Dell Data Protection

구성 가이드

2014-02

목차

1

Compatibility Server 구성

이 장에서는 Compatibility Server를 사용자 환경에 맞게 조정하기 위해 변경할 수 있는 매개 변수에 대해 설명합니다. 편집하기 전 항상 구성 파일을 백업해 두십시오.

이러한 파일에 나와 있는 매개 변수만 변경할 수 있습니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Compatibility Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

server_config.xml

다음 매개 변수 중 일부는 **<Compatibility Server 설치 디렉토리>\conf\server_config.xml**에서 변경할 수 있습니다. 변경하면 안 되는 매개 변수는 변경할 수 없다는 내용이 표시되어 있습니다. Compatibility Server가 실행 중일 때에는 Compatibility Server Service를 중단하고 server_config.xml 파일을 편집한 다음 Compatibility Server Service를 다시 시작해야 이 파일에 대한 변경 사항이 적용됩니다.

server_config.xml

매개 변수	기본값	설명
secrets.location	$dell.home$/conf/secretKeyStore	secretkeystore의 기본 위치. 이 파일을 기본 위치에서 변경할 경우 이 매개 변수를 업데이트하십시오.
archive.location	$dell.home$/conf/archive	아카이브의 기본 위치. 이 파일을 기본 위치에서 변경할 경우 이 매개 변수를 업데이트하십시오.
domain.qualified.authentication	true	Server에 대한 모든 요청에 정규화된 사용자 로그인 이름이 필요한지 여부를 나타냅니다. 이 값이 변경되는 경우 새 값을 적용하기 전에 Device Server를 다시 시작해야 합니다.
directory.max.search.size	1000	디렉토리 *찾기*에 대한 제한으로서 이 제한을 초과하면 예외가 발생합니다.
directory.server.search.timeout.seconds	60	LDAP 검색에 대한 서버 제한 시간(초)
directory.client.search.timeout	60	LDAP 검색에 대한 클라이언트 제한 시간(초)

server_config.xml		
매개 변수	기본값	설명
rmi.recovery.host		다중 서버 EMS 복구 사용: <!-- - 주석 처리를 제거하고 정규화된 도메인 이름에 대한 호스트 이름을 체인 복구로 변경 <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	모든 Policy Proxy가 기본적으로 속한 그룹의 기본 이름으로서 이 이름은 여기 또는 Device Server context.properties에서 변경할 수 있습니다. 여기에서 그룹 이름을 변경할 경우 다음 작업을 계획한다면 Device Server에서도 변경해야 합니다. • Windows 장치를 Shield로 보호 • CREDActivate 사용 모든 정책 프록시를 단일 그룹에 포함하는 것이 좋습니다.
rsa.securid.enabled	false	GINA를 대체하기 위해 Microsoft Windows 버전 6용 RSA SecurID를 사용할 경우 이 매개 변수를 true로 설정한 다음 Compatibility Server Service를 중지했다 다시 시작하십시오. RSA GINA 대체 환경에서 Shield 사용자를 등록하면 LDAP 인증 대신 RSA 인증이 사용됩니다.
inv.queue.task.worker.size	10	인벤토리 대기열을 처리하는 스레드의 수
inv.queue.task.timeout.seconds	900	시간 초과가 발생하기 전 시간(초)
inv.queue.task.retry.count	3	취소하기 전 Server에서 인벤토리 처리를 시도하는 횟수
report.retry.max	120	최대 재시도 횟수
report.retry.wait.millis	250	재시도 전 대기하는 시간(밀리초)

server_config.xml		
매개 변수	기본값	설명
triage.execute.time	0 0 0/6 * *	심사는 Server가 이미 알고 있는 사용자와 그룹을 조정하는 프로세스입니다. 기본 설정은 0 0 0/6 * * ?입니다. 즉, 자정부터 시작하여 6시간마다(자정, 오전 6시, 정오, 오후 6시...) 심사합니다.
gatekeeper.service.max.sessions	5	정책 프록시 세션의 최대 수
gatekeeper.service.max.session.timeout	5	정책 프록시 세션의 최대 수에 설정된 제한 시간
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	그룹 또는 사용자 관리 역할을 업데이트하는 데 필요한 권한
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	그룹 또는 사용자 관리 역할을 업데이트하는 데 필요한 권한
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	로그 세션을 검색하는 데 필요한 권한
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	로그를 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	로그 열 목록을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	로그 범주 목록을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	로그 우선 순위 목록을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	고유 ID 이름을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	시스템에서 관리자 목록을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	슈퍼 관리자 암호를 설정하는 데 필요한 역할
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	슈퍼 관리자 암호를 재설정하는 데 필요한 역할
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin,SecAdmin	도메인을 추가하는 데 필요한 역할
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin,SecAdmin	도메인을 제거하는 데 필요한 역할
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin,SecAdmin	도메인을 업데이트하는 데 필요한 역할
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin,SecAdmin	그룹을 추가하는 데 필요한 역할
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin,SecAdmin	그룹을 제거하는 데 필요한 역할

server_config.xml		
매개 변수	기본값	설명
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin,SecAdmin	LDAP 그룹을 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin,SecAdmin	LDAP 사용자를 검색하는 데 필요한 역할
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	사용자를 추가하는 데 필요한 역할
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	엔터프라이즈 라이센스를 추가하는 데 필요한 역할
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	엔터프라이즈 라이센스를 보는 데 필요한 역할
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	장치를 복구하는 데 필요한 역할
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	사용자를 일시 중단하는 데 필요한 역할
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	프록시로 장치를 등록하는 데 필요한 역할
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	장치를 프록시로 수동 복구하는 데 필요한 역할
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Gatekeeper 리소스 파일을 검색하는 데 필요한 역할
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Gatekeeper 리소스 파일을 승인하는 데 필요한 역할
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Gatekeeper 구성을 승인하는 데 필요한 역할
policy.arbiter.security.mode	most-restrictive	이 속성은 정책에 여러 상위 노드가 있을 경우 보안에 중점을 두는 정책 요소에 대한 정책 매핑 알고리즘의 작동 방식을 제어합니다. 값: Least-restrictive - 상위 노드에서 가장 제한 수준이 낮은 요소 값이 사용됩니다. Most-restrictive - 모든 상위 노드에서 가장 제한 수준이 높은 요소 값이 사용됩니다.
policy.set.synchronization.sync-unmodified	true	이 플래그는 수정된 플래그를 true로 설정하지 않고 다음 외부 동기화에서 모든 정책 요소를 추가 또는 다시 매핑해야 함을 나타냅니다. 이 플래그는 모든 동기화 이후 false로 전환되므로 보안 관리자가 수정하지 않고 추가하려면 재설정해야 합니다. 이 플래그는 고급 옵션입니다.
db.schema.version.major		주 데이터베이스 스키마
db.schema.version.minor		보조 데이터베이스 스키마

server_config.xml		
매개 변수	기본값	설명
db.schema.version.patch		데이터베이스 스키마의 패치 버전
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	데이터베이스 드라이버의 기본 위치. 이 파일을 기본 위치에서 변경할 경우 이 매개 변수를 업데이트하십시오.
dao.db.host		데이터베이스 서버의 호스트 이름. 이 매개 변수는 구성 도구에서 변경합니다.
dao.db.name		데이터베이스 이름. 이 매개 변수는 구성 도구에서 변경합니다.
dao.db.user		데이터베이스에 대한 전체 권한이 있는 사용자 이름. 이 매개 변수는 구성 도구에서 변경합니다.
dao.db.password		데이터베이스에 대한 전체 권한이 있는 사용자 이름의 암호. 이 매개 변수는 구성 도구에서 변경합니다.
dao.db.max.retry.count	10	지정된 소켓 오류가 발생할 경우 Compatibility Server가 SQL Server에 다시 연결을 시도하는 최대 횟수
dao.db.connection.retry.wait.seconds	5	첫 번째 재연결 시도는 즉시 실행됩니다. 두 번째 시도는 지정된 시간(초) 이후에 발생합니다. 세 번째 시도는 지정된 시간(초)의 2배의 시간이 경과한 후 발생하고, 네 번째 시도는 3배의 시간이 경과한 후 발생하고, 그 다음 시도도 같은 방식으로 발생합니다.
dao.connection.pool.max.uses	10000	연결을 중지할 수 있습니다. 0은 중지하지 않음을 의미합니다.
dao.connection.pool.inactive.threshold.seconds	900	연결이 사용되지 않아 종료할 수 있는 시기를 결정하는 데 사용됩니다.
dao.db.driver.socket.errors	0	Compatibility Server는 쉼표로 구분된 이 목록에 해당하는 오류가 발생하는 경우 SQL Server에 재연결을 시도합니다. 0은 Microsoft SQL의 소켓 오류에 대한 오류 코드입니다. 또한 서버 일시 중지 오류에 17142, 서버 종료 오류에 6002를 추가할 수 있습니다.
dao.db.mssql.compatability.level	90	SQL 2005 이상의 값
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	인증 파일 처리기
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	인벤토리 파일 처리기

