Dell Data Protection

構成ガイド

2014 年 02 月

目次

1

Compatibility Server の構成

この章では、Compatibility Server をご使用の環境に適用させるために変更するパラメータについて詳しく説明します。構成ファイルは、編集する前に必ずバックアップしてください。

これらのファイル内のパラメータは、本ドキュメントで説明されているもののみを変更してください。これらのファイル内のその他のデータ（タグなど）を変更すると、システムの破損や障害が発生するおそれがあります。Dell は、これらのファイルの許可されていない変更に起因する問題が、Compatibility Server の再インストールなしで解決できることを保証できません。

server_config.xml

<Compatibility Server のインストールディレクトリ >\conf\server_config.xml の次のパラメータを変更できます。変更してはいけないパラメータには、その旨の注記があります。Compatibility Server が起動されている場合、Compatibility Server Service を停止して server_config.xml ファイルを編集し、Compatibility Server Service を再起動してこのファイルの変更内容を有効にします。

server_config.xml		
パラメータ	**デフォルト**	**説明**
secrets.location	$dell.home$/conf/secretKeyStore	secretkeystore のデフォルトの場所。このファイルをデフォルトの場所から変更する場合は、このパラメータを更新します。
archive.location	$dell.home$/conf/archive	アーカイブのデフォルトの場所。このファイルをデフォルトの場所から変更する場合は、このパラメータを更新します。
domain.qualified.authentication	true	サーバーへのすべての要求に完全修飾ユーザーログイン名が必要かどうかを示します。 この値を変更した場合は、Device Server を再起動しないと新しい値が有効になりません。
directory.max.search.size	1000	ディレクトリ検索の制限の後、例外がスローされます。
directory.server.search.timeout.seconds	60	LDAP 検索のサーバータイムアウト（秒単位）。
directory.client.search.timeout	60	LDAP 検索のクライアントタイムアウト（秒単位）。

server_config.xml		
パラメータ	デフォルト	説明
rmi.recovery.host		マルチサーバー EMS 復元を使用するには: <!-- - uncomment and change host names to your fully qualified domain names to chain recovery <property name="rmi.recovery.host"> <value>rmi://foo.fabrikam.com:1099</value> </property> <property name="rmi.recovery.host"> <value>rmi://foo.fabrikam2.com:1099</value> </property> -->
default.gatekeeper.group.remote	CMGREMOTE	すべてのポリシープロキシがデフォルトで所属しているグループのデフォルト名。この名前をここで、または Device Server の context.properties で変更できます。 ここでグループ名を変更しときに次の事項を実行する場合は、Device Server でもグループ名を変更する必要があります。 • Windows デバイスの Shield • CREDActivate の使用 すべてのポリシープロキシを単一のグループに所属させることを推奨します。
rsa.securid.enabled	false	Microsoft Windows バージョン 6 に RSA SecurID を GINA Replacement として使用している場合は、このパラメータを true に設定して、Compatibility Server Service の停止と再起動を行います。 RSA GINA Replacement 環境で Shield ユーザーがアクティベーションされたら、RSA 認証が LDAP 認証を置換します。
inv.queue.task.worker.size	10	インベントリキューを処理するスレッドの数。
inv.queue.task.timeout.seconds	900	タイムアウトが発生するまでの秒数。
inv.queue.task.retry.count	3	サーバーがインベントリを、廃棄される前に処理を試行する回数。
report.retry.max	120	再試行の最大回数。
report.retry.wait.millis	250	再試行までのミリ秒数。

server_config.xml		
パラメータ	デフォルト	説明
triage.execute.time	0 0 0/6 * *	トリアージは、サーバーがすでに認識しているユーザーおよびグループを調整する処理です。 デフォルト設定は 0 0 0/6 * * ? で、夜中から 6 時間ごと（午前 0 時、午前 6 時、正午、午後 6 時、午前 0 時、以下同様）にトリアージを実行することを意味します。
gatekeeper.service.max.sessions	5	ポリシープロキシセッションの最大回数。
gatekeeper.service.max.session.timeout	5	ポリシープロキシセッションの最大回数のタイムアウト。
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	グループまたはユーザーの管理ロールを更新するために必要なロール。
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	グループまたはユーザーの管理ロールを更新するために必要なロール
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin、LogAdmin	ログセッションを取得するために必要なロール。
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin、LogAdmin	ログを取得するために必要なロール。
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin、LogAdmin	ログ列リストを取得するために必要なロール。
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin、LogAdmin	ログカテゴリリストを取得するために必要なロール。
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin、LogAdmin	ログ優先順位リストを取得するために必要なロール。
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin、SecAdmin、HelpDeskAdmin、SystemAdmin	固有 ID 名を取得するために必要なロール。
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	システムの管理者リストを取得するために必要なロール。
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	superadmin パスワードを設定するために必要なロール。
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	superadmin パスワードをリセットするために必要なロール。
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin、SecAdmin	ドメインを追加するために必要なロール。
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin、SecAdmin	ドメインを削除するために必要なロール。
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin、SecAdmin	ドメインを更新するために必要なロール。
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin、SecAdmin	グループを追加するために必要なロール。
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin、SecAdmin	グループを削除するために必要なロール。

server_config.xml		
パラメータ	デフォルト	説明
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin、SecAdmin	LDAP グループを検索するために必要なロール。
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin、SecAdmin	LDAP ユーザーを検索するために必要なロール。
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin、SecAdmin	ユーザーを追加するために必要なロール。
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	エンタープライズライセンスを追加するために必要なロール。
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	エンタープライズライセンスを表示するために必要なロール。
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin、SecAdmin	デバイスを復元するために必要なロール。
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin、SecAdmin	ユーザーを一時停止するために必要なロール。
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	プロキシによってデバイスをアクティベーションするために必要なロール。
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin、SecAdmin	プロキシによってデバイスを手動で復元するために必要なロール。
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Gatekeeper リソースファイルを取得するために必要なロール。
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Gatekeeper リソースファイルを承認するために必要なロール。
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Gatekeeper 構成を承認するために必要なロール。
policy.arbiter.security.mode	most-restrictive	このプロパティは、ポリシーに複数の親ノードがあるときに、セキュリティバイアスを持つポリシー要素に対してポリシーマッピングアルゴリズムをどのように機能させるかを制御します。 値： Least-restrictive に設定すると、制限が最も緩い、親からの要素値が使用されます Most-restrictive に設定すると、制限が最も厳しい、すべての親からの要素値が使用されます
policy.set.synchronization.sync-unmodified	true	このフラグは、次の外部同期によって、変更されたフラグを true に設定せずに、すべてのポリシー要素を追加または再マッピングされる必要があることを示します。このフラグは同期ごとに false に切り替えられるため、セキュリティ管理者が変更なしに追加する場合はリセットする必要があります。これは詳細オプションです。
db.schema.version.major		メジャーデータベーススキーマ。
db.schema.version.minor		マイナーデータベーススキーマ。

server_config.xml		
パラメータ	デフォルト	説明
db.schema.version.patch		データベーススキーマのパッチバージョン。
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	データベースドライバのデフォルトの場所。このファイルをデフォルトの場所から変更する場合は、このパラメータを更新します。
dao.db.host		データベースサーバーのホスト名。 このパラメータは、構成ツール内で変更されます。
dao.db.name		データベースの名前。 このパラメータは、構成ツール内で変更されます。
dao.db.user		データベースに対して完全な権限を持つユーザー名。 このパラメータは、構成ツール内で変更されます。
dao.db.password		データベースに対して完全な権限を持つユーザー名のパスワード。 このパラメータは、構成ツール内で変更されます。
dao.db.max.retry.count	10	指定されたソケットエラーの発生時に Compatibility Server が SQL Server への再接続を試行する最大回数。
dao.db.connection.retry.wait.seconds	5	最初の再接続試行は、ただちに行われます。2 回目は、指定された秒数後に行われます。3 回目は、指定された秒数の 2 倍の時間が経過した後に行われ、4 回目は 3 倍の時間が経過した後、以下同様となります。
dao.connection.pool.max.uses	10000	接続を再試行できます。0 は試行しないことを意味します。
dao.connection.pool.inactive.threshold.seconds	900	接続を使用していない時間、および接続を切断できる時間を指定するために使用されます。
dao.db.driver.socket.errors	0	このコンマで区切られたリスト内のコードに対応するエラーが発生すると、Compatibility Server は SQL Server への再接続を試行します。0 は Microsoft SQL のソケットエラーのエラーコードです。サーバー一時停止エラーの 17142、サーバーシャットダウンエラーの 6002 が加えられます。
dao.db.mssql.compatability.level	90	SQL 2005 以降の値。
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	権限ファイルハンドラ。
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	インベントリファイルハンドラ。

