㈜디지털모아

Forefront Client Security 설치 및 배포 가이드

1 Server Topology

이동훈

2007-07-21

목차

1. Forefront Client Security 소개

1.1. Forefront Client Security 란?

1.2. 제품 이점

2. Forefront Client Security 구성

3. Forefront Client Security 설치 준비 사항

3.1. Forefront Client Security 시스템 요구 사항

3.2. 설치를 위한 네트워크 준비

3.3. 설치 및 서비스에 필요한 계정 생성

3.4. 컴퓨터 및 계정 정보 기록

4. 단일 서버 토폴로지 소프트웨어 필수 구성 요소 설치 및 구성

4.1. 단일 서버 토폴로지의 소프트웨어 필수 구성요소

4.2. IIS 및 ASP.NET 설치

4.3. SQL Server 2005 설치

4.4. SQL Server 2005 Service Pack 설치

4.5. MMC 3.0 설치

4.6. GPMC SP1 설치

4.7. WSUS SP1 설치

4.8. WSUS SP1 구성 및 동기화

4.9. Internet Explorer의 로컬 인트라넷 영역에 보고 서버 사이트 추가

5. 단일 서버 토폴로지에 Client Security 설치

5.1. Forefront Client Security 설치

5.2. Forefront Client Security 구성

5.3. 서비스 계정에 대한 올바른 권한 부여

5.4. Client Security 설치 확인

6. Forefront Client Security 배포

6.1. 개요

6.2. 네트워크 배포 준비

6.2.1. 트러스트된 도메인의 클라이언트 컴퓨터

6.2.2. Client Security 구성 요소를 위한 포트 사용법

6.2.3. Windows 방화벽에서 포트 열기

6.3. WSUS의 클라이언트 구성 요소 승인

6.4. 자동 업데이트 구성

6.5. 클라이언트 컴퓨터에 Client Security 배포

6.5.1. 정책 생성

6.5.2. 정책 배포

6.5.3. MOM 서버를 통해 클라이언트 승인

6.6. Client Security 배포 확인

1. Forefront Client Security 소개

1.1. Forefront Client Security 란?

Microsoft Forefront Client Security(이전 이름: Microsoft Client Protection)는 비즈니스 데스크톱, 랩톱 및 서버 운영 체제를 위한 관리와 제어가 간편한 통합 맬웨어 방지 기능을 제공합니다.
전 세계 수 백만명이 이미 사용하고 있는 인증된 Microsoft 보호 기술을 바탕으로 하는 Forefront Client Security는 바이러스, 웜, 트로이 목마 등의 기존 위협뿐 아니라 스파이웨어, 루트 키트 등의 최신 위협까지 방지합니다.
Forefront Client Security는 중앙 관리 방식의 간단한 관리를 제공하고 위협과 취약점에 중요 가시성을 제공함으로써 사용자가 효율적으로 비즈니스를 보호할 수 있도록 도와줍니다.
Forefront Client Security는 Active Directory 등 기존 인프라 소프트웨어에 통합되며 다른 Microsoft 보안 기술을 보완하여 보호 및 제어 기능을 향상시킵니다.

1.2. 제품 이점

Microsoft Forefront Client Security는 다음과 같은 이점을 제공합니다.

• 통합 보호: Forefront Client Security는 최신 맬웨어와 발전하는 맬웨어에 대한 통합 보호 기능을 통해 비즈니스 시스템이 다양한 위협에 대해 보다 나은 보안 체계를 갖추게 됩니다.

• 간단한 관리: Forefront Client Security에서는 중앙 관리 방식을 통해 관리가 간편해지므로 보다 효율적으로 비즈니스를 보호할 수 있습니다.

• 중요 가시성 및 제어: Forefront Client Security는 정보가 풍부하고 우선 순위화된 보안 보고서와 요약 대시보드 보기를 제공하므로 맬웨어와 위협에 대한 가시성과 제어 기능이 확보됩니다.

2. Forefront Client Security 구성

Forefront Client Security는 서버 구성에 따라 6가지 토폴로지로 구성될 수 있습니다.

- 단일 서버 토폴로지
- 2 서버 토폴로지
- 3 서버 토폴로지
- 4 서버 토폴로지
- 5 서버 토폴로지
- 6 서버 토폴로지

*참고 : 이 가이드에서는 단일 서버 토폴로지에서의 Forefront Client Security 구성에 대한 내용을 다루고 있습니다.

3. Forefront Client Security 설치 준비 사항

3.1. Forefront Client Security 시스템 요구 사항

하드웨어	프로세서 및 메모리	운영 체제	소프트웨어	하드 디스크
관리 서버	1GHz 이상의 프로세서 1GB 이상의 RAM 권장	Microsoft Windows Server® 2003 서비스 팩 1(SP1), Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	.NET Framework 2.0 GPMC SP1 MMC 3.0	512MB 이상
컬렉션 서버 (데이터베이스 포함 안 됨)	1-GHz 이상의 프로세서 512MB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	.NET Framework 2.0	1GB 이상
컬렉션 서버 (데이터베이스 포함) 또는 컬렉션 데이터베이스서버	듀얼 2GHz 이상의 프로세서 2GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services 및 워크스테이션 구성 요소 포함)	30GB 이상
보고 서버 (데이터베이스 포함 안 됨)	1-GHz 이상의 프로세서 512MB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Reporting Services) IIS 6.0 및 ASP.NET	512MB 이상
보고 서버 (데이터베이스 포함) 또는 보고 데이터베이스 서버	듀얼 2GHz 이상의 프로세서 2GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services, Integration Services, Reporting Services 및 워크스테이션 구성 요소 포함)	75GB 이상

하드웨어	프로세서 및 메모리	운영 체제	소프트웨어	하드 디스크
배포 서버	WSUS 배포 설계 (http://go.microsoft.com/fwlink/?LinkId=77980)(영문)를 참조하십시오.	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	IIS 6.0 및 ASP.NET .NET Framework 2.0 WSUS 2.0 SP1 데이터베이스 요구 사항은 WSUS 배포 설계 (http://go.microsoft.com/fwlink/?LinkId=77980)(영문)를 참조하십시오.	WSUS 배포 설계 (http://go.microsoft.com/fwlink/?LinkId=77980)(영문)를 참조하십시오.
함께 제공: 관리 서버, 컬렉션 서버 및 보고 서버	듀얼 2.85GHz 이상의 프로세서 4GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services, Integration Services, Reporting Services 및 워크스테이션 구성 요소 포함) .NET Framework 2.0 GPMC SP1 WSUS 2.0 SP1 IIS 6.0 및 ASP.NET MMC 3.0	100GB 이상
함께 제공: 컬렉션 데이터베이스 및 보고 데이터베이스	듀얼 2.85GHz 이상의 프로세서 4GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services, Integration Services, Reporting Services 및 워크스테이션 구성 요소 포함)	100GB 이상