server_config.xml		
매개 변수	기본값	설명
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	이벤트 파일 처리기
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Gatekeeper 리소스 파일을 기본 위치에서 이동할 경우 이 매개 변수를 업데이트하십시오.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Gatekeeper 리소스 파일을 기본 위치에서 이동할 경우 이 매개 변수를 업데이트하십시오.
rmi.server.registry.host	localhost	호스트 속성은 레지스트리 위치를 확인하기 위해 클라이언트 프로그램에서만 사용합니다. RMI 레지스트리 및 원격 개체를 생성하는 동안에는 사용되지 않습니다. localhost에서 생성됩니다.
rmi.server.registry.port	1099	RMI 레지스트리 포트는 설치 중 구성할 수 있습니다. 이 매개 변수를 사용하여 설치한 후에도 포트를 변경할 수 있습니다. 이 값을 변경하면 Gatekeeper Web Services도 구성해야 합니다.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Server 보고서 인증을 설정하는 데 필요한 역할
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Server 엔티티를 제거하는 데 필요한 역할
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Server 엔티티 가시성을 설정하는 데 필요한 역할
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	장치 세부 정보 페이지를 보는 데 필요한 역할
security.authorization.method.IReportingService.openSession	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Server 세션을 여는 데 필요한 역할
security.authorization.method.IReportingService.getPagedReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	장치 형식 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	운영 체제 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	장치 모델 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	정책 세부 정보 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	워크스테이션 세부 정보 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	암호화 실패 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	암호화 요약 보고서를 보는 데 필요한 역할

server_config.xml		
매개 변수	기본값	설명
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	사용자 세부 정보 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	그룹 세부 정보 보고서를 보는 데 필요한 역할
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	도메인 보고서 목록을 보는 데 필요한 역할
security.authorization.method.IKeyService.getKeys	ForensicAdmin	이 설정은 Forensic 통합 플러그인과 함께 사용합니다. Forensic 도구 통합이 필요할 경우 Dell 지원 부서에 문의하십시오.
accountType.nonActiveDirectory.enabled	false	비도메인 등록 활성화는 고급 구성이며, 다양한 결과가 발생할 수 있습니다. 이 구성을 활성화하기 *전에* 고객 지원 센터에 연락하여 특정 환경 요구 사항에 대해 문의하십시오. 이 값을 변경한 후에는 Compatibility Server Service를 다시 시작하십시오. 이 설정 이외에도, Windows 컴퓨터의 레지스트리 설정을 다음과 같이 생성 또는 수정하십시오. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations= REG_DWORD:1

gkresource.xml

<Compatibility Server 설치 디렉토리>\conf\gkresource.xml에서 매개 변수를 변경할 수 있습니다.

파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다. 그러면 업그레이드할 때 변경 사항이 새 파일로 쉽게 옮겨가도록 할 수 있습니다.

참고: gkresource.xml 파일은 올바른 형식의 XML 파일이어야 합니다. XML에 익숙하지 않을 경우 이 파일을 편집하지 않는 것이 좋습니다. 적절한 경우에는 원시(이스케이프되지 않은) 특수 문자 대신 엔티티 참조를 사용하십시오.

Gatekeeper 리소스 파일에 대한 변경 사항은 시스템 관리자가 승인한 후 적용됩니다.

도메인\사용자 이름 형식 활성화

도메인\사용자 이름 형식을 활성화(또는 비활성화)하려면 다음 문자열을 추가합니다. 파일에 해당 문자열이 없으면 형식이 비활성화됩니다. 값을 0으로 설정하여 비활성화할 수도 있습니다.

1. <Compatibility Server 설치 디렉토리>\conf로 이동합니다.
2. .xml 편집기로 gkresource.xml을 엽니다.
3. 다음 문자열을 추가합니다.
   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. 파일을 저장하고 닫습니다.

run-service.conf

<Compatibility Server 설치 디렉토리>\conf\run-service.conf에서 다음 매개 변수 중 일부를 변경할 수 있습니다. 이러한 매개 변수는 설치 시 자동으로 설정됩니다. Service를 사용자 지정하거나 구성을 변경하려면 다음과 같이 하십시오.

1. Service를 중지합니다.
2. Service를 제거합니다.
3. **run-service.conf** 파일을 편집하고 저장합니다. 파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다.
4. Service를 다시 설치합니다.
5. Service를 시작합니다.

run-service.conf

매개 변수	기본값	설명
JAVA_HOME	Dell\Java Runtime\jreX.x	Java 설치 디렉토리 위치
wrapper.java.additional.5	해당 없음	이 행의 mac 주소는 로컬 이더넷 어댑터의 mac 주소입니다. 서버에 여러 NICS가 있거나 기본 어댑터 이외의 어댑터에 연결하려는 경우 여기에 대시를 포함하지 않은 NIC의 물리적 mac 주소를 입력합니다.
wrapper.ntservice.name	EpmCompatSvr	Service 이름
wrapper.ntservice.displayname	Dell Compatibility Server	Service의 표시 이름
wrapper.ntservice.description	Enterprise Compatibility Server	Service에 대한 설명
wrapper.ntservice.dependency.1		Service 종속성. 필요에 따라 1부터 시작하는 종속성을 추가합니다.
wrapper.ntservice.starttype	AUTO_START	Service를 설치하는 모드: AUTO_START 또는 DEMAND_START
wrapper.ntservice.interactive	false	true로 설정하면 Service가 데스크톱과 상호 작용할 수 있습니다.

2

Core Server 구성

이 장에서는 Core Server를 사용자 환경에 맞게 조정하기 위해 변경할 수 있는 매개 변수에 대해 설명합니다.

이러한 파일에 나와 있는 매개 변수만 변경할 수 있습니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Core Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

정책 중재를 가장 안전에서 가장 취약으로 변경

PolicyService.config

정책 중재를 가장 안전에서 가장 취약으로 변경하려면 이 설정을 수정합니다. **<Core Server 설치 디렉토리>\PolicyService.config**에서 설정을 변경합니다. Core Server가 실행 중인 경우 Service를 중단하고 PolicyService.config 파일을 편집한 다음 Service를 다시 시작해야 이 파일에 대한 변경 사항이 적용됩니다.

파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다. 그러면 업그레이드할 때 변경 사항이 새 PolicyServiceConfig.xml 파일로 쉽게 옮겨가도록 할 수 있습니다.

다음 섹션을 수정합니다.

```
<!-- 웹 서비스 대상 -->
<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" /> [값을 가장 취약으로 설정하려면 이 값을 "0"에서 "1"로 변경]
</object>
```

웹 서비스 비활성화

참고: 이 설정은 고객 지원 센터의 안내 하에서만 변경해야 하는 고급 설정입니다.

Core Server에서 웹 서비스를 비활성화하려면(예: 인벤토리 처리만 수행하는 두 번째 Core Server 설치를 수행한 경우) 다음에서 설정을 변경합니다.

<Core Server 설치 디렉토리>
Credant.Server2.WindowsService.exe.Config

및

<Core Server 설치 디렉토리>\Spring.config

Core Server가 실행 중인 경우 Service를 중지하고 두 파일에서 설정을 편집한 다음 Service를 다시 시작해야 이 파일에 대한 변경 사항이 적용됩니다.

Credant.Server2.WindowsService.exe.Config

다음 섹션을 제거합니다.

```
<!-- 웹 서비스 구성 -->
<system.serviceModel>
    <services configSource="Services.config"/>
    <behaviors configSource="Behaviors.config"/>
    <bindings configSource="Bindings.config"/>
</system.serviceModel>
```

Spring.config

다음을 제거합니다.

AOP Advice, **웹 서비스 대상 정의**, **웹 서비스 호스트 정의** 제목 아래의 모든 <object> </object> 정의를 제거합니다.

라이센스 이메일 알림에 SMTP 서버 사용

Dell Data Protection | Cloud Edition을 사용할 경우 이러한 설정은 서버 구성 도구를 사용하여 자동화됩니다. Dell Data Protection | Cloud Edition 이외의 목적으로 라이센스 이메일 알림용 SMTP 서버를 사용해야 할 경우 이 절차를 사용합니다.

NotificationObjects.config

라이센스 이메일 알림용 SMTP 서버를 구성하려면 **<Core Server 설치 디렉토리>**에 있는 **NotificationObjects.config** 파일을 수정합니다.

다음을 수정합니다.

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [이 값을 변경하지 마십시오]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [이 값을 변경하지 마십시오]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="username"/>
  <property name="Password" value="${SmtpPassword}"/> [이 값을 변경하지 마십시오]
  <property name="Logger" ref="NotificationLogger"/> [이 값을 변경하지 마십시오]
</object>
```

Notification.config

이메일 서버에 인증이 필요할 경우 **<Core Server 설치 디렉토리>**에 있는 **Notification.config** 파일을 수정합니다.

다음을 수정합니다.

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

Compatibility Server의 폴더 위치를 Core Server 구성 파일에 추가

Core Server는 .Net 응용 프로그램이기 때문에 권한으로 인해 레지스트리 정보에 액세스하지 못할 수 있습니다. 문제는 Core Server가 secretkeystore(데이터베이스 암호화 키)를 읽기 위해 Compatibility Server의 레지스트리 구성 정보에 액세스하여 secretkeystore 위치를 확인해야 한다는 점입니다. 레지스트리 권한으로 인해 이 액세스가 차단되면 Core Server가 Console 사용자를 인증할 수 없습니다. 이 설정은 레지스트리 액세스 문제가 발생할 경우 Compatibility Server의 폴더 위치를 Core Server의 구성 파일에 추가합니다.

1. <Core Server 설치 디렉토리>\EntityDataAccessObjects.config를 탐색합니다.
2. 아래에서 **굵은 글꼴** 항목을 변경합니다.