server_config.xml		
パラメータ	デフォルト	説明
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	イベントファイルハンドラ。
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Gatekeeper リソースファイルをデフォルトの場所から移動する場合は、このパラメータを更新します。
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Gatekeeper リソースファイルをデフォルトの場所から移動する場合は、このパラメータを更新します。
rmi.server.registry.host	localhost	このホストプロパティは、レジストリの場所を指定するクライアントプログラムだけのためのものです。RMI レジストリおよびリモートオブジェクトの作成時には使用されません。localhost で作成されます。
rmi.server.registry.port	1099	RMI レジストリポートは、インストール中に構成できます。インストール後に、このパラメータを使用してポートを変更することもできます。 この値を変更する場合は、Gatekeeper Web Services を構成する必要もあります。
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	サーバーレポート権限を設定するために必要なロール。
security.authorization.method.IReportingService.removeEntity	SystemAdmin	サーバーエンティティを削除するために必要なロール。
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	サーバーエンティティの表示を設定するために必要なロール。
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	デバイス詳細ページを表示するために必要なロール。
security.authorization.method.IReportingService.openSession	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	サーバーセッションを開くために必要なロール。
security.authorization.method.IReportingService.getPagedReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	デバイスタイプレポートを表示するために必要なロール。
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	オペレーティングシステムレポートを表示するために必要なロール。
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	デバイスモデルレポートを表示するために必要なロール。
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	ポリシー詳細レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	ワークステーション詳細レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	暗号化失敗レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	暗号化サマリーレポートを表示するために必要なロール。

server_config.xml		
パラメータ	デフォルト	説明
security.authorization.method.IReportingService.getUserDetail	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	ユーザー詳細レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	グループ詳細レポートを表示するために必要なロール。
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin、HelpDeskAdmin、SystemAdmin、SecAdmin	ドメインレポートのリストを表示するために必要なロール。
security.authorization.method.IKeyService.getKeys	ForensicAdmin	この設定は、フォレンジック統合プラグインと併用されます。フォレンジックツール統合が必要な場合は、Dell サポートに連絡してください。
accountType.nonActiveDirectory.enabled	false	ドメイン以外のアクティベーションの有効化は、広範な結果を伴う高度な構成です。この構成を有効化する前に、カスタマサポートに問い合わせて特定の環境のニーズについて話し合ってください。この値の変更後は Compatibility Server Service を再開します。 この設定に加え、Windows コンピュータのレジストリ設定を以下のように作成または変更します。 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations= REG_DWORD:1

gkresource.xml

<Compatibility Server インストールディレクトリ >\conf\gkresource.xml のパラメータを変更できます。

変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。こうすると、アップグレード時に変更内容を新しいファイルに容易に転送できます。

注： gkresource.xml ファイルは、適格な XML ファイルである必要があります。XML に精通していない場合は、このファイルを編集しないようにすることを推奨します。適切な場合には、未処理（非エスケープ）の特殊文字ではなくエンティティリファレンスを必ず使用してください。

システム管理者は、Gatekeeper リソースファイルの変更内容を、有効になる前に承認する必要があります。

ドメイン\ユーザー名の形式の有効化

次の文字列を追加すると、ドメイン\ユーザー名の形式が有効または無効になります。この形式は、ファイル内に文字列が存在しない場合は無効になります。値を 0 に設定しても無効にできます。

1. <Compatibility Server インストールディレクトリ >\conf に移動します。
2. XML エディタで gkresource.xml を開きます。
3. 次の文字列を追加します。

   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. ［保存］をクリックしてファイルを保存し、閉じます。

run-service.conf

<Compatibility Server インストールディレクトリ >\conf\run-service.conf の次のパラメータの一部を変更できます。パラメータは、インストール時に自動的に設定されています。サービスのカスタマイズまたは構成変更を実行するには、次の手順に従います。

1. サービスを停止します。
2. サービスを削除します。
3. run-service.conf ファイルを編集および保存します。変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。
4. サービスを再インストールします。
5. サービスを開始します。

run-service.conf

パラメータ	デフォルト	説明
JAVA_HOME	Dell\Java Runtime\jreX.x	Java インストールディレクトリの場所。
wrapper.java.additional.5	n/a	この行の MAC アドレスは、ローカルイーサネットアダプタの MAC アドレスです。 サーバーに複数の NIC がある場合、またはプライマリアダプタ以外のアダプタにバインドする場合は、ここに NIC の物理 MAC アドレスをダッシュを付けずに入力します。
wrapper.ntservice.name	EpmCompatSvr	サービスの名前。
wrapper.ntservice.displayname	Dell Compatibility Server	サービスの表示名。
wrapper.ntservice.description	Enterprise Compatibility Server	サービスの説明。
wrapper.ntservice.dependency.1		サービスの依存関係。必要に応じて、依存関係（開始値 1）を追加します。
wrapper.ntservice.starttype	AUTO_START	サービスがインストールされるモード。AUTO_START または DEMAND_START です。
wrapper.ntservice.interactive	false	true に設定すると、サービスはデスクトップと相互作用できます。

2

Core Server の構成

この章では、Core Server をご使用の環境に適用させるために変更できるパラメータについて詳しく説明します。

これらのファイル内のパラメータは、本ドキュメントで説明されているもののみを変更してください。これらのファイル内のその他のデータ（タグなど）を変更すると、システムの破損や障害が発生するおそれがあります。Dell は、これらのファイルの許可されていない変更に起因する問題が、Core Server の再インストールなしで解決できることを保証できません。

ポリシーアービトレーションの最高セキュアから最低セキュアへの変更

PolicyService.config

この設定を変更して、ポリシーアービトレーションを最高セキュアから最低セキュアに変更します。**<Core Server インストールディレクトリ >\PolicyService.config** 内の設定を変更します。Core Server が起動されている場合、サービスを停止して PolicyService.config ファイルを編集し、サービスを再起動してこのファイルの変更内容を有効にします。

変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。こうすると、アップグレード時に変更内容を新しい PolicyServiceConfig.xml ファイルに容易に転送できます。

次のセクションを変更します。

```
<!-- Web Service Targets -->
<object id="PolicyService" singleton="false" type="Credant.Policy.Service.PolicyService,
Credant.Policy.ServiceImplementation">
    <property name="TemplateDataAccess" ref="TemplateDataAccess"/>
    <property name="PolicyDataAccess" ref="PolicyDataAccess"/>
    <property name="SupportDataAccess" ref="SupportDataAccess"/>
    <property name="AuditLog" ref="ServiceAuditLog"/>
    <property name="GlobalArbitrationBias" value="1" /> [ この値を「0」から「1」に変更して、値を最低セキュアに設定する ]
</object>
```

Web Services の無効化

注：これはカスタマサポートの指示がある場合にのみ変更すべきである高度な設定です。

Core Server の Web Services を無効にするには（例えば、インベントリ処理のみを実行する第 2 の Core Server がインストールされている場合）、次の設定を変更します。

<Core Server インストールディレクトリ >
Credant.Server2.WindowsService.exe.Config

および

<Core Server インストールディレクトリ >\Spring.config

Core Server が実行されている場合、サービスを停止してこれら 2 つのファイルの設定を編集し、サービスを再開してこのファイルの変更内容を有効にします。

Credant.Server2.WindowsService.exe.Config

次のセクションを削除します。

```
<!-- Web Services Configuration -->
<system.serviceModel>
    <services configSource="Services.config"/>
    <behaviors configSource="Behaviors.config"/>
    <bindings configSource="Bindings.config"/>
</system.serviceModel>
```

Spring.config

次を削除します。

AOP Advice、Web Service Target Definition、Web Service Host Definition の各ヘッダーにあるすべての <object> </object> 定義を削除します。

SMTP サーバーのライセンスメール通知の有効化

Dell Data Protection | Cloud Edition を使用している場合は、これらの設定はサーバー構成ツールで自動的に行われます。以下の手順は、Dell Data Protection | Cloud Edition を使わずに SMTP サーバーのライセンスメール通知を有効化する必要がある場合に使用します。

NotificationObjects.config

SMTP サーバーでライセンスメール通知を構成するには、<Core Server インストールディレクトリ > の NotificationObjects.config ファイルを変更します。

次を変更します。

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [この値は変更しない]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [この値は変更しない]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="username"/>
  <property name="Password" value="${SmtpPassword}"/> [この値は変更しない]
  <property name="Logger" ref="NotificationLogger"/> [この値は変更しない]
</object>
```

Notification.config

メールサーバーが認証を要求する場合、<Core Server インストールディレクトリ > 内にある Notification.config ファイルを変更します。

次を変更します。

