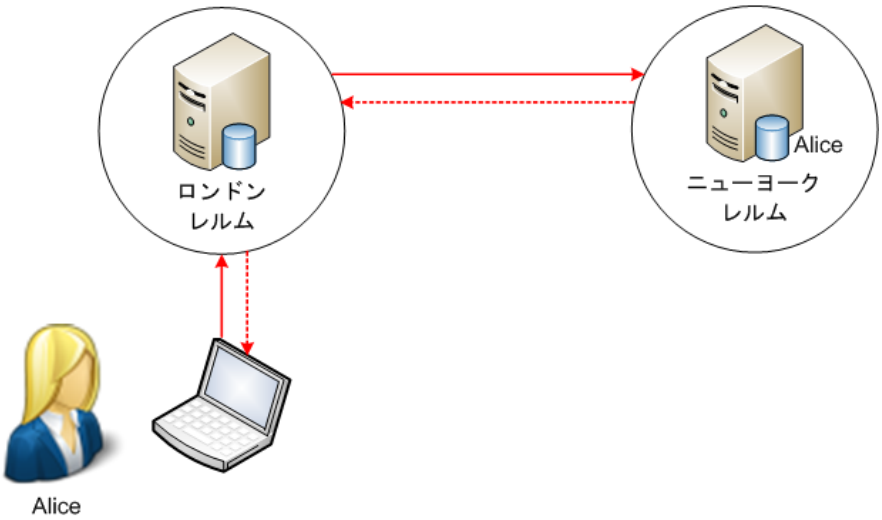
信頼関係は次のタスクを実行して作成します。

- 外部レルムをトラステッド レルムとして追加します。
- トラステッド レルムに属するトラステッド ユーザーを認証するエージェントを指定します。
- トラステッド ユーザーを指定します。トラステッド レルムの全ユーザーが認証を受けられるようにはしたくない場合があります。その場合は、トラステッド レルムのどのユーザーをトラステッド ユーザーとするかを指定します。トラステッド ユーザーだけが、認証を受けることができます。

信頼関係には単方向の信頼または双方向の信頼があります。単方向の信頼では、一方のレルムのトラステッド ユーザーだけが相手レルムで認証を受けることができます。

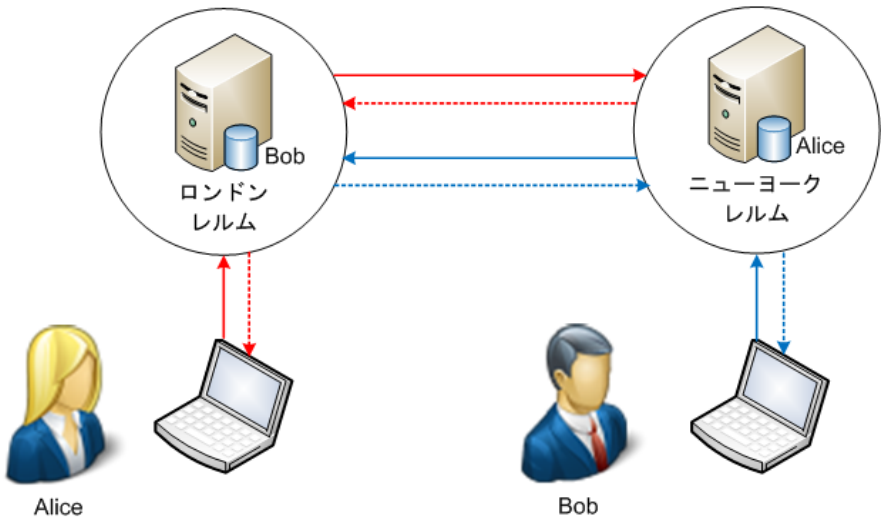
たとえば、ロンドンとニューヨークの間の信頼関係が単方向である場合、ロンドンのトラステッド ユーザーがニューヨークで認証を受けるか、ニューヨークのトラステッド ユーザーがロンドンで認証を受けるか、そのどちらか一方のみが可能です。双方向の信頼では、どちらのレルムのトラステッド ユーザーも、相手方のレルムで認証を受けられます。たとえば、ロンドンとニューヨークの間の信頼関係が双方向である場合、ロンドンのトラステッド ユーザーはニューヨークで認証を受けることができ、ニューヨークのトラステッド ユーザーもロンドンで認証を受けることができます。

次の図に、単方向の信頼を示します。ロンドンはニューヨークをトラステッド レルムとして追加しました。これにより、ニューヨーク レルムのトラステッド ユーザーである Alice は、ロンドン出張中にロンドン レルムで認証を受けることが可能になります。



ロンドン滞在中に、Alice はニューヨーク レルムの自分のクレデンシャル（ユーザー名とパスコード）を使用してロンドンの VPN（バーチャル プライベート ネットワーク）へアクセスを試行します。ロンドンの VPN サーバはエージェントによって保護されており、そのエージェントはトラステッドレルム認証に対応するよう構成されています。このエージェントは自分のレルム内では Alice というユーザーが見つからないため、他のレルムに Alice というユーザーがいないか探します。エージェントがニューヨーク レルムで Alice を見つけた後、ニューヨーク レルムは Alice のクレデンシャルを検証し、Alice を認証した後、Alice のアクセスを許可するようエージェントに指示します。

次の図に、双方向の信頼を示します。ロンドンはニューヨークをトラステッド レルムとして追加し、ニューヨークはロンドンをトラステッド レルムとして追加しました。これにより、ニューヨーク レルムのトラステッド ユーザーである Alice がロンドン レルムで認証を受けられるのと同時に、ロンドン レルムのトラステッド ユーザーである Bob がニューヨーク レルムで認証を受けられるようになります。



信頼関係の作成

2 つ以上のレルムが信頼関係を持つことができます。この信頼関係において、一方のレルムのユーザーは、他方のレルムで認証を受け、他方のレルムのリソースにアクセスすることができます。Security Console を使用して、これらのレルム間の信頼関係を作成して管理します。

- Authentication Manager 8.0 の 2 つのレルム
- Authentication Manager 8.0 のレルムと Authentication Manager 7.1 のレルム

手順

1. トラステッド レルムを追加します。操作手順については、468 ページのトラステッド レルムの追加を参照してください。
2. エージェントにトラステッド レルム認証の構成を行います。操作手順については、469 ページのトラステッド レルム認証のためのエージェントの構成を参照してください。
3. トラステッド ユーザーを追加します。操作手順については、472 ページのトラステッド ユーザーの追加を参照してください。
4. （オプション）トラステッド ユーザー グループを追加します。操作手順については、474 ページのトラステッド ユーザー グループの追加を参照してください。
5. （オプション）トラステッド ユーザーをトラステッド ユーザー グループに追加します。操作手順については、474 ページのトラステッド ユーザー グループへのトラステッド ユーザーの追加を参照してください。

トラステッド レルムの追加

信頼関係を作成するには、外部レルムをトラステッド レルムとして追加します。信頼関係により、ユーザーは次のレルム間で認証を行うことができます。

- 2 つの RSA Authentication Manager 8.0 のレルム
- Authentication Manager 8.0 のレルムと Authentication Manager 7.1 のレルム

開始する前に

- ホーム レルムの管理者とトラステッド レルムとして追加されるレルムの管理者が、次の手順を同時に実行する必要があります。
- ホーム レルムの管理者とトラステッド レルムとして追加されるレルムの管理者同士が、次の手順を実行するときにコミュニケーションをとれる必要があります。

手順

1. Security Console で、[**Administration（管理）**] > [**Trusted Realms（トラステッド レルム）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**Generate Trust Package（信頼パッケージの生成）**] で、[**Generate & Download（生成とダウンロード）**] をクリックします。
3. 信頼パッケージが生成されたら、安全性の高い方法で、信頼パッケージをトラステッド レルムの管理者に渡します。交換に、トラステッド レルムの管理者が生成した信頼パッケージを受け取ります。信頼パッケージを受け取ってから次の操作に進みます。
4. [**Trust Package from Trusted Realm（トラステッド レルムの信頼パッケージ）**] フィールドで、受け取った信頼パッケージを参照してそのパッケージ ファイルへのパスを入力し、[**Open（開く）**] をクリックします。
5. [**Next（次へ）**] をクリックします。
6. トラステッド レルムの管理者に、信頼パッケージ確認コードを確認します。確認コードを確認した後でのみ次のステップに進んでください。
7. [**Confirm and Next（確認して次へ）**] をクリックします。
8. [**Trusted Realm Name（トラステッド レルム名）**] フィールドに、トラステッド レルムを識別する一意のユーザー フレンドリーな名前（たとえば、ロンドン オフィス）を入力します。
9. トラステッド レルムのユーザーをレルムで認証する場合は、[**Authentication Status（認証ステータス）**] で、[**Authenticate Trusted Users（トラステッド ユーザーを認証する）**] を選択します。
10. [**Trusted Realm Status（トラステッド レルムのステータス）**] で、[**Enable Trusted Realm（トラステッド レルムを有効化する）**] を選択します。有効化すると、認証要求をトラステッド レルムに送信できるようになります。

11. ［**Create Trusted Users in Security Domain（セキュリティ ドメインにトラステッド ユーザーを作成）**］では、トラステッド レルムのユーザーが属するセキュリティ ドメインを選択します。

    トラステッド レルムのユーザーを認証したら、そのユーザーはレルム内のセキュリティ ドメインに属する必要があります。選択するセキュリティ ドメインは、内部データベースをアイデンティティ ソースとして使用するように構成する必要があります。

12. ［**Trusted User Name Identifier（トラステッド ユーザーの名前識別子）**］フィールドで、トラステッド ユーザーであることを認識するための一意の識別子を入力し、［**Add（追加）**］をクリックします。一意の識別子として使用できるのは、ユーザーのドメイン名や、jsmith@company.com などのメール アドレスです。この値は、すべてのトラステッド レルムを通じて一意でなければなりません。

    たとえば、レルム A の John Smith がローカル レルムでは jsmith であるとします。あなたのレルムは、jsmith という ID を知りません。このフィールドに yourcompany.com と入力した場合、John Smith はあなたのレルム内では、jsmith@yourcompany.com として認識されます。

13. ［**Save（保存）**］をクリックします。

14. Security Console で、［**Administration（管理）**］＞［**Trusted Realms（トラステッド レルム）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。

15. トラステッド レルムとのネットワーク接続をテストします。トラステッド レルムの名前をクリックし、コンテキスト メニューの［**Test Trusted Realm（トラステッド レルムのテスト）**］を選択します。

次のステップ

トラステッド ユーザーの認証を行う前に、トラステッド ユーザーからの認証要求を処理するように、エージェントを有効化する必要があります。詳細については、469 ページのトラステッド レルム認証のためのエージェントの構成を参照してください。

トラステッド レルム認証のためのエージェントの構成

どの認証エージェントがトラステッド レルム認証に対応するかを指定する必要があります。

レルムの各エージェントで、次のいずれかを指定します。

- Not open to trusted users（トラステッド ユーザーに開放しない）
- Open to all trusted users（すべてのトラステッド ユーザーに開放する）
- Open only to trusted users in trusted user groups（トラステッド ユーザー グループのトラステッド ユーザーにのみ開放する）

一方向の信頼の場合は、トラステッド レルムの管理者が、トラステッド レルム内で認証エージェントを有効化します。双方向の信頼の場合は、管理者およびトラステッド レルムの管理者がそれぞれのレルムで認証エージェントを有効化します。

開始する前に

- トラステッド レルムを追加する。操作手順については、468 ページのトラステッド レルムの追加を参照してください。
- サーバからのレスポンス時間を 25 秒に指定した新しいエージェント構成ファイルを作成する。
  新しいエージェント構成ファイルの作成手順については、RSA Security Console ヘルプのトピック「Authentication Manager 構成ファイルの生成」を参照してください。

手順

1. Security Console で、[**Access（アクセス）**] > [**Authentication Agents（認証エージェント）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、構成するエージェントを検索します。
3. 検索結果から、構成する認証エージェントをクリックします。
4. コンテキスト メニューで [**Edit（編集）**] をクリックします。
5. 以下のいずれかの操作を実行します。
   - トラステッド ユーザーがこのエージェントにアクセスしないようにする場合
     a. [Trusted Realm Settings（トラステッド レルムの設定）] で、[**Enable Trusted Realm Authentication（トラステッド レルム認証を有効にする）**] が選択されていないことを確認します。
     b. [**Save（保存）**] をクリックします。
   - トラステッド ユーザーがこのエージェントにアクセスできるようにする場合
     a. [**Trusted Realm Settings（トラステッド レルムの設定）**] で、[**Enable Trusted Realm Authentication（トラステッド レルム認証を有効にする）**] を選択します。
     b. [**Trusted User Authentication（トラステッド ユーザーの認証）**] では、次のいずれかを選択します。
     – [**Open to all trusted users（すべてのトラステッド ユーザーに開放する）**]：このオプションを選択すると、認証が成功した後に、トラステッド レルムのユーザーは自動的にトラステッド ユーザーになります。

– ［**Only Trusted Users in Trusted User Groups with access to the agent can authenticate（エージェントにアクセスを許可されたトラステッド ユーザー グループのトラステッド ユーザーのみを認証する）**］：これらのトラステッド ユーザーおよびトラステッド ユーザー グループは、管理者が手動で作成できます。

c. ［**Save（保存）**］をクリックします。

アクセス制御のための複製エージェント レコード

トラステッド レルムで認証エージェントにアクセスできるユーザーを制御するには、トラステッド レルムにエージェントの複製エージェント レコードを追加します。複製エージェント レコードを使用すると、ユーザー アクセスをグループ メンバーに制限できます。このグループに割り当てられたユーザーのみがトラステッド レルムでエージェントにアクセスできます。

たとえば、ある会社に信頼関係を持つ 2 つのレルムがあり、あなたがそのうちの 1 つであるロンドンレルムの管理者であるとします。2 つのレルムとは、ニューヨークとロンドンです。ニューヨークレルムには「VPN1」という制限なしの VPN エージェントがあります。この VPN1 にアクセスできるロンドンのユーザーを制限するには、ロンドンレルムにこのエージェント レコードの複製エージェント レコード（同名の「VPN1」）を作成します。このエージェント レコードには、ニューヨーク レルムのエージェント レコードと同じデータ（IP アドレスを含む）を指定します。VPN1 を制限付きエージェントに設定し、「VPN ユーザー」という名のユーザー グループを作成します。「VPN ユーザー」のメンバーになっているロンドンレルムのユーザーのみがニューヨークの VPN1 にアクセスできます。

「VPN ユーザー」ユーザーグループにユーザー「jsmith」を追加します。jsmith がニューヨークに出張し、ニューヨークレルムで VPN1 へのアクセスを試行したとします。この時、ニューヨークレルムには jsmith というユーザーが見つからないため、情報はロンドンレルムに転送されます。転送される情報は、ユーザー名、エージェント名、パスコードです。ロンドンレルムではユーザー名とエージェント名を認識し、エージェントが制限付きかどうかを直ちにチェックします。エージェントは制限付きで、jsmith は「VPN ユーザー」のメンバーであるため、認証リクエストが承認され、ニューヨークレルムは jsmith の認証を許可します。

複製エージェント レコードを作成する場合は、トラステッド レルム内の対応するエージェントに、トラステッド ユーザー グループが割り当てられているか否かを確認することが重要です。複製エージェント レコード側のユーザー グループに、トラステッド レルムのエージェント側のトラステッド ユーザーグループと同じユーザーが含まれない場合、ユーザーは認証できません。次の点に注意してください。

- 前述の例で、ニューヨーク レルムの VPN1 にトラステッド ユーザー グループが関連づけられているとします。jsmith がそのトラステッド ユーザー グループのメンバーに含まれていない場合は、jsmith がロンドン レルムの対応するユーザー グループのメンバーであっても、認証を受けることができません。
- 次に、この例でロンドンレルムのもう 1 人のユーザー「sbrown」がトラステッド ユーザー グループのメンバーに含まれているものの、自分のレルム内の対応するユーザー グループのメンバーではないとします。sbrown は、トラステッド ユーザー グループのメンバーであるにもかかわらず、自分のレルム内ではエージェントへのアクセスが許可されていないため、認証を受けることができません。

エイリアスを解決するための複製エージェント レコード

ユーザー グループでエイリアスを使用している場合、ユーザーはエイリアスを使ってトラステッド レルム内の認証エージェントにログオンを試みる可能性があります。この場合、認証が正常に行われるよう、トラステッド レルム内のエージェントの複製レコードを、ユーザー グループとエイリアスと関連づけてレルムに追加します。