```
<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"/> -->
    이 행을 주석 처리에서 제거하고 Compatibility Server에 대한 정규화된 경로를 설정합니다.
</object>
```

3. 파일을 저장하고 닫습니다.
4. Core Server 및 Compatibility Server Service를 다시 시작합니다.

Core Server가 여러 인증 방법을 시도하도록 허용

Core Server 인증 시도는 허용된 인증 방법에 설정된 정책으로 인해 도메인 컨트롤러에 의해 차단될 수 있습니다. 이를 개선하기 위해 Core Server가 올바른 방법을 찾을 때까지 여러 인증 방법을 시도해 볼 수 있도록 Core Server 구성 파일에 "스위치"를 구현하였습니다.

1. <Core Server 설치 디렉토리>\Spring.config를 탐색합니다.
2. 아래에서 **굵은 글꼴** 항목을 변경합니다.

```
<object id="DomainCache" singleton="true" type="Credant.Authorization.DomainCache.DomainCache,
Credant.Authorization.DomainCache">
  <!-- 이 로거의 변경 여부 -->
  <property name="Logger" ref="DataAccessLogger" />
  <property name="DomainDataAccess"       ref="DomainDataAccess" />
  <property name="RefreshFrequency" value="300" />
  <property name="TryAllAuthTypes" value="false" />      이 기능을 사용하려면 이 값을 "true"로 변경합니다.
    <!-- 도메인별 AuthType을 변경하는 데 사용: 키는 도메인의 CID이며 값은
    System.DirectoryServices.AuthenticationTypes 값임
  <property name="DomainAuthType">
    <dictionary key-type="string" value-type="int" >
      <entry key="5A23TPM2" value="0" />
    </dictionary>
  </property>
  -->
</object>
```

3. 파일을 저장하고 닫습니다.
4. Core Server Service를 다시 시작합니다.

3

Device Server 구성

이 장에서는 Device Server를 사용자 환경에 맞게 조정하기 위해 변경할 수 있는 매개 변수에 대해 설명합니다.

이러한 파일에 나와 있는 매개 변수만 변경할 수 있습니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Device Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

eserver.properties

<Device Server 설치 디렉토리>\conf\eserver.properties에서 다음 매개 변수를 변경할 수 있습니다.

파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다. 그러면 업그레이드할 때 변경 사항이 새 파일로 쉽게 옮겨가도록 할 수 있습니다.

eserver.properties

매개 변수	기본값	설명
eserver.default.host	Device Server Service	Device Server Service가 설치된 FQDN
eserver.default.port	v7.7 이상 Enterprise Server - 8443 v7.7 이전 Enterprise Server - 8081	Device Server가 장치가 보내는 등록 요청을 수신 대기하는 포트
eserver.use.ssl	True	SSL은 기본적으로 사용하도록 설정되어 있습니다. SSL을 사용하지 않으려면 이 매개 변수를 False로 변경합니다.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Device Server가 사용하는 SSL 인증서의 위치
eserver.keystore.password	changeit	구성 도구에서 cacert 암호를 수정하면 이 매개 변수도 그에 따라 업데이트됩니다. 초기 구성 후 구성 도구에서 cacert를 수정할 경우 키 저장소 암호를 사용하여 이 매개 변수를 업데이트합니다.

eserver.properties		
매개 변수	기본값	설명
eserver.ciphers		암호화 방법의 목록을 설정합니다. 각 암호화 방법은 쉼표로 구분해야 합니다. 이 목록을 비워두는 경우 소켓은 Tomcat에서 지원하는 암호화 중 사용 가능한 모든 암호화 방법을 허용합니다. 아래 예에서 주석 처리를 제거하고 암호화 방법 목록을 설정합니다. 각 암호화 방법은 쉼표로 구분합니다. 유효한 암호화 그룹 이름 목록을 보려면 Sun의 JSSE 참조 안내서를 참조하십시오. #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 설치 디렉토리>\conf\run-service.conf에서 다음 매개 변수 중 일부를 변경할 수 있습니다. 이러한 매개 변수는 설치 시 자동으로 설정됩니다. Service를 사용자 지정하거나 구성을 변경하려면 다음과 같이 하십시오.

1. Service를 중지합니다.
2. Service를 제거합니다.
3. **run-service.conf** 파일을 편집하고 저장합니다. 파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다.
4. Service를 다시 설치합니다.
5. Service를 시작합니다.

run-service.conf		
매개 변수	기본값	설명
JAVA_HOME	Dell\Java Runtime\jreX.x	Java 설치 디렉토리 위치
wrapper.ntservice.name	EpmDeviceSvr	Service 이름
wrapper.ntservice.displayname	Dell Device Server	Service의 표시 이름
wrapper.ntservice.description	Enterprise Device Server	Service에 대한 설명
wrapper.ntservice.dependency.1		Service 종속성. 필요에 따라 1부터 시작하는 종속성을 추가합니다.
wrapper.ntservice.starttype	AUTO_START	Service를 설치하는 모드: AUTO_START 또는 DEMAND_START

run-service.conf		
매개 변수	기본값	설명
wrapper.ntservice.interactive	false	true로 설정하면 Service가 데스크톱과 상호 작용할 수 있습니다.

4

Security Server 구성

이 장에서는 Security Server를 사용자 환경에 맞게 조정하기 위해 변경할 수 있는 매개 변수에 대해 설명합니다.

이러한 파일에 나와 있는 매개 변수만 변경할 수 있습니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Security Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

context.properties

<Security Server 설치 디렉토리>\webapps\xapi\WEB-INF\context.properties에서 다음 매개 변수를 변경할 수 있습니다.

파일 앞부분에서 주석의 변경 사항을 추적하는 것이 좋습니다. 그러면 업그레이드할 때 변경 사항이 새 파일로 쉽게 옮겨가도록 할 수 있습니다.

context.properties

매개 변수	기본값	설명
default.gatekeeper.group.remote	CMGREMOTE	장치 원격 그룹 이름 **수정하지 마십시오.**
xmlrpc.max.threads	250	이 Device Server 내 동시 스레드의 최대 수
default.auth.upn.suffix		서버에서 정규화된 로그인 이름을 요청하는데 요청에 정규화된 로그인 이름이 제공되지 않은 경우 사용자 로그인 이름에 추가되는 UPN 접미사
device.manual.auth.enable	true	수동 인증을 사용하는지 여부를 나타냅니다. **수정하지 마십시오.**
service.activation.enable	true	Device Server에서 등록을 처리하는지 여부를 나타냅니다. **수정하지 마십시오.**
service.policy.enable	true	정책을 사용하는지 여부를 나타냅니다. **수정하지 마십시오**.
service.auth.enable	true	Device Server에서 인증을 처리하는지 여부를 나타냅니다.
service.forensic.enable	true	이 설정은 Forensic 통합 플러그인과 함께 사용합니다. Forensic 도구 통합이 필요할 경우 Dell 지원 부서에 문의하십시오.
service.support.enable	true	서버에 대한 메타 정보 검색을 사용합니다.
service.device.enable	true	SDE 키 저장소와 같은 Shield 서비스 지원을 사용합니다.

5

암호화 기능 구성

이 섹션에서는 암호화 기능을 독립적으로 관리하는 방법에 대해 설명합니다.

임시 파일 삭제 방지

기본적으로 c:\windows\temp directory에 있는 모든 임시 파일은 DDPE 설치/업그레이드 중 자동으로 삭제됩니다. 임시 파일을 삭제하면 초기 암호화가 빠르게 수행됩니다. 임시 파일은 초기 암호화 스윕 전에 삭제됩니다.

하지만 조직에서 \temp 디렉토리 내에 파일 구조를 유지해야 하는 타사 응용 프로그램을 사용하는 경우에는 이와 같이 삭제되지 않도록 해야 합니다.

임시 파일이 삭제되지 않도록 하려면 다음과 같이 레지스트리 설정을 만들거나 수정합니다.

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

임시 파일을 삭제하지 **않으면** 초기 암호화 시간이 늘어납니다.

오버레이 아이콘 숨기기

기본적으로 설치 중 모든 암호화 오버레이 아이콘이 표시되도록 설정됩니다. 최초 설치 후 컴퓨터에서 관리되는 모든 사용자의 암호화 오버레이 아이콘을 숨기려면 다음 레지스트리 설정을 사용하십시오.

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons(DWORD 값)=1

적절한 권한이 있는 사용자가 암호화 오버레이 아이콘을 표시하도록 선택하면 해당 설정이 이 레지스트리 값을 무시합니다.

시스템 트레이 아이콘 숨기기

기본적으로 설치 중 시스템 트레이 아이콘이 표시됩니다. 최초 설치 후 컴퓨터에서 관리되는 모든 사용자의 시스템 트레이 아이콘을 숨기려면 다음 레지스트리 설정을 사용하십시오.

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON(DWORD 값)=1

슬롯 등록

슬롯 등록은 대규모 배포 중 서버 부하를 줄이기 위해 정해진 시간 동안 Shield 등록을 분산할 수 있는 기능입니다. 알고리즘에 따라 생성된 시간 슬롯을 기준으로 등록이 지연되어 등록 시간이 원활히 분산됩니다.

슬롯 등록은 Shield 설치 프로그램 또는 Shield 워크스테이션을 통해 사용하도록 설정 및 구성됩니다.

VPN을 통해 등록해야 하는 사용자의 경우 VPN 클라이언트 소프트웨어가 네트워크 연결을 설정할 수 있도록 Shield에 대한 슬롯 등록 구성으로 초기 등록을 충분한 시간 동안 지연해야 할 수 있습니다.

주의: 슬롯 등록을 구성할 경우 반드시 고객 지원 센터의 도움을 받으십시오. 시간 슬롯을 잘못 구성할 경우 많은 클라이언트가 동시에 등록을 시도하여 심각한 성능 문제가 발생할 수 있습니다.

다음 레지스트리 키를 사용하여 슬롯 등록을 구성합니다. 이러한 레지스트리 키를 변경할 경우 업데이트를 적용하려면 Shield 워크스테이션을 다시 시작해야 합니다.

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

  이 설정으로 슬롯 등록 기능을 사용하거나 사용하지 않도록 지정할 수 있습니다.
  사용하지 않음=0(기본값)
  사용=1

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

  등록 슬롯 간격 시간(초). 이 속성을 사용하여 등록 슬롯 간격 시간(초)을 재정의할 수 있습니다. 7시간 동안 슬롯 등록에 대해 25200초를 사용할 수 있습니다. 기본 설정은 매일 반복을 나타내는 86400초입니다.

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

  모든 등록 시간 슬롯이 발생할 경우 반복 내의 간격은 ACTIVATION_SLOT_CALREPEAT입니다. 하나의 간격만 허용됩니다. 이 설정은 0,<CalRepeat>이어야 합니다. 0으로 설정하지 않을 경우 예기치 않은 결과가 발생할 수 있습니다. 기본 설정은 0,86400입니다. 7시간 반복을 설정하려면 0,25200 설정을 사용하십시오. CALREPEAT은 Shield 사용자가 로그인할 때 활성화됩니다.

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

  등록이 슬롯화된 사용자가 다음에 로그인할 때 컴퓨터가 등록을 시도하기 전 누락할 수 있는 등록 슬롯 수. 이러한 즉각적 시도 중 등록이 실패하면 Shield에서 슬롯 등록 시도를 재개합니다. 네트워크 오류로 인해 등록이 실패할 경우 네트워크가 다시 연결되면 MISSTHRESHOLD가 초과되지 않은 경우라도 등록이 시도됩니다. 등록 슬롯 시간에 도달하기 전에 사용자가 로그아웃하면 다음 로그인 시 새 슬롯이 할당됩니다.

- HKCU/Software/CREDANT/ActivationSlot(사용자별 데이터)

  슬롯 등록을 시도하기 위해 지연된 시간으로, 슬롯 등록을 사용하도록 설정한 후 사용자가 네트워크에 처음으로 로그인할 때 설정됩니다. 등록 설정은 등록을 시도할 때마다 재계산됩니다.

- HKCU/Software/CREDANT/SlotAttemptCount(사용자별 데이터)

  시간 슬롯에 도달하고 등록이 시도되었지만 실패할 경우 실패 또는 누락한 시도 횟수. 이 횟수가 ACTIVATION_SLOT_MISSTHRESHOLD에 설정된 값에 도달할 경우 컴퓨터는 네트워크에 연결되는 즉시 한 번의 등록을 시도합니다.

명령줄을 통해 슬롯 등록을 사용하도록 설정하려면 다음과 유사한 명령을 사용합니다.