```
<notification>
    <add key="SmtpPassword" value="your_email_server_password"/>
</notification>
```

Core Server 構成ファイルへの Compatibility Server のフォルダ位置の追加

Core Server は .Net アプリケーションであるため、権限の問題によりレジストリ情報にアクセスできないことがあります。secretkeystore（データベース暗号化キー）を読み取るために Core Server が Compatibility Server のレジストリ構成情報にアクセスして secretkeystore の位置を取得する必要がある場合に問題となります。レジストリの権限が原因でアクセスがブロックされると、Core Server はコンソールユーザーを認証できません。以下の設定では、レジストリのアクセス権が問題になる場合に、Compatibility Server のフォルダ位置を Core Server の構成ファイルに追加します。

1. <Core Server インストールディレクトリ >\EntityDataAccessObjects.config に移動します。
2. 次の**太字**部分を変更します。

   <object id="DomainDataAccess" singleton="false" type="Credant.Entity.DataAccess.DomainDataAccess, Credant.Entity.DataAccess">

   <property name="Logger" ref="DataAccessLogger"/>

   <!--<property name="CompatibilityServerPath" value="PATH_TO_COMPATIBILITY_SERVER"/> -->
   この行のコメントを外し、Compatibility Server への完全修飾パスを設定します。

   </object>
3. ［保存］をクリックしてファイルを保存し、閉じます。
4. Core Server Service および Compatibility Server Service を再起動します。

Core Server による認証方法の反復の許可

許可された認証方法に設定されるポリシーが原因で Core Server の認証がドメインコントローラーによってブロックされる場合があります。Core Server の構成ファイルに「スイッチ」を実装することにより、Core Server は複数の認証方法を反復的に試行して、機能する方法を見つけることができるようになりました。

1. <Core Server インストールディレクトリ >\Spring.config に移動します。
2. 次の**太字**部分を変更します。

   <object id="DomainCache" singleton="true" type="Credant.Authorization.DomainCache.DomainCache, Credant.Authorization.DomainCache">

   <!-- Change this logger? -->

   <property name="Logger" ref="DataAccessLogger" />

   <property name="DomainDataAccess" ref="DomainDataAccess" />

   <property name="RefreshFrequency" value="300" />

   <property name="TryAllAuthTypes" value="false" /> この値を「true」に変更するとこの機能が有効になります

   <!-- Used to change the AuthType per domain: key is domain's CID and value is the System.DirectoryServices.AuthenticationTypes value

   <property name="DomainAuthType">

   <dictionary key-type="string" value-type="int" >

   <entry key="5A23TPM2" value="0" />

   </dictionary>

   </property>

   -->

   </object>
3. ［保存］をクリックしてファイルを保存し、閉じます。
4. Core Server Service を再起動します。

3

Device Server の構成

この章では、Device Server をご使用の環境に適用させるために変更できるパラメータについて詳しく説明します。

これらのファイル内のパラメータは、本ドキュメントで説明されているもののみを変更してください。これらのファイル内のその他のデータ（タグなど）を変更すると、システムの破損や障害が発生するおそれがあります。Dell は、これらのファイルの許可されていない変更に起因する問題が、Device Server の再インストールなしで解決できることを保証できません。

eserver.properties

<Device Server インストールディレクトリ >\conf\eserver.properties の次のパラメータを変更できます。

変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。こうすると、アップグレード時に変更内容を新しいファイルに容易に転送できます。

eserver.properties

パラメータ	デフォルト	説明
eserver.default.host	Device Server Service	Device Server Service がインストールされている場所の FQDN。
eserver.default.port	v7.7 以降の Enterprise Server - 8443 v7.7 より前の Enterprise Server - 8081	Device Server がデバイスからの入力アクティベーション要求をリスンするポート。
eserver.use.ssl	True	デフォルトでは、SSL は有効にされています。SSL を無効にするには、このパラメータを False に変更します。
eserver.keystore.location	${context['server.home']}/conf/cacerts	Device Server に使用される SSL 証明書の場所。
eserver.keystore.password	changeit	構成ツールの cacerts パスワードを変更した場合、このパラメータは適宜更新されます。初期設定後に構成ツール内の cacert を変更する場合は、使用されている Keystore パスワードでこのパラメータを更新します。

eserver.properties		
パラメータ	デフォルト	説明
eserver.ciphers		暗号化文字のリストを設定します。各暗号文字は、コンマで区切る必要があります。左が空である場合、ソケットは Tomcat によりサポートされる使用可能な暗号文字を許可します。 下の例のコメントを外して、暗号化文字のリストを設定します。各暗号文字をコンマで区切ります。有効な暗号文字スイート名のリストについては、Sun の JSSE リファレンスガイドを参照してください。 #eserver.ciphers= SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

run-service.conf

<Device Server インストールディレクトリ >\conf\run-service.conf の次のパラメータの一部を変更できます。パラメータは、インストール時に自動的に設定されています。サービスのカスタマイズまたは構成変更を実行するには、次の手順に従います。

1. サービスを停止します。
2. サービスを削除します。
3. run-service.conf ファイルを編集および保存します。変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。
4. サービスを再インストールします。
5. サービスを開始します。

run-service.conf		
パラメータ	デフォルト	説明
JAVA_HOME	Dell\Java Runtime\jreX.x	Java インストールディレクトリの場所。
wrapper.ntservice.name	EpmDeviceSvr	サービスの名前。
wrapper.ntservice.displayname	Dell Device Server	サービスの表示名。
wrapper.ntservice.description	Enterprise Device Server	サービスの説明。
wrapper.ntservice.dependency.1		サービスの依存関係。必要に応じて、依存関係（開始値 1）を追加します。
wrapper.ntservice.starttype	AUTO_START	サービスがインストールされるモード。AUTO_START または DEMAND_START です。
wrapper.ntservice.interactive	false	true に設定すると、サービスはデスクトップと相互作用できます。

4

Security Server の構成

この章では、Security Server をご使用の環境に適用させるために変更するパラメータについて詳しく説明します。

これらのファイル内のパラメータは、本ドキュメントで説明されているもののみを変更してください。これらのファイル内のその他のデータ（タグなど）を変更すると、システムの破損や障害が発生するおそれがあります。Dell は、これらのファイルの許可されていない変更に起因する問題が、Security Server の再インストールなしで解決できることを保証できません。

context.properties

<Security Server インストールディレクトリ >\webapps\xapi\WEB-INF\context.properties の次のパラメータを変更できます。

変更内容を示すコメントを、ファイル内の先頭に記録することを推奨します。こうすると、アップグレード時に変更内容を新しいファイルに容易に転送できます。

context.properties		
パラメータ	**デフォルト**	**説明**
default.gatekeeper.group.remote	CMGREMOTE	デバイスリモートグループ名。**変更しないでください。**
xmlrpc.max.threads	250	この Device Server 内の並列スレッドの最大数。
default.auth.upn.suffix		サーバーが完全修飾ログイン名を要求する場合にユーザーログイン名に付加される UPN サフィックス。この要求では提供されません。
device.manual.auth.enable	true	手動認証が有効か無効かを示します。**変更しないでください**
service.activation.enable	true	Device Server によってアクティベーションが処理されるかどうかを示します。**変更しないでください**
service.policy.enable	true	ポリシーが有効か無効かを示します。**変更しないでください。**
service.auth.enable	true	Device Server によって認証が処理されるかどうかを示します。
service.forensic.enable	true	この設定は、フォレンジック統合プラグインと併用されます。フォレンジックツール統合が必要な場合は、Dell サポートに連絡してください。
service.support.enable	true	サーバーに関するメタ情報の取得を有効にします。
service.device.enable	true	SDE キーストレージなどの Shield サービスのサポートを有効にします。

5

暗号化機能の構成

このセクションでは、暗号化機能を自由に制御する方法について説明します。

一時ファイル削除の防止

デフォルトでは、DDPE のインストールまたはアップグレード時に c:\windows\temp ディレクトリ内のすべての一時ファイルが自動的に削除されます。一時ファイルの削除は初期暗号化スイープの前に実行され、一時ファイルの削除によって初期暗号化が高速化されます。

しかし、\temp ディレクトリ内のファイル構成の維持を要求するサードパーティのアプリケーションが組織で使用されている場合、この削除を防止する必要があります。

一時ファイル削除を無効にするには、レジストリ設定を次のように作成または変更します。

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)＝0

一時ファイルを削除**しない**と、初期暗号化時間が長くなることに注意してください。

オーバーレイアイコンの非表示

デフォルトでは、インストール中はすべての暗号化オーバーレイアイコンが表示されるように設定されています。次のレジストリ設定を使用して、最初のインストールの後、コンピュータ上のすべての管理対象ユーザーの暗号化オーバーレイアイコンを非表示にすることができます。

レジストリ設定を次のように作成または変更します。

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)＝1

ユーザー（適切な権限を持つ）が暗号化オーバーレイアイコンを表示するように選択した場合、その設定値はこのレジストリ値より優先されます。

システムトレイアイコンの非表示

デフォルトでは、インストール中にシステムトレイアイコンは表示されます。次のレジストリ設定を使用して、最初のインストールの後、コンピュータ上のすべての管理対象ユーザーのシステムトレイアイコンを非表示にすることができます。

レジストリ設定を次のように作成または変更します。

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)＝1

スロットアクティベーション

スロットアクティベーションは、大量デプロイ中にサーバー負荷を軽減するために、Shield のアクティベーションを設定時間周期にわたって拡張できる機能です。アクティベーション時間を円滑に分散するために、アクティベーションは、アルゴリズムによって生成されたタイムスロットに基づいて延期されます。

スロットアクティベーションは、Shield インストーラまたは Shield ワークステーションから有効化および設定されます。

VPN からアクティベーションを要求するユーザーの場合は、VPN クライアントソフトウェアがネットワーク接続を確立するまでにかかる時間を見込んだ十分な時間分初期アクティベーションを延期させるよう、Shield のスロットアクティベーションの構成を変更する必要がある場合があります。

注意：スロットアクティベーションは、カスタマサポートの支援を受けた場合のみ構成してください。タイムスロットの設定を誤ると、多数のクライアントが同時にアクティベーションを実行しようとするため、パフォーマンス上の重大な問題が発生するおそれがあります。

スロットアクティベーションの設定には、次のレジストリキーが使用されます。次のレジストリキーを変更した場合、Shield ワークステーションを再起動して更新内容を有効にする必要があります。

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\SlottedActivation

  この設定でスロットアクティベーション機能を有効または無効にします。
  無効 = 0（デフォルト）
  有効 = 1

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat

  アクティベーションスロット間隔が発生する時間周期（秒単位）。このプロパティを使用して、アクティベーションスロット間隔が発生する期間（秒単位）を上書きできます。7 時間の期間の場合、スロットアクティベーションに 25200 秒が使用できます。デフォルト設定は 86400 秒で、これは、毎日繰り返されることを表します。

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals

  すべてのアクティベーション時間スロットが発生するときの、繰り返し中の間隔（ACTIVATION_SLOT_CALREPEAT）。1 つの間隔しか許可されません。この設定は 0,<CalRepeat> である必要があります。0 に設定すると、予期せぬ結果が発生する可能性があります。デフォルト設定は 0,86400 です。7 時間の繰り返しに設定するには、0,25200 の設定を使用します。Shield ユーザーがログインすると、CALREPEAT が有効になります。

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold

  アクティベーションがスロット化されたユーザーが次にログインするときに、コンピュータがアクティベーションを実行しようとする前に失われる可能性のあるアクティベーションスロットの数。この試行中にアクティベーションが失敗した場合、Shield はスロットアクティベーション試行を再開します。ネットワーク障害によりアクティベーションが失敗した場合は、MISSTHRESHOLD の値を超えても、ネットワークの再接続時にアクティベーションが試行されます。アクティベーションスロット時間に達する前にユーザーがログアウトした場合は、次のログイン時に新しいスロットが割り当てられます。

- HKCU/Software/CREDANT/ActivationSlot（ユーザーごとのデータ）

  スロットアクティベーションが有効にされた後にユーザーが初めてネットワークにログオンするときに設定される、スロットアクティベーションを試行する延期時間。アクティベーションスロットは、アクティベーション試行ごとに再計算されます。

- HKCU/Software/CREDANT/SlotAttemptCount（ユーザーごとのデータ）

  時間スロットが到達して、アクティベーション試行に失敗したときの、失敗または損失した試行回数。この回数が ACTIVATION_SLOT_MISSTHRESHOLD に設定された値に達すると、コンピュータは、ネットワークに接続するとすぐに、アクティベーションを 1 回試行します。

コマンドラインからスロットアクティベーションを有効にするには、次のようなコマンドを使用します。