たとえば、レルムに制限付き VPN エージェントである「VPN2」があるとします。VPN2 には、VPN2 ユーザー グループのメンバーのみがアクセスできます。このユーザー グループには、ユーザーが VPN2 でのみ使用する特別なユーザー名、つまりエイリアスがあります。たとえば、ユーザー「jdoe」はエイリアス「jdoeVPN」を持っていて、VPN2 のログオンの際に使用します。

もし jdoe が、エイリアス「jdoeVPN」を使ってトラステッド レルムの VPN エージェント「VPN1」で認証を試行すると、トラステッド レルムには jdoeVPN というユーザーが見つからないため、ユーザー名とエージェント情報が jdoe のレルムに転送されます。しかし、jdoe のレルムでは、エージェント「VPN1」あるいはユーザー名「jdoeVPN」が認識されません。このため、アクセスが拒否され、ユーザーは認証を受けることができません。

jdoe のレルムに同じく「VPN1」という名前の複製エージェント レコードがあり、jdoe がその VPN1 に関連づけられたユーザー グループのメンバーであり、「jdoeVPN」というエイリアスをもつ場合、問題は解決します。「jdoeVPN」がトラステッド レルム内の VPN1 にアクセスしようとすると、トラステッド レルムはユーザー名とエージェント情報を jdoe のレルムに転送します。Jdoe のレルムはエージェント名とエイリアスを認識します。そのため、jdoe は正常に認証されることになります。

トラステッド ユーザーの追加

トラステッド レルム認証が有効化されたエージェントにアクセスできるのは、トラステッド ユーザーのみです。認証エージェントは、トラステッド レルムのすべてのユーザーを自動的にトラステッド ユーザーとするよう構成できます。より多くの制限が必要な場合は、トラステッド ユーザーを手動で追加できます。トラステッド ユーザーを手動で追加すると、追加したユーザーのみがトラステッド ユーザーとなります。

開始する前に

- トラステッド レルムを追加する。操作手順については、468 ページのトラステッド レルムの追加を参照してください。
- エージェントにトラステッド レルム認証の構成を行う。操作手順については、469 ページのトラステッド レルム認証のためのエージェントの構成を参照してください。

手順

1. Security Console で、[**Administration（管理）**] > [**Trusted Realms（トラステッド レルム）**] > [**Trusted Users（トラステッド ユーザー）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**Trusted User ID（トラステッド ユーザー ID）**] フィールドに、ユーザーのユーザー ID を入力します。
3. [**Trusted Realm Name（トラステッド レルム名）**] ドロップダウン メニューで、ユーザーが所属するトラステッド レルムを選択します。
4. [**Security Domains（セキュリティ ドメイン）**] ドロップダウン メニューで、このトラステッド ユーザーのポリシーを管理するセキュリティ ドメインを選択します。
   選択したセキュリティ ドメインが権限適用範囲に含まれる管理者のみが、ユーザーを管理できます。
5. [**Default Shell（デフォルト シェル）**] フィールドに、ユーザーが UNIX マシンにアクセスするために使用するシェルを入力します。
6. [**Save（保存）**] をクリックします。

RSA RADIUS を使用したトラステッド ユーザーの認証を許可する

RSA RADIUS を使用したトラステッド ユーザーの認証を許可するには、認証前に、それらのトラステッド ユーザーをトラステッド レルムで定義します。トラステッド ユーザーに対して特別な RADIUS プロファイルを設定することもできます。

トラステッド ユーザーを認証するための RADIUS の構成の詳細については、360 ページのトラステッド ユーザーへの割り当てを参照してください。

トラステッド ユーザーと RADIUS 属性の関連づけの詳細については、367 ページのアイデンティティ ソース属性への RADIUS ユーザー属性定義のマッピングを参照してください。

トラステッド ユーザー グループの追加

トラステッド ユーザー グループは、トラステッド レルム認証が有効化されたエージェントへのアクセスを制限します。トラステッド ユーザー グループを作成し、エージェントに関連づけると、トラステッド ユーザー グループのメンバーのみがその認証エージェントにアクセスできるようになります。

トラステッド ユーザー グループを追加することにより、エージェントによって保護されているリソースに業務上アクセスする必要性があるユーザーのみが認証を受けることができます。たとえば、人事部門の従業員向けにトラステッド ユーザー グループを作成すると、グループのメンバーのみが個人情報レコードにアクセスできるよう制限できます。

開始する前に

- トラステッド レルムを追加する。操作手順については、468 ページのトラステッド レルムの追加を参照してください。
- エージェントにトラステッド レルム認証の構成を行う。操作手順については、469 ページのトラステッド レルム認証のためのエージェントの構成を参照してください。

手順

1. Security Console で、[**Administration（管理）**] > [**Trusted Realms（トラステッド レルム）**] > [**Trusted User Groups（トラステッド ユーザー グループ）**] > [**Add New（新規追加）**] の順にクリックします。
2. [**Trusted User Group Name（トラステッド ユーザー グループ名）**] フィールドに、トラステッド ユーザー グループの一意の名前を入力します。

   トラステッド ユーザー グループ名の最大文字数は 255 文字です。
3. [**Security Domain（セキュリティ ドメイン）**] ドロップダウン メニューで、このトラステッド ユーザー グループのポリシーを管理するセキュリティ ドメインを選択します。

   選択したセキュリティ ドメインが権限適用範囲に含まれる管理者のみが、トラステッド ユーザー グループを管理できます。
4. [**Save（保存）**] をクリックします。

トラステッド ユーザー グループへのトラステッド ユーザーの追加

トラステッド ユーザー グループは、トラステッド レルム認証が有効化されたエージェントへのアクセスを制限します。トラステッド ユーザー グループを作成すると、トラステッド ユーザー グループのメンバーのみが、トラステッド レルム認証が有効化されたエージェントにアクセスできるようになります。

新しいトラステッド ユーザーを既存のトラステッド ユーザー グループに追加できます。

手順

1. Security Console で、[**Administration（管理）**] > [**Trusted Realms（トラステッド レルム）**] > [**Trusted User Groups（トラステッド ユーザー グループ）**] > [**Manage Existing（既存項目の管理）**] の順にクリックします。
2. 検索フィールドを使用して、ユーザーを追加するトラステッド ユーザー グループを検索します。
3. 検索結果から、トラステッド ユーザー グループの名前をクリックします。
4. コンテキスト メニューで [**Add More（追加）**] をクリックします。
5. 追加するトラステッド ユーザーの横のチェックボックスをオンにします。
6. [**Add to Trusted User Group（トラステッド ユーザー グループに追加）**] をクリックします。

レガシー レルムとの信頼関係の作成

レルム間認証を有効化することにより、RSA Authentication Manager 8.0 のレルムと RSA Authentication Manager 6.1 のレガシー レルムの間に信頼関係を作成することができます。

手順

1. Authentication Manager 6.1 導入環境でレルム間認証を有効化します。
   操作手順については、「RSA Authentication Manager 6.1 管理者ガイド」の「レルム管理」の章を参照してください。
2. レルム間認証を有効化したら、Authentication Manager 8.0 側で、レガシー トラステッド レルムとの認証に使用するポートを構成する必要があります。
   操作手順については、475 ページのレガシー トラステッド レルム認証のためのポートの構成を参照してください。

注： Authentication Manager 8.0 のレルムと 6.1 のレルムの間の信頼関係は、RSA_RADIUS を使用した認証をサポートしません。

レガシー トラステッド レルム認証のためのポートの構成

RSA Authentication Manager 6.1 のレガシー レルムと Authentication Manager 8.0 との間のレルム間認証を有効化する場合は、Authentication Manager 8.0 で認証に使用されるポート範囲を構成する必要があります。このポート範囲は、Security Console を使用して構成します。デフォルト値は次のとおりです。

- ポート範囲：10 ポート
- 最小ポート：10001
- 最大ポート：10010

これらのポートは、Authentication Manager 6.1 のレガシー信頼関係が確立されるまで閉じています。導入環境間でのアクセスを許可するよう、ファイアウォールを構成する必要があります。

デフォルトの設定を変更することにより、パフォーマンスを向上させたり、導入環境の他のネットワーク サービスと共存させることができます。たとえば、Authentication Manager 8.0 の多数のユーザーが複数のレガシー トラステッド レルムで同時に認証を受ける場合は、ポート範囲をデフォルトのポート範囲よりも拡大することをお勧めします。

指定するポート数を調べるには、レガシー トラステッド レルムの数に、典型的な 5 秒間の間に発生すると予想されるレガシー レルム認証の回数を掛けます。たとえば、10 個のレガシー トラステッド レルムがあり、5 秒間に 2 回の認証が行われると予想される場合は、ポート範囲として 20 を指定します。

Security Console ではポートがすでに使用されているかどうかの確認が行われないため、変更を加える前にポートが利用可能であることを確認する必要があります。10 に満たないポート範囲を設定しないでください。レガシー レルムでは、認証用に 10 個以上のポートが必要です。

開始する前に

Authentication Manager 6.1 導入環境でレルム間認証を有効化します。

手順

1. Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。[**Advanced Settings 詳細設定）**] セクションで、[**Ports for Legacy Cross (Trusted) Realms（レガシー トラステッド レルムのポート）**] をクリックします。
2. [Ports for Legacy Cross (Trusted) Realms（レガシー トラステッド レルムのポート）] ページの [**Port Range（ポート範囲）**] で、デフォルトの設定を受け入れるか、または新しい最小ポート番号と最大ポート番号を入力します。10 個以上のポートが必要です。
3. [**Save（保存）**] をクリックします。

次のステップ

アプライアンスをリブートしてポート設定を有効化します。操作手順については、419 ページのアプライアンスのリブートを参照してください。

信頼関係の修復

新しいホスト名のマシンに RSA Authentication Manager 8.0 プライマリ インスタンスをリストアするか、移行を実行する場合に、以前に別のレルムと信頼関係を構築していた場合は、次の信頼関係を修復する必要があります。

- **トラステッド レルム**。2 つの Authentication Manager 8.0 導入環境の間、または Authentication Manager 8.0 導入環境と Authentication Manager 7.1 導入環境の間の信頼関係です。操作手順については、448 ページのバージョン 8.0 レルムとの信頼関係の修復または 450 ページのバージョン 7.1 レルムとの信頼関係の修復を参照してください。

  トラステッド レルムの場合、修復プロセスにより、トラステッド ユーザーやグループなど、元のトラステッド レルムの情報が保持されます。このプロセスは、トラステッド レルムを追加するプロセスと似ています。移行またはリストアされるバージョン 8.0 導入環境の管理者と、相手のバージョン 8.0 または 7.1 導入環境の管理者の両方がこの修復プロセスに参加します。ただし、信頼パッケージをインポートするのは、トラステッド レルムの相手側の管理者だけです。移行またはリストアする導入環境の管理者は、信頼を修復する相手側の導入環境の管理者に信頼パッケージを提供します。このパッケージは、トラステッド レルムを修復するために使用されます。

- **クロス トラスト**。バージョン 8.0 とバージョン 6.1 の導入環境の間のレガシー信頼関係です。操作手順については、454 ページのレガシー トラステッド レルムの修復を参照してください。

  レガシー信頼関係の場合、修復プロセスでは、Authentication Manager 6.1 導入環境でレルム レコードのホスト名と IP アドレスを更新する必要があります。

A インスタンス ネットワーク設定の変更

プライマリまたはレプリカ インスタンスのネットワーク設定の更新

Operations Console で、Authentication Manager のプライマリまたはレプリカ インスタンスのネットワーク設定を更新できます。IPv4 ネットワーク設定は、Quick Setup 実行時に作成され、Authentication Manager のほとんどの機能で使用されます。レプリケーション導入環境で、プライマリ インスタンスの IPv4 の IP アドレスまたはホスト名を変更した場合は、Operations Console を使用し、レプリカ インスタンスに更新された情報を設定する必要があります。IPv6 準拠エージェントをサポートするために IPv6 ネットワーク設定を追加できます。

上級管理者は、インスタンスにログオンし、IPv4 および IPv6 の静的ルートを作成するコマンドを実行することができます。静的ルートは、特定のネットワークに、予測可能な固定パスを使用してデータを送信するルートです。永続的な静的ルートと非永続的な静的ルートの両方がサポートされています。

プライマリまたはレプリカ インスタンスの IPv4 ネットワーク設定が正しくない場合は、Operations Console で変更できます。Operations Console にアクセスできない場合は、VMware vSphere Client を使用し、アプライアンス オペレーティング システムにログオンして設定を修正します。これらの手順には、オペレーティング システム レベルの Linux テキスト エディタ（vi editor など）に関する知識が必要です。

プライマリまたはレプリカ インスタンスのネットワーク設定の更新方法の詳細については、次の手順を参照してください。

- 480 ページのプライマリ インスタンスの IPv4 ネットワーク設定の変更
- 483 ページのレプリカ インスタンスでのプライマリ インスタンスのホスト名と IP アドレスの更新
- 484 ページのレプリカ インスタンスの IPv4 ネットワーク設定の変更
- 507 ページのプライマリまたはレプリカ インスタンスでの IPv6 ネットワーク設定の追加

高度な管理タスクを実行するには、仮想アプライアンス オペレーティング システムにログオンする必要があります。詳細については、以下のトピックを参照してください。

- 487 ページの静的ルート
- 493 ページの不正なネットワーク設定からの復旧

プライマリ インスタンスの IPv4 ネットワーク設定の変更

Quick Setup で設定したサブネット マスク、デフォルト ゲートウェイ、ホスト名、IP アドレスなどの IPv4 ネットワーク設定は変更することができます。ネットワーク設定の変更が必要になる理由はいくつかあります。たとえば、別のリソースとの IP アドレスの競合を解決するために IP アドレスの変更が必要になる場合、ネットワークの再構成時にサブネット マスクの変更が必要になる場合、あるデータセンターから別のデータセンターへのアプライアンスの移動時にネットワーク設定の変更が必要になる場合などです。

開始する前に

- 管理者がこの処理手順を実行しているときは、ユーザーはこのインスタンスで認証を受けることはできず、一部の管理機能は使用不可能になります。この処理手順は、認証サービスが停止することの影響が最小限で済むときに行うようにしてください。
- Web Tier を使用する単一プライマリ インスタンスの導入環境で、プライマリ インスタンスのホスト名を変更する場合は、Web Tier を再インストールする必要があります。レプリケーション導入環境では、Web Tier は更新されたホスト名を自動的に取得します。
- Operations Console 管理者である必要があります。
- レプリケーション導入環境でプライマリ インスタンスのホスト名や IP アドレスを変更する場合、変更後の「次のステップ」を実行するにはスーパー管理者のクレデンシャルが必要になります。

手順

1. プライマリ インスタンスで、Operations Console にログオンします。
2. **［Administration（管理）］＞［Network（ネットワーク）］＞［Appliance Network Settings（アプライアンスのネットワーク設定）］**の順にクリックします。
3. **［Fully Qualified Domain Name（完全修飾ドメイン名）］**フィールドで、FQDN（完全修飾ドメイン名）を変更します。
4. **［IPv4 Address（IPv4 アドレス）］**フィールドで、IP アドレスを変更します。
5. 次のように構成します。
   - **［IPv4 Subnet Mask（IPv4 サブネット マスク）］**フィールドで、サブネット マスクを変更します。
   - **［IPv4 Default Gateway（IPv4 デフォルト ゲートウェイ）］**フィールドで、デフォルト ゲートウェイを変更します。
   - **DNS サーバ**の場合は、DNS サーバのリストに IP アドレスを追加または削除します。複数の IP アドレスを入力して、順番を指定することもできます。は、表示された順番で各 DNS サーバに DNS ルックアップ クエリーを送信します。

- **DNS 検索ドメイン**の場合は、リストに DNS 検索ドメインを追加または削除します。複数の検索ドメインを入力して、順番を指定することもできます。Manager は、表示された順番で検索ドメインを使用します。

6. ［**Save（保存）**］をクリックします。Operations Console に確認のページが表示されます。
7. ［**Yes, change network settings（はい、ネットワーク設定を変更します）**］を選択して、［**Change Network Settings（ネットワーク設定の変更）**］をクリックします。
   変更を適用するために、Authentication Manager は、システム レベルでネットワーク サービスを再起動します。ホスト名または IP アドレスを変更した場合、Manager は、その他のサービスも再起動します。サービスが起動したら、新しいホスト名および IP アドレスで Operations Console と Security Console を使用できるようになります。

次のステップ

プライマリ インスタンスのホスト名または IP アドレスを変更した後に、これらのタスクを完了してください。ホスト名と IP アドレスの両方を変更した場合は、導入環境に該当するタスクをすべて実行する必要があります。サブネット マスクなどのその他のネットワーク設定を変更した場合は、これらの追加タスクは必要ありません。