하드웨어	프로세서 및 메모리	운영 체제	소프트웨어	하드 디스크
함께 제공: 단일 서버 운영 토폴로지 (하나의 서버에 모든 구성 요소)	듀얼 2.85GHz 이상의 프로세서 4GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services, Integration Services, Reporting Services 및 워크스테이션 구성 요소 포함) .NET Framework 2.0 GPMC SP1 WSUS 2.0 SP1 IIS 6.0 및 ASP.NET MMC 3.0	100GB 이상
함께 제공: 단일 서버 평가 토폴로지 (하나의 서버에 모든 구성 요소)	1-GHz 이상의 프로세서 1GB 이상의 RAM	Windows Server 2003 SP1, Standard Edition 또는 Enterprise Edition **x64 버전은 지원되지 않음**	SQL Server 2005 SP1 Enterprise Edition 또는 Standard Edition (Database Services, Integration Services, Reporting Services 및 워크스테이션 구성 요소 포함) .NET Framework 2.0 GPMC SP1 WSUS 2.0 SP1 IIS 6.0 및 ASP.NET MMC 3.0	6GB 이상
클라이언트 컴퓨터	700MHz 이상의 프로세서 256MB 이상의 RAM	Microsoft Windows® 2000 Server SP4 및 업데이트 롤업 1 Windows XP 서비스 팩 2(SP2) Windows Server 2003 SP1 Windows Vista™ Business, Enterprise 또는 Ultimate 클라이언트 컴퓨터에 지원되는 x64 버전	Windows Update Agent 2.0 Windows Installer 3.1	350MB 이상

3.2. 설치를 위한 네트워크 준비

Client Security 서버 구성 요소를 설치하기 전에 서버 방화벽에 적절한 네트워크 포트가 열려 있는지 확인해야 합니다. 경우에 따라 Client Security 서버 간에 방화벽을 사용하지 말아야 합니다.

다음 표에는 Client Security 서버 간과 배포 서버 및 Microsoft Update 간의 통신에 사용되는 네트워크 포트와 프로토콜이 나열되어 있습니다. 사용하는 방화벽의 유형과 위치에 따라 이러한 포트를 열어야 할 수 있습니다.

구성 요소	연결	토폴로지	포트(프로토콜)	참고
컬렉션 서버	컬렉션 데이터베이스	5 서버 및 6 서버	1433 (TCP 및 UDP)	없음.
관리 서버	컬렉션 서버	4 서버, 5 서버, 6 서버	445(TCP 및 UDP), 135(TCP) 및 DCOM 포트 범위	이러한 두 서버 간의 방화벽 사용이 지원되지 않습니다. 관리 서버의 MOM(Microsoft Operations Manager) 관리자 및 운영자 콘솔은 컬렉션 서버에 대한 연결이 필요합니다.
관리 서버	컬렉션 데이터베이스	4 서버, 5 서버, 6 서버	1433(TCP) 및 1434(UDP)	없음.
관리 서버	보고 서버	3 서버, 4 서버, 5 서버 및 6 서버	80(TCP) 또는 443(TCP)	포트 80은 HTTP에 사용되고 포트 443은 HTTPS에 사용됩니다.
보고 데이터베이스	컬렉션 데이터베이스	3 서버, 4 서버 및 6 서버	1433(TCP) 및 1434(UDP)	이러한 두 서버 간의 방화벽 사용은 지원되지 않습니다.
보고 서버	컬렉션 데이터베이스	4 서버, 5 서버, 6 서버	1433(TCP) 및 1434(UDP)	없음.
보고 서버	보고 데이터베이스	3 서버, 5 서버 및 6 서버	1433(TCP) 및 1434(UDP)	없음.
배포 서버	Microsoft Update 또는 업스트림 WSUS 서버	모두	80(TCP) 또는 443(TCP)	배포 서버는 Microsoft Update에서 업데이트를 얻기 위해 HTTP에 포트 80을 사용하고 HTTPS에 포트 443을 사용합니다.

3.3. 설치 및 서비스에 필요한 계정 생성

Client Security를 설치하기 전에 적절한 설치 및 서비스 계정을 만들고 여기에 필요한 권한을 할당해야 합니다. 대부분의 경우 Client Security는 설치 중에 권한을 서비스 계정에 자동으로 할당합니다. 그러나 작업 계정의 경우 컬렉션 서버에 대한 로컬 관리자 권한을 부여해야 합니다

설치 계정

Client Security를 설치 및 배포하기 전에 설치 및 설치 확인을 위한 적절한 설치 계정을 만들어야 합니다. 이 계정은 모든 서버의 로컬 관리자 계정이어야 합니다.

Client Security를 클라이언트 컴퓨터에 배포하려면 정책 생성, 편집 및 배포 권한이 있는 계정을 사용해야 합니다.

서비스 계정

Client Security 및 관련 소프트웨어 필수 구성 요소 설치 중 서비스 계정에 대한 정보를 입력해야 합니다. Client Security를 설치한 후에는 권한을 수동으로 부여해야 합니다.

모든 Client Security 서비스 계정에 단일 도메인 사용자 계정을 사용하는 것이 좋습니다.

계정	유형	설명
DAS (Data Access Server) 계정	컬렉션 서버의 도메인 사용자 및 로컬 관리자(경우에 따라)	작업 계정에 DAS 계정을 다시 사용할 경우 컬렉션 서버에 대한 로컬 관리자 권한을 DAS 계정에 부여해야 합니다. 컬렉션 서버는 DAS 계정을 사용하여 컬렉션 데이터베이스에 액세스합니다. Client Security는 설치 중 DAS 계정에 권한을 자동으로 부여합니다.
보고 계정	도메인 사용자	보고 서버는 보고 계정을 사용하여 보고 데이터베이스 및 컬렉션 데이터베이스에 액세스합니다.
작업 계정	컬렉션 서버의 도메인 사용자 및 로컬 관리자	작업 계정은 컬렉션 서버에 대한 로컬 관리자 계정이여야 합니다. 작업 계정에 이러한 권한을 부여하거나 작업 계정에 DAS 계정을 다시 사용할 경우 DAS 계정에 이러한 권한을 부여해야 합니다. 컬렉션 서버는 작업 계정을 사용하여 서버측 스크립트 및 보안 상태 평가 검사를 실행합니다. 작업 계정은 도메인 사용자 계정이어야 합니다.

계정	유형	설명
DTS (Data Transformation Services) 계정	도메인 사용자	보고 서버는 데이터를 컬렉션 데이터베이스에서 보고 데이터베이스로 전송하는 Windows 스케줄러 작업(DTS 작업)을 실행하는 데 DTS 계정을 사용합니다.