```
setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0,25200 <기타 매개 변수>"
```

참고: 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표 안에 포함해야 합니다.

강제 폴링

Shield에서 Server를 폴링하여 강제 정책 업데이트를 수행하려면 다음 레지스트리 설정을 사용합니다.

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy(DWORD 값)=1

Shield 버전에 따라 레지스트리 설정이 자동으로 사라집니다. *또는* 폴링이 완료된 후 1에서 0으로 변경합니다.

관리자의 권한 설정에 따라, 이 레지스트리 설정을 만들려면 권한을 변경해야 할 수 있습니다. 새 DWORD를 만드는 데 문제가 발생할 경우 다음 단계에 따라 권한을 변경하십시오.

1. Windows 레지스트리에서 HKLM\SOFTWARE\Credant\CMGShield\Notify로 이동합니다.
2. 마우스 오른쪽 버튼으로 **알림** > **권한**을 클릭합니다.
3. *알림 권한* 창이 열리면 **모든 권한** 확인란을 선택합니다.
4. **확인**을 클릭합니다.

이제 새 레지스트리 설정을 만들 수 있습니다.

인벤토리 옵션

Shield에서 Server에 최적화된 인벤토리를 전송하거나, 전체 인벤토리를 Server로 전송하거나, 등록된 모든 사용자의 전체 인벤토리를 Server로 전송할 수 있도록 허용하려면 다음 레지스트리 설정을 사용합니다.

최적화된 인벤토리를 Server로 전송

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

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

OnlySendInvChanges (REG_DWORD)=1

항목이 없을 경우 최적화된 인벤토리가 Server로 전송됩니다.

전체 인벤토리를 Server로 전송

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

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

OnlySendInvChanges (REG_DWORD)=0

항목이 없을 경우 최적화된 인벤토리가 Server로 전송됩니다.

전체 인벤토리를 등록된 모든 사용자에게 전송

다음과 같이 레지스트리 설정을 만들거나 수정합니다.

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

RefreshInventory (REG_DWORD)=1

이 항목은 처리되는 즉시 레지스트리에서 삭제됩니다. 이 값은 Vault에 저장되므로 인벤토리 업로드가 발생하기 전에 컴퓨터를 재부팅할 경우에도 다음에 인벤토리 업로드에 성공하면 Shield에서 이 요청에 응합니다.

이 항목은 OnlySendInvChanges 레지스트리 값을 대체합니다.

비도메인 등록

비도메인 등록 활성화는 고급 구성이며, 다양한 결과가 발생할 수 있습니다. 환경의 특정 요구 사항에 대해 논의하고 이 기능을 어떻게 사용할 수 있는지 안내를 받으려면 고객 지원 센터에 연락하십시오.

6

Kerberos 인증을 위한 요소 구성

이 섹션에서는 Kerberos 인증에 사용하기 위한 요소를 구성하는 방법에 대해 설명합니다.

Kerberos 인증을 위한 요소 구성

참고: Kerberos 인증을 사용하려는 경우 Key Server 구성 요소가 포함된 서버가 영향을 받는 도메인에 포함되어야 합니다.

Key Server는 소켓에서 연결할 클라이언트를 수신 대기하는 Service입니다. 클라이언트가 연결되면 보안 연결이 협상, 인증되고 Kerberos API를 사용하여 암호화됩니다(보안 연결을 협상할 수 없는 경우 클라이언트 연결이 끊어집니다).

그런 다음 Key Server가 Device Server와 함께 클라이언트를 실행하는 사용자가 키에 액세스할 수 있는지 여부를 확인합니다. 이 액세스 권한은 *개별* 도메인을 통해 Remote Management Console에 부여됩니다.

Windows Service 지침

1. Windows Service 패널로 이동합니다(시작 > 실행... > services.msc > 확인).
2. Dell Key Server를 마우스 오른쪽 버튼으로 클릭한 다음 **속성**을 선택합니다.
3. **로그온** 탭으로 이동하여 **이 계정:** 옵션 버튼을 선택합니다.
4. **이 계정:** 필드에서 원하는 도메인 사용자를 추가합니다. 이 도메인 사용자는 Key Server 폴더에 대해 로컬 관리자 이상의 권한이 있어야 합니다(Key Server 구성 파일뿐만 아니라 log.txt 파일에도 데이터를 쓸 수 있어야 함).
5. **확인**을 클릭합니다.
6. Service를 다시 시작합니다(추가 작업을 위해 Windows Service 패널을 열어 둡니다).
7. <Key Server 설치 디렉토리> log.txt를 탐색하여 Service가 올바르게 시작되었는지 확인합니다.

Key Server 구성 파일 지침

1. <Key Server 설치 디렉토리>를 탐색합니다.
2. 텍스트 편집기로 Credant.KeyServer.exe.config를 엽니다.
3. <add key="user" value="superadmin" />으로 이동한 다음 "superadmin" 값을 적절한 사용자 이름으로 변경합니다("superadmin"을 유지할 수도 있음).

   "superadmin" 형식으로는 Server에 인증할 수 있는 모든 방법이 허용됩니다. SAM 계정 이름, UPN 또는 도메인\사용자 이름이 허용됩니다. Active Directory에 인증하려면 *해당* 사용자 계정에 대한 유효성 검사가 필요하므로 Server에 인증할 수 있는 모든 방법이 허용됩니다.

   예를 들어, 다중 도메인 환경에서 "jdoe"와 같은 SAM 계정 이름만 입력하면 서버가 "jdoe"를 찾을 수 없어 "jdoe"를 인증할 수 없으므로 실패할 가능성이 높습니다. 다중 도메인 환경에서는 도메인\사용자 이름 형식이 허용되더라도 UPN을 사용하는 것이 좋습니다.

   단일 도메인 환경에서는 SAM 계정 이름이 허용됩니다.

4 <add key="epw" value="<암호의 암호화된 값>" />으로 가서 "epw"를 "password"로 변경합니다. 그런 다음 "<암호의 암호화된 값>"을 3단계의 사용자 암호로 변경합니다. 이 암호는 Server가 다시 시작할 때 다시 암호화됩니다.

3단계에서 "superadmin"을 사용할 경우 superadmin 암호가 "changeit"이 아니면 여기에서 변경해야 합니다.

5 변경 사항을 저장하고 파일을 닫습니다.

예시 구성 파일:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [Server가 수신 대기할 TCP 포트. 기본값은 8050입니다. 필요하면 변경합니다.]
        <add key="maxConnections" value="2000" /> [Server가 허용할 활성 소켓 연결 수.]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [장치 서버의 URL입니다. Enterprise Server가 v7.7 이상인 경우 형식은 https://keyserver.domain.com:8443/xapi/입니다. Enterprise Server가 v7.7 이전인 경우는 https://keyserver.domain.com:8081/xapi 형식입니다(맨 끝의 슬래시가 없음).]
        <add key="verifyCertificate" value="false" /> [True일 경우 인증서를 검증함/검증하지 않거나 자체 서명 인증서를 사용할 경우 false로 설정함]
        <add key="user" value="superadmin" /> [Device Server와 통신하는 데 사용하는 사용자 이름. 이 사용자는 Remote Management Console에서 Forensic 관리자 유형을 선택한 상태여야 합니다. "superadmin" 형식으로는 Server에 인증할 수 있는 모든 방법이 허용됩니다. SAM 계정 이름, UPN 또는 도메인\사용자 이름이 허용됩니다. Active Directory에 인증하려면 해당 사용자 계정에 대한 유효성 검사가 필요하므로 Server에 인증할 수 있는 모든 방법이 허용됩니다. 예를 들어, 다중 도메인 환경에서 "jdoe"와 같은 SAM 계정 이름만 입력하면 서버가 "jdoe"를 찾을 수 없어 "jdoe"를 인증할 수 없으므로 실패할 가능성이 높습니다. 다중 도메인 환경에서는 도메인\사용자 이름 형식이 허용되더라도 UPN을 사용하는 것이 좋습니다. 단일 도메인 환경에서는 SAM 계정 이름이 허용됩니다.]
        <add key="cacheExpiration" value="30" /> [Service가 키를 요청할 수 있는 사용자를 확인해야 하는 빈도(초). Service는 캐시를 유지하고 경과 기간을 추적합니다. 캐시가 값(초)보다 오래된 경우 새 목록을 가져옵니다. 사용자가 연결되면 Key Server가 Device Server에서 인증된 사용자를 다운로드해야 합니다. 이러한 사용자의 캐시가 없거나 마지막 "x"초 동안 다운로드된 목록이 없을 경우 다시 다운로드됩니다. 폴링은 수행되지 않지만 이 값은 새로 고침이 필요할 경우 새로 고침 전 목록의 기간을 구성합니다.
        <add key="epw" value="암호의 암호화된 값" /> [Device Server와 통신하는 데 사용하는 암호. superadmin 암호가 변경된 경우 여기에서 변경해야 합니다.]
    </appSettings>
</configuration>
```