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
新しいホスト名または IP アドレスの情報で、DNS サーバを更新します。	はい	はい
RSA Console（Operations Console、Security Console、Self-Service Console）へのアクセスに使用するホスト名が新しい IP アドレスに解決されることを確認します。	いいえ	はい
レプリケーション導入環境で、DNS サーバの更新後に、レプリカ インスタンスの Operations Console にログオンし、プライマリ インスタンスのホスト名と IP アドレスを更新します。プライマリ インスタンスと通信するために、レプリカ インスタンスでは、プライマリ インスタンスのホスト名と IP アドレスが必要です。 操作手順については、483 ページのレプリカ インスタンスでのプライマリ インスタンスのホスト名と IP アドレスの更新を参照してください。	はい	はい

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
サード パーティの CA（認証局）によって署名された SSL 証明書をインストールしていた場合、ホスト名を変更すると、元の RSA Authentication Manager CA によって署名された SSL 証明書が使用されるようになります。この SSL 証明書は、インスタンスの導入時に有効化された証明書です。 新しい SSL 証明書をインストールするには、CN（共通名）に新しいホスト名を指定した新しい SSL 証明書をサード パーティの認証局から取得し、インポートします。RSA Operations Console ヘルプのトピック「コンソール証明書の置換」を参照してください。	はい	いいえ
新しい IP アドレスと通信するように認証エージェントを構成します。新しい構成ファイル **sdconf.rec** を生成して、すべての認証エージェントに展開します。操作手順については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。	いいえ	はい
トラステッド レルムの信頼関係を修復します。操作手順については、448 ページのバージョン 8.0 レルムとの信頼関係の修復を参照してください。	はい	いいえ
Web Tier を使用するレプリケーション導入環境でホスト名を変更した場合、その Web Tier はプライマリ インスタンスのホスト名をレプリカ インスタンスから取得します。各レプリカ インスタンスでプライマリ インスタンス ホスト名を更新したら、Web Tier が更新されるまで 5 分間待機します。その後で、必要に応じて、追加のレプリカ インスタンスのホスト名の変更を実行できます。	レプリケーション導入環境で必要	いいえ
レプリカ インスタンスのないプライマリ インスタンス単独の導入環境で WebTier を使用している場合、プライマリ インスタンスのホスト名を変更すると、Web Tier の再インストールが必要になります。 操作手順については、「セットアップと構成ガイド」の「Web Tier のインストール」の章を参照してください。	Authentication Manager インスタンスが 1 つしかない場合に必要	いいえ

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
新しい IP アドレスを使用するよう、RADIUS や SNMP などのすべての外部クライアントを更新します。プライマリ インスタンスの IP アドレスを変更すると、RADIUS サーバの IP アドレスも更新されます。新しい IP アドレスにリクエストを送信するように RADIUS クライアントを再構成します。	いいえ	はい
新しいホスト名を使用するよう、RADIUS や SNMP などのすべての外部クライアントを更新します。	はい	いいえ
導入環境にレプリカ インスタンスが含まれている場合は、プライマリ インスタンスのレプリケーション ステータスを確認します。必要に応じて、レプリカ インスタンスを同期します。操作手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの同期」を参照してください。	はい	はい
RADIUS サーバのレプリケーションのステータスを確認します。操作手順については、RSA Security Console ヘルプのトピック「RADIUS レプリカ サーバへのレプリケーションの手動開始」を参照してください。	はい	はい

レプリカ インスタンスでのプライマリ インスタンスのホスト名と IP アドレスの更新

レプリカ インスタンスは、プライマリ インスタンスの IPv4 ホスト名および IP アドレスを使用して、プライマリ インスタンスと通信します。プライマリ インスタンスのホスト名や IP アドレスを変更した場合は、新しいネットワーク設定を導入環境の各レプリカ インスタンスに構成する必要があります。

開始する前に

スーパー管理者である必要があります。

手順

1. レプリカ インスタンスで、RSA Operations Console にログオンします。
2. **［Administration（管理）］＞［Network（ネットワーク）］＞［Update Primary Hostname（プライマリ ホスト名の更新）］**の順にクリックします。

3. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。
4. ［**Primary Hostname（プライマリ ホスト名）**］フィールドに、プライマリ インスタンスのホスト名を入力します。
5. ［**Test Connection（接続のテスト）**］をクリックします。システムによってホスト名が解決され、必要に応じて［**Primary IP Address（プライマリ IP アドレス）**］フィールドが更新されます。
6. ［**Save（保存）**］をクリックします。

レプリカ インスタンスの IPv4 ネットワーク設定の変更

サブネット マスク、デフォルト ゲートウェイ、ホスト名、IP アドレスなど、レプリカ インスタンスの IPv4 ネットワーク設定は変更することができます。ネットワーク設定の変更が必要になる理由はいくつかあります。たとえば、別のリソースとの IP アドレスの競合を解決するために IP アドレスの変更が必要になる場合、ネットワークの再構成時にサブネット マスクの変更が必要になる場合、あるデータセンターから別のデータセンターへのアプライアンスの移動時にネットワーク設定の変更が必要になる場合などです。

開始する前に

- 管理者がこの処理手順を実行しているときは、ユーザーはこのインスタンスで認証を受けることはできず、一部の管理機能は使用不可能になります。この処理手順は、認証サービスが停止することの影響が最小限で済むときに行うようにしてください。
- スーパー管理者である必要があります。

手順

1. レプリカ インスタンスで、Operations Console にログオンします。
2. ［**Administration（管理）**］＞［**Network（ネットワーク）**］＞［**Appliance Network Settings（アプライアンスのネットワーク設定）**］の順にクリックします。
3. ［**Fully Qualified Domain Name（完全修飾ドメイン名）**］フィールドで、FQDN（完全修飾ドメイン名）を変更します。
4. ［**IPv4 Address（IPv4 アドレス）**］フィールドで、IP アドレスを変更します。
5. 次のように構成します。
   - ［**IPv4 Subnet Mask（IPv4 サブネット マスク）**］フィールドで、サブネット マスクを変更します。
   - ［**IPv4 Default Gateway（IPv4 デフォルト ゲートウェイ）**］フィールドで、デフォルト ゲートウェイを変更します。

- **DNS サーバ**の場合は、DNS サーバのリストに IP アドレスを追加または削除します。複数の IP アドレスを入力して、順番を指定することもできます。Manager は、表示された順番で各 DNS サーバに DNS ルックアップ クエリーを送信します。
- **DNS 検索ドメイン**の場合は、リストに DNS 検索ドメインを追加または削除します。複数の検索ドメインを入力して、順番を指定することもできます。Manager は、表示された順番で検索ドメインを使用します。

6. ［**Save（保存）**］をクリックします。Operations Console に確認のページが表示されます。
7. ［**Yes, change network settings（はい、ネットワーク設定を変更します）**］を選択して、［**Change Network Settings（ネットワーク設定の変更）**］をクリックします。
   変更を適用するために、Authentication Manager は、システム レベルでネットワーク サービスを再起動します。ホスト名または IP アドレスを変更した場合、Authentication Manager は、その他のサービスも再起動します。サービスが起動したら、新しいホスト名および IP アドレスで Operations Console と Security Console を使用できるようになります。

次のステップ

レプリカ インスタンスのホスト名または IP アドレスを変更した後に、これらのタスクを完了してください。ホスト名と IP アドレスの両方を変更した場合は、導入環境に該当するタスクをすべて実行する必要があります。サブネット マスクなどのその他のネットワーク設定を変更した場合は、これらの追加タスクは必要ありません。

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
新しいホスト名または IP アドレスの情報で、DNS サーバを更新します。	はい	はい
Console（Operations Console、Security Console、Self-Service Console）へのアクセスに使用するホスト名が新しい IP アドレスに解決されることを確認します。	いいえ	はい

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
サード パーティの CA（認証局）によって署名された SSL 証明書をインストールしていた場合、ホスト名を変更すると、元の RSA Authentication Manager CA によって署名された SSL 証明書が使用されるようになります。この SSL 証明書は、インスタンスの導入時に有効化された証明書です。 新しい SSL 証明書をインストールするには、CN（共通名）に新しいホスト名を指定した新しい SSL 証明書をサード パーティの認証局から取得し、インポートします。RSA Operations Console ヘルプのトピック「コンソール証明書の置換」を参照してください。	はい	いいえ
新しい IP アドレスと通信するように認証エージェントを構成します。新しい構成ファイル **sdconf.rec** を生成して、すべての認証エージェントに展開します。操作手順については、71 ページの Authentication Manager 構成ファイルの生成を参照してください。	いいえ	はい
トラステッド レルムの信頼関係を修復します。操作手順については、448 ページのバージョン 8.0 レルムとの信頼関係の修復を参照してください。	はい	いいえ
Web Tier が更新されるまで 5 分間待機します。その後で、必要に応じて、追加のホスト名の変更を実行できます。 レプリケーション導入環境では、Web Tier はレプリカ インスタンス ホスト名をプライマリ インスタンスから取得します。待機中も、Web Tier は Authentication Manager インスタンスとの通信を維持できます。	はい	いいえ
新しい IP アドレスを使用するよう、RADIUS や SNMP などのすべての外部クライアントを更新します。レプリカ インスタンスの IP アドレスを変更すると、RADIUS サーバの IP アドレスも更新されます。新しい IP アドレスにリクエストを送信するように RADIUS クライアントを再構成します。	いいえ	はい
新しいホスト名を使用するよう、RADIUS や SNMP などのすべての外部クライアントを更新します。	はい	いいえ

タスク	ホスト名変更時に必要	IP アドレス変更時に必要
レプリカ インスタンスのレプリケーション ステータスを確認し、必要に応じてレプリカ インスタンスを同期します。操作手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの同期」を参照してください。	はい	はい
RADIUS サーバのレプリケーションのステータスを確認します。操作手順については、RSA Security Console ヘルプのトピック「RADIUS レプリカ サーバへのレプリケーションの手動開始」を参照してください。	はい	はい

静的ルート

RSA Authentication Manager は、IPv4 および IPv6 の静的ルートの作成をサポートしています。静的ルートは、ネットワークを通じて、予測可能な固定パスでデータを送信するルートです。

たとえば、Authentication Manager インスタンスから Authentication Manager Web Tier へのすべてのネットワーク トラフィックのために IPv4 静的ルートを作成できます。インスタンスからの他のネットワーク トラフィックには、内部ルータへのデフォルト ルートが使用されます。Web Tier への静的ルートが使用不可になると、そのルートを使用予定であったネットワーク トラフィックは送信されません。

永続的な静的ルートと非永続的な静的ルートを作成できます。

- Authentication Manager インスタンスをリブートしたり、静的ルートを設定したインタフェースが使用不可になっても、永続的な静的ルートは削除されません。
- Authentication Manager インスタンスをリブートしたり、静的ルートを設定したインタフェースが使用不可になると、非永続的な静的ルートは削除されます。非永続的な静的ルートはネットワーク ルートのテストに使用できます。また、ネットワークの一部が障害から復旧するまでの間、一時的なパスとして使用することもできます。

静的ルートを追加するには、使用しているネットワークに合った手順を参照してください。

- 488 ページの永続的な IPv4 静的ルートの追加
- 489 ページの永続的な IPv6 静的ルートの追加
- 490 ページの非永続的な IPv4 静的ルートの追加
- 490 ページの非永続的な IPv6 静的ルートの追加

静的ルートを削除するには、該当する手順を参照してください。

- 491 ページの永続的な IPv4 または IPv6 静的ルートの削除
- 492 ページの非永続的な IPv4 または IPv6 静的ルートの削除

永続的な IPv4 静的ルートの追加

永続的な IPv4 静的ルートを追加するには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. 現在のルーティング テーブルを表示するには、次のように入力します。

   ```
   sudo ip -4 route show
   ```

5. 永続的な IPv4 ルート エントリーを **ifroute-eth0** ファイルに追加するには、次のように入力します。

   ```
   sudo bash -c "echo 'destination gateway subnet_mask eth0'
   >> /etc/sysconfig/network/ifroute-eth0"
   ```

   各パラメータの意味を以下に示します。

   - `destination` では、静的ルートを追加するネットワークまたはホストの IP アドレスを指定します。宛先 IP アドレスへのネットワーク トラフィックは、エントリーで定義されたルートを通ります。
   - `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。
   - `subnet_mask` では、宛先 IP アドレスに関連づけられたサブネット マスクを指定します。

   たとえば、サブネット 10.100.212.0（サブネット マスク 255.255.252.0）のホスト宛てのネットワーク トラフィックをすべてゲートウェイ 10.100.219.102 に送信する永続的な静的ルートを追加するには、次のように入力します。

   ```
   sudo bash -c "echo '10.100.212.0 10.100.219.102
   255.255.252.0 eth0' >>
   /etc/sysconfig/network/ifroute-eth0"
   ```

6. ネットワーク サービスをリスタートして新しい静的ルートを適用します。次のように入力します。

   ```
   sudo service network restart
   ```

   Enter キーを押します。

永続的な IPv6 静的ルートの追加

永続的な IPv6 静的ルートを追加して IPv6 準拠エージェントをサポートするには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. 現在のルーティング テーブルを表示するには、次のように入力します。

   ```
   sudo ip -6 route show
   ```

5. 永続的な IPv6 ルート エントリーを **ifroute-eth0** ファイルに追加するには、次のように入力します。

   ```
   sudo bash -c "echo 'destination gateway prefix_length -
   -' >> /etc/sysconfig/network/ifroute-eth0"
   ```

   各パラメータの意味を以下に示します。

   - `destination` では、静的ルートを追加するネットワークまたはホストの IP アドレスを指定します。宛先 IP アドレスへのネットワーク トラフィックは、エントリーで定義されたルートを通ります。
   - `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。
   - `prefix_length` では、宛先 IP アドレスに関連づけられたプレフィックス長を指定します。

   IPv6 の特殊表記を使用できます。たとえば、ネットワーク 2005::0/64 内の IPv6 準拠エージェント宛てのネットワーク トラフィックをすべてゲートウェイ 2001::2 に送信する永続的な静的ルートを追加するには、次のように入力します。

   ```
   sudo bash -c "echo '2005::0 2001::2 64 - -' >>
   /etc/sysconfig/network/ifroute-eth0"
   ```

6. ネットワーク サービスをリスタートして新しい静的ルートを適用します。次のように入力します。

   ```
   sudo service network restart
   ```

   Enter キーを押します。

非永続的な IPv4 静的ルートの追加

非永続的な IPv4 静的ルートを追加するには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. 現在のルーティング テーブルを表示するには、次のように入力します。

   ```
   sudo ip -4 route show
   ```

5. 非永続的な IPv4 ルートを追加するには、次のように入力します。

   ```
   sudo ip route add destination/nn via gateway dev eth0
   ```

   各パラメータの意味を以下に示します。

   - `destination` では、静的ルートを追加するネットワークまたはホストの IP アドレスを指定します。宛先 IP アドレスへのネットワーク トラフィックは、エントリーで定義されたルートを通ります。
   - `/nn` は、宛先 IP アドレスに関連づけられたサブネット マスクを指定するために使用するプレフィックス長表記です。
   - `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。

   たとえば、ネットワーク 10.100.212.0/22 のホスト宛てのネットワーク トラフィックをすべてゲートウェイ 10.100.219.102 に送信する非永続的な静的ルートを追加するには、次のように入力します。

   ```
   sudo ip route add 10.100.212.0/22 via 10.100.219.102 dev eth0
   ```

6. Enter キーを押します。非永続的なルートは、ただちに有効になります。

非永続的な IPv6 静的ルートの追加

非永続的な IPv6 静的ルートを追加して IPv6 準拠エージェントをサポートするには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。

4. 現在のルーティング テーブルを表示するには、次のように入力します。

   ```
   sudo ip -6 route show
   ```

5. 非永続的な IPv6 ルートを追加するには、次のように入力します。

   ```
   sudo ip -6 route add destination/nn via gateway dev eth0
   ```

   各パラメータの意味を以下に示します。

   - `destination` では、静的ルートを追加するネットワークまたはホストの IP アドレスを指定します。宛先 IP アドレスへのネットワーク トラフィックは、エントリーで定義されたルートを通ります。
   - /nn は、宛先 IP アドレスに関連づけられたサブネット マスクを指定するために使用するプレフィックス長表記です。
   - `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。

   IPv6 の特殊表記を使用できます。たとえば、ネットワーク 2005::0/64 内の IPv6 準拠エージェント宛てのネットワーク トラフィックをすべてゲートウェイ 2001::2 に送信する非永続的な静的ルートを追加するには、次のように入力します。