3.4. 컴퓨터 및 계정 정보 기록

Client Security를 설치하기 전에 다음 정보를 기록해야 합니다. 이는 다중 서버 토폴로지의 경우 특히 중요합니다

항목	설명	메모
관리 서버	서버 이름	
컬렉션 서버	서버 이름	
컬렉션 데이터베이스	서버 이름 및 SQL Server 인스턴스 이름(기본값이 아닌 경우)	
보고 서버	서버 이름	
보고 데이터베이스	서버 이름 및 SQL Server 인스턴스 이름(기본값이 아닌 경우)	
배포 서버	서버 이름	
DAS 계정	도메인 사용자 계정 필요	
DTS 계정	도메인 사용자 계정 필요 (권장 사항: DAS 계정 다시 사용)	
보고 계정	도메인 사용자 계정 필요 (권장 사항: DAS 계정 다시 사용)	
작업 계정	도메인 사용자 계정 필요 (권장 사항: DAS 계정 다시 사용)	
관리 그룹 이름	Client Security 설치 중 정의됨	
보고 서버 URL	SQL Server 2005 설치 중 정의됨 (기본값: http://*reportingservername*/ReportServer)	
보고서 관리자 URL	SQL Server 2005 설치 중 정의됨 (기본값: http://*reportingservername*/Reports)	
컬렉션 데이터베이스의 크기	Client Security 설치 중 정의됨	
보고 데이터베이스의 크기	Client Security 설치 중 정의됨	
WSUS 관리 URL	WSUS 설치 시 생성됨	
WSUS 클라이언트 구성 URL	WSUS 설치 시 생성됨	

4. 단일 서버 토폴로지 설치 과정

4.1. 단일 서버 토폴로지의 소프트웨어 필수 구성요소

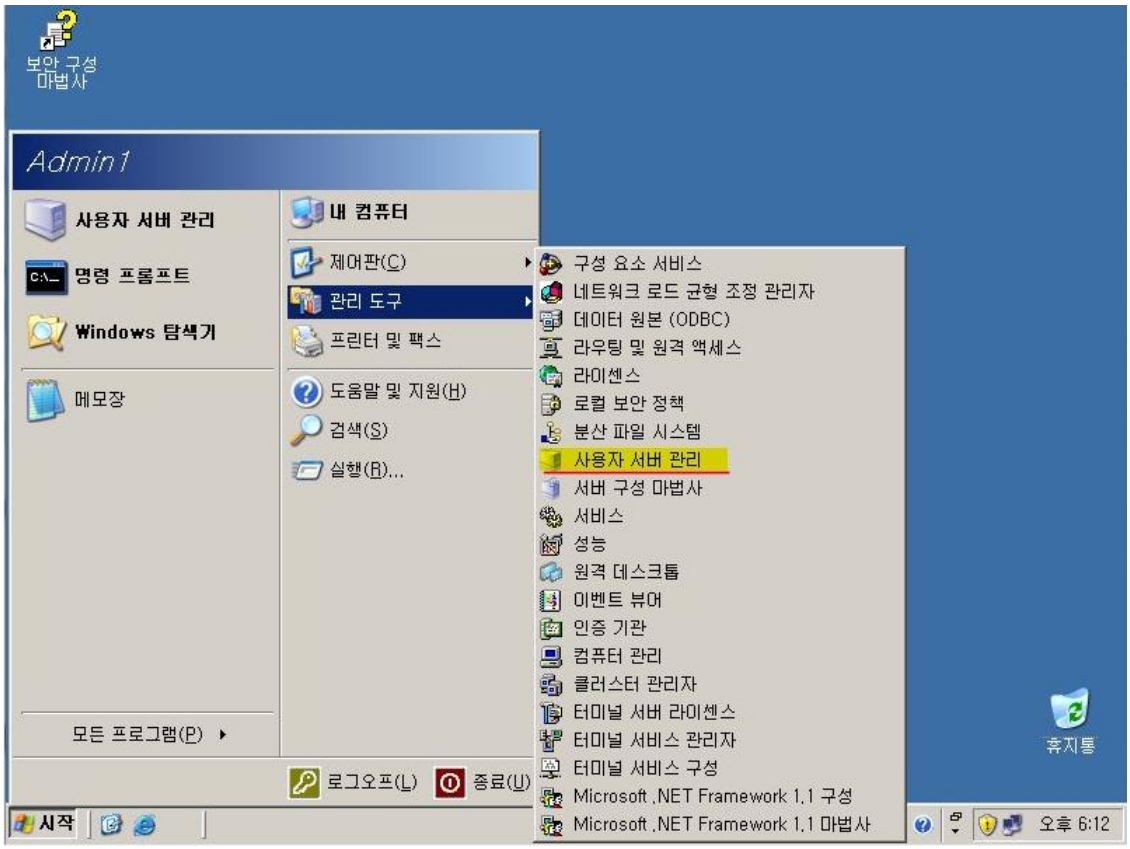
- IIS 및 ASP.NET
- SQL Server 2005 SP2 또는 SP1
- MMC 3.0
- GPMC SP1
- WSUS SP1

*참고 사항

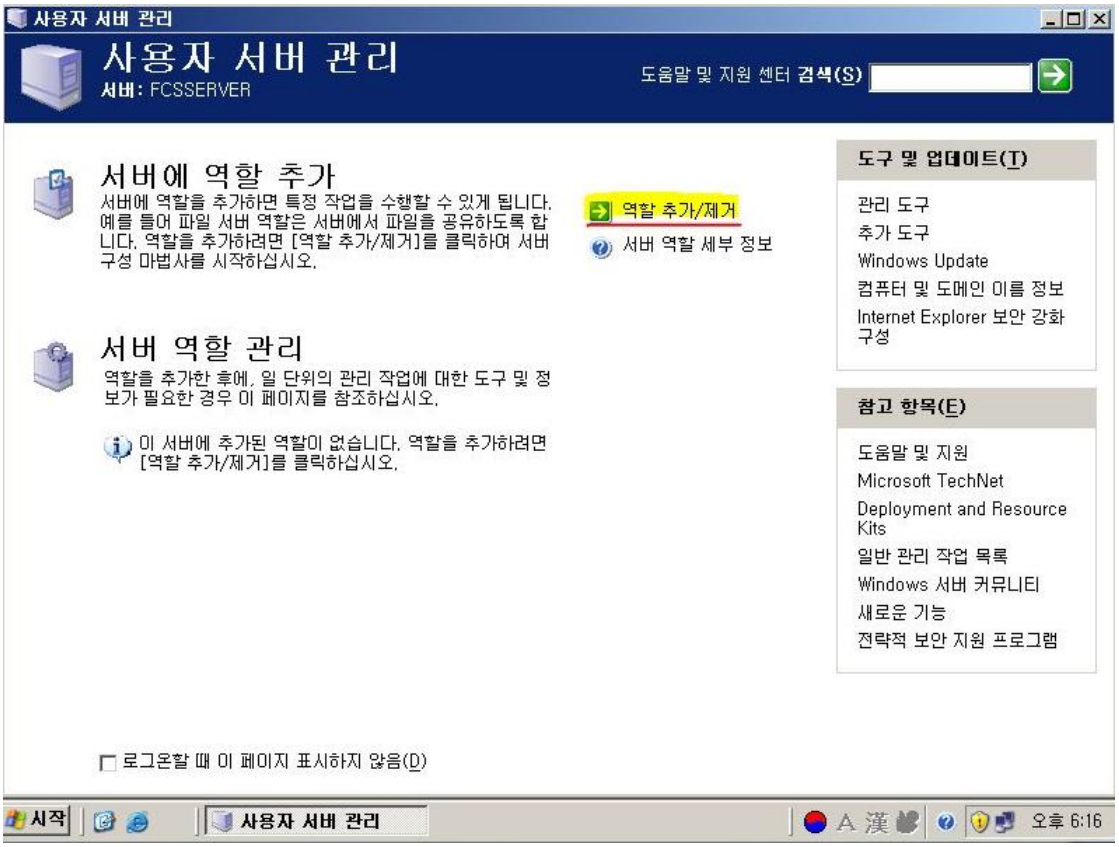
필수 구성요소를 설치하기 전에 서버가 하드웨어 및 운영 체제 요구사항을 만족하고, 모든 중요한 컴퓨터 및 보안 업데이트를 설치했는지 확인하십시오.