Windows Service 지침

1 Windows Service 패널로 돌아갑니다.

2 Dell Key Server Service를 **다시 시작**합니다.

3 <Key Server 설치 디렉토리> log.txt를 탐색하여 Service가 올바르게 시작되었는지 확인합니다.

4 Windows Service 패널을 닫습니다.

Remote Management Console 지침

1. 필요할 경우 Remote Management Console에 로그인합니다.
2. **도메인**을 클릭하고 **세부 정보** 아이콘을 클릭합니다.
3. **Key Server**를 클릭합니다.
4. Key Server 계정 목록에서 관리자 활동을 수행할 사용자를 추가합니다. 형식은 도메인\사용자 이름입니다. **계정 추가**를 클릭합니다.
5. 왼쪽 메뉴에서 **사용자**를 클릭합니다. 검색 상자에 4단계에서 추가한 사용자 이름을 입력하여 검색합니다. **검색**을 클릭합니다.
6. 올바른 사용자를 찾았으면 **세부 정보** 아이콘을 클릭합니다.
7. **Forensic 관리자**를 선택합니다. **업데이트**를 클릭합니다.

Kerberos 인증을 위한 요소가 구성되었습니다.

7

Forensic 관리자 역할 할당

기본적으로 Forensic 인증은 백 엔드 서버에서 사용하고 프런트 엔드 서버에서는 사용하지 않도록 설정되어 있습니다. 이러한 설정은 Device Server 및 Security Server를 설치할 때 적절히 지정됩니다.

Remote Management Console 지침

1. 필요할 경우 Remote Management Console에 로그인합니다.
2. 왼쪽 창에서 **관리자** > **사용자**를 클릭합니다.
3. *사용자 검색* 페이지에서 Forensic 관리자 역할을 부여하려는 사용자의 이름을 입력하고 **검색**을 클릭합니다(이 사용자의 자격 증명은 Forensic 모드에서 CMGAd, CMGAu, CMGAlu 유틸리티 및 Decryption Agent를 실행하는 동안 제공됨).
4. *사용자 검색 결과* 페이지에서 **세부 정보** 아이콘을 클릭합니다.
5. *다음의 사용자 세부 정보: <사용자 이름>* 페이지에서 **관리자**를 선택합니다.
6. 사용자 열에서 **Forensic 관리자**를 선택하고 **업데이트**를 클릭합니다.

이제 Forensic 관리자 역할이 설정되었습니다.

Forensic 인증 해제

1. 백 엔드 서버에서 <Security Server 설치 디렉토리>\webapps\xapi\WEB-INF\context.properties를 탐색하여 다음과 같이 속성을 변경합니다.

   service.forensic.enable=true

   →

   service.forensic.enable=false
2. Security Server 서비스를 다시 시작합니다.
3. <Device Server 설치 디렉토리>\webapps\ROOT\WEB-INF\web.xml 탐색하여. 다음을 수정합니다.

   <init-param>

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

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

   </init-param>
4. Device Server Service를 **다시 시작**합니다.
5. Forensic 관리자 역할 권한을 활발하게 사용하지 않는 사용자들의 해당 관리자 역할을 제거하는 것이 좋습니다.

8

Cron 식

이 섹션에서는 Cron 식의 형식과 특수 문자를 사용하는 방법에 대해 설명합니다.

Cron 식 소개

Cron은 오랫동안 사용되어 왔으며 강력하고 입증된 예약 기능을 제공하는 UNIX 도구입니다. CronTrigger 클래스는 Cron의 예약 기능을 기반으로 합니다.

CronTrigger는 발생 일정을 만들 수 있는 Cron 식을 사용합니다. 예를 들어, 매주 월요일부터 금요일까지 오전 8시에 발생하거나 매월 마지막 금요일 오전 1시 30분에 발생하도록 예약할 수 있습니다.

Cron 식은 강력하지만 혼동하기 쉽습니다. 이 문서는 Cron 식 작성 시 까다로운 부분에 대해 설명하고 외부 도움을 구하기 전 참조할 수 있는 리소스를 제공합니다.

Cron 식의 형식

Cron 식은 공백으로 구분된 6개의 필수 필드와 1개의 옵션 필드로 구성되어 있습니다. 필드에는 허용된 모든 값과 해당 필드에 허용되는 특수 문자의 다양한 조합을 포함할 수 있습니다.

Cron 식은 * * * * ? *과 같이 간단하게 지정하거나

0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010과 같이 복잡하게 지정할 수도 있습니다.

다음은 필드에 대한 설명입니다.

필드 이름	필수 여부	허용 값	허용되는 특수 문자
Minutes	예	0-59	, - * /
Hours	예	0-23	, - * /
Day of month	예	1-31	, - * ? / L W C
Month	예	1-12 또는 JAN-DEC	, - * /
Day of week	예	1-7 또는 SUN-SAT	, - * ? / L C #
연도	아니요	비워둠, 1970-2099	, - * /

특수 문자

- * 문자는 모든 값을 지정하는 데 사용합니다. 예를 들어, 분 필드의 *는 모든 분을 의미합니다.
- ? 문자(특정 값이 없음)는 문자가 허용되는 두 필드 중 하나에 어떤 내용을 지정하고 다른 필드에는 아무 것도 지정하지 않으려는 경우 유용합니다. 예를 들어, 요일과 상관없이 특정 일(10일)에 트리거하려는 경우 일 필드에 10을 사용하고 요일 필드에 ?를 사용합니다.
- - 문자는 범위를 지정하는 데 사용합니다. 예를 들어, 시간 필드의 10-12는 10, 11, 12를 의미합니다.
- , 문자는 추가 값을 지정하는 데 사용합니다. 예를 들어, 요일 필드의 MON,WED,FRI는 월요일, 수요일, 금요일을 의미합니다.

- / 문자는 증분을 지정하는 데 사용합니다.

  초 필드의 0/15는 0, 15, 30, 45를 의미합니다.

  초 필드의 5/15는 5, 20, 35, 50을 의미합니다.

  / 앞에 *을 지정할 경우 시작 값으로 0을 지정하는 것과 동일합니다.

  일 필드의 1/3은 1일부터 시작하여 3일마다 발생함을 의미합니다.

  기본적으로 식의 각 필드에 켜거나 끌 수 있는 숫자 집합이 있습니다. 초와 분의 숫자 범위는 0 ~ 59이며, 시는 0 ~ 23, 일은 0 ~ 31, 월은 1 ~ 12입니다. / 문자를 사용하면 지정된 집합에서 '몇 번째'마다가 적용됩니다. 따라서 월 필드의 7/6의 경우 7월에만 켜지며 6개월마다를 의미하지 않습니다.