```
setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0,25200 <other parameters>"
```

注：空白など、特殊文字を 1 つ以上含む値は、必ずエスケープした引用符で囲んでください。

強制ポーリング

次のレジストリ設定を使用して、強制ポリシー更新のために、Shield がサーバーをポーリングするようにします。

レジストリ設定を次のように作成または変更します。

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD value)=1

Shield のバージョンに応じて、レジストリ設定は自動的に非表示になるか、**または**ポーリングの完了後に 1 から 0 に変更されます。

管理ユーザーの許可セットによっては、このレジストリ設定を作成するために許可の変更が必要となる場合があります。新しい DWORD を作成しようとしたときに問題が生じた場合は、次の手順に従って許可を変更します。

1. Windows レジストリで、HKLM\SOFTWARE\Credant\CMGShield\Notify に移動します。
2. ［Notify］を右クリックして、［Permissions］を選択します。
3. ［Permission for Notify］ウィンドウが開いたら、［Full Control］チェックボックスをオンにします。
4. ［OK］をクリックします。

これで新しいレジストリ設定を作成できます。

インベントリオプション

次のレジストリ設定を使用して、Shield からサーバーへの最適化されたインベントリの送信、完全なインベントリの送信、またはアクティベーションされたすべてのユーザーの完全なインベントリの送信を許可します。

最適化されたインベントリのサーバーへの送信

レジストリ設定を次のように作成または変更します。

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

OnlySendInvChanges（REG_DWORD）＝1

エントリがない場合は、最適化されたインベントリがサーバーに送信されます。

完全なインベントリのサーバーへの送信

レジストリ設定を次のように作成または変更します。

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

OnlySendInvChanges（REG_DWORD）＝0

エントリがない場合は、最適化されたインベントリがサーバーに送信されます。

アクティベーションされたすべてのユーザーの完全なインベントリの送信

レジストリ設定を次のように作成または変更します。

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

RefreshInventory（REG_DWORD）＝1

このエントリは、処理されるとすぐにレジストリから削除されます。値は保管庫に保存され、インベントリのアップロード前にコンピュータがリブートされた場合でも、インベントリのアップロードを次に正常に実行するときに Shield でこの要求が維持されます。

このエントリは OnlySendInvChanges レジストリ値よりも優先されます。

ドメイン以外のアクティベーション

ドメイン以外のアクティベーションの有効化は、広範な結果を伴う高度な構成です。カスタマサポートに問い合わせて特定の環境のニーズについて相談し、この機能を有効にするための指示を受けてください。

6

Kerberos 認証／権限のコンポーネントの構成

このセクションでは、Kerberos 認証／権限で使用するコンポーネントの設定方法について説明します。

Kerberos 認証／権限のコンポーネントの構成

注： Kerberos 認証／権限を使用する場合は、Key Server コンポーネントを含んでいるサーバーを、その影響を受けるドメインに含ませる必要があります。

Key Server は、ソケット上で接続されるクライアントをリスンするサービスです。クライアントが接続されたら、Kerberos API を使用して、セキュア接続のネゴシエーション、認証、暗号化が行われます。セキュア接続がネゴシエーションできない場合、クライアントが切断されます。

Key Server は、クライアントを実行しているユーザーがキーにアクセスできるかどうかを知るために Device Server に確認します。このアクセスは、**個別の**ドメインを経由したリモート管理コンソール上で許可されます。

Windows サービスの手順

1. Windows の［サービス］パネル（［スタート］>［ファイル名を指定して実行］>［services.msc］>［OK］）に移動します。
2. ［Dell Key Server］を右クリックして、［**プロパティ**］を選択します。
3. ［**ログオン**］タブに移動して、［**アカウント:**］オプションボタンを選択します。
4. ［**アカウント:**］フィールドで、希望するドメインユーザーを追加します。このドメインユーザーは、少なくとも Key Server フォルダのローカル管理権限を持つ必要があります。つまり、Key Server の config ファイル、log.txt ファイルへの書き込みができる必要があります。
5. ［OK］をクリックします。
6. サービスを再起動します。後で操作できるように、Windows の［サービス］パネルを開いたままにします。
7. <Key Server インストールディレクトリ > log.txt に移動して、サービスが正しく開始していることを確認します。

Key Server の構成ファイルの手順

1. <Key Server インストールディレクトリ > に移動します。
2. テキストエディタで Credant.KeyServer.exe.config を開きます。
3. <add key="user" value="superadmin" /> に移動して、"superadmin" の値を、適切なユーザーの名前に変更します。"superadmin" のままとすることもできます。

   "superadmin" の形式は、サーバーを認証できる任意の方法に指定できます。SAM アカウント名、UPN、またはドメイン\ユーザー名は容認できます。アクティブディレクトリに対する権限のための、**そのユーザーアカウントに検証が必要であるため、サーバーを認証できるすべての方法が容認できます。**

   例えば、マルチドメイン環境では、"jdoe" などの SAM アカウント名のみを入力すると失敗する可能性があります。その理由は、サーバーが "jdoe" を検索できないため、"jdoe" を認証できないからです。マルチドメイン環境では、ドメイン\ユーザー名の形式が容認できますが、UPN が推奨されます。

   単一ドメイン環境では、SAM アカウント名が容認できます。

4 <add key="epw" value="<encrypted value of the password>" /> に移動して、"epw" を "password" に変更します。"<encrypted value of the password>" を、手順 3 で設定したユーザーのパスワードに変更します。このパスワードは、サーバーを再起動すると再暗号化されます。

手順 3 で "superadmin" を使用して、superadmin パスワードが "changeit" でない場合は、ここで変更します。

5 変更内容を保存して、ファイルを閉じます。

サンプル構成ファイル：

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [サーバーがリスンする TCP ポート。デフォルトは 8050 で、必要に応じて変更する。]
        <add key="maxConnections" value="2000" /> [サーバーに許可されるアクティブなソケット接続数。]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [Device Server の URL。Enterprise Server が v7.7 以降の場合の形式：https://keyserver.domain.com:8443/xapi/ -- Enterprise Server が v7.7 より前の場合の形式：https://keyserver.domain.com:8081/xapi（末尾にスラッシュは指定しません）]
        <add key="verifyCertificate" value="false" /> [暗号を検証する場合は true に設定し、検証しない場合または自己署名暗号化を使用する場合は false に設定]
        <add key="user" value="superadmin" /> [Device Server と通信するために使用されるユーザー名。このユーザーはリモート管理コンソールで選択したフォレンジック管理者の種類を持つ必要があります。"superadmin" の形式は、サーバーを認証できる任意の方法に指定できます。SAM アカウント名、UPN、またはドメイン\ユーザー名は容認できます。アクティブディレクトリに対する権限のための、そのユーザーアカウントに検証が必要であるため、サーバーを認証できるすべての方法が容認できます。例えば、マルチドメイン環境では、"jdoe" などの SAM アカウント名のみを入力すると失敗する可能性があります。その理由は、サーバーが "jdoe" を検索できないため、"jdoe" を認証できないからです。マルチドメイン環境では、ドメイン\ユーザー名の形式が容認できますが、UPN が推奨されます。単一ドメイン環境では、SAM アカウント名が容認できます。]
        <add key="cacheExpiration" value="30" /> [キーを要求することができるユーザーをサービスが確認する必要がある頻度（秒単位）。このサービスは、キャッシュを維持して、キャッシュがどれほど古いかを追跡します。キャッシュがこの値（秒単位）より古くなると、サービスは新しいリストを取得します。ユーザーが接続されると、Key Server は権限のあるユーザーを Device Server からダウンロードする必要があります。ユーザーのキャッシュがない場合、または最後の「x」秒でリストがダウンロードされなかった場合、再度ダウンロードされます。ポーリングはありませんが、この値によって、リストが必要に応じて更新される前に、リストをどのようなステートにするかが構成されます。]
        <add key="epw" value="encrypted value of the password" /> [Device Server と通信するために使用されるパスワード。superadmin パスワードが変更された場合、ここで変更する必要があります。]
    </appSettings>
</configuration>
```