4.2. IIS 및 ASP.NET 설치

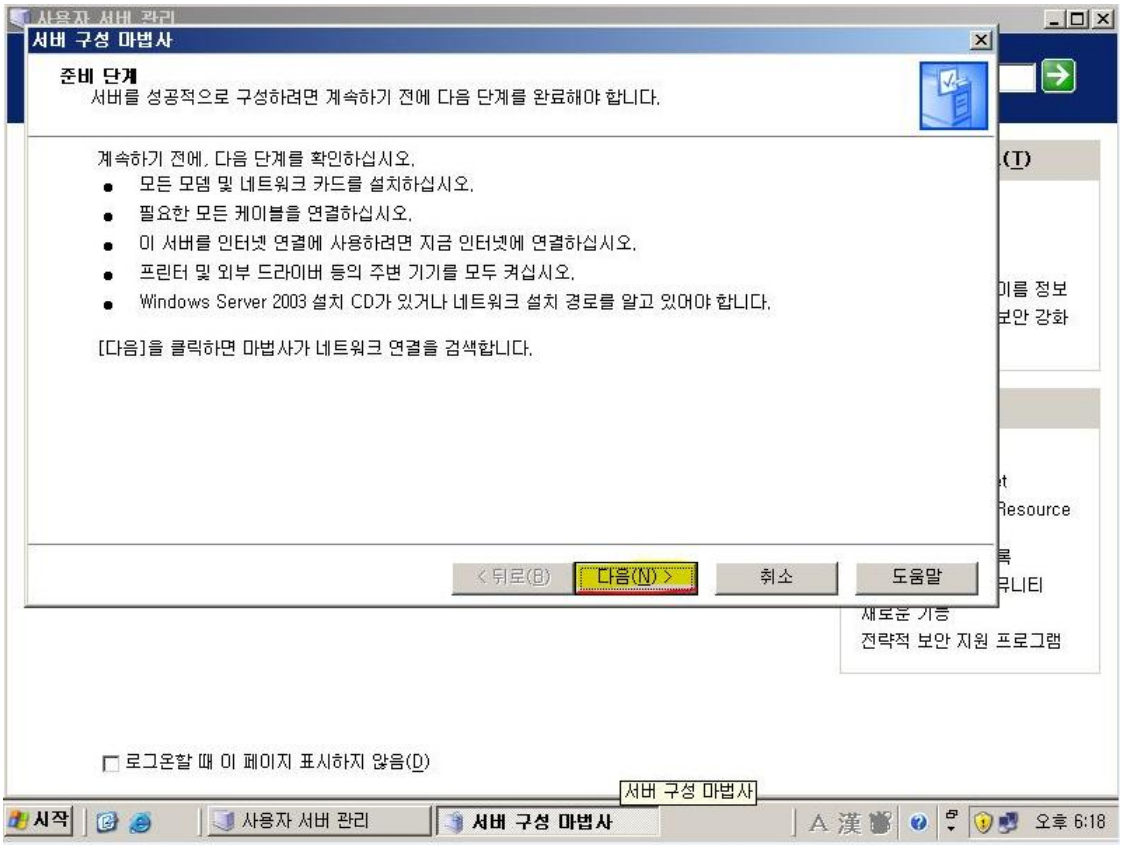
1. 시작 -> 관리 도구 -> 사용자 서버 관리



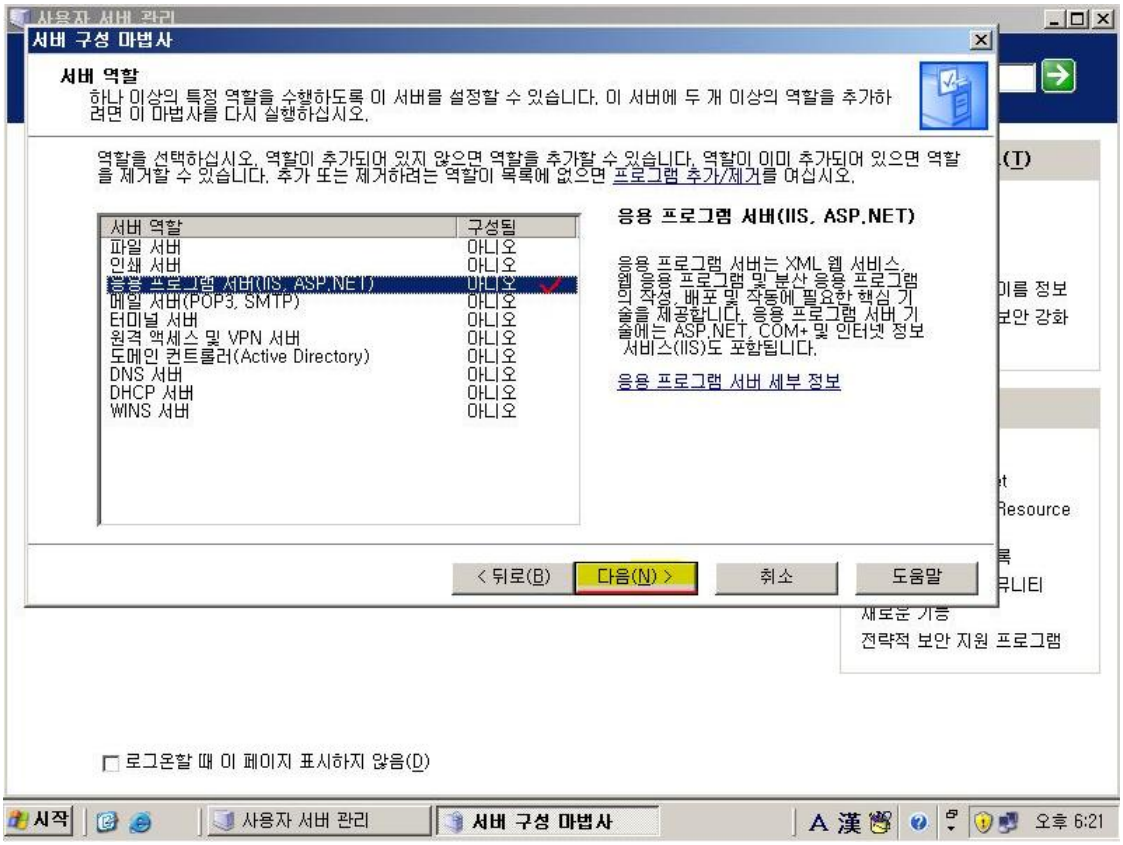
2. 역할 추가/제거 클릭



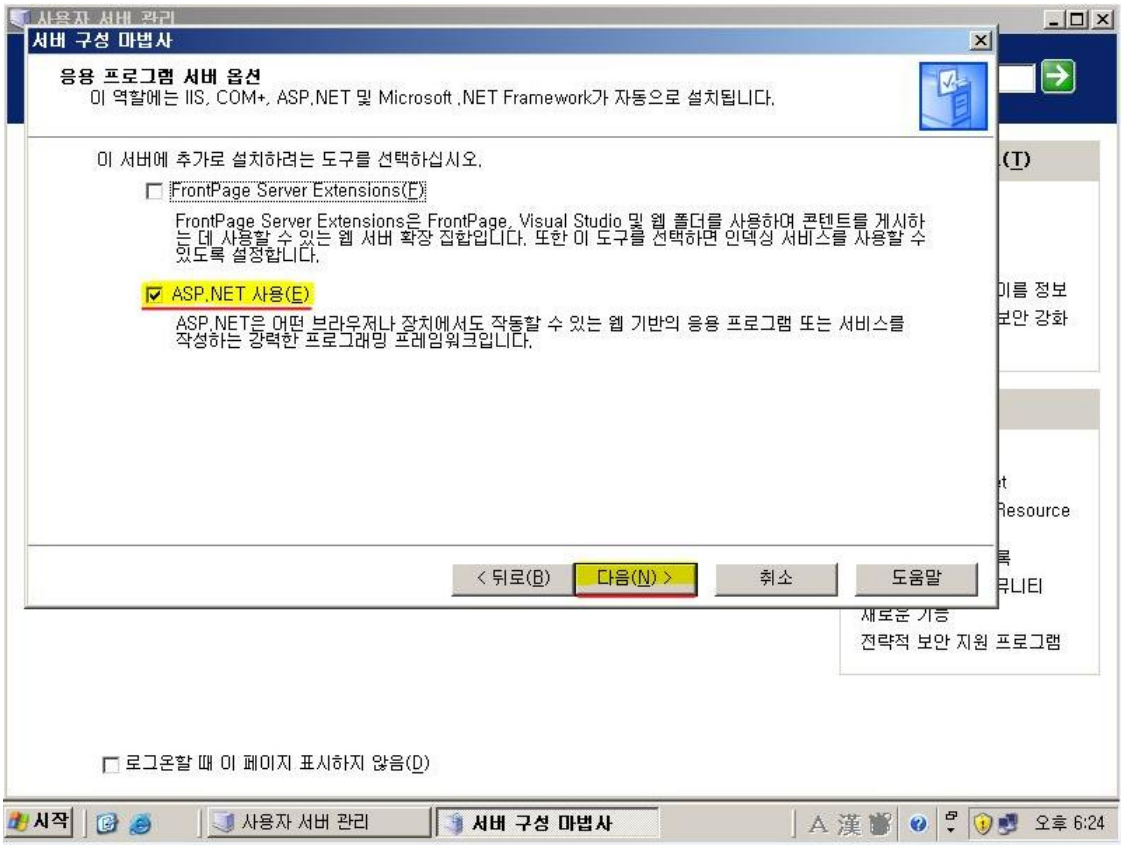