- L 문자는 일 및 요일 필드에 허용됩니다. 이 문자는 마지막을 의미하지만 두 필드에 다른 의미로 사용됩니다.

  일 필드의 L 값은 월의 마지막 날을 의미합니다(1월은 31일, 윤년이 아닌 해의 2월의 경우 28일).

  요일 필드에 단독으로 사용할 경우 7 또는 SAT를 의미합니다.

  요일 필드에서 다른 값 다음에 사용하면 월의 마지막 x요일을 의미합니다. 예를 들어, 6L은 월의 마지막 금요일을 의미합니다. L 옵션을 사용할 경우 혼란스러운 결과를 피하기 위해 목록이나 값 범위를 사용하지 않는 것이 중요합니다.

- W 문자는 일 필드에 허용됩니다. 이 문자는 지정된 일과 가장 가까운 평일(월-금)을 지정하는 데 사용합니다. 예를 들어, 일 필드 값으로 15W를 지정하는 경우 15일과 가장 가까운 평일을 의미합니다. 따라서 15일이 토요일인 경우 14일 금요일에 트리거됩니다. 15일이 일요일인 경우는 16일 월요일에 트리거되며 15일이 화요일인 경우는 15일 화요일에 트리거됩니다. 하지만 일 값으로 1W를 지정한 경우 1일이 토요일이면 달의 경계를 '넘지' 않으므로 3일 월요일에 트리거됩니다. W 문자는 일이 일 범위 또는 목록이 아닌 하루일 경우에만 지정할 수 있습니다.

  또한 L 및 W 문자를 일 식과 결합하여 월의 마지막 평일을 의미하는 LW를 만들 수 있습니다.

- # 문자는 요일 필드에 허용됩니다. 이 문자는 월의 '몇 번째' x요일을 지정하는 데 사용합니다. 예를 들어, 요일 필드의 6#3은 월의 세 번째 금요일을 의미합니다(6일 = 금요일, #3 = 월의 세 번째).

  다른 예:
  2#1 = 월의 첫 번째 월요일
  4#5 = 월의 다섯 번째 수요일

  #5를 지정한 경우 월에 지정된 다섯 번째 요일이 없으면 해당 월에는 발생하지 않습니다.

- C 문자는 캘린더에 허용됩니다. 이 문자를 사용하면 연결된 캘린더(있는 경우)를 기준으로 값이 계산된다는 의미입니다. 연결된 캘린더가 없으면 전체를 포함하는 캘린더를 사용하는 것과 동일합니다. 일 필드의 5C 값은 5일 또는 5일 이후 캘린더에 포함된 첫날을 의미합니다. 요일 필드의 1C 값은 일요일 또는 일요일 이후 캘린더에 나오는 첫날을 의미합니다.

참고: 현재 일 및 요일 값을 동시에 지정하는 것은 아직 완전히 지원되지 않습니다. 이러한 필드 중 하나에 **?** 문자를 사용하십시오. **C** 문자에 대해 설명한 기능은 아직 완전히 지원되지 않습니다. 월 및 요일에 사용 가능한 문자와 이름은 대/소문자를 구분하지 않습니다. **MON**은 **mon**과 동일합니다. 요일 및 월 필드에서 **?** 및 *가 어떤 영향을 미치는지 세심한 주의를 기울이십시오. 자정부터 오전 1시까지의 발생 시간을 설정할 경우 주의가 필요합니다. 일광 절약 시간은 시간이 앞으로 또는 뒤로 이동하는 가에 따라 누락(또는 반복)이 발생할 수 있습니다.

예

식	의미
0 0 12 * * ?	매일 오후 12시(정오)에 발생
0 15 10 ? * *	매일 오전 10시 15분에 발생
0 15 10 * * ?	매일 오전 10시 15분에 발생
0 15 10 * * ? *	매일 오전 10시 15분에 발생
0 15 10 * * ? 2005	2005년 동안 매일 오전 10시 15분에 발생
0 * 14 * * ?	매일 오후 2시부터 오후 2시 59분까지 1분마다 발생
0 0/5 14 * * ?	매일 오후 2시부터 오후 2시 55분까지 5분마다 발생
0 0/5 14,18 * * ?	매일 오후 2시부터 오후 2시 55분까지 5분마다 발생하며 매일 오후 6시부터 오후 6시 55분까지 5분마다 발생
0 0-5 14 * * ?	매일 오후 2시부터 오후 2시 05분까지 1분마다 발생
0 10,44 14 ? 3 WED	3월 동안 수요일마다 오후 2시 10분과 오후 2시 44분에 발생
0 15 10 ? * MON-FRI	월요일, 화요일, 수요일, 목요일, 금요일마다 오전 10시 15분에 발생
0 15 10 15 * ?	매월 15일 오전 10시 15분에 발생
0 15 10 L * ?	매월 말일 오전 10시 15분에 발생
0 15 10 ? * 6L	매월 마지막 금요일 오전 10시 15분에 발생
0 15 10 ? * 6L	매월 마지막 금요일 오전 10시 15분에 발생
0 15 10 ? * 6L 2002-2005	2002, 2003, 2004, 2005년 동안 매월 마지막 금요일마다 오전 10시 15분에 발생
0 15 10 ? * 6#3	매월 세 번째 금요일 오전 10시 15분에 발생
0 0 12 1/5 * ?	매월 1일부터 시작하여 5일째마다 오후 12시(정오)에 발생
0 11 11 11 11 ?	11월 11일마다 오전 11시 11분에 발생

9

Keytool을 이용한 자체 서명 인증서 생성 및 CSR(Certificate Signing Request) 생성

참고: 이 섹션에서는 Java 기반 구성 요소의 자체 서명 인증서를 만드는 단계에 대해 설명합니다. 이 프로세스는 .NET 기반 구성 요소의 자체 서명 인증서를 만드는 데 사용할 수 *없습니다*.

자체 서명 인증서는 개발 및 테스팅 환경에서 *만* 사용하는 것이 좋습니다.

조직에서 SSL 서버 인증서를 요구하거나 다른 이유로 인증서를 만들어야 할 경우 이 섹션에서 Keytool을 이용한 Java 키 저장소를 만드는 방법을 참조할 수 있습니다.

Keytool은 VeriSign® 또는 Entrust®와 같은 CSR(Certificate Signing Request)의 형식으로 CA(인증 기관)에 전달해야 하는 개인 키를 만듭니다. 그런 다음 CA가 이 CSR을 기준으로 서명하는 서버 인증서를 만들고 서버 인증서가 서명 기관 인증서와 함께 파일로 다운로드됩니다. 그런 다음 인증서를 cacert 파일로 가져옵니다.

새 키 쌍 및 자체 서명 인증서 생성

1. Compliance Reporter, Console Web Services, Device Server 또는 Gatekeeper Web Services의 **conf** 디렉토리로 이동합니다.
2. 다음과 같이 기본 인증서 데이터베이스를 백업합니다.

   시작 > **실행**을 클릭하고 **move cacerts cacerts.old**를 입력합니다.
3. 시스템 경로에 Keytool을 추가합니다. 명령 프롬프트에 다음 명령을 입력합니다.

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. 인증서를 생성하려면 다음과 같이 Keytool을 실행합니다.

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Keytool에 정보를 입력하라는 메시지가 표시되면 다음과 같이 입력합니다.

참고: 편집하기 전 구성 파일을 백업해 두십시오. 지정된 매개 변수만 변경해야 합니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Enterprise Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

- *키 저장소 암호:* 암호를 입력하고(지원되지 않는 문자 <>;&" ') 구성 요소 **conf** 파일의 변수를 다음과 동일한 값으로 설정합니다.

  <Compliance Reporter 설치 디렉토리>\conf\eserver.properties. eserver.keystore.password = 값 설정

  <Console Web Services 설치 디렉토리>\conf\eserver.properties. eserver.keystore.password = 값 설정

  <Device Server 설치 디렉토리>\conf\eserver.properties. eserver.keystore.password = 값 설정
- *이름 및 성:* 사용하는 구성 요소가 설치된 서버의 정규화된 이름을 입력합니다. 이 정규화된 이름에는 호스트 이름과 도메인 이름이 포함됩니다(예: server.dell.com).

- *조직 부서:* 적절한 값을 입력합니다(예: 보안).
- *조직:* 적절한 값을 입력합니다(예: Dell).
- *시 또는 지역:* 적절한 값을 입력합니다(예: Austin).
- *주 또는 도:* 주 또는 도의 전체 이름을 입력합니다(예: Texas).
- 2문자로 이루어진 국가 코드:

  미국 = US

  캐나다 = CA

  스위스 = CH

  독일 = DE

  스페인 = ES

  프랑스 = FR

  영국 = GB

  아일랜드 = IE

  이탈리아 = IT

  네덜란드 = NL
- 정보가 정확한지 확인을 요청하는 메시지가 표시됩니다. 정확할 경우 예를 입력합니다.
  정확하지 않을 경우 아니요를 입력합니다. Keytool에 이전에 입력된 각 값이 표시됩니다. **Enter**를 클릭해서 값을 승인하거나 값을 변경하고 **Enter**를 클릭합니다.
- *별칭 키 암호:* 여기에서 다른 암호를 입력하지 않을 경우 이 암호에 기본적으로 키 저장소 암호가 적용됩니다.

인증 기관에서 서명된 인증서 요청

새 키 쌍 및 자체 서명 인증서 생성에서 만든 자체 서명 인증서에 대해 CSR(Certificate Signing Request)을 생성하려면 이 절차를 사용합니다.