Windows サービスの手順

1 Windows の［サービス］パネルに戻ります。

2 Dell Key Server Service を再起動します。

3 <Key Server インストールディレクトリ > log.txt に移動して、サービスが正しく開始していることを確認します。

4 Windows の［サービス］パネルを閉じます。

リモート管理コンソールの手順

1. 必要な場合は、リモート管理コンソールにログオンします。
2. ［**ドメイン**］をクリックして、［**詳細**］アイコンをクリックします。
3. ［**Key Server**］をクリックします。
4. Key Server アカウントリストに、管理活動を実行するユーザーを追加します。この形式はドメイン\ユーザー名です。［**アカウントの追加**］をクリックします。
5. 左のメニューで、［**ユーザー**］をクリックします。検索ボックスで、手順 4 で追加したユーザー名を検索します。［**検索**］をクリックします。
6. 正しいユーザーが検索されたら、［**詳細**］アイコンをクリックします。
7. ［**フォレンジック管理**］を選択します。［**更新**］をクリックします。

これで、コンポーネントが Kerberos 認証/権限に設定されました。

7

フォレンジック管理者ロールの割り当て

フォレンジック権限はデフォルトで、バックエンドサーバーでは有効、フロントエンドサーバーでは無効になっています。この設定は、Device Server および Security Server のインストール時に適宜実行されます。

リモート管理コンソールの手順

1 必要な場合は、リモート管理コンソールにログオンします。

2 左のペインで、[**管理**] > [**ユーザー**] をクリックします。

3 [**ユーザーの検索**] ページで、フォレンジック管理者ロールを付与するユーザーの名前を入力して、[**検索**] をクリックします。このユーザーの資格情報は、フォレンジックモードで CMGAd、CMGAu、CMGAlu ユーティリティ、および Decryption Agent が実行されているときに提供されます。

4 [**ユーザーの検索結果**] ページで、[**詳細**] アイコンをクリックします。

5 [**<Username> のユーザー詳細**] ページで、[**管理者**] を選択します。

6 [ユーザー] 列で、[**フォレンジック管理者**] をオンにして、[**更新**] をクリックします。

現在、フォレンジック管理者ロールが設定されています。

フォレンジック認証の無効化

1 バックエンドサーバーで、**<Security Server インストールディレクトリ >\webapps\xapi\WEB-INF\context.properties** に移動して以下のプロパティ：

service.forensic.enable=true

を、次のように変更します

service.forensic.enable=false

2 Security Server Service を**起動**します。

3 **<Device Server インストールディレクトリ >\webapps\ROOT\WEB-INF\web.xml** に移動して。次を変更します。

<init-param>

<param-name>forensic</param-name>

<param-value>**@FORENSIC_DISABLE@**</param-value>

</init-param>

4 Device Server Service を**再起動**します。

5 ベストプラクティスとして、ロール権限をアクティブに使用していないユーザーのフォレンジック管理者ロールを削除します。

8

Cron 表現

このセクションでは、Cron 表現の形式および特殊文字の使用方法について説明します。

Cron 表現入門

Cron は長期にわたって普及してきた UNIX ツールであるため、そのスケジューリング機能は高性能であり、実績があります。CronTrigger クラスは、Cron のスケジューリング機能に基づいています。

CronTrigger は Cron 表現を使用します。これにより、毎週月曜日から金曜日の午前 8 時、または毎月の最終金曜日の午前 1 時 30 分のような始動スケジュールを作成できます。

Cron 表現は高性能ですが、わかりにくいことがあります。このドキュメントの目的は、Cron 表現を作成する場合のいくつかの不明点を取り上げ、外部へ支援を求める前に使用できるリソースを提供することです。

Cron 表現の形式

Cron 表現は、空白で区切られた 6 つの必須フィールドと 1 つの任意フィールドから成ります。各フィールドには、そのフィールドに許可された特殊文字のさまざまな組み合わせに加えて、許可された値を含ませることができます。

Cron 表現は、「* * * * ? *」のように単純にできます。

または、「0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010」のように複雑にすることもできます。

各フィールドの説明を次に示します。

フィールド名	必須かどうか	使用可能な値	使用可能な特殊文字
Minutes	はい	0 ～ 59	, - * /
Hours	はい	0 ～ 23	, - * /
Day of month	はい	1 ～ 31	, - * ? / L W C
Month	はい	1 ～ 12 または JAN ～ DEC	, - * /
Day of week	はい	1 ～ 7 または SUN ～ SAT	, - * ? / L C #
Year	いいえ	空、1970 ～ 2099	, - * /

特殊文字

- 文字「*」は、すべての値を指定するために使用されます。例えば、フィールドの「*」は、すべての秒を意味します。
- 文字「?」（不特定の値）は、文字を使用できる 2 つのフィールドの一方に何かを指定して、もう一方には指定しない場合に便利です。例えば、特定の日（10 日）に始動をトリガーするときに、その日が何曜日でも構わない場合は、day-of-month フィールドに「10」を使用して、day-of-week フィールドに「?」を使用します。
- 文字「-」は、範囲を指定するために使用されます。例えば、hour フィールドの「10-12」は、10 時間、11 時間、および 12 時間を意味します。
- 文字「,」は、追加の値を指定するために使用されます。例えば、day-of-week フィールドの「MON,WED,FRI」は、月曜日、水曜日、および金曜日を意味します。

- 文字「/」は、増分を指定するために使用されます。

  seconds フィールドの「0/15」は、0 秒、15 秒、30 秒、および 45 秒を意味します。

  seconds フィールドの「5/15」は、5 秒、20 秒、35 秒、および 50 秒を意味します。

  「/」の前に「*」を指定すると、開始する値として 0 を指定した場合と同等となります。

  day-of-month フィールドの「1/3」は、月の初日から開始して 3 日ごとを意味します。

  基本的に、表現の各フィールドにはオンまたはオフにできる数字セットがあります。seconds および minutes の数字の範囲は 0 ～ 59 です。hours は 0 ～ 23 で、days of the month は 0 ～ 31 です。months は 1 ～ 12 です。文字「/」は、所定のセットの「n 番目」ごとの値だけをオンにします。したがって、month フィールドの「7/6」は 7 の月だけをオンにし、6 ヵ月ごとの月を意味しません。