3. 다음 클릭



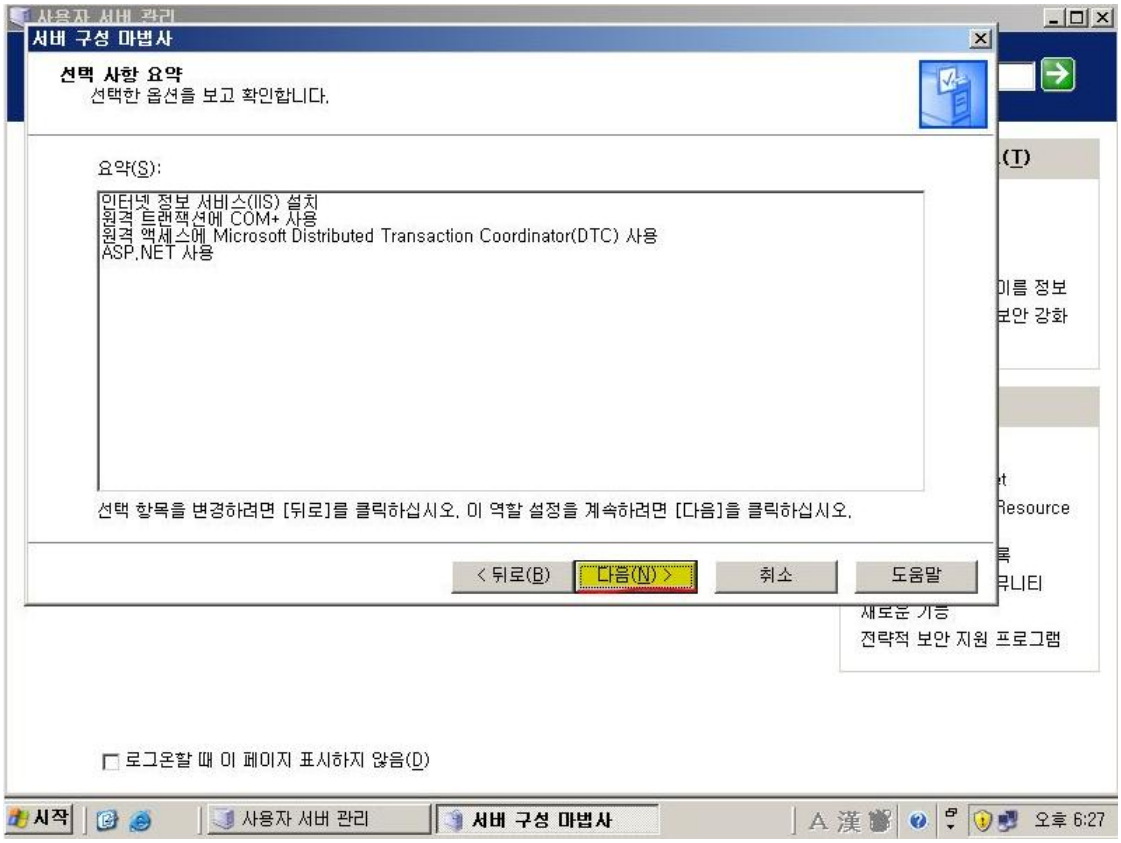
4. 응용 프로그램 서버(IIS, ASP.NET) 선택 후 다음



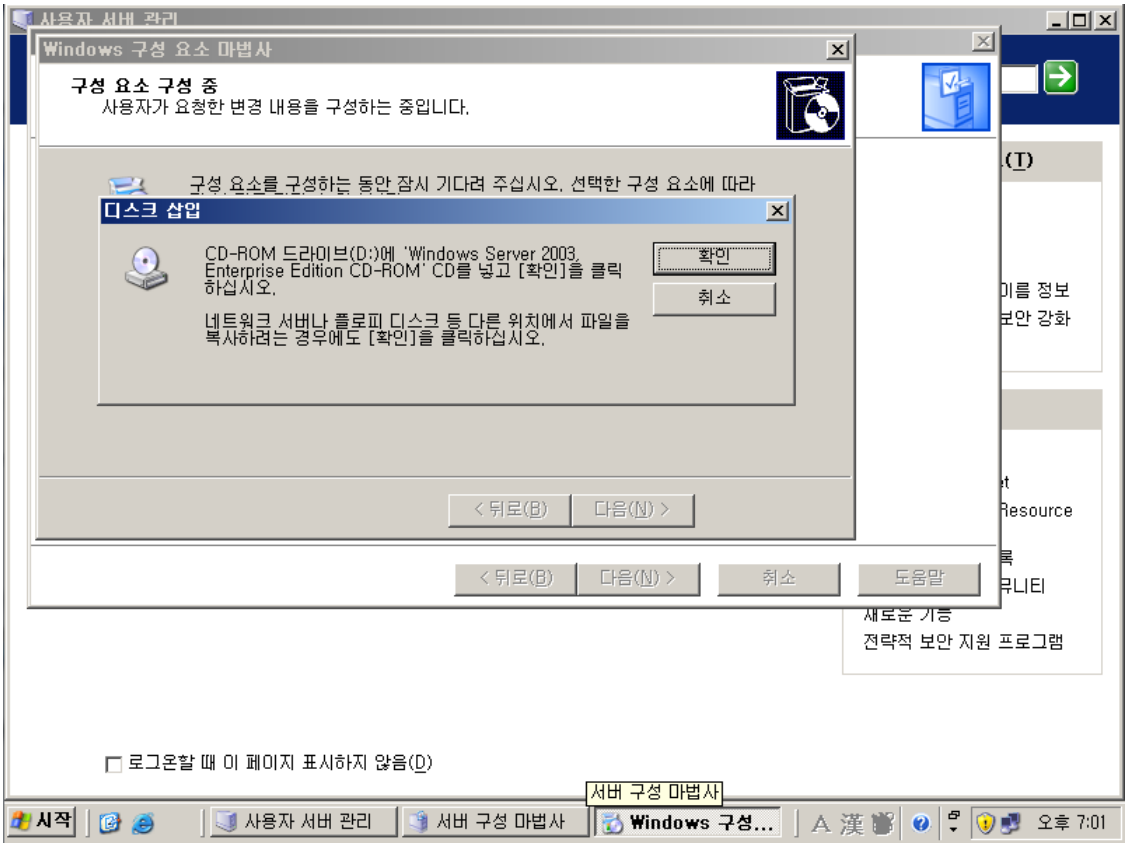
5. ASP.NET 사용(E) 체크 후 다음



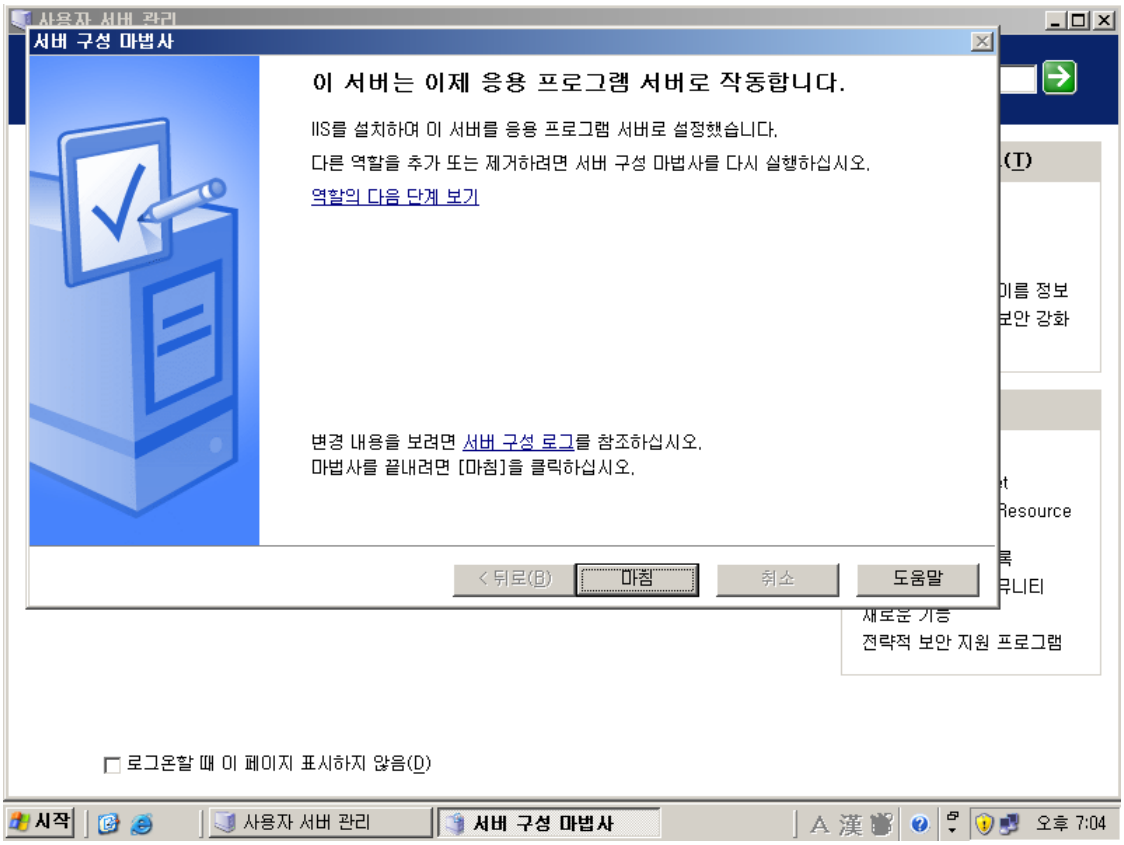