1 이전에 **<인증서 별칭>**에 사용된 값과 동일한 값으로 대체합니다.

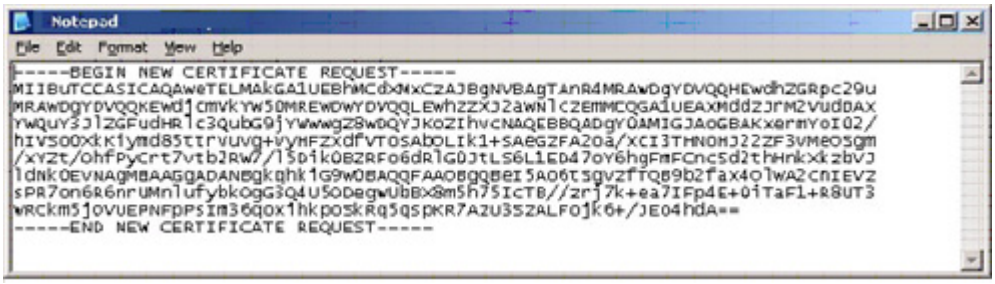
```
keytool -certreq -sigalg MD5withRSA -alias <인증서 별칭> -keystore .\cacerts -file
<csr 파일 이름>
```

예:

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

.csr 파일에는 CA에서 인증서를 만드는 동안 사용될 BEGIN/END 쌍이 포함됩니다.

그림 9-1. 예제 .CSR 파일



2 조직이 인증 기관에서 SSL 서버 인증서를 취득하는 데 사용하는 절차를 따르십시오. 서명할 <csr 파일 이름>의 내용을 전송합니다.

참고: 유효한 인증서를 요청하는 방법은 여러 가지가 있습니다. 인증서 요청 방법 예에 **예시** 방법이 나와 있습니다.

3 서명된 인증서를 받으면 파일에 저장하십시오.

4 가져오기 프로세스 중 오류가 발생할 경우에 대비하여 이 인증서를 백업해 두는 것이 좋습니다. 이와 같이 백업해 두면 프로세스를 다시 시작하지 않아도 됩니다.

루트 인증서 가져오기

참고: 루트 인증서 인증 기관이 Verisign(Verisign Test 제외)인 경우 다음 절차로 건너 뛰어 서명된 인증서를 가져오십시오.

인증 기관 루트 인증서는 서명된 인증서의 유효성을 검사합니다.

1 다음 중 **하나**를 수행하십시오.

- 인증 기관 루트 인증서를 다운로드하고 파일에 저장합니다.
- 엔터프라이즈 디렉토리 서버 루트 인증서를 얻습니다.

2 다음 중 **하나**를 수행하십시오.

- Compliance Reporter, Console Web Services, Device Server 또는 Legacy Gatekeeper Connector에 대한 SSL을 활성화하려는 경우 구성 요소 **conf** 디렉토리로 변경합니다.
- Server와 엔터프라이즈 디렉토리 서버 사이에서 SSL을 활성화하려면 **<Dell 설치 디렉토리>\Java Runtimes\jre1.x.x_xx\lib\security**로 변경합니다(JRE cacert의 기본 암호는 **changeit**).

3 다음과 같이 Keytool을 실행하여 루트 인증서를 설치합니다.

```
keytool -import -trustcacerts -alias <인증 기관 인증서 별칭> -keystore .\cacerts
-file <인증 기관 인증서 파일 이름>
```

예:

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

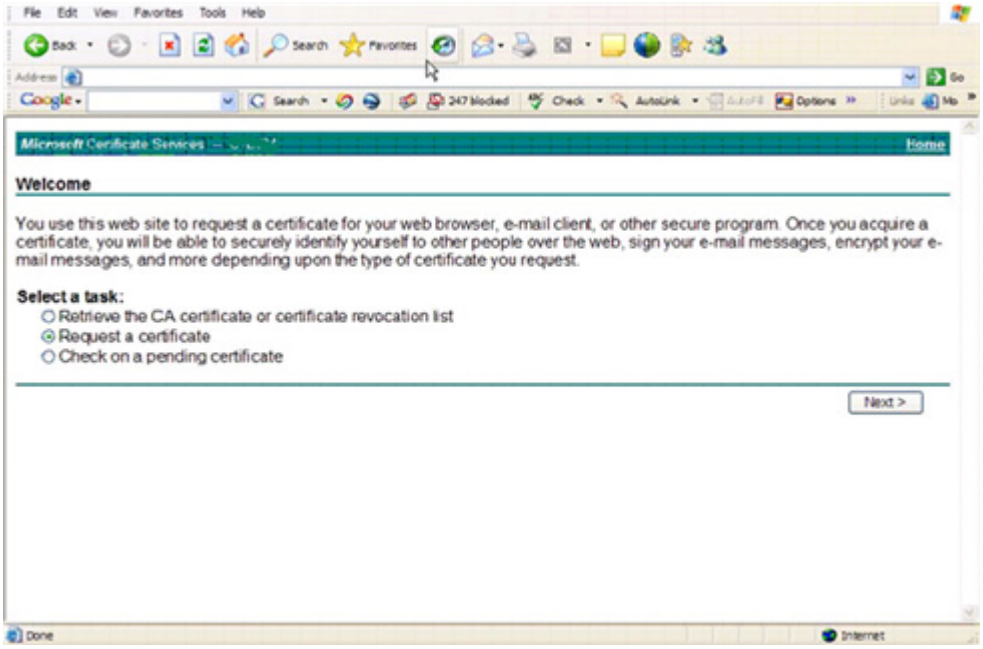
인증서 요청 방법 예

조직에서 내부적으로 설정한 인증서를 요청하는 방법을 예로 들면 웹 브라우저를 사용하여 Microsoft CA Server에 액세스하는 방법이 있습니다.

1 Microsoft CA Server를 탐색합니다. IP 주소는 조직이 제공합니다.

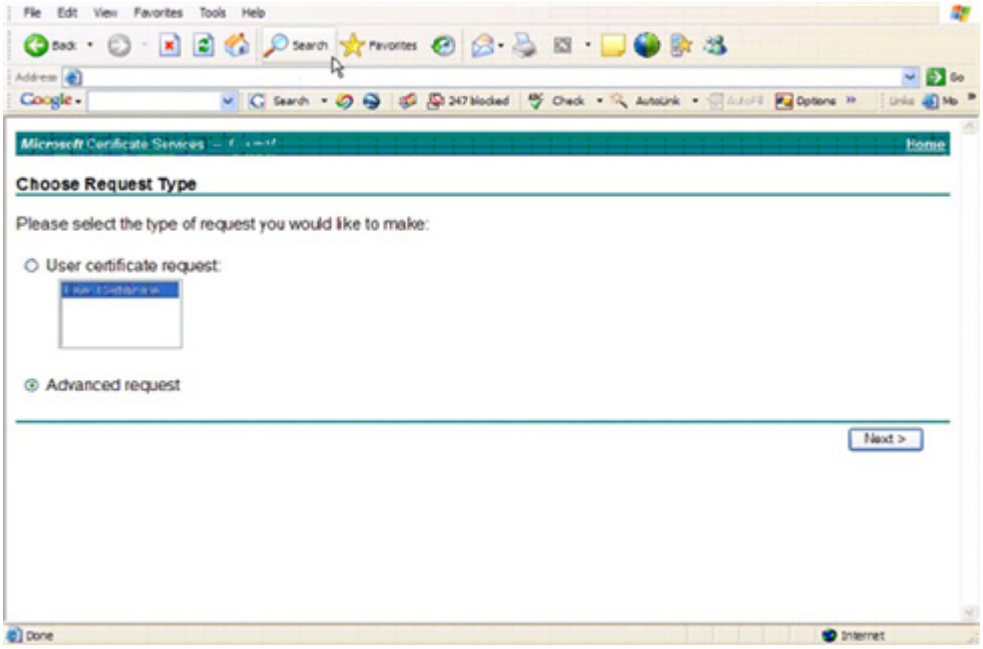
2 **인증서 요청**을 선택하고 **다음**을 클릭합니다.

그림 9-2. Microsoft 인증서 서비스



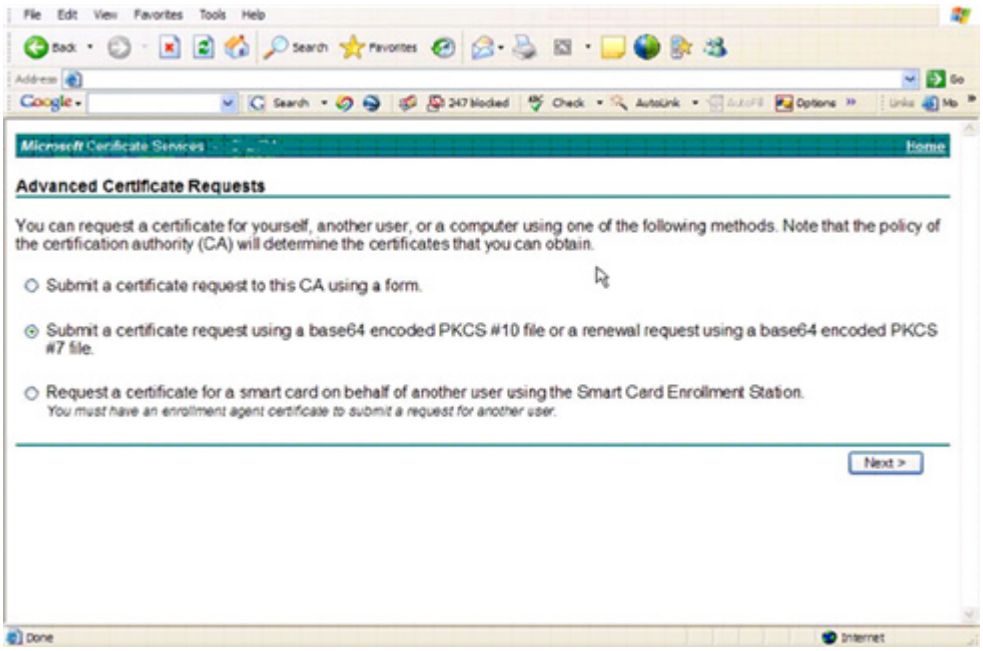
3 **고급 요청**을 선택하고 **다음**을 클릭합니다.