- 文字「L」は、day-of-month フィールドおよび day-of-week フィールドに使用できます。この文字は最後を意味しますが、2 つの各フィールドの意味は異なります。

  day-of-month フィールドの値「L」は月の最終日を意味します。1 月は 31 日、閏年でない 2 月の場合は 28 日となります。

  day-of-week フィールドで単独で使用される場合は、7 または土曜を意味します。

  day-of-week フィールドで別の値の後に使用される場合は、月の最終 xxx 曜日を意味します。例えば、「6L」は月の最終金曜日を意味します。「L」オプションを使用する場合は結果がわかりにくいため、リストまたは値の範囲を指定しないことが重要です。

- 文字「W」は、day-of-month フィールドに使用できます。この文字は、所定の日に最も近い平日（月曜日～金曜日）を指定するために使用されます。例えば、day-of-month フィールドの値として「15W」を指定した場合、月の 15 日に最も近い平日を意味します。したがって、15 日が土曜日の場合は、14 日の金曜日にトリガーがかけられます。15 日が日曜日の場合は、16 日の月曜日にトリガーがかけられます。15 日が火曜日の場合は、15 日の火曜日にトリガーがかけられます。しかし、day-of-month の値として 1W を指定し、かつ、1 日が土曜日の場合は、1 ヵ月の日数の境界を飛び超えられないため、3 日の月曜日にトリガーがかけられます。文字「W」は、day-of-month が範囲や複数日のリストではなく、単独の日である場合のみ指定できます。

  文字「L」と「W」はまた、day-of-month 表現で組み合わせて「LW」としても使用でき、月の最終平日を意味します。

- 文字「#」は、day-of-week フィールドに使用できます。この文字は、月の「n 番目」の xxx 曜日を指定するために使用されます。例えば、day-of-week フィールドの値「6#3」は、月の 3 番目の金曜日（6 = 金曜日、#3 = 月の 3 番目の金曜日）を意味します。

  その他の例：
  2#1 = 月の最初の月曜日
  4#5 = 月の 5 番目の水曜日。

  #5 を指定しても、月に 5 番目の所定の曜日がない場合は、その月にトリガーがかけられないことに注意してください。

- 文字「C」はカレンダーに使用できます。この文字を使用すると、関連付けられているカレンダーがある場合、そのカレンダーに対して値が計算されます。関連付けられているカレンダーがない場合は、すべて込みのカレンダーを持つことと同じとなります。day-of-month フィールドの値「5C」は、カレンダーに含まれる 5 日以降の最初の日を意味します。day-of-week フィールドの値「1C」は、カレンダーに含まれる日曜日以降の最初の日を意味します。

注： day-of-week と day-of-month の両方に値を指定することは完全にはサポートされていません。いずれかのフィールドで、文字「?」を使用してください。文字「C」で記述される機能は、完全にはサポートされていません。有効な文字、および月と曜日の名前では、大文字と小文字が区別されません。MON は mon と同じです。day-of-week フィールドおよび day-of-month フィールドに影響する「?」と「*」の使用には、細心の注意が必要です。
始動時間を夜中の 12 時と午前 1 時の間に設定する場合は注意してください。サマータイムは、時間を遅らせるか進ませるかによって、スキップまたは繰り返しが発生する可能性があります。

例

表現	意味
0 0 12 * * ?	毎日、午後 12 時（正午）に始動
0 15 10 ? * *	毎日、午前 10 時 15 分に始動
0 15 10 * * ?	毎日、午前 10 時 15 分に始動
0 15 10 * * ? *	毎日、午前 10 時 15 分に始動
0 15 10 * * ? 2005	2005 年の間、毎日、午前 10 時 15 分に始動
0 * 14 * * ?	毎日、午後 2 時から午後 2 時 59 分まで 1 分ごとに始動
0 0/5 14 * * ?	毎日、午後 2 時から午後 2 時 55 分まで 5 分ごとに始動
0 0/5 14,18 * * ?	毎日、午後 2 時から午後 2 時 55 分まで 5 分ごとに始動、かつ、午後 6 時から午後 6 時 55 分まで 5 分ごとに始動
0 0-5 14 * * ?	毎日、午後 2 時から午後 2 時 5 分まで 1 分ごとに始動
0 10,44 14 ? 3 WED	3 月の毎水曜日の午後 2 時 10 分および午後 2 時 44 分に始動
0 15 10 ? * MON-FRI	毎月曜日、毎火曜日、毎水曜日、毎木曜日、および毎金曜日の午前 10 時 15 分に始動
0 15 10 15 * ?	毎月 15 日の午前 10 時 15 分に始動
0 15 10 L * ?	毎月の最終日の午前 10 時 15 分に始動
0 15 10 ? * 6L	毎月の最終金曜日の午前 10 時 15 分に始動
0 15 10 ? * 6L	毎月の最終金曜日の午前 10 時 15 分に始動
0 15 10 ? * 6L 2002-2005	2002 年、2003 年、2004 年、および 2005 年の間、毎月、毎最終金曜日の午前 10 時 15 分に始動
0 15 10 ? * 6#3	毎月の第 3 金曜日の午前 10 時 15 分に始動
0 0 12 1/5 * ?	毎月の初日から 5 日ごとの午後 12 時（正午）に始動
0 11 11 11 11 ?	毎年 11 月 11 日の午前 11 時 11 分に始動

9

Keytool を使用した自己署名証明書の作成と証明書署名要求の生成

注：このセクションでは、Java ベースのコンポーネントの自己署名証明書を作成する手順について詳しく説明します。このプロセスは、.NET ベースのコンポーネントの自己署名証明書を作成する目的には使用できません。

本稼働ではない環境**のみ**で自己署名証明書を作成することを推奨します。

組織で SSL サーバー証明書が必要な場合、または他の理由で証明書を作成する必要がある場合は、このセクションで、Keytool を使用した Java キーストアの作成プロセスが説明されています。

Keytool は、証明書署名要求（CSR; Certificate Signing Request）の形式で、VeriSign® や Entrust® などの証明機関（CA; Certificate Authority）に渡される秘密鍵を作成します。その後、CA はこの CSR に基づいて署名したサーバー証明書を作成します。サーバー証明書は、署名機関証明書とともにファイルにダウンロードされます。その後、証明書は cacerts ファイルにインポートされます。

新しい鍵ペアと自己署名証明書の生成

1. Compliance Reporter、Console Web Services、Device Server、または Gatekeeper Web Services の **conf** ディレクトリに移動します。
2. デフォルトの証明書データベースをバックアップします。

   ［**スタート**］> ［**ファイル名を指定して実行**］をクリックして、「**move cacerts cacerts.old**」と入力します。
3. Keytool をシステムパスに追加します。コマンドプロンプトで次のコマンドを入力します。

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. 証明書を生成するため、次のようにして Keytool を実行します。

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Keytool プロンプトが表示されたら次の情報を入力します。

注：構成ファイルは、編集する前にバックアップしてください。指定されたパラメータのみを変更してください。これらのファイル内のその他のデータ（タグを含む）を変更すると、システムの破損や障害が発生するおそれがあります。Dell は、これらのファイルの許可されていない変更に起因する問題が、Enterprise Server の再インストールなしで解決できることを保証できません。

- **キーストアのパスワード：**パスワードを入力し（<>;&" ' の文字はサポートされていません）、次のコンポーネント **conf** ファイルの変数を同じ値に設定します。

  <Compliance Reporter インストールディレクトリ >\conf\eserver.properties の eserver.keystore.password = の値を設定します。

  <Console Web Services インストールディレクトリ >\conf\eserver.properties の eserver.keystore.password = の値を設定します。

  <Device Server インストールディレクトリ >\conf\eserver.properties の eserver.keystore.password = の値を設定します。
- **姓名：**現在作業中のコンポーネントがインストールされているサーバーの完全修飾名を入力します。この完全修飾名には、ホスト名とドメイン名を含めます（例：server.dell.com）。

- **組織単位：**適切な値を入力します（例：Security）。
- **組織：**適切な値を入力します（例：Dell）。
- **市区町村：**適切な値を入力します（例：Austin）。
- **都道府県：**省略形でない都道府県の名前を入力します（例：Texas）。
- 2 文字の国コード：

  米国 = US

  カナダ = CA

  スイス = CH

  ドイツ = DE

  スペイン = ES

  フランス = FR

  英国 = GB

  アイルランド = IE

  イタリア = IT

  オランダ = NL
- ユーティリティによって、情報が正しいことを確認するように求められます。正しければ「yes」と入力します。正しくなければ「no」と入力します。Keytool は以前に入力された各値を表示します。［Enter］をクリックして値を確定するか、値を変更して［Enter］をクリックします。
- **別名のキーパスワード：**ここに別のパスワードを入力しなかった場合は、このパスワードはデフォルトであるキーストアのパスワードになります。