   ```
   sudo ip -6 route add 2005::0/64 via 2001::2 dev eth0
   ```

6. Enter キーを押します。非永続的なルートは、ただちに有効になります。

永続的な IPv4 または IPv6 静的ルートの削除

永続的な IPv4 または IPv6 静的ルートを削除するには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. vi エディタを使用して、**ifroute-eth0** ファイルからエントリーを削除します。
5. 削除する静的ルートがファイル内の唯一のエントリーである場合は、**ifroute-eth0** ファイルを削除します。
6. ネットワーク サービスをリスタートして変更を適用します。次のように入力します。

   ```
   sudo service network restart
   ```

   Enter キーを押します。

非永続的な IPv4 または IPv6 静的ルートの削除

非永続的な IPv4 または IPv6 静的ルートを削除するには、次の手順を使用します。

手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューの［**Open Console（コンソールを開く）**］を選択します。
3. **rsaadmin** というユーザー名とオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. 使用可能な静的ルートのリストは、現在のルーティング テーブルで確認できます。
   IPv4 の場合、次のように入力します。

   ```
   sudo ip -4 route show
   ```

   IPv6 の場合、次のように入力します。

   ```
   sudo ip -6 route show
   ```

5. 以下のいずれかの操作を行います。
   - ネットワーク サービスをリスタートしたり、Authentication Manager インスタンスをリブートすることなく、非永続的な IPv4 静的ルートを手動で削除するには、次のように入力します。

     ```
     sudo ip route del destination/nn via gateway dev eth0
     ```

     各パラメータの意味を以下に示します。
     - `destination` では、静的ルートを削除するネットワークまたはホストの IP アドレスを指定します。
     - `/nn` は、宛先 IP アドレスに関連づけられたサブネット マスクを指定するために使用するプレフィックス長表記です。
     - `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。

     Enter キーを押します。
   - ネットワーク サービスをリスタートしたり、Authentication Manager インスタンスをリブートすることなく、非永続的な IPv6 静的ルートを手動で削除するには、次のように入力します。

     ```
     sudo ip -6 route del destination/nn via gateway dev eth0
     ```

     各パラメータの意味を以下に示します。
     - `destination` では、静的ルートを削除するネットワークまたはホストの IP アドレスを指定します。
     - /nn は、宛先 IP アドレスに関連づけられたサブネット マスクを指定するために使用するプレフィックス長表記です。

– `gateway` では、トラフィックを宛先のネットワークまたはホストにルーティングするノードの IP アドレスを指定します。

Enter キーを押します。

- 非永続的な IPv4 および IPv6 静的ルートをすべて自動的に削除するには、RSA Authentication Manager インスタンスでネットワーク サービスをリスタートします。ネットワーク サービスは数秒間使用できなくなります。次のように入力します。

  ```
  sudo service network restart
  ```

  Enter キーを押します。

不正なネットワーク設定からの復旧

アプライアンス ネットワーク設定が間違っている場合、それらを変更できます。通常は Operations Console を使用して次の IPv4 設定を修正できます。

- FQDN（完全修飾ドメイン名）
- DNS（ドメイン ネーム サービス）設定
- 有効だが不正な Operations Console の IP アドレス

Operations Console にアクセスできない場合、VMware vSphere Client を使用してアプライアンス オペレーティング システムにログオンし、設定を修正します。次の手順を参照してください。

- 493 ページの不正な IP アドレスの変更からの復旧
- 495 ページの不正なサブネット マスクからの復旧
- 496 ページの不正なゲートウェイからの復旧

不正な IP アドレスの変更からの復旧

不正な IPv4 IP アドレスに変更したため、プライマリ インスタンスまたはレプリカ インスタンスの Operations Console にアクセスできない場合は、この処理手順を使用して復旧します。

開始する前に

この処理手順は、vi エディタの使用方法を理解していることを想定しています。

処理手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を右クリックし、コンテキスト メニューで［**Open Console（コンソールを開く）**］を選択します。

3. 「**rsaadmin**」というユーザー名と、Quick Setup の実行中に指定したオペレーティング システム パスワードを使用して仮想アプライアンスにログオンします。
4. **hosts** ファイルを更新し、正しい IP アドレスを指定します。
   a. vi を使用して、**/etc/hosts** にある **hosts** ファイルを開きます。
   b. **"local address"** のセクションで、仮想アプライアンスの FQDN（完全修飾ドメイン名）に関連づけられている IP アドレスを修正します。
   c. **hosts** ファイルを保存して閉じます。
5. 正しい IP アドレスで **ifcfg-eth0** ファイルを更新します。
   a. vi を使用して、以下にある **ifcfg-eth0** ファイルを開きます（**/etc/sysconfig/network/ifcfg-eth0**）。
   b. **IPADDR** の値に、正しい IP アドレスを指定します。
   c. **ifcfg-eth0** ファイルを保存して閉じます。
6. **routes** ファイルを更新し、正しいゲートウェイ IP アドレスを指定します。
   a. vi を使用して、**/etc/sysconfig/network/routes** にある **routes** ファイルを開きます。
   b. **ゲートウェイ IP** の IP アドレス値を修正します。
   c. **routes** ファイルを保存して閉じます。
7. ネットワーク サービスを再起動します。以下のように入力します。

   ```
   sudo /etc/service network restart
   ```

   Enter キーを押します。
8. RSA Authentication Manager サービスを再起動します。
   a. ディレクトリを **/opt/rsa/am/server** に変更します。
   b. 以下のように入力します。

      ```
      ./rsaserv restart all
      ```

      Enter キーを押します。

次のステップ

- レプリケーション導入環境でプライマリ インスタンスの IP アドレスを変更した場合、レプリカ インスタンスの Operations Console にログオンし、レプリカ インスタンス上のプライマリ インスタンスのホスト名と IP アドレスを更新する必要があります。レプリカ インスタンスは、プライマリ インスタンスと通信するためにプライマリ インスタンスのホスト名および IP アドレスを必要とします。

  操作手順については、483 ページのレプリカ インスタンスでのプライマリ インスタンスのホスト名と IP アドレスの更新を参照してください。

- 更新したインスタンスの Operations Console にログインして、変更を確認します。[**Deployment Configuration（導入環境の構成）**] > [**Instances（インスタンス）**] > [**Status Report（ステータス レポート）**] の順にクリックします。[**Status（ステータス）**] が正常であることを確認します。

  レプリケーション導入環境では、レプリケーション ステータスを確認します。必要に応じてレプリカ インスタンスを同期します。手順については、Operations Console ヘルプのトピック「Synchronize a Replica Instance（レプリカ インスタンスの同期）」を参照してください。
- プライマリ インスタンスの IP アドレスを変更した場合、DNS サーバ、レプリカ インスタンス、トラステッド レルム、Web Tier、RADIUS、認証エージェントに対して実行する手順については、480 ページのプライマリ インスタンスの IPv4 ネットワーク設定の変更を参照してください。
- レプリカ インスタンスの IP アドレスを変更した場合、DNS サーバ、Web Tier、RADIUS、認証エージェントに対して実行する手順については、484 ページのレプリカ インスタンスの IPv4 ネットワーク設定の変更を参照してください。

不正なサブネット マスクからの復旧

Operations Console を使用してアプライアンス ネットワーク設定を変更できない場合、仮想アプライアンスにログオンして IPv4 サブネット マスクを変更する必要があります。

開始する前に

この処理手順は、vi エディタの使用方法を理解していることを想定しています。

処理手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を選択し、[**Console（コンソール）**] タブをクリックします。
3. 「**rsaadmin**」というユーザー名とオペレーティング システム パスワードを使用して、仮想アプライアンスにログオンします。
4. **ifcg-eth0** ファイルを更新し、正しいサブネット マスクを指定します。
   a. vi を使用して、**/etc/sysconfig/network/ifcg-eth0** にある **ifcg-eth0** ファイルを開きます。
   b. **NETMASK 行の値**という行を正しいサブネット マスクに変更します。
   c. **ifcg-eth0** ファイルを保存して閉じます。
5. ネットワーク サービスを再起動します。以下のように入力します。

   ```
   sudo /sbin/service network restart
   ```

不正なゲートウェイからの復旧

Operations Console を使用してアプライアンス ネットワーク設定を変更できない場合、仮想アプライアンスにログオンして IPv4 ゲートウェイを変更する必要があります。

開始する前に

この処理手順は、vi エディタの使用方法を理解していることを想定しています。

処理手順

1. VMware vSphere Client にログオンします。
2. 仮想アプライアンス名を選択し、[**Console（コンソール）**] タブをクリックします。
3. 「**rsaadmin**」というユーザー名とオペレーティング システム パスワードを使用して、仮想アプライアンスにログオンします。
4. **routes** ファイルを更新し、正しいゲートウェイを指定します。
   a. vi を使用して、**/etc/sysconfig/network/routes** にある **routes** ファイルを開きます。
   b. **default** 行の値を、正しい**ゲートウェイ IP** アドレスに変更します。
   c. **routes** ファイルを保存して閉じます。
5. ネットワーク サービスを再起動します。以下のように入力します。

```
sudo /sbin/service network restart
```

B MMC（Microsoft 管理コンソール）を使用した RSA SecurID トークンの管理

概要

RSA Token Management スナップインは、Active Directory アイデンティティ ソースを使用する導入環境で RSA SecurID トークンを管理する便利な手段を提供します。RSA Token Management スナップインは、MMC（Microsoft Management Console）の「Active Directory Users and Computers（Active Directory ユーザーとコンピュータ）」スナップインのコンテキスト メニュー、プロパティ ページ、コントロール バー、ツールバーを拡張します。RSA Token Management スナップインを使用すると、Security Console にログオンすることなく、トークンの有効化または無効化、トークンの割り当て、トークン関連のその他のタスクを実行できます。

RSA Token Management スナップインへのアクセス

RSA Token Management スナップインを表示するには、MMC（Microsoft Management Console）のメニュー オプション［Manage SecurID Token(s)（SecurID トークンの管理）］を使用します。

手順

1. **［スタート］＞［管理ツール］＞［Active Directory ユーザーとコンピュータ］**の順にクリックします。
2. ［Users］フォルダを開くと、Active Directory の全ユーザーおよび全ユーザー グループが表示されます。
3. RSA Token Management を起動するには、ユーザー名を右クリックして、**［All Tasks（すべてのタスク）］＞［Manage SecurID Token(s)（SecurID トークンの管理）］**をクリックします。
   ［RSA Token Management（RSA トークン管理）］ページが表示されます。

注：F1 キーを押して MMC ヘルプ トピックにアクセスします。

RSA Token Management スナップインを使用したトークンの管理

RSA Token Management スナップインを使用すると、次のトークン管理タスクを実行できます。

- **トークンの割り当てと割り当て解除**。トークンをユーザーに割り当てると、自動的に有効になります。同じく割り当てを解除すると、トークンは無効になります。詳細については、MMC ヘルプのトピック「Managing Tokens（トークンの管理）」を参照してください。
- **トークンの無効化と有効化**。［Assigned SecurID Tokens（割り当てられた SecurID トークン）］ページでは、手動でトークンを有効化 / 無効化できます。無効なトークンは、認証で使用できません。詳細については、MMC ヘルプのトピック「Managing Tokens（トークンの管理）」を参照してください。
- **ユーザー認証属性の編集**。固定パスコードの割り当て、不正なパスコードのクリア、Windows パスワード統合およびログオン エイリアスなど、ユーザーの認証属性を表示および編集します。詳細については、MMC ヘルプのトピック「Edit Authentication Attributes（認証属性の編集）」を参照してください。
- **トークン プロパティの編集**。セキュリティ ドメイン、トークン シリアル番号、トークン タイプ、認証属性などのトークン プロパティを表示および編集します。詳細については、MMC ヘルプのトピック「Edit Token Properties（トークン プロパティの編集）」を参照してください。
- **トークンのリプレース**。紛失、盗難、破損したトークンをリプレースします。詳細については、MMC ヘルプのトピック「Replace a Token（トークンのリプレース）」を参照してください。
- **PIN の管理**。ユーザーが PIN を忘れたり、PIN を他人に知られた場合、既存の PIN をクリアし、ユーザーに強制的に新しい PIN を作成してもらう必要があります。また、トークンコードのみ使用して、PIN なしでもユーザーが認証されるようにできます。詳細については、MMC ヘルプのトピック「Clear an RSA SecurID PIN（RSA SecurID PIN のクリア）」および「Require a User to Change a PIN（ユーザーに PIN の変更を要求する）」を参照してください。
- **エマージェンシー アクセスの許可**。トークンが一時的または永久に使用できない場合、ユーザーがエマージェンシー アクセスをリクエストすることがあります。詳細については、MMC ヘルプのトピック「Generate an Online Emergency Access Code（オンライン エマージェンシー アクセス コードの生成）」および「Assign an Offline Emergency Access Tokencode（オフライン エマージェンシー アクセス トークンコードの割り当て）」を参照してください。

RSA Token Management スナップインを使用したハードウェア トークンの割り当て

ユーザーがハードウェア トークンで認証できるようにするには、ユーザーにトークンを割り当てる必要があります。1 ユーザーに対し、最大 3 つのトークンを割り当てることができます。1 人のユーザーに複数のハードウェア トークンを割り当てないことを推奨します。複数のハードウェア トークンを割り当てると、ユーザーがトークンの紛失や盗難を報告する可能性が高くなるからです。

手順

1. ［RSA Token Management（RSA トークンの管理）］ページの［Assigned SecurID Tokens（割り当てられた SecurID トークン）］タブで、［**Assign Token（トークンの割り当て）**］をクリックします。
2. ［Assign Token to User（ユーザーへのトークンの割り当て）］ウィンドウで、利用可能な RSA SecurID トークンのリストからトークンを選択します。検索オプションを使用して特定のトークンを見つけることもできます。
3. ［**Assign**（割り当て）］をクリックします。
   トークンが正常にユーザーに割り当てられたことを示すダイアログ ボックスが表示されます。
4. ［**OK**］をクリックして、［Assign Token to User（ユーザーへのトークンの割り当て）］ウィンドウを閉じます。

RSA Token Management スナップインを使用したソフトウェア トークンの割り当て

ユーザーがソフトウェア トークンで認証できるようにするには、まずユーザーにトークンを割り当て、次にそれらのトークンを配布する必要があります。1 ユーザーに対し、最大 3 つのトークンを割り当てることができます。

手順

1. RSA Token Management スナップインを使用した RSA SecurID ソフトウェア トークンの割り当て。
2. RSA Token Management スナップインを使用したソフトウェア トークンの配布。

RSA Token Management スナップインを使用した RSA SecurID ソフトウェア トークンの割り当て

これは、ソフトウェア トークンを割り当てるための 2 つの手順のうちの最初の手順です。この手順では、使用可能なトークンを検索し、ユーザーに割り当てます。

手順

1. ［RSA Token Management（RSA トークンの管理）］ページの［Assigned SecurID Tokens（割り当てられた SecurID トークン）］タブで、［**Assign Token（トークンの割り当て）**］をクリックします。
2. ［Assign Token to User（ユーザーへのトークンの割り当て）］ウィンドウで、検索パラメータを使用して利用可能なトークンを検索します。
3. 割り当てるトークンを選択します。
4. ［**Assign**（割り当て）］をクリックします。トークンが正常にユーザーに割り当てられたことを示すダイアログ ボックスが開きます。
5. ［**OK**］をクリックして、［Assign Token to User（ユーザーへのトークンの割り当て）］ウィンドウを閉じます。

RSA Token Management スナップインを使用したソフトウェア トークンの配布

この手順では、割り当てられたのトークンのトークン プロパティを構成し、トークンを配布します。

手順

1. ［RSA Token Management（RSA トークンの管理）］ページの［Assigned SecurID Tokens（割り当てられた SecurID トークン）］タブで、ソフトウェア トークンを選択します。
2. ［**Token Properties（トークン プロパティ）**］をクリックします。
3. ［Token Basics（トークンの基本設定）］タブで、**[Distribute Token（トークンの配布）]**をクリックしてトークン プロファイルと属性を構成します。
4. ［Software Token Profile（ソフトウェア トークン プロファイル）］ドロップダウン リストから、ソフトウェア トークン プロファイルを選択します。

   注：配布方法は、ファイル ベース（SDTID）- SDTID 3.0 または動的シード配布（CT-KIP）のいずれかです。選択したソフトウェア トークン プロファイルによって、配布方法は自動的に指定されます。