그림 9-3. 요청 유형 선택



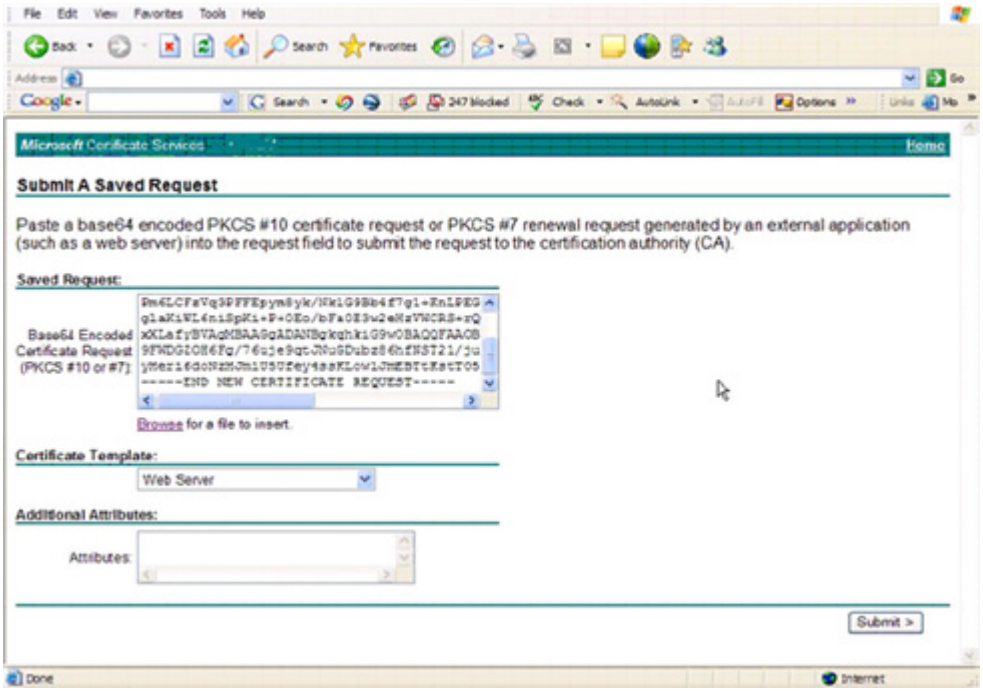
4 Base64로 인코딩된 PKCS #10 파일을 사용하여 인증서 요청을 제출하는 옵션을 선택하고 **다음 >**을 클릭합니다.

그림 9-4. 고급 인증서 요청



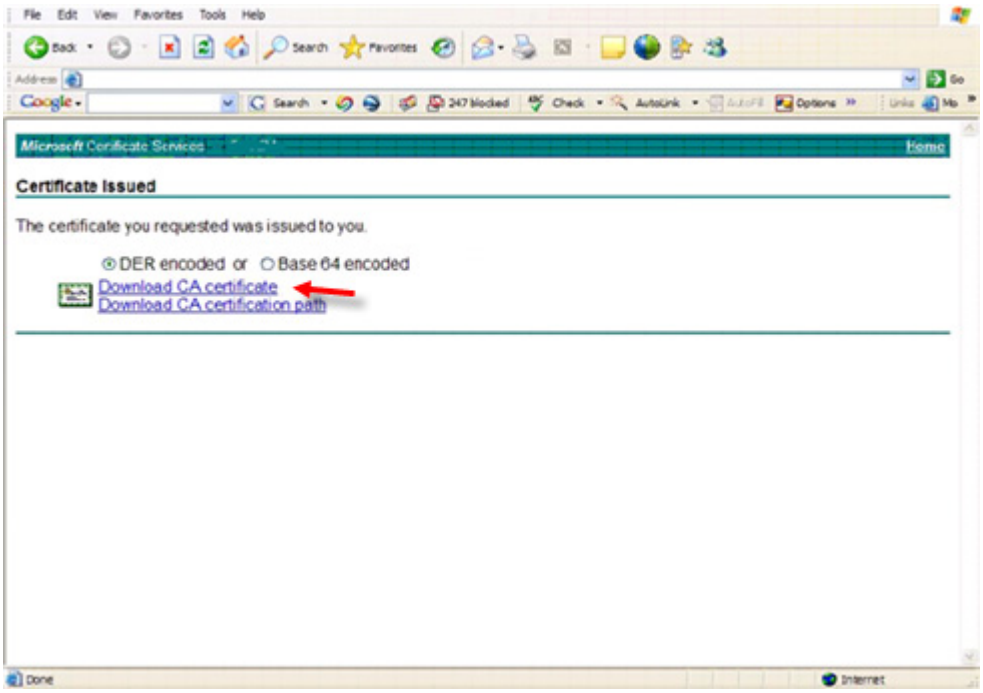
5 텍스트 상자에 CSR 요청의 내용을 붙여 넣습니다. Web Server의 인증서 템플릿을 선택하고 **제출 >**을 클릭합니다.

그림 9-5. 저장된 요청 제출



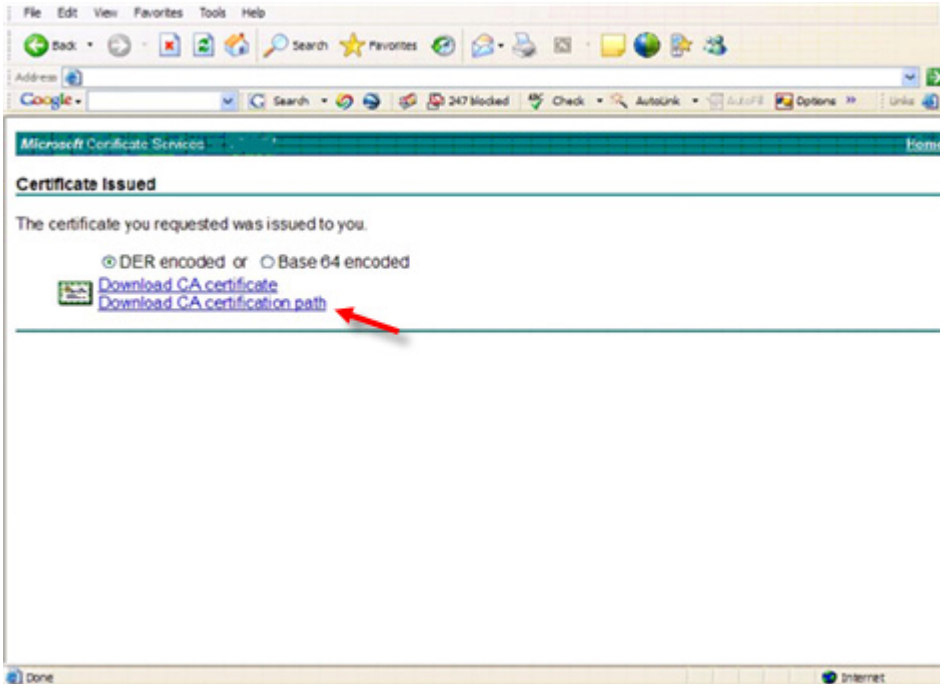
6 인증서를 저장합니다. **DER 인코딩**을 선택하고 **CA 인증서 다운로드**를 클릭합니다.

그림 9-6. CA 인증서 다운로드



7 인증서를 저장합니다. **DER 인코딩**을 선택하고 **CA 인증서 다운로드 경로**를 클릭합니다.

그림 9-7. CA 인증서 다운로드 경로



8 변환된 서명 기관 인증서를 가져옵니다. DOS 창으로 돌아갑니다. 유형:

```
keytool -import -trustcacerts -file <csr 파일 이름> -keystore cacerts
```

9 서명 기관 인증서를 가져왔으므로 서버 인증서를 가져올 수 있습니다(신뢰 체인을 구축할 수 있음). 유형:

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

자체 서명 인증서의 별칭을 사용하여 CSR 요청과 서버 인증서를 연결합니다.

10 cacert 파일 목록에 서버 인증서의 **인증서 체인 길이**가 **2**라는 정보가 표시됩니다. 즉, 자체 서명된 인증서가 아님을 나타냅니다. 유형:

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

체인에서 두 번째 인증서의 인증서 지문은 가져온 서명 기관 인증서(목록의 서버 인증서 아래에도 나열됨)입니다.

서버 인증서와 서명 기관 인증서를 가져왔습니다.


0 XXXXXA0 X