証明機関への署名付き証明書の要求

以下の手順を使って、「新しい鍵ペアと自己署名証明書の生成」で作成した自己署名証明書の証明書署名要求（CSR）を作成します。

1 以前使用した値と同じ値を <certificate-alias> に入力します。

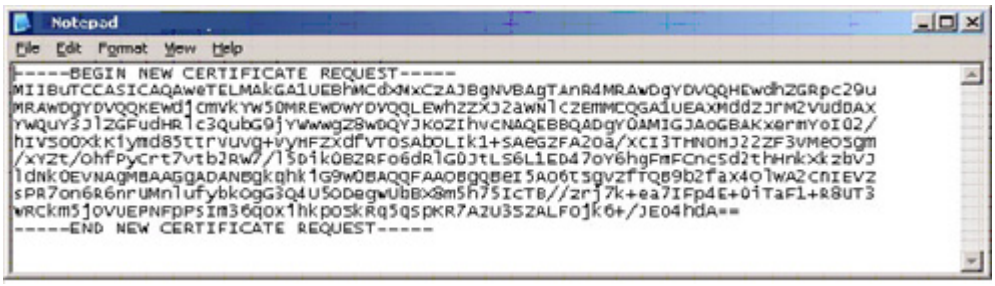
```
keytool -certreq -sigalg MD5withRSA -alias <certificate-alias> -keystore
.\cacerts -file <csr-filename>
```

例：

```
keytool -certreq -sigalg MD5withRSA -alias dell -keystore .\cacerts -file
credant.csr
```

証明機関での証明書の作成時に使用される BEGIN/END ペアが .csr ファイルに格納されます。

図 9-1. .CSR ファイルの例



2 証明機関から SSL サーバー証明書を取得するための組織のプロセスに従います。署名用に <csr-filename> の内容を送信します。

注： 有効な証明書を要求する方法は数通りあります。その例は、「証明書の要求方法の例」に示されています。

3 署名付き証明書を受信したら、ファイルに保存します。

4 ベストプラクティスとして、インポートプロセスでエラーが発生した場合に備え、この証明書をバックアップします。このバックアップにより、プロセスをやり直す必要が生じるのを防ぐことができます。

ルート証明書のインポート

注： ルート証明書の証明機関が Verisign（Verisign Test ではない）の場合は、この手順をスキップして次の手順に進み、署名付き証明書をインポートしてください。

証明機関のルート証明書により、署名付き証明書を認証します。

1 次のいずれか 1 つを実行します。

- 証明機関のルート証明書をダウンロードして、ファイルに保存します。
- エンタープライズディレクトリサーバーのルート証明書を取得します。

2 次のいずれか 1 つを実行します。

- Compliance Reporter、Console Web Services、Device Server、または Legacy Gatekeeper Connector の SSL を有効にする場合は、コンポーネント **conf** ディレクトリに変更します。
- サーバーとエンタープライズディレクトリサーバー間の SSL を有効にする場合は、**<Dell インストールディレクトリ >\Java Runtimes\jre1.x.x_xx\lib\security** に変更します（JRE cacerts のデフォルトのパスワードは **changeit** です）。

3 次のようにして Keytool を実行し、ルート証明書をインストールします。

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file
<ca-cert-filename>
```

例：