5. ［Device Attributes（デバイス属性）］セクションで、必要に応じて属性の値を入力します。
6. 以下のいずれかの操作を実行します。
   - 配布方法が動的シード配布（CT-KIP）の場合、［**CT-KIP Activation Code（CT-KIP アクティベーション コード）**］ドロップダウン リストからオプションを選択します。
   - 配布方法がファイル ベース（SDTID）- SDTID 3.0 の場合、［Token File Options（トークン ファイル オプション）］セクションで、［**Password Protection（パスワード保護）**］の適切なオプションを選択します。
7. ［**Save and Distribute（保存して配布）**］をクリックします。

C IPv4/IPv6 認証エージェントの導入

概要

IPv4/IPv6 認証エージェントは、RSA Authentication Manager との間でユーザー認証リクエストを安全にやりとりするソフトウェア アプリケーションです。IPv4/IPv6 エージェントは、IPv4 または IPv6 アドレスを使用します。また、UDP プロトコルではなく HTTP および TCP プロトコルを使用します。

重要：Authentication Manager 8.0 の現在のリリースには、下位互換性のある SDK（ソフトウェア開発キット）が含まれます。IPv4/IPv6 エージェントは含まれていません。

TCP エージェント プロトコルは 3 つのコア サービスから構成されます。

- **構成サービス**。エージェントの構成データの取得および検証を行います。
- **メッセージ キー サービス**。エージェントが認証の暗号化に使用するキーのネゴシエーションを行います。
- **認証サービス**。認証リクエストを処理します。

IPv4/IPv6 エージェント名

UDP エージェントと異なり、IPv4/IPv6 エージェントは論理名を使用してエージェントを特定します。エージェント名は完全修飾ホスト名である必要がなく、IP アドレスを必要としません。別々の物理ホスト上で稼働する複数のエージェントが 1 つの論理エージェント名を共有できます。1 つの物理ホスト上でそれぞれ異なる論理名をもつ複数のエージェントを稼働させることも可能です。

IPv4/IPv6 認証エージェントの取得

現在使用できる IPv4/IPv6 認証エージェントはありません。ただし、Authentication Manager 8.0 の SDK（ソフトウェア開発キット）を使用して、IPv4/IPv6 の互換性をテストできます。

IPv4/IPv6 認証エージェントの導入

認証エージェントが RSA Authentication Manager との通信を行うためには、エージェントを導入する必要があります。

開始する前に

- 認証エージェントが制限付きと制限なしのどちらであるかを決定します。詳細については、69 ページの認証エージェントのタイプを参照してください。
- （オプション）プライマリ インスタンスおよびレプリカ インスタンスの IPv6 ネットワーク設定を定義します。IPv4/IPv6 認証エージェントでは IPv4 アドレスまたは IPv6 アドレスが使用できます。IPv6 アドレスを使用する場合、RSA では複数のインスタンスに IPv6 ネットワーク設定を構成することを強く推奨します。いずれかのインスタンスが応答しなくなった場合、マルチ インスタンスによって導入環境レベルでの認証の冗長性とフェイルオーバーが提供されます。

  操作手順については、507 ページのプライマリまたはレプリカ インスタンスでの IPv6 ネットワーク設定の追加を参照してください。

処理手順

1. Security Console を使用してエージェントの構成ファイルを生成します。これにより、エージェントが Authentication Manager サーバの場所を特定できるようになります。操作手順については、Authentication Manager 構成ファイルの生成を参照してください。
2. Security Console を使用して、新しいエージェントレコードを内部データベースに追加します。このステップで、制限付きエージェントを作成するかどうかを指定できます。エージェント レコードは、RSA Authentication Manager によるエージェントの識別に使用されます。このプロセスはエージェントの登録と呼ばれます。操作手順については、認証エージェントの追加を参照してください。IPV4/IPv6 エージェントは自動登録に対応していません。手動で追加する必要があります。

   注：単一の論理エージェントを作成して複数の物理エージェントを参照できます。たとえば、「Finance Laptop（経理ラップトップ）」という 1 つの論理エージェントを作成して、複数の物理エージェントで使用できます。これにより、エージェントの保守に必要なオーバーヘッドが削減されます。

3. IPv4/IPv6 エージェントの構成を実行します。

IPv4/IPv6 エージェントの構成

IPv4/IPv6 エージェントの構成は、2 つのステップからなるエージェントの登録プロセスの 2 番目のステップです。

開始する前に

- 71 ページの Authentication Manager 構成ファイルの生成
- 72 ページの認証エージェントの追加

手順

1. Security Console で、[**Setup（セットアップ）**] > [**System Settings（システム設定）**] の順にクリックします。
2. [**Authentication Settings（認証設定）**] セクションで、[**Agents（エージェント）**] をクリックします。
3. [Agents（エージェント）] ページで、IPv6 エージェントを構成するためのリンクをクリックします。
   [IPv4/ IPv6 Agents（IPv4/IPv6 エージェント）] ページが表示されます。
4. [Authentication Servers（認証サーバ）] セクションで、次の操作を実行します。
   - IPv4/IPv6 エージェントが現在の導入環境内の任意のプライマリ インスタンスまたはレプリカ インスタンスとやり取りできるようにするには、[**All Instances（すべてのインスタンス）**] を選択します。エージェントは、認証要求のために任意のインスタンスを選択できます。
   - 特定のインスタンスの完全修飾ホスト名、IP アドレス、またはインスタンスのリストに解決される DNS 名を選択するには、[**Specified Server Names or Addresses（特定のサーバ名またはアドレス）**] を選択します。
     [**Hostname or IP Addresses（ホスト名または IP アドレス）**] フィールドでは、完全修飾ホスト名または IP アドレスをリストに追加または削除できます。RSA では、複数のインスタンスを入力することを強くお勧めします。複数のインスタンスを使用することで、冗長性が得られ、認証のフェイルオーバーがサポートされます。
5. [**Authentication Service Port（認証サービス ポート）**] フィールドに、1025 ～ 49151 のポート番号を入力します。デフォルトのポート番号は 5500 です。

重要：ポート番号を変更した場合、新しい構成ファイル（**sdconf.rec**）をエージェントに提供しない限り、エージェントは構成データを取得できなくなります。対象のポートを TCP トラフィックが通過するようにルータとファイアウォールを構成します。

6. ［**Connection Timeout（接続タイムアウト）**］フィールドで、エージェントがサーバとの接続の確立を試行するときに待機する時間を指定します。デフォルト値は 60 秒です。
7. ［**Read Timeout（読み取りタイムアウト）**］フィールドに、エージェントが既に確立された接続からのデータの取得を試行するときに待機する時間を指定します。デフォルト値は 60 秒です。
8. （オプション）［**Import Certificate of the New Primary Server（新しいプライマリ サーバの証明書のインポート）**］フィールドで、［**Browse（参照）**］をクリックし、新しいルート証明書を参照してインポートします。

   注：エージェントを新しい導入環境に移行する場合のみ、新しいルート証明書をインポートする必要があります。この機能は、RSA Authentication Manager 8.0 から Authentication Manager の将来のバージョンへの移行をサポートしています。

9. ［**Update（更新）**］をクリックします。

次のステップ

新しいノード シークレットのロード（オプション）

新しいノード シークレットのロード

ノード シークレットは、IPv4/IPv6 認証エージェントと RSA Authentication Manager の間でのみ使用される共有シークレットです。認証エージェントは、ノード シークレットを使用して認証リクエストを暗号化したうえで、Authentication Manager に送信します。Authentication Manager は、ノード シークレットを使用して IPv4/IPv6 認証エージェントを認証します。IPv4/IPv6 認証エージェントではノード シークレットは必須ではありません。

Authentication Manager サーバ側で手動でノード シークレットを作成し、エージェント ホストにエクスポートできます。ノード シークレット ファイルをエージェント ホスト マシンに転送したら、**agent_nsload** ユーティリティを実行してノード シークレット ファイルを展開し、適切に格納する必要があります。ノード シークレットは、デフォルトのパスかユーザー定義のパスに格納できます。

Node Secret Load ユーティリティ（**agent_nsload**）は、RSA Authentication Manager 8.0 - Virtual Appliance DVD に含まれています。

開始する前に

- Windows 2008、Windows Vista、Windows 7 以降でユーザー アカウント制御機能を有効化している場合、ノード シークレットをデフォルトの場所（**drive:¥%windir%¥system32**）に格納するには、管理者特権のコマンド プロンプトから **agent_nsload** ユーティリティを実行する必要があります。
- **sdconf.rec** ファイルが、ホスト マシンの所定のフォルダに存在している必要があります。

処理手順

1. **agent_nsload** ユーティリティを使用してノード シークレットをデフォルトの場所に展開するには、以下のように入力します。

   - UNIX の場合：

     ```
     agent_nsload -f /default_dir/nodesecret.rec
     ```

   - Windows の場合：

     ```
     agent_nsload -f C:¥default_path¥nodesecret.rec
     ```

   agent_nsload ユーティリティを使用してノード シークレットをユーザー定義の場所に展開するには、以下のように入力します。

   - UNIX の場合：

     ```
     agent_nsload -f /VAR_ACE/nodesecret.rec -d
     /VAR_ACE/new_dir/
     ```

   - Windows の場合：

     ```
     agent_nsload -f C:<windows path>¥System32¥
     nodesecret.rec -d C:¥<windows path>¥System32¥new_dir¥
     ```

2. プロンプトが表示されたら、パスワードを入力して **Enter** キーを押します。

一般的な IPv4/IPv6 の問題の解決

次の表は、一般的な IPv4/IPv6 エージェントの問題と想定される原因、対応する解決方法を示しています。

問題	想定される原因	解決方法
Bootstrap.xml が見つからない。	**sdconf.rec** ファイルが正しくないか見つかりません。またはアクセスできない場所にあります。	71 ページの Authentication Manager 構成ファイルの生成
構成データを取得できない	• エージェントがサーバに接続できません。 • サーバ上に作成されたエージェンレコード。	• エージェントとサーバ間の通信を確認します • サーバ上に正しいエージェント名が存在していることを確認します
エージェント クレデンシャルの不整合エラー	ノード シークレットがサーバ上では存在するのにエージェント上に存在しないか、サーバ上には存在しないのにエージェント上に存在している。	502 ページの IPv4/IPv6 認証エージェントの導入
暗号アルゴリズムがサポートされていない。	無制限強度暗号ポリシーがインストールされていません（エージェント SDK）。	無制限強度暗号ポリシーをインストールします。詳細については、**http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html** を参照してください
DH 鍵交換を実行できない	RSA 暗号プロバイダがインストールされていません。（エージェント SDK）	com.sun providers を com.rsa equivalents に置換し、セキュリティ プロバイダを変更します。

プライマリまたはレプリカ インスタンスでの IPv6 ネットワーク設定の追加

プライマリまたはレプリカ インスタンスで Operations Console を使用して、IPv6 準拠エージェントをサポートするための IPv6 ネットワーク設定を追加できます。Authentication Manager は、TCP エージェント プロトコルをサポートします。デフォルトで、Authentication Manager のポート 5500 で、IPv4 準拠および IPv6 準拠のエージェントをサポートします。他のすべてのサービスおよびポートについては、IPv4 がサポートされています。Operations Console で IPv6 を構成しても、プライマリ インスタンスとレプリカ インスタンスとの間の通信には使用できません。

手順

1. Operations Console で、［**Administration（管理）**］＞［**Network（ネットワーク）**］＞［**Appliance Network Settings（アプライアンスネットワーク設定）**］の順にクリックします。
2. ［**IPv6 Settings (for agents only)（IPv6 設定（エージェントのみ）**］で、［**Yes（はい）**］をクリックして IPv6 を有効化します。
3. ［**IPv6 Address（IPv6 アドレス）**］フィールドに有効な IPv6 アドレス（たとえば、「2001:0db8:85a3:0000:0000:8a2e:0370:7335」）を入力します。
4. ［**IPv6 Prefix Length**（IPv6 プレフィックス長）］フィールドにプレフィックス長（たとえば、64）を入力します。
5. ［**IPv6 Default Gateway（IPv6 デフォルト ゲートウェイ）**］フィールドにデフォルト ゲートウェイ（たとえば、「2001:0db8:85a3:0000:0000:8a2e:0370:7330」）を入力します。
6. ［**Save（保存）**］をクリックします。
   Operations Console に確認のページが表示されます。
7. ［**Yes, change network settings（はい、ネットワーク設定を変更します）**］を選択して、［**Change Network Settings（ネットワーク設定の変更）**］をクリックします。
   Authentication Manager により、サービスが再起動されます。

次のステップ

新しい IP アドレスを DNS サーバに登録します。

VMware インフラストラクチャ内の IPv6 の有効化

IPv6 アドレスを使用してエージェントから送信される認証リクエストを処理するよう、VMware インフラストラクチャを有効化できます。詳細については、VMWare のドキュメントを参照してください。

用語集

Active Directory

Microsoft Windows Server 2003 SP2、Microsoft Windows Server 2008、Microsoft Windows Server 2008 R2 に搭載されているディレクトリ サービス。

Active Directory フォレスト

Windows Server 環境で使用する認証サーバの集合体。すべての認証サーバで、共通のスキーマ、構成、グローバル カタログが使用されます。

CLU（コマンド ライン ユーティリティ）

コマンド ライン ユーザー インタフェースを提供するユーティリティ。

CT-KIP（Cryptographic Token-Key Initialization Protocol）

ソフトウェア トークンの安全な初期化と構成のためのクライアント サーバ プロトコル。このプロトコルでは、トークン内の秘密鍵機能および確立された公開鍵基盤のどちらも必要ありません。プロトコルが正常に実行されると、サーバとトークンの両方で、同じ共有シークレットが生成されます。

DMZ（非武装地帯）

2 つのファイアウォールの間に構成されるネットワークの領域。

DMZ

「DMZ（非武装地帯）」を参照してください。

On-Demand トークンコード

SMS または SMTP により配布されるトークンコード。ユーザーに PIN の入力を要求することにより、2 要素認証を実現します。On-Demand トークンコードはユーザー始動のコードで、Authentication Manager はユーザー要求を受け取った場合のみユーザーにトークンコードを送信します。On-Demand トークンコードは一度だけ使用できます。管理者が On-Demand トークンコードの有効期間を構成します。「On-Demand トークンコード サービス」を参照してください。

On-Demand トークンコード サービス

有効化されたユーザーがトークンの代わりにテキスト メッセージまたはメールでトークンコードを受信できるサービス。On-Demand トークンコード サービスの構成とユーザーの有効化は、Security Console で行います。

Operations Console

ユーザーが Authentication Manager の構成や設定（アイデンティティ ソースの追加と管理、インスタンスの追加と管理、災害復旧など）を行う管理ユーザー インタフェース。

RADIUS

「RADIUS（Remote Authentication Dial-In User Service）」を参照してください。

RADIUS（Remote Authentication Dial-In User Service）

ネットワークへのリモート アクセスを管理および保護するためのプロトコル。RADIUS サーバは、VPN などの RADIUS クライアントからユーザー アクセス リクエストを受信します。

RBA

「RBA（リスクベース認証）」を参照してください。

RBA（リスクベース認証）

保護対象のリソースへのアクセスを許可する前に、ユーザーのプロファイル、認証履歴、認証デバイスを分析する認証方式。

RBA 統合スクリプト

Web ベース アプリケーションのデフォルト ログオン ページからカスタマイズされたログオン ページにユーザーをリダイレクトするスクリプト。これにより、Authentication Manager は、リスク ベース認証を使用してユーザーを認証できます。統合スクリプトを作成するには、統合スクリプトのテンプレートが必要です。

Request Approver

ユーザーからのアカウント登録、トークン、ユーザー グループ メンバーシップのリクエストを許可する権限を付与する、事前定義された管理者ロール。

Security Console

日常的な管理作業の大半を実行するために使用する管理ユーザー インタフェース。

Self-Service Console

ユーザー プロファイルの更新、Self-Service Console のパスワードの変更、セキュリティ クエスチョンの設定、リスク ベース認証で登録したデバイスのクリア、On-Demand トークン用の電子メール アドレスまたは電話番号の変更、On-Demand トークンの PIN の管理などを行う、エンドユーザー向けのユーザー インタフェース。エンドユーザーは、Self-Service Console からトークンのリクエスト、保守、トラブルシューティングも実行できる。

SSL

「SSL（Secure Socket Layer）」を参照してください。

SSL（Secure Socket Layer）

暗号化を使用してインターネット経由のセキュア通信を可能にするプロトコル。SSL は主要な Web ブラウザや Web サーバで広くサポートされています。

Trace ログ

トレース情報を永続的に記録したもの。

UDP

「UDP（User Datagram Protocol）」を参照してください。

UDP（User Datagram Protocol）

データグラムと呼ばれる短いメッセージを送信することで、ネットワーク コンピュータのプログラム同士が通信できるようにするプロトコル。

Web Tier

Web Tier は、DMZ に Self-Service Console、動的シード配布サービスおよび RBA（リスク ベース認証）サービスをインストールおよび導入するためのプラットフォームです。Web Tier は、企業のプライベート ネットワークの手前でエンド ユーザーからのインバウンド インターネット トラフィックを受信および管理し、プライベート ネットワークが直接アクセスされるのを防ぎます。