6. 선택 사항 요약 확인 후 다음



7. 운영 체제 CD 삽입



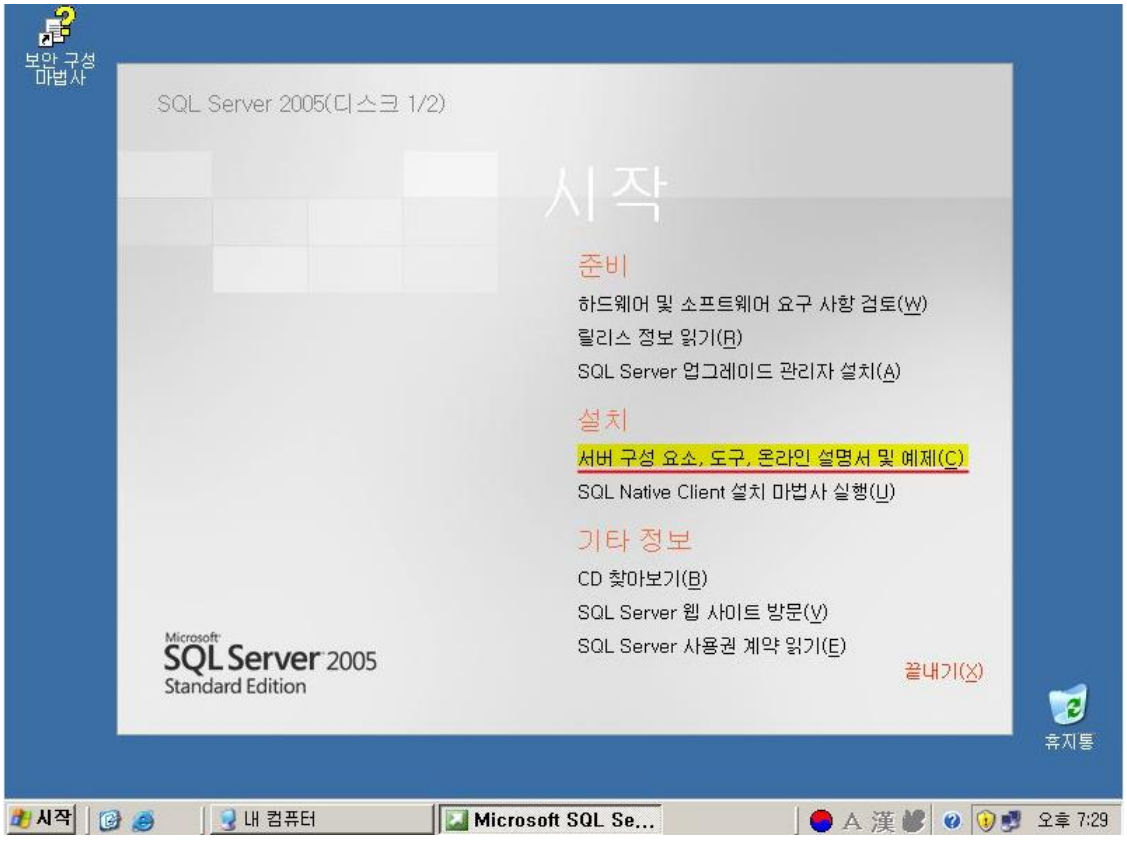
8. 마침



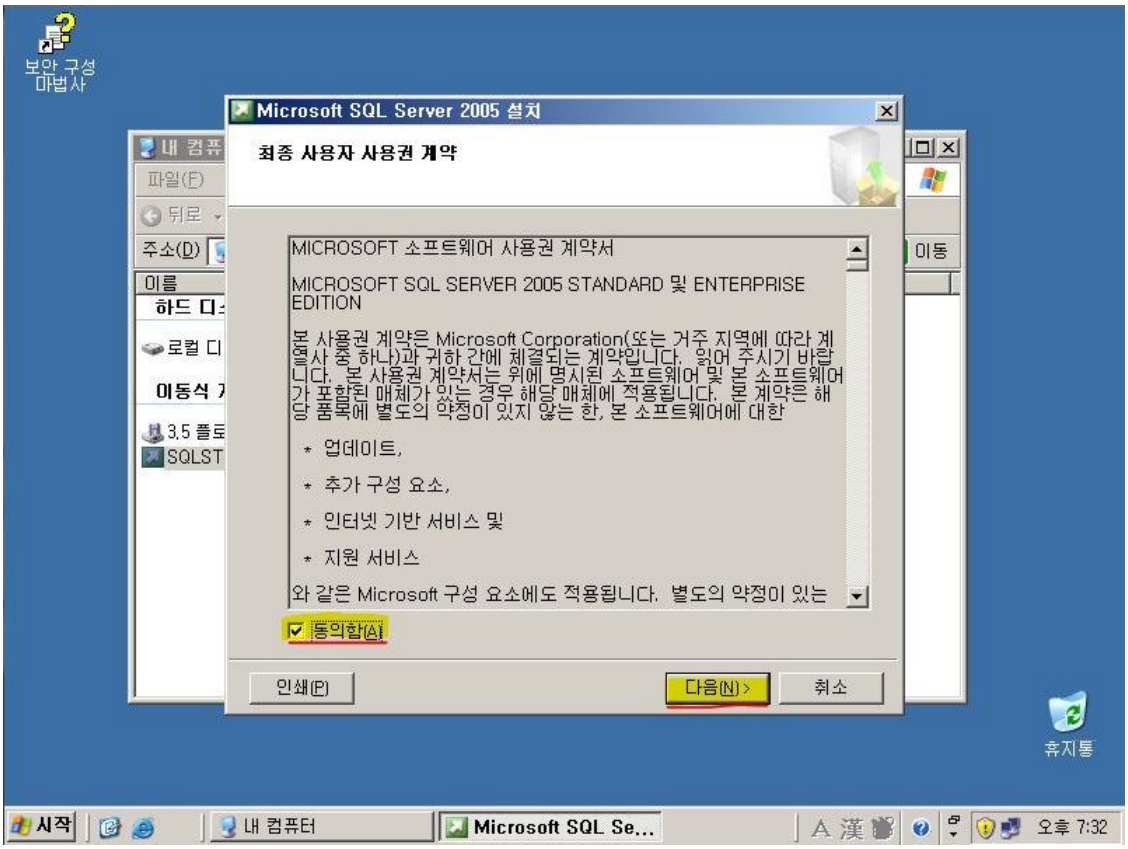
4.3. SQL Server 2005 설치

기존 설치된 SQL Server를 사용하려면 Client Security 설치 마법사를 실행할 때 서버 위치를 입력하십시오. 단, SQL Server 2005 SP2 또는 SP1을 사용해야 합니다. 또한 기존의 SQL Server에는 OnePoint 또는 SystemCenterReporting 데이터베이스가 없어야 합니다. (이 데이터베이스는 Client Security를 설치하는 중에 생성됩니다.)