```
keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer
```

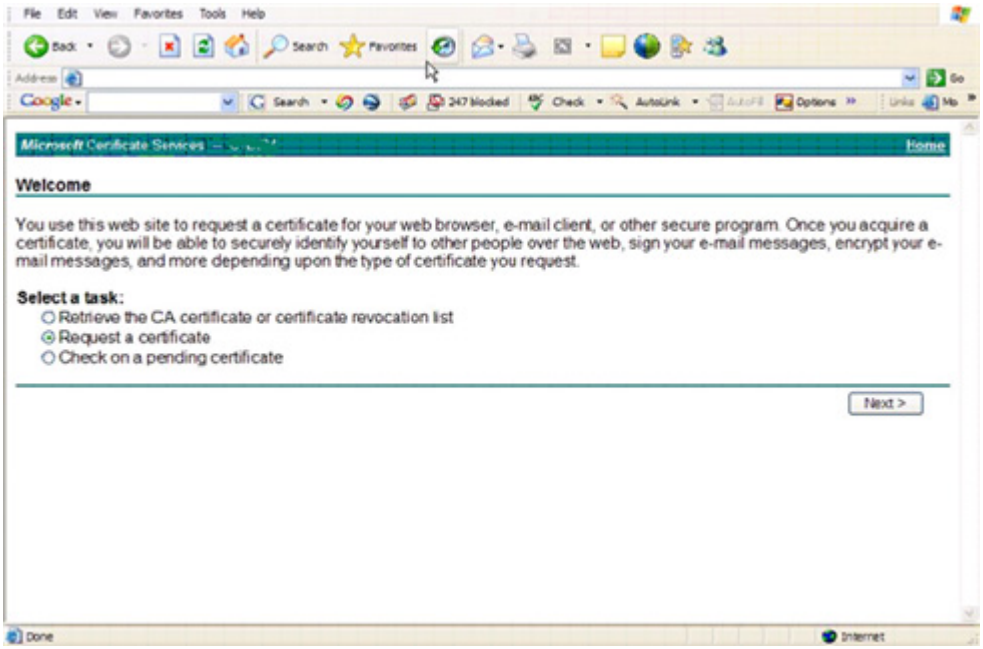
証明書の要求方法の例

証明書の要求方法の 1 つの例は、Web ブラウザを使用して、組織によって内部的に設定されている Microsoft CA Server にアクセスする方法です。

1 Microsoft CA Server に移動します。IP アドレスは、組織によって提供されます。

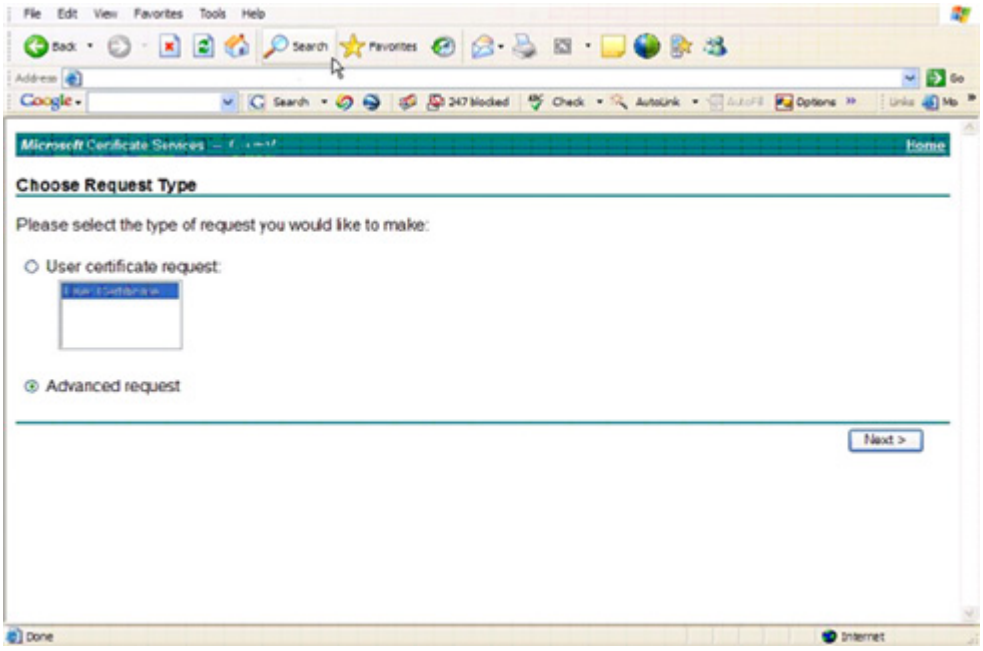
2 ［Request a certificate］を選択し、［Next >］をクリックします。

図 9-2. Microsoft Certificate Services



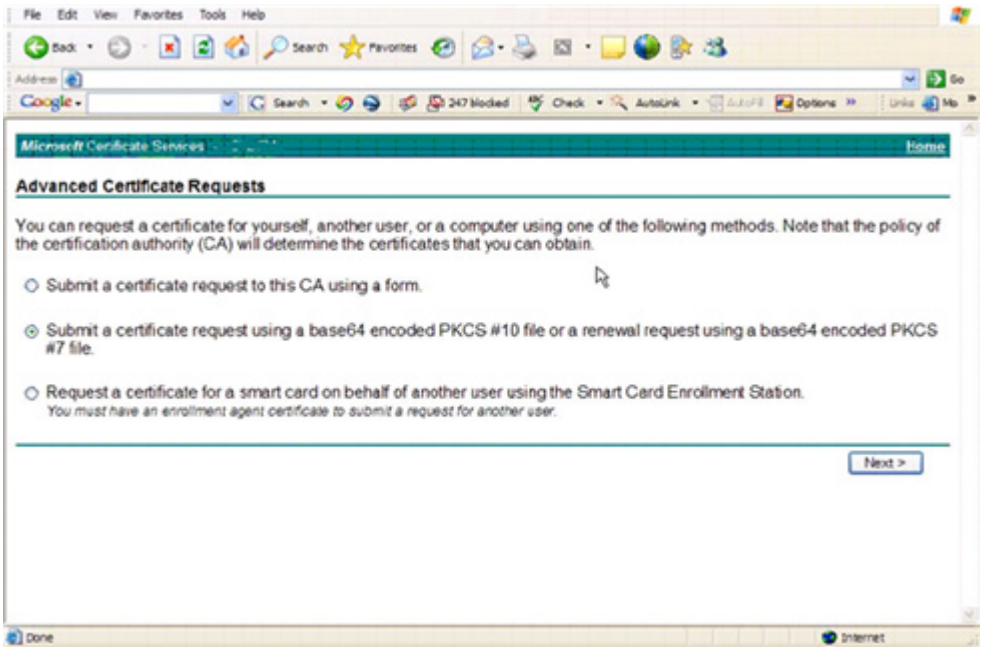
3 ［Advanced Request］を選択し、［Next >］をクリックします。

図 9-3. 要求タイプの選択



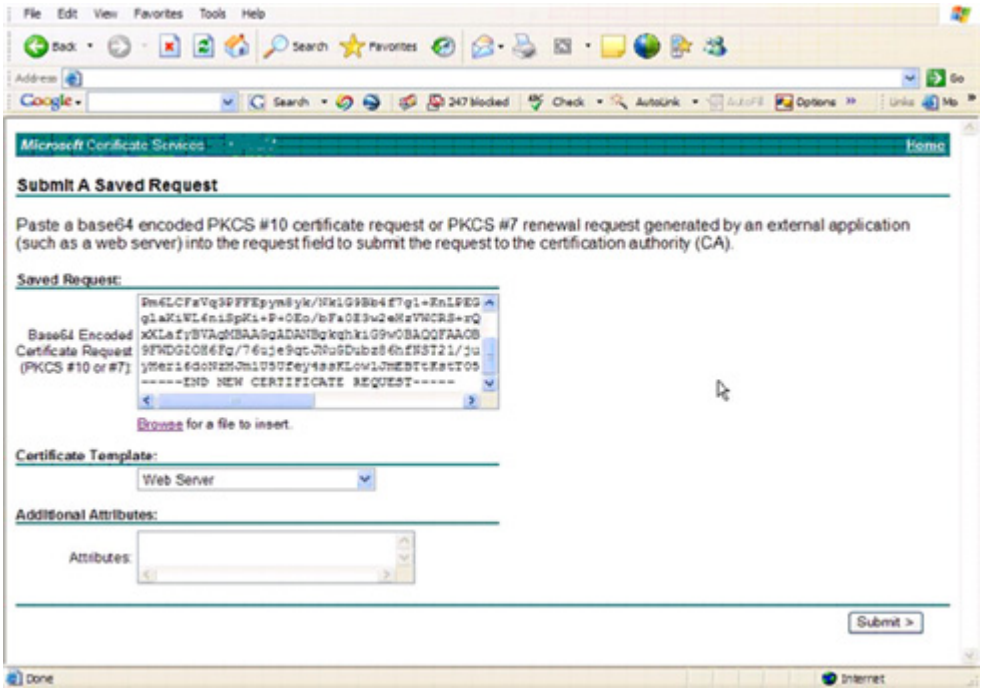
4 base64 エンコード PKCS #10 ファイルを使用して証明書要求を送信するためのオプションを選択して、[Next >] をクリックします。

図 9-4. 高度な証明書要求



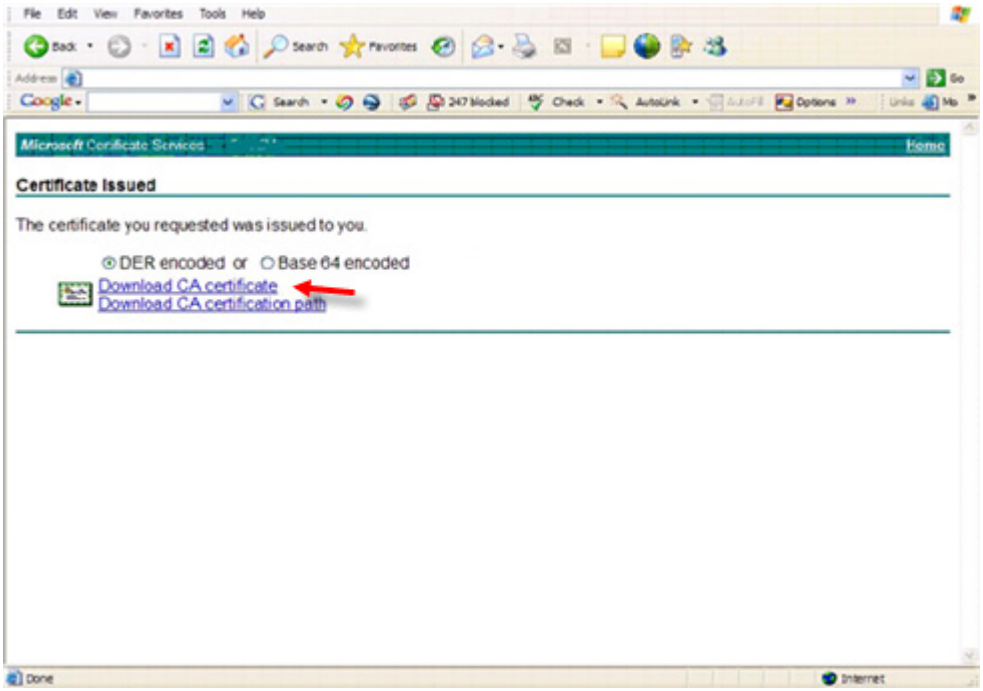
5 CSR 要求の内容をテキストボックスに貼り付けます。Web Server の証明書テンプレートを選択して、[Submit >] をクリックします。

図 9-5. 保存された要求の送信



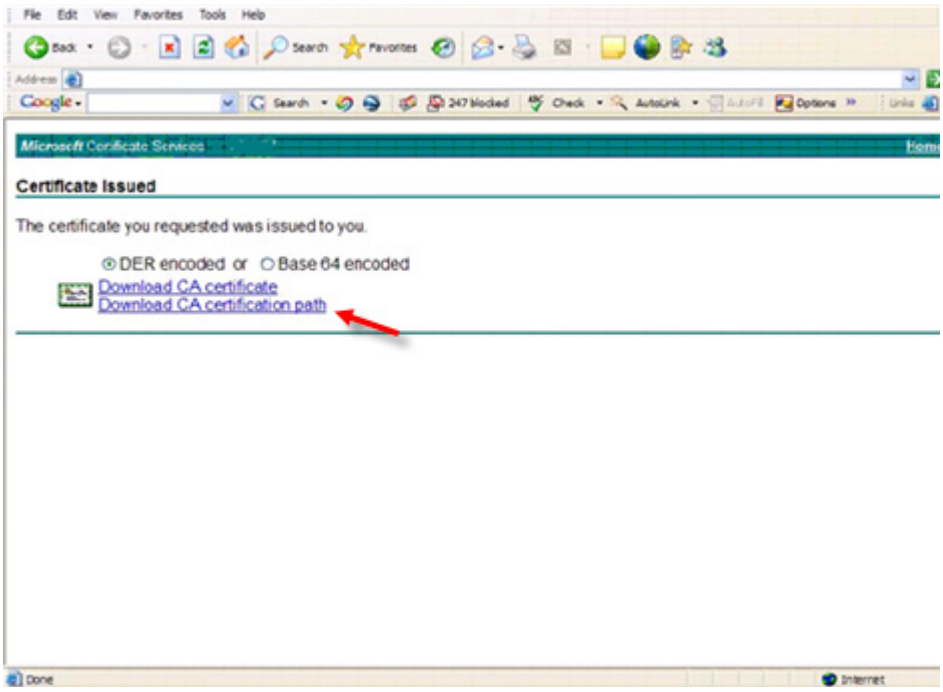
6 証明書を保存します。[DER encoded] を選択し、[Download CA certificate] をクリックします。

図 9-6. CA 証明書のダウンロード



7 証明書を保存します。[DER encoded] を選択し、[Download CA certification path] をクリックします。

図 9-7. CA 証明書のダウンロードパス



8 変換された署名機関証明書をインポートします。DOS ウィンドウに戻ります。次を入力します。

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 署名機関証明書がインポートされたので、次にサーバー証明書をインポートできます（信頼チェーンを確立できます）。次を入力します。

```
keytool -import -alias dell -file <csr-filename> -keystore cacerts
```

自己署名証明書の別名を使用して、CSR 要求とサーバー証明書をペアにします。

10 cacerts ファイルのリストは、サーバー証明書の**証明書チェーン**の長さが 2 であることを示しています。これは、証明書が自己署名されていないことを示しています。次を入力します。

```
keytool -list -v -keystore cacerts
```

チェーン内の 2 番目の証明書の証明書フィンガープリントは、インポートされた署名機関証明書である点に注意してください（リストのサーバー証明書の下にもリストされます）。

サーバー証明書は、署名機関証明書とともに正常にインポートされました。


0 XXXXXA0 X