アイデンティティ ソース

ユーザーおよびユーザー グループのデータが保存されているデータストア。内部データベースまたは外部ディレクトリ サーバ（Microsoft Active Directory など）を使用できます。

アイデンティティ属性

カスタム定義の属性。常にユーザーまたはユーザー グループのコア属性データと同じ物理リポジトリに保存されます。これらの属性で検索、クエリ、レポートを実行できます。各アイデンティティ属性定義は、LDAP ディレクトリの既存の属性にマッピングする必要があります。

アプライアンス

RSA Authentication Manager がインストールされている仮想アプライアンス。アプライアンスは、プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。

委譲管理

管理者の権限の集合とそれらの適用範囲を定義するためのスキーム。管理者が一部の権限を別の管理者に委譲することを許可します。

インスタンス

RSA Authentication Manager の単一のインストール。プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。1 つのインスタンスには、1 つの RADIUS サーバも含まれます。

エージェント ホスト

エージェントがインストールされたマシン。

下位のセキュリティ ドメイン

セキュリティ ドメインの階層において、他のセキュリティ ドメインの下にネストされたセキュリティ ドメイン。

鍵ストア

鍵と証明書を保管するための機能。

カスタム属性

ユーザーが Authentication Manager に作成する属性です。LDAP ディレクトリのフィールドにマッピングされます。たとえば、ユーザーの部署を表すカスタム属性を作成できます。

仮想アプライアンス

Authentication Manager がインストールされている仮想マシン。仮想アプライアンスは、プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。

仮想ホスト

仮想マシンがインストールされている物理コンピュータ。仮想ホストは、Web ベースのアプリケーション、Web Tier、Web Tier に関連づけられたプライマリ インスタンスとレプリカ インスタンスの間のトラフィックを管理するのに役立ちます。

仮想ホスト名

パブリックにアクセス可能なホスト名。エンド ユーザーは Web Tier 経由で認証を受ける場合、この仮想ホスト名にアクセスします。また、仮想ホスト名に基づいて SSL 情報が生成されます。仮想ホスト名は、ロードバランサのホスト名と同じにする必要があります。

監査情報

システムのイベントやアクティビティ（ポリシーや構成の変更、認証、承認など）の履歴を示す監査ログに含まれているデータ。

監査ログ

システムのイベントやアクティビティを記録したシステム生成ファイル。システムには Trace ログ、Administrative ログ、Runtime Audit ログ、System ログと呼ばれる 4 つのファイルがあります。

管理者

システムを管理するための管理者権限を付与する管理者ロールを 1 つ以上割り当てられたユーザー。

管理者ロール

権限の集合とそれらの権限が適用される範囲。

許可

リソースに対する操作をユーザーに許可するかどうかを判別するプロセス。

グローバル カタログ

レプリケートされた読み取り専用のリポジトリであり、Active Directory フォレストにある全エントリーの属性のサブセットが格納されます。

グローバル カタログ アイデンティティ ソース

Active Directory グローバル カタログと関連づけられているアイデンティティ ソース。このアイデンティティ ソースは、ユーザーの検索と認証、フォレスト内のグループ メンバーシップの解決に使用されます。

権限

管理者が実行できるタスクを指定します。

権限適用範囲

導入環境内で、ロールの権限が適用されるセキュリティ ドメイン。

コア属性

すべての RSA 製品でユーザーの作成に共通して利用される固定の属性セット。導入環境が LDAP か内部データベースかに関係なく、これらの属性は常にプライマリ ユーザー レコードの一部となります。コア属性を非表示にすることはできませんが、委譲には利用できます。

固定パスコード

ユーザーがアクセス権を得るために PIN およびトークンコードの代わりに入力します。パスワードに似ています。固定パスコードの形式は、セキュリティ ドメインに割り当てられたトークン ポリシーで定義されます。管理者は、各ユーザーの認証設定ページで固定パスコードを作成します。固定パスコードには英数字を使用できます。トークン ポリシーによっては、特殊文字を含めることができる場合があります。

最上位のセキュリティ ドメイン

最上位のセキュリティ ドメインは、セキュリティ ドメイン階層における 1 番目のセキュリティ ドメインです。1 つまたは複数のアイデンティティ ソースにリンクし、導入環境全体のパスワード ポリシー、ロックアウト ポリシー、認証ポリシーを管理するという点で、他のセキュリティ ドメインとは異なります。

最低保証レベル

「保証レベル」を参照してください。

サイレント収集

リスクベース認証において、各ユーザーのプロファイル、認証履歴、認証デバイスに関するデータを、ログオン時にユーザー確認をすることなく、サイレントに収集する期間。

システム イベント

システムが生成するイベントのうち、製品の機能に関するもの以外のイベント（サーバの起動とシャットダウン、フェイルオーバー イベント、レプリケーション イベントなど）。

システム ログ

システム イベントを永続的に記録したもの。

昇格

レプリカ インスタンスを新しいプライマリ インスタンスにするための構成処理。昇格処理により、元のプライマリ インスタンスは導入環境からデタッチされます。元のプライマリ インスタンスを参照しているすべての構成データは、新しいプライマリ インスタンスから削除されます。

承認者

Request Approver、つまり承認者の権限を持つ管理者。

証明書

秘密鍵に対応する非対称公開鍵。証明書には自己署名または別の証明書の秘密鍵で署名します。

証明書 DN

認証用にユーザーに発行される証明書の識別名。

除外単語辞書

ユーザーのパスワードに使用できない単語を記録した辞書。除外単語辞書を使用すると、一般的で容易に推測される単語をパスワードとして使用できなくなります。

信頼パッケージ

導入環境に関する構成情報が含まれている XML ファイル。

スーパー管理者

Security Console 内のすべての管理タスクを実行する権限を持つ管理者。スーパー管理者には次の権限があります。

- アイデンティティ ソースのシステムへのリンク
- 1 つの導入環境におけるすべての権限
- 1 つの導入環境における管理者ロールの割り当て

セキュリティ クエスチョン

ユーザーが標準的な方法を使用せずに認証を行えるようにする方法。このサービスを利用するには、ユーザーは複数のセキュリティ クエスチョンに回答し、あらかじめ回答を登録しておく必要があります。このサービスを使用して認証を行う時は、元々回答していた質問のすべてまたは一部に正しく回答する必要があります。

セキュリティ ドメイン

一般にビジネスユニット、部門、取引先などの単位に応じて、管理運営の責任領域を定義するコンテナ。セキュリティ ドメインはシステム内のオブジェクト（ユーザー、ロール、権限など）の所有権やネームスペースを構築します。セキュリティ ドメインは階層構造になっています。

セッション

ユーザーとソフトウェア アプリケーションのやり取りに関するデータを含むアプリケーションとユーザーが行う対話。ユーザーがソフトウェア アプリケーションにログオンするとセッションが開始され、ログオフすると終了します。

セルフ サービス

ユーザー プロファイルの更新、Self-Service Console のパスワードの変更、セキュリティ クエスチョンの設定、リスク ベース認証で登録したデバイスのクリア、On-Demand トークン用の電子メール アドレスまたは電話番号の変更、On-Demand トークンの PIN の管理などを行う、エンドユーザー向けの Authentication Manager のコンポーネント。エンドユーザーは、トークンのリクエスト、保守、トラブルシューティングも実行できる。

送付先住所

配布者がハードウェア トークンを送付する住所。

属性

状態、外見、値、または何らかの設定を定義する特性。Authentication Manager では、属性とはユーザーおよびユーザー グループに関連づけられた値を指します。たとえば、各ユーザー グループには 3 つの標準的な属性（「名前」、「アイデンティティ ソース」、「セキュリティ ドメイン」）があります。

属性のマッピング

User ID や Last Name などのユーザーまたはユーザー グループの属性を、システムにリンクされた 1 つ以上のアイデンティティ ソースと関連づけるプロセス。内部データベースをプライマリ アイデンティティ ソースとして使用する導入環境では、属性のマッピングは不要です。

タイムアウト

指定した時間が経過するまでにユーザーがデスクトップ上で何も操作を行わないと再認証が要求されます（秒単位）。

データストア

リレーショナル データベース（Oracle や DB2）またはディレクトリ サーバ（Microsoft Active Directory または Oracle Directory Server）などのデータ ソース。データ ソースのタイプごとに別々にデータを管理したり、データにアクセスします。

デバイス登録

リスクベース認証において、認証に使用したデバイスをユーザーのデバイス履歴に保存するプロセス。

デバイス履歴

リスクベース認証の場合、システムが各ユーザーのデバイス履歴を保持します。デバイス履歴には、保護対象のリソースへのアクセスに使用したデバイスの情報が含まれます。

電子メール テンプレート

管理者がユーザーの要求（アカウント登録、トークン、ユーザー グループ メンバーシップ、On-Demand トークンコード サービス）に関する電子メール通知をカスタマイズする際に使用できるテンプレート。「メール通知」を参照してください。

動的シード配布

Web ブラウザなどのソフトウェア トークンをホストするデバイスに、CT-KIP（Cryptographic Token-Key Initialization Protocol）を使用してトークン ファイルを提供するために必要なすべてのステップの自動化。

導入環境

1 つのプライマリ インスタンスと、オプションで 1 つ以上のレプリカ インスタンスで構成される、Authentication Manager のインストール環境。

トークン

Authentication Manager で本人確認に使用するデバイス。ハードウェア トークン（キー フォブなど）またはソフトウェア トークンがあります。

トークン プロビジョニング

アカウント登録、ユーザー グループ メンバーシップ、RSA SecurID トークン、On-Demand トークンコード サービスをユーザーに提供するために必要な全ステップを自動化したもの。「セルフ サービス」も参照してください。

トークン配布者

ユーザーからのトークン リクエストを処理する権限を付与する、事前定義された管理者ロール。配布者は、ユーザーにどのようにトークンを配布してリクエストを完了する予定かを記録します。

トラステッド レルム

トラステッド レルムとは、別のレルムと信頼関係にあるレルムのことです。トラステッド レルムのユーザーは、別のレルムで認証を受け、別のレルムのリソースにアクセスすることができます。**2** つ以上のレルムが存在すれば、信頼関係を持つことができます。信頼関係は一方向でも双方向でも可能です。

内部データベース

Authentication Manager 独自のデータ ソース。

認証

ユーザーまたはプロセスが確かにそのユーザーまたはプロセスであるということを確実に判別するプロセス。

認証エージェント

ドメイン サーバ、Web サーバ、デスクトップ コンピュータなどのデバイスにインストールされ、ネットワーク上の Authentication Manager との認証通信を行うソフトウェア アプリケーション。「エージェント ホスト」を参照してください。

認証サーバ

認証リクエスト処理、データベース操作、Security Console への接続を提供するサービスで構成されるコンポーネント。

認証プロトコル

認証時にユーザーのクレデンシャルを転送するために使用される規則（HTTP-BASIC/DIGEST、NTLM、Kerberos、SPNEGO など）。

認証方式

ワンステップ認証、マルチ オプション認証（ユーザー名やパスワードなど）、チェーン認証などの認証要求手続きの種類。

ノード シークレット

認証要求時にエージェントがデータの暗号化に使用する長寿命の対称鍵。ノード シークレットは Authentication Manager とエージェントのみが知っています。

配信先

On-Demand トークンコードの送付先となる電子メール アドレスまたは携帯電話番号。

配布者

Token Distributor、つまり配布者権限を持つ管理者。

配布ファイル用パスワード

配布ファイルを電子メールでユーザーに送る際に、配布ファイルの保護に使用されるパスワード。

バックアップ

プライマリ インスタンス データのコピーを含むファイル。バックアップ ファイルを使用して、災害復旧時にプライマリ インスタンスをリストアできます。RSA Authentication Manager バックアップ ファイルには、次のものが含まれます。内部データベース、アプライアンス固有のデータと構成、内部サービスにアクセスするために使用される鍵とパスワード、内部データベース ログ ファイル。アプライアンスおよびオペレーティング システムのログ ファイルは含まれません。

プライマリ インスタンス

認証およびすべての管理アクションが実行される導入環境。

プロビジョニング

「トークン プロビジョニング」を参照してください。

プロビジョニング データ

プロビジョニング のサーバ定義のデータ。トークン デバイスのプロビジョニングを完了させるために必要な情報のコンテナです。

保証レベル

リスクベース認証では、ユーザーの毎回の認証試行が、ユーザーのプロファイル、デバイス、認証履歴に基づいて保証レベルに分類されます。その認証試行の保証レベルが、RBA ポリシーで設定された最低保証レベルに達している場合、ユーザーは RBA で保護されたリソースへのアクセスを許可されます。最低保証レベルに達していない場合、ユーザーはユーザー確認方法により本人であることを証明しなければ、RBA で保護されたリソースへのアクセスを許可されません。

ホスト

仮想マシンがインストールされている物理コンピュータ。

メール通知

アカウント登録、トークン、ユーザー グループ メンバーシップの要求に関するステータス情報が記載されており、要求を提出したユーザーに送信されます。トークンを要求した場合の電子メール通知には、トークンのダウンロードやアクティブ化の方法に関する情報も含まれています。Request Approver と Token Distributor は、それぞれに必要なアクションを要求する電子メール通知を受信します。「電子メール テンプレート」を参照してください。

ユーザー ID

システムが認証を試みているユーザーの識別に使用する文字列。
通常、ユーザー ID はユーザーの名前の頭文字と、その後ろに苗字を続けたものです。たとえば、Jane Doe のユーザー ID は *jdoe* となります。

ユーザー確認方法

リスクベース認証において、ユーザーが本人であることを確認するために使用する認証方法。

優先インスタンス

Web Tier 上のリスク ベース認証サービスが最初に通信する Authentication Manager インスタンス。また、Web Tier への更新を提供するインスタンス。任意のインスタンスを優先インスタンスとして構成できます。たとえば、レプリカ インスタンスを優先インスタンスとして構成できます。

ラウンドロビン DNS

専用のソフトウェアまたはハードウェアを必要としない、ロード バランシングの代替方法。DNS（ドメイン ネーム システム）サーバを構成してラウンド ロビンを有効化した場合、DNS サーバにより、RBA（リスク ベース認証）リクエストを複数の Web Tier サーバに送信することができます。「ロードバランサ」を参照してください。

リクエスト

ユーザーは、アカウント登録、トークン、On-Demand トークンコード サービス、ユーザー グループ メンバーシップをリクエストすることができます。

リスクエンジン

Authentication Manager では、リスクエンジンが、ユーザーごとの認証リスクをインテリジェントに評価します。リスクエンジンは、各ユーザーのデバイスと行動パターンに関する情報を長期間にわたり蓄積します。ユーザーが認証を試行すると、リスクエンジンは収集したデータを参照してそのリスクを評価します。そのリスク評価に基づき、ユーザーの認証試行に、保証レベル（高、中、低など）を割り当てます。

レプリカ インスタンス

認証を処理し、管理者が管理データを参照できる導入環境。レプリカ インスタンスではどの管理操作も実行されません。

レプリカ パッケージ

レプリカ アプライアンスがプライマリ アプライアンスに接続するための構成データを含んだファイル。レプリカ アプライアンスのセットアップを開始する前に、レプリカ パッケージ ファイルを生成する必要があります。

レルム

レルムは 1 つの組織単位であり、ユーザーとユーザー グループ、トークン、パスワード ポリシー、エージェントなど、1 つの導入環境で管理されるすべてのオブジェクトが含まれます。各導入環境にはレルムが 1 つだけあります。

ロードバランサ

リソース使用率の最適化を目的として、認証リクエストを複数のコンピュータに分散させるために導入するコンポーネント。通常、ロードバランサは、専用のハードウェアまたはソフトウェアとして実装され、冗長性の実現、信頼性の向上、レスポンス タイムの最小化を可能にします。「ラウンドロビン DNS」を参照してください。

ワークフロー

作業やビジネスの過程における情報やタスクの一連の動き。ワークフローは、ユーザーからのさまざまな要求に対して、1 つまたは 2 つの承認ステップと 1 つの配布ステップで構成できます。

ワークフロー参加者

承認者または配布者。承認者は、ユーザーからの要求をレビュー、承認、または保留します。配布者は、要求されたトークンの配布方法を決定したり、各要求に対する配布方法を記録します。「ワークフロー」も参照してください。

索引

A

account.ini，374
Active Directory
　Global Catalog ではない，123
　Global Catalog 導入要件，124
　Global Catalog 導入例，126
　アイデンティティ ソース，40, 113
　グループ，125
　グループ メンバーシップ，124
　グローバル カタログ，124
　制限付きエージェントへのグループ アクセス，174
　ドメイン ユーザーの管理，123
　フォレスト，124
Active Directory ユーザーの管理，123
Active Directory
　グループへのアクセス権の付与，174
adadmreg.exe，78
Administrative Audit ログ
　定義，381
agent_nsload ユーティリティ，504
Authentication Manager
　サービスの起動，457
　サービスの停止，457
Authentication Manager サービスの起動，457
Authentication Manager サービスの停止，457
Automated Agent Registration and Update ユーティリティ，78

B

Back Up Now（今すぐバックアップ），425
Base Server ライセンス，208

C

Clam Antivirus
　使用，456
Compressed Token Format 配布，231
CSR。「証明書署名リクエスト」を参照

E

EAP32
　セッション有効期間，195
Enterprise Server ライセンス，208

G

Global Catalog
　導入例，126

H

HTTP プラグ イン
　On-Demand トークンコードの配信の構成，266
　Short Message Service プロバイダの変更，272
　SMS パラメータの構成，270

I

import-puk，164
IPv4/IPv6 エージェント
　agent_nsload，504
　アプライアンスの構成，507
　コア サービス，501
　構成，503
　定義，501
　導入，502
　問題，506
IPv4 ネットワーク設定
　永続的な静的ルートの削除，491
　永続的な静的ルートの追加，488
　概要，479
　静的ルートの定義，487
　トラブルシューティング，493
　非永続的な静的ルートの削除，492
　非永続的な静的ルートの追加，490
　プライマリ インスタンス，480
　レプリカ インスタンス，484
　レプリカ インスタンスでのプライマリ インスタンスの設定の更新，483
IPv6 ネットワーク設定，507
　永続的な静的ルートの削除，491
　永続的な静的ルートの追加，489
　概要，479
　静的ルート，487
　非永続的な静的ルートの削除，492
　非永続的な静的ルートの追加，490
IP アドレス
　Web Tier サーバの IP の変更，212
　Web Tier での解決，213
　トラブルシューティング，493

プライマリ インスタンスでの更新 , 480
レプリカ インスタンスでの更新 , 484

L

LDAP
read-only アクセスの制限 , 40, 113
管理者 ID, 117
管理者パスワード , 117
ディレクトリ内でユーザーが移動された場合の影響 , 183
ユーザーが解決不可能になる仕組み , 175
ユーザー グループが解決不可能になる仕組み , 176
ユーザー データ変更の影響 , 175
ユーザーの移動 , 183
ユーザーの追加 , 141
ユーザーの変更 , 186
ユーザー
LDAP ディレクトリでの移動 , 183
LDAP 内でのユーザーの移動 , 183
license
ID, 17
LogAccept, 375
LogLevel, 375
LogReject, 375

N

Node Secret Load ユーティリティ
ノード シークレットの更新 , 77
バージョン , 77
プラットフォーム バージョン , 77

O

On-Demand トークンコードの配信
HTTP プラグ インの構成 , 266, 270
On-Demand 認証
HTTP プラグ イン , 266, 270
PIN, 278, 282
PIN の設定 , 278
RADIUS クライアント , 281
SMTP メール サービス , 272
アイデンティティ ソース属性へのアクセス , 264
一時ユーザー PIN, 279
概略 , 30, 263
構成処理 , 263
テキスト メッセージ属性の構成 , 264
テキスト メッセージの配信の構成 , 272
トークンコードの制限 , 282
認証エージェント , 281
メール , 273
メールの構成 , 271, 275
ユーザーの PIN のクリア , 278
ユーザーの PIN の変更 , 278
ユーザーの構成 , 276
ユーザーの初期 PIN の設定 , 278
ユーザーの有効化 , 276
ユーザーの連絡先情報 , 279
ユーザー ログオンの例 , 30
Operations Console
IP アドレスまたはホスト名の確認 , 463
管理者 , 189
管理者権限 , 191
機能 , 193
証明書 , 201
セッション有効期間の制限 , 194
ログオン , 194
Oracle Directory Server
アイデンティティ ソース , 40, 113

P

passwords
lost, 191–192
PIN, 309
On-Demand 認証 , 278
On-Demand 認証のクリア , 161
On-Demand 認証用の PIN の設定 , 161
RADIUS クライアント , 282
RSA SecurID PIN のクリア , 163
SecurID 800 のロック解除キーの取得 , 163
一時 , 278, 279
クリア , 278
再使用の制限 , 96
詳細 , 160
定義 , 160
認証エージェント , 282
変更 , 278
ユーザー設定 , 278
ユーザーに対する変更の強制 , 162
PIN の変更を強制 , 278

R

RADIUS
Dictionary ファイルの編集 , 346
replication, 23, 333
アカウンティング シークレット , 336
アカウンティング ログ ファイル , 375
概要 , 333
管理 , 338
共有シークレット , 336
クライアント , 334
クライアント認証およびアカウンティングの統計情報 , 370
サーバ構成ファイルの編集 , 346
サーバの管理 , 338
サーバ ログ ファイル , 374
サービス , 335
システム使用の監視 , 367
順序指定可能な属性 , 355
使用状況に関する統計情報 , 368
属性値 , 355
チェックリスト , 355
定期的レプリケーション , 340
定期的レプリケーションの有効化 , 343
ディクショナリ , 357
デフォルト プロファイル , 356
ネットワーク トポロジー , 335
ノード シークレット , 337
プロファイル , 354
ユーザー属性の管理 , 363
リターン リスト , 356
レプリケーション , 338, 339, 340
レプリケーション シークレット , 336
レプリケーション ステータス , 341
レプリケーションの開始 , 340
レプリケーションの管理 , 339
Request Approver
タスク , 301
RSA Authentication Manager
構成ファイルの生成 , 71
RSA SecurID トークン
定義 , 22, 26
Self-Service Console ヘルプ
ヘルプ , 297
RSA トークン管理スナップイン
Authentication Manager スナップインのヘルプへのアクセス , 497
ソフトウェア トークンの割り当て , 499
定義 , 497
トークンの管理 , 498
ハードウェア トークンの割り当て , 499
Runtime Audit ログ
定義 , 381

S

sdconf.rec, 71
Secure Shell
for accessing the appliance, 192
Secure Sockets Layer, 202
SSL 証明書の管理 , 200
アイデンティティ ソース , 134
仮想ホスト証明書のインポート , 221
コンソール証明書 , 201
コンソール証明書のインポート , 204
コンソール証明書の交換 , 201
有効期限の切れた証明書の交換 , 206
SecurID
Microsoft Windows 用 , 93
PIN の目的 , 26
SecurID800 のロック解除キーの取得 , 163
ソフトウェア , 29
認証の概要 , 25
認証プロセス , 26
Security Console
LDAP への read-only アクセス , 40, 113
URL, 34
監査ログ , 381
個人用の環境設定の構成 , 34
証明書 , 201
セッション有効期間の制限 , 194
設定の構成 , 34
内部データベース , 40, 114
表示オプションの設定 , 36
保護 , 38
ログオン , 34
SecurityQuestions.xsd, 153
SecurityQuestionSample.xml, 153

Self-Service Console, 24, 283
エマージェンシー アクセス , 154
構成メニュー , 283
証明書 , 201
セルフ サービス , 24
セルフサービス , 284
タスク , 24, 284
ユーザーが実行するタスク , 284
ログアウト エラー , 223
インストール先 , 283
SharePoint
トラブルシューティング , 417
Short Message Service
サービス プロバイダの変更 , 271
証明書の削除 , 272
設定のレプリケーション , 272
文字制限 , 266
レプリカでは未構成 , 272
Short Message Service プロバイダの変更 , 272
Simple Mail Transfer Protocol, 273
On-Demand トークンコードの配布 , 271
SMS, 271
SMTP。「Simple Mail Transfer Protocol」を参照
SSH. *See* Secure Shell.
SSL。「Secure Sockets Layer」を参照。
Sun Java System Directory Server
アイデンティティ ソース , 40, 113
System ログ
定義 , 381

T

TraceLevel, 375
Trace ログ
定義 , 381

U

URL, 34
ディレクトリ フェイルオーバー , 117

V

Verify Archive Log ユーティリティ , 399
version
viewing, 17
VMware
スナップショット , 428
VPN。「仮想プライベート ネットワーク」を参照

W

Web Tier
Linux からのアンインストール , 216
Windows からのアンインストール , 215
オープン可能ファイル数のハード制限 , 211, 212
仮想ホスト証明書の交換 , 221
更新 , 215
構成の編集 , 211
サーバの IP アドレスの変更 , 212
バージョンの更新 , 215, 296
バージョンのチェック , 214
バーチャル ホストの構成 , 213
ブートストラッパの起動 , 217
変更が反映されるタイミング , 212
リストア , 446
Web Tier の更新 , 215
Web Tier
ログアウト エラー , 223
Windows パスワード
RSA SecurID との統合 , 93

あ

アイデンティティ ソース , 116
Active Directory, 123, 124
LDAP 内でユーザーを移動する場合の制限 , 183
Secure Sockets Layer 証明書 , 134
アイデンティティ ソース マッピングの更新 , 197
削除 , 128
サポートされるディレクトリ , 40, 113
システムのリンク解除 , 197
セルフ サービス ユーザーのアカウント登録 , 286
属性の更新 , 197
属性マッピング , 264
データ エレメントの分散 , 114
定義 , 39, 113
適用範囲の変更 , 123
統合 , 22, 127
プロパティ , 116
編集 , 198
リンク解除 , 128
アカウンティング シークレット
RADIUS, 336
アクセス時間制限 , 173
時間の設定 , 173

制限付きアクセス時間 , 172
アクティビティ モニタ
メッセージの表示 , 385
新しいノード シークレット , 504
宛先アドレス
On-Demand トークンコード
配信の構成 , 273
構成 , 265
アプライアンス
キャッシュのフラッシュ , 423
セキュア シェルの有効化 , 455
ソフトウェア バージョンの表示 , 463
リブート , 419
ログオン , 455, 456
アプライアンスのリブート , 419
アンインストーラ
Windows での Web Tier, 215
暗号化キー
ダウンロード , 254
暗証番号 , 160
アンチウイルス ソフトウェア
使用 , 456

い

一時 PIN, 278
一時固定トークンコード , 154
割り当て , 156
移動されたユーザーの追跡
要件 , 183
今すぐバックアップ , 423

え

エージェント自動登録 , 78
エージェント レコード
定義 , 26
永続的な静的ルート
IPv4 の追加 , 488
IPv6 の追加 , 489
削除 , 491
定義 , 487
エマージェンシー アクセス , 154
オフライン トークンコード , 158
オフライン パスコード , 159
トークンコード , 156
トークンコード設定の構成 , 307
トークンコードの有効期間 , 156
トラブルシューティングのための トークンコード , 154
ワン タイム トークンコード , 154
認証
エマージェンシー オンライン認証 , 153

お

オプション
事業継続 , 208
セキュリティ ドメイン向けのカスタム ポリシー , 83
プロビジョニング , 208
オフライン認証 , 93, 157
オフライン認証ポリシー
セキュリティ勧告を満たさないデバイスの処理 , 92
オペレーティング システム
ログオン , 455, 456
オペレーティングシステム
アカウント , 191
On-Demand 認証
サービス プロバイダの変更 , 271
オンライン パスコード
最小長の設定 , 94

か

解決不可能なユーザー
クリーンアップのスケジュール , 180
クリーンアップのスケジュール 設定 , 179
手動でのクリーンアップ , 177
猶予期間 , 180
下位のセキュリティ ドメイン
ポリシーの継承 , 83
カスタマイズ
Self-Service Console ヘルプ , 297
メール通知 , 294
カスタマイズする
ユーザー プロファイル , 289
カスタム属性 , 290
仮想ホスト
証明書 , 219
デフォルト証明書の交換 , 220
導入環境
IP アドレスまたはホスト名の確認 , 463
Web Tier のリストア , 446
ソフトウェア バージョンの表示 , 463
データ リストア , 428
プライマリ インスタンス リストア , 433

問題のソリューション , 419
レプリカ インスタンスの交換 , 444
監査
Authentication Manager, 381
監査証跡
ログのタイプ , 381
監査ログ
Security Console, 381
監視
Authentication Manager, 381
管理者
Operations Console, 189
Operations Console の追加 , 193
システム管理者 , 190
スーパー管理者 , 189
追加 , 47
管理者 ID
LDAP, 117
ディレクトリ , 117
管理者パスワード
LDAP, 117
ディレクトリ , 117
管理者ロール , 47
権限 , 48, 49
権限適用範囲 , 52, 299
コンポーネント , 49
事前定義 , 47
複数の割り当て , 48
プロビジョニング , 298
割り当て , 48
管理セッション
EAP32 セッション有効期間 , 195
コンソールおよびコマンド , 195
設定の編集 , 196
有効期間の制限 , 194
有効期間の制限のタイプ , 195
ログオン セッション , 195

き

期限切れの PIN
変更 , 278
キャッシュのフラッシュ , 423

く

クリーンアップ
手動で解決不可能なユーザー , 177
クリーンアップ制限 , 123
クリーンアップのスケジュール
解決不可能なユーザー , 180
クリーンアップのスケジュール設定
解決不可能なユーザー , 179
クリア
On-Demand 認証 PIN, 161

け

ゲートウェイ
トラブルシューティング , 496
プライマリ インスタンスでの更新 , 480
レプリカ インスタンスでの更新 , 484
警告ログ メッセージ , 412
権限 , 299
管理者 , 49
権限適用範囲
管理者 , 52
言語の変更 , 151

こ

構成
宛先アドレス , 273
エマージェンシー アクセス設定 , 307
ユーザー グループ , 288
認証エージェント
構成ファイル , 71
構成ファイル
RSA Authentication Manager, 71
Node Secret Load ユーティリティ , 75
コマンド ライン ユーティリティ
Import PIN Unlocking Key ユーティリティ , 164
Node Secret Load ユーティリティ , 77
reset-server-cert, 206
Restore Admin, 461
Verify Archive Log, 399
コンソール証明書 , 201
インポート , 204
交換 , 201
有効期限の切れた証明書の交換 , 206
コンソール証明書の交換
ユーティリティ , 206

さ

サービス
自動起動 , 458
手動管理 , 458
災害復旧
データのバックアップ , 423

再同期
トークン , 249
サブネット マスク
トラブルシューティング , 495
プライマリ インスタンスでの更新 , 480
レプリカ インスタンスでの更新 , 484
サポート プラットフォーム
アイデンティティ ソース , 40, 113

し

シード ファイル
トークン , 26
システム管理者アカウント , 190
重大システム イベント
イベント タイプ , 414
条件文
メール テンプレート , 294
詳細ログ メッセージ , 412
承認ステップ , 301
情報ログ メッセージ , 412
証明書
Secure Sockets Layer コンソール 証明書 , 206
Short Message Service プロバイダ の削除 , 272
SSL の管理 , 200
仮想ホストでの交換 , 219
仮想ホストの交換 , 221
仮想ホストへのインポート , 221
証明書署名リクエストの生成 , 202
デフォルトの交換 , 220
ファイル タイプ , 219
証明書署名リクエスト
Operations Console を使用した生成 , 202
サード パーティ ツールを使用した 生成 , 201
証明書署名リクエストの生成
サード パーティ ツール , 201
除外単語辞書 , 88, 99
パスワード ポリシーへの適用 , 88, 99
ファイル サイズ , 88, 99
新規デバイス登録 , 330
信頼関係
単方向の信頼 , 466
双方向の信頼 , 466
信頼されるレガシー レルム
修復 , 454
認証のためのポートの構成 , 475

す

スーパー管理者 , 55, 189
権限 , 190
追加 , 192
リストア , 460, 461
スケジュール レポート ジョブ , 390
スコープ
セルフ サービスの例外 , 299
スタンドアロン導入環境でのデータのリストア , 429–430

せ

制限
PIN の再使用 , 96
パスワードの有効期間 , 98
制限付きエージェント
許可されたユーザー グループの 表示 , 175
ネストされたユーザー グループ 内のユーザー , 174
複数ユーザー グループ内の ユーザー , 174
ユーザー グループの認証の許可 , 171
静的ルート , 487
IPv4 の追加 , 488, 490
IPv6 の追加 , 489, 490
削除 , 491, 492
製品の更新 , 462
セキュア シェル
アプライアンスへのアクセス , 457
有効化 , 455
セキュリティ クエスチョン
アカウント登録要件の設定 , 151
カスタム , 151
管理 , 150
クエスチョン ファイル スキーマ , 153
クエスチョン ファイルの変更 , 152
クリア , 150
サンプル ファイル , 153
セルフ サービス トラブルシューティング , 103
定義 , 150
認証用に指定 , 150

セキュリティ ドメイン
セルフ サービスのアカウント登録 , 287
ポリシーの継承 , 83
ユーザーの移動 , 146
セルフ サービス , 24, 298
Web Tier 構成の編集 , 211
アカウント登録 , 288
定義 , 283
トラブルシューティング , 307
トラブルシューティングの要件 , 103
トラブルシューティング ポリシー , 106, 309, 310
トラブルシューティング ポリシーの継承 , 104
メール アドレス , 275
ユーザーアカウント登録用のセキュリティ ドメイン , 287
セルフサービス
ユーザーの登録 , 284
ユーザーの登録用のアイデンティティ ソース , 285
セルフサービス ユーザー用の Active Directory, 285
セルフサービス ユーザー用の内部データベース , 285

そ

送付先住所
ディレクトリ サーバ属性へのマップ , 308
属性
アイデンティティ ソースの更新 , 197
除外 , 54
デバイス , 231
ソフトウェア トークン
Compressed Token Format 配布 , 231
構成 , 229
デバイス属性 , 231
デバイス定義ファイル , 229
動的シード配布 , 230, 238
配信方法 , 230
パスワード設定の構成 , 307
ファイル ベースの配布 , 230, 234
プロファイル , 229

た

ダイナミック ホスト構成プロトコル , 78
タイム ゾーン
アクセス時間制限の設定 , 173
タグ
メール通知 , 294
単方向の信頼 , 466

ち

致命的ログ メッセージ , 412

て

データのリストア
バックアップ , 431
レプリケーション導入環境 , 430
ディレクトリ
URL, 116
管理者 ID, 117
管理者パスワード , 117
接続のプロパティ , 116
統合 , 22
フェイルオーバー URL, 117
ディレクトリ サーバ
統合 , 127
テキスト メッセージ
トークンコードの配信の構成 , 272
文字制限 , 266
テスト
リスク ベース認証 , 324
デバイス
属性 , 231
履歴設定 , 330
履歴の設定 , 331
デバイス定義ファイル , 229
デフォルトメール
テンプレート タグ , 294
テンプレート
メール通知のカスタマイズ , 294
リスク ベース認証の統合 , 322

と

トークン
Compressed Token Format 配布 , 231
管理タスク , 498
更新設定の構成 , 307
再同期 , 249
削除 , 247
シード ファイル , 26

送付先住所の構成，308
ソフトウェア，29
ソフトウェア トークンの構成，229
デバイス属性，231
トークン レコード ファイルのインポート，226
動的シード配布，230
導入環境設定の構成，307
2 要素認証，26
ハードウェアの配布，234
配布者タスク，301
パスコード，26
ファイル ベースの配布，230, 236, 234
複数の動的シード，238
プロビジョニング，307
プロファイル，229
ポリシー，83, 84
ポリシーの設定，85
無効化，246, 247
ユーザーへの割り当て，228
有効化，246
リクエスト，300
レコード ファイルの移動，227
トークンコード
一時固定トークンコードの割り当て，156
エマージェンシー アクセス トラブルシューティング，154
オフライン エマージェンシー アクセス，158
生成，27
トークンコードの有効期間，156
2 要素認証，26
認証におけるロール，26
ワン タイム トークンコードの割り当て，154
トークンのインポート，226
トークンの交換
次に使用可能なトークン，249
トークンの無効化，246
トークンの有効化，246
トークン レコード
定義，26
動的シード配布，230
導入
IPv4/IPv6 エージェント，502
アプライアンスのリブート，419
導入環境
アンチウイルスソフトウェアの使用，456
キャッシュのフラッシュ，423
自動起動サービス，458
手動管理サービス，458
信頼されるレガシー レルムの修復，454
スタンドアロン導入環境でのデータのリストア，429
スタンドアロン プライマリ インスタンスの交換，433
スナップショット，428
スナップショットによるプライマリ インスタンスの復元，442
スナップショットによるレプリカ インスタンスの復元，445
製品の更新，462
データのリストア，431
トラステッド レルムの修復，447, 448, 477
トラステッド レルムの不一致の修復，451
バックアップ，423
非レプリケーション導入環境でのレプリカ インスタンスの昇格，436
プライマリ インスタンスの交換，433
レプリカ インスタンスの昇格，436, 439
レプリカ インスタンスの同期，422
レプリカ インスタンスのリストア，444
レプリケーション ステータス，420
レプリケーション ステータスの確認，419
レプリケーション導入環境でのデータのリストア，430
レプリケーション導入環境でのプライマリ インスタンスの交換，435
レプリケーション導入環境でのレプリカ インスタンスの昇格，438
導入要件
Global Catalog，124
導入例
Global Catalog，126
登録
セルフサービス，284
登録解除
非アクティブ デバイス，330
トラステッド ユーザー
RADIUS 認証の許可，473

トラステッド レルム
RADIUS 認証 , 473
アクセス制御のための複製エージェント レコード , 471
エージェントの構成 , 469
エイリアスを解決するための複製エージェント レコード , 472
グループへのトラステッド ユーザーの追加 , 474
修復 , 447, 448, 477
信頼関係の作成 , 467
トラステッド ユーザー , 473
トラステッド ユーザー グループ , 473
トラステッド ユーザーの追加 , 472
トラステッド レルムの追加 , 468
トラステッド レルムの不一致の修復 , 451
トラブルシューティング , 309
IPv4/IPv6 エージェント , 506
応答しない Web Tier, 418
応答しないプライマリ インスタンス , 417
応答しないレプリカ インスタンス , 418
欠落データ , 417
セルフ サービスの要件 , 103
トラブルシューティング ファイルのダウンロード , 382
不正確なネットワーク設定 , 493
問題のソリューション , 419
リスク ベース認証 , 325
レプリケーション , 418
ドロップされたパケット , 368

な

内部データベース
Security Console の機能 , 40, 114
外部データベースとの比較 , 22, 127
格納されたデータ , 41, 114
格納されているユーザー パスワード , 96
ユーザーの追加 , 141

に

2 要素認証
トークン , 26
認証
Authentication Manager に必要なデータ , 26
エマージェンシー オフライン , 157
エマージェンシー オフライン アクセス トークンコード , 158
エマージェンシー固定トークンコード , 156
エマージェンシー ワン タイム トークンコード , 154
エンド ユーザー操作 , 26
セキュリティ クエスチョン , 150
ユーザー設定の管理 , 147
例 , 29
認証エージェント , 69, 321
構成ファイル , 71
インストール , 72
取得 , 70, 321
制限付きエージェントの構成 , 170
ソフトウェアのダウンロード , 72
タイプ , 69
追加 , 72
導入ガイドのソース , 70, 321
ユーザー アクセスの制御 , 170
ユーザーの認証 , 26
認証エージェントのタイプ , 69
認証失敗 , 369

ね

ネットワーク
RADIUS トポロジー , 335
ネットワーク設定の更新
概要 , 479

の

ノード シークレット
IPv4/IPv6 エージェント , 504
RADIUS, 337
手動での送付 , 75

は

バージョン
表示 , 463
バージョン番号
統合スクリプト , 322
バーチャル ホスト
Web Tier の構成 , 213
ハードウェア トークン
配布 , 234

配布 , 238
Compressed Token Format, 231
動的シード , 230
ファイル ベース , 230

ファイル ベースの単一のトークン , 236
ワークフロー内のステップ , 301
パスコード
オフライン エマージェンシー アクセス , 159
カウントのクリア , 150
コンポーネント , 26
トークン , 26
パスワード
格納場所 , 96
システム生成を使用 , 96
除外単語辞書の使用 , 88, 99
セルフ サービス トラブルシューティング , 309
デフォルト ポリシーの設定 , 96
文字に対する要件の設定 , 99
有効期間 , 98
バックアップ
Back Up Now（今すぐバックアップ）の使用 , 425
Schedule Backups（スケジュール バックアップ）の使用 , 426
概要 , 423
データのリストア , 431
導入環境 , 423
含まれるデータ , 424
バックアップのスケジュール , 423, 426

ひ

非アクティブ デバイス
登録解除 , 330
非永続的な静的ルート
IPv4 の追加 , 490
IPv6 の追加 , 490
削除 , 492
定義 , 487

ふ

ブートストラッパ サーバ
Linux での管理 , 218
Web Tier での起動 , 217
Windows での管理 , 217
ファイル サイズ
除外単語辞書 , 88, 99
ファイル ベースの配布 , 230
フェイルオーバー
ロードバランサの使用 , 25
フェイルオーバー ディレクトリ URL, 117
双方向の信頼 , 466
プライベート ネットワーク
信頼関係 , 466
プライマリ インスタンス
IPv4 ネットワーク設定の更新 , 480
IPv6 ネットワーク設定 , 507
IP アドレスまたはホスト名の確認 , 463
交換 , 433
スタンドアロンの交換 , 433
スナップショット , 428
スナップショットの復元 , 442
データのリストア , 429, 431
データ リストア , 428
ネットワーク設定の概要 , 479
ネットワーク設定のトラブルシューティング , 493
リストア , 433
レプリケーション導入環境での交換 , 435
プロビジョニング , 24, 298
管理者ロール , 298
セルフ サービスのユーザー グループ , 288
定義 , 283
プロビジョニング , 299
ライセンス , 208
ワン タイム トークンコード , 154
分散
アイデンティティ ソース データ , 114

へ

ヘルプ
カスタマイズ , 297

ほ

ポート
計画 , 275
信頼されるレガシー レルム認証の構成 , 475
ホスト名
プライマリ インスタンスでの更新 , 480
レプリカ インスタンスでの更新 , 484
ポリシー
PIN の再使用 , 96
カスタムの割り当て , 83
継承 , 83
システム生成パスワード , 96

セルフ サービス トラブルシューティング , 103, 309
セルフ サービス トラブルシューティングの継承 , 104
デフォルト パスワード , 96
ロックアウトされたユーザーのロック解除 , 102, 105

み

未サポート アプリケーション
リスク ベース認証 , 332

め

メール
On-Demand 認証の構成 , 273
サーバ , 275
サーバの構成 , 275
サーバ ログオン , 275
通知構文 , 294
通知のホスト名 , 275
テンプレート タグ , 294
メッセージ
RADIUS ステータス , 341

も

文字に対する要件
パスワードの設定 , 99
文字の要件
SMS テキスト メッセージ , 266
モニタ システム
ログのタイプ , 381

ゆ

ユーザー
LDAP ディレクトリ内での移動のインパクト , 184
LDAP ディレクトリ内での変更 , 186
LDAP で解決不可能になる , 175
LDAP 内でのユーザー ID の変更 , 186
On-Demand 認証 PIN のクリア , 161
PIN の変更 , 162
RSA SecurID PIN のクリア , 163
アカウントの無効化 , 144
アカウントの有効化 , 145
アクセスの制御 , 170
新しいセキュリティ ドメインへの移動 , 146
新しいセキュリティ ドメインへの転送 , 145
解決不可能なユーザーの手動クリーンアップ , 176
格納されているパスワード , 96
管理者が初期 PIN を設定 , 278
休暇不在の管理 , 144
グループ メンバーシップによるアクセス制限 , 174
初期 PIN の設定 , 278
制限付きエージェントでのアクセス制御 , 170
セルフサービス , 284
トークンの再同期 , 249
トークンの削除 , 247
トークンの割り当て , 228
内部データベースへの追加 , 141
認証設定の管理 , 147
ネストされたグループによるアクセス制限 , 174
パスコード カウントのクリア , 150
元のアイデンティティ ソース外への移動 , 183
ユーザー グループ , 165
ユーザー グループへのユーザーの追加 , 169
ユーザー データ変更の影響 , 175
ライセンスに追加 , 207
リモート ユーザー用のアクセス制限 , 173
ログオン エイリアス , 149
ロックアウト後にロック解除 , 102, 105
ロック解除 , 149
ユーザー ID
LDAP 内での変更 , 186
重複の解決 , 146
有効なユーザ , 191
ユーザー アカウント
休暇不在の管理 , 144
無効化 , 144
有効化 , 145
ユーザー アクション , 298
LDAP
ユーザー移動のインパクト , 184
ユーザーおよびグループの手動クリーンアップ , 176
ユーザー確認方法
RBA 用 , 319, 330

ユーザー グループ , 165
Active Directory の変更 , 187
LDAP ディレクトリ内での変更 , 187
LDAP で解決不可能になる , 176
アクセス時間制限 , 172
解決不可能なグループの手動クリーンアップ , 176
グループの追加 , 168
作成 , 166
制限付きエージェント , 174
制限付きエージェントでの認証 , 171
制限付きエージェントへのアクセス権の付与 , 174
組織 , 165
特性 , 165
内部データベース , 167
認証が許可されたグループの表示 , 175
ネスト化 , 167
プロビジョニングの構成 , 288
ユーザーの追加 , 169
ユーザーの管理
トークンの削除 , 247
ユーザー プロファイル , 290
ユーザー ベース DN, 122
ユーザー リクエスト , 301
タイプ , 300
ユーザー レコード
ソース , 26
定義 , 26
ユーティリティ
Import PIN Unlocking Key ユーティリティ , 164
Verify Archive Log, 399
有効期間
パスワード , 98
有効なユーザ
ユーザー ID, 191
優先 RBA インスタンス
Web Tier 構成の編集 , 211
猶予期間 , 123
ユーザー確認方法 , 319, 330

よ

読み取り専用
LDAP アイデンティティ ソース , 40, 113

ら

ライセンス , 298
Base Server, 208
Enterprise Server, 208
アップグレード , 208
インストール , 208
インストール済みの表示 , 209
最大ユーザー数 , 207
事業継続オプション , 208
シリアル番号 , 17
ユーザーの追加 , 207
ライセンス タイプ , 207

り

リクエスト
Authentication Manager の使用 , 25
エージェントから , 26
タイプ , 306
ワークフロー , 301
リスク エンジン
学習期間 , 316
自己調節 , 316
ソフト マッチング技術 , 316
リスク ベース認証
カスタム ソリューション , 312
最低保証レベル , 316
サポートされる Web ベース アプリケーション , 312
実装とテスト , 319
設定のトラブルシューティング , 325
デバイス , 330
デバイスの設定 , 319, 330
統合スクリプト テンプレート , 322
統合スクリプトの目的 , 322
ブラウザ エラー , 325
未サポート アプリケーション , 332
ユーザー確認方法 , 319, 330
ユーザー確認方法の構成 , 329
ユーザーの有効化 , 316
リソース不足 , 369

れ

レガシー レルム
信頼関係 , 475
ポートの構成 , 475
レコード
エージェント , 26
トークン , 26
ユーザー , 26

レプリカ インスタンス
定義 , 21
IPv4 ネットワーク設定の更新 , 484
IPv6 ネットワーク設定 , 507
IP アドレスまたはホスト名の確認 , 463
交換 , 444
ステータス , 420
ステータスの確認 , 419
スナップショット , 428
スナップショットの復元 , 445
同期 , 422
ネットワーク設定の更新 , 479
ネットワーク設定のトラブルシューティング , 493
非レプリケーション導入環境での昇格 , 436
プライマリ インスタンスのネットワーク設定の更新 , 483
プライマリ インスタンスへの昇格 , 436, 439
リストア , 444
レプリケーション導入環境での昇格 , 438
レプリカ インスタンスの昇格 , 436, 439
非レプリケーション導入環境 , 436
レプリカ インスタンスの同期 , 422
レプリケーション
RADIUS しーくれっと , 336
RADIUS データ , 339
ステータスの確認 , 419
ステータスの説明 , 420
レポート , 386
スケジュール レポート ジョブ , 390
それぞれの管理者ロールで実行できる , 386
追加 , 391
レルムからアイデンティティ ソースのリンク解除 , 128

ろ

ログ , 398
Authentication Manager, 381
エラー メッセージ , 412
警告レベル メッセージ , 412
構成 , 412
詳細レベル メッセージ , 412
情報レベル メッセージ , 412
致命的レベル メッセージ , 412
トレース ログのレベル , 412
ログ アーカイブ , 398
ログオン
Operations Console, 194
アプライアンス , 455
メール サーバ , 275
ログオン]Security Console, 34
ログオン エイリアス , 149
ログのタイプ , 381
ロックアウト ポリシー
ユーザーのロック解除 , 102, 105
ロック解除
ユーザー , 149
ロックアウト後のユーザー , 102, 105

わ

ワークフロー , 300
説明 , 301
ワークフロー ポリシー , 301
ワン タイム トークンコード , 154
割り当て , 154