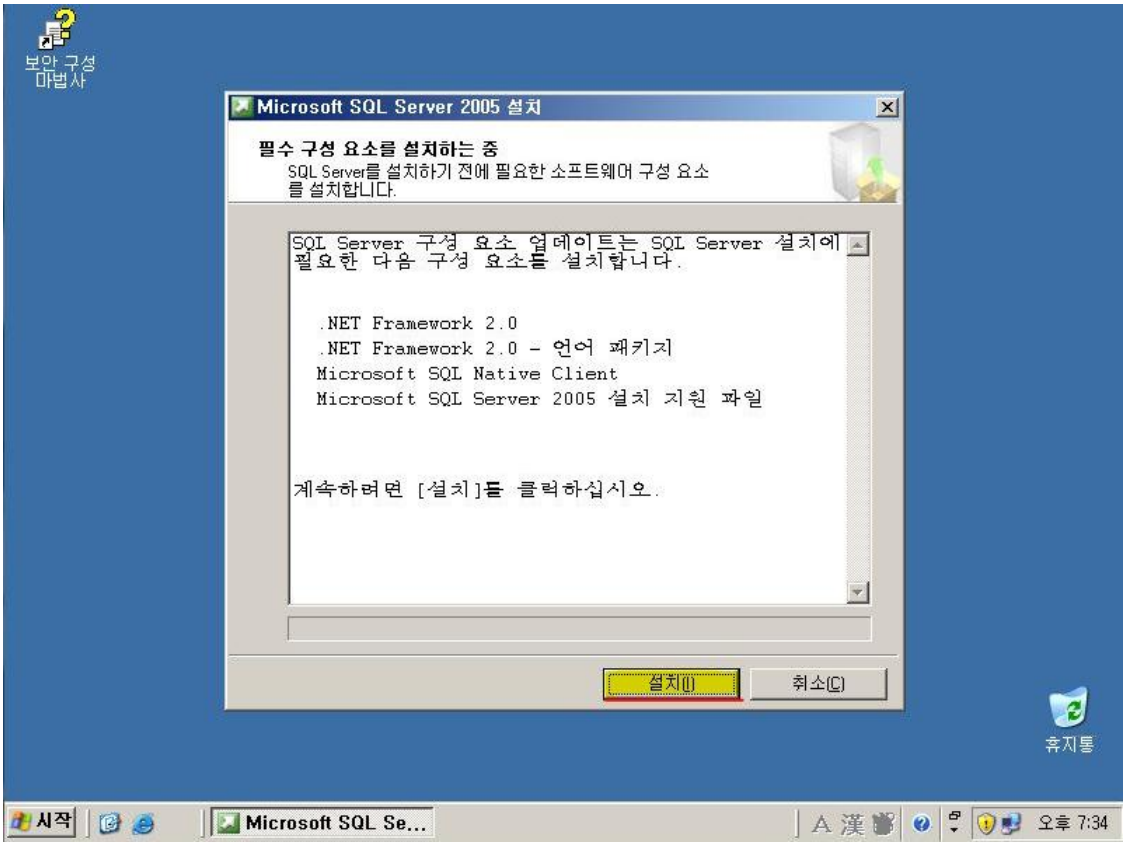
1. SQL Server 2005 설치



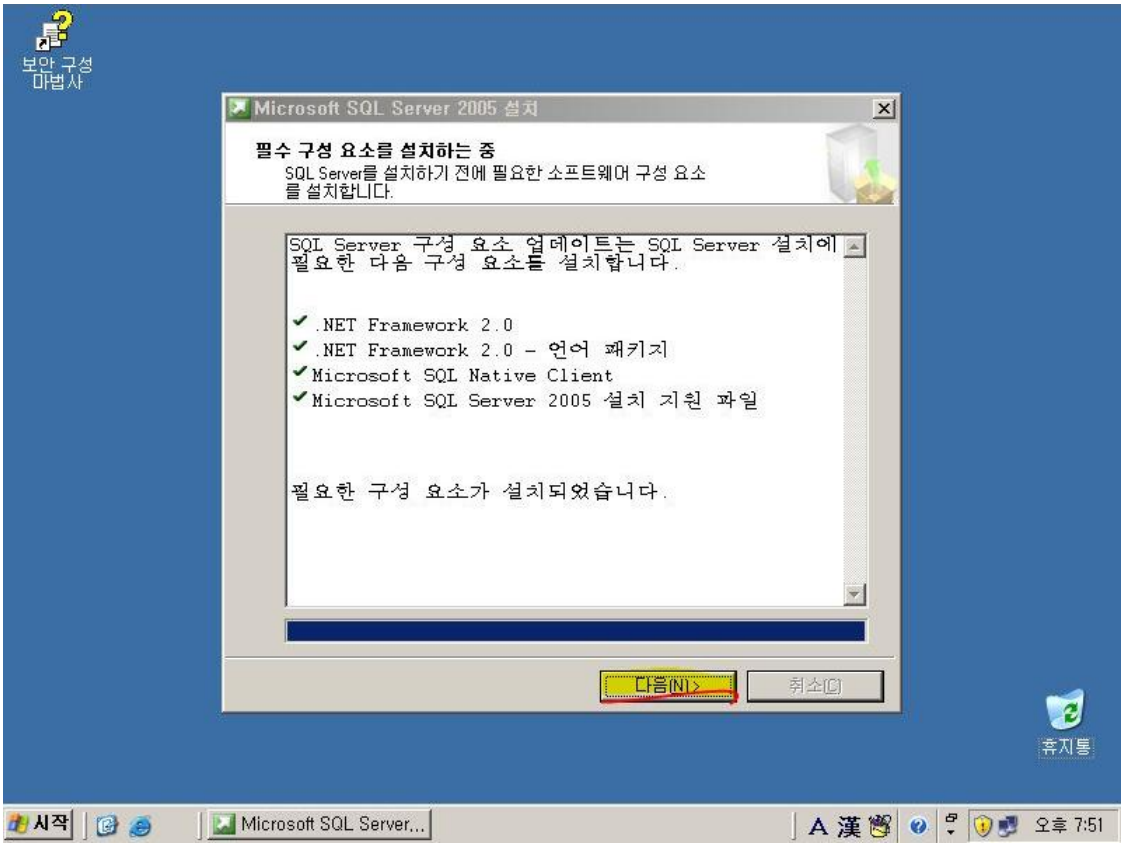
2. 동의함 체크 후 다음



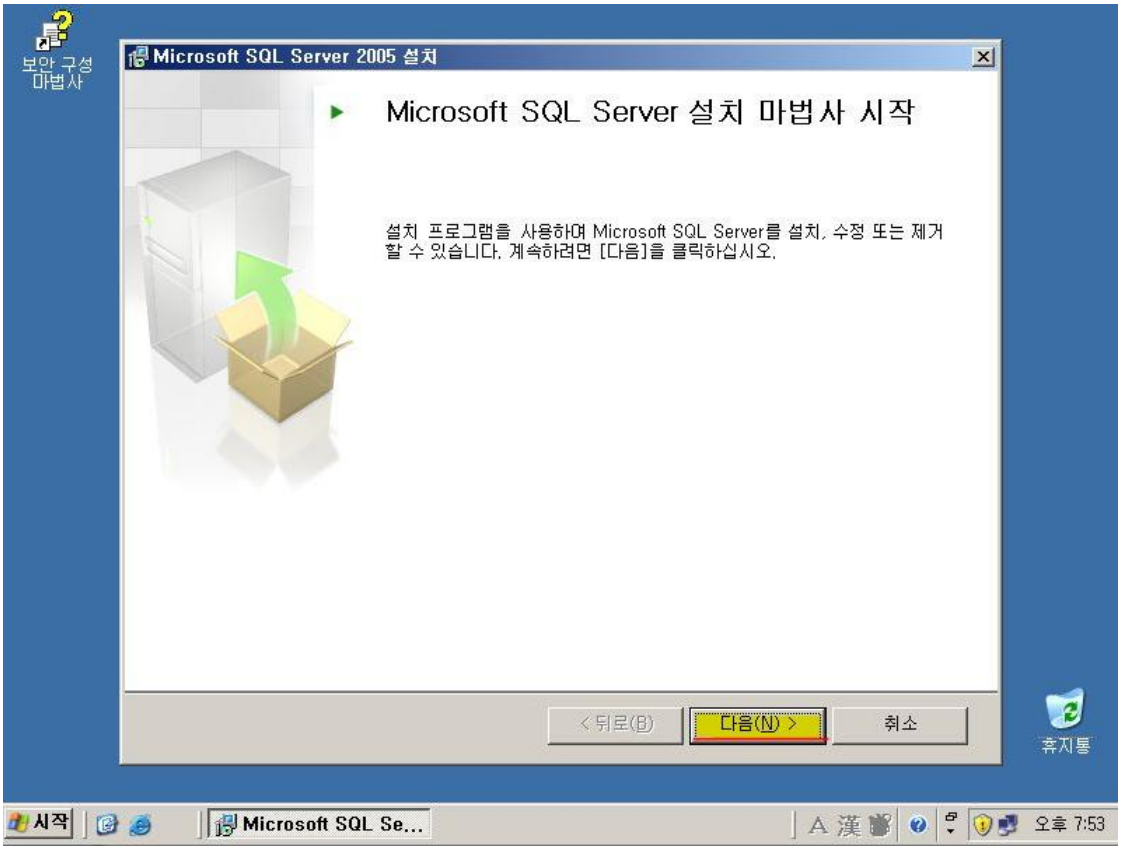
3. 필수 구성 요소 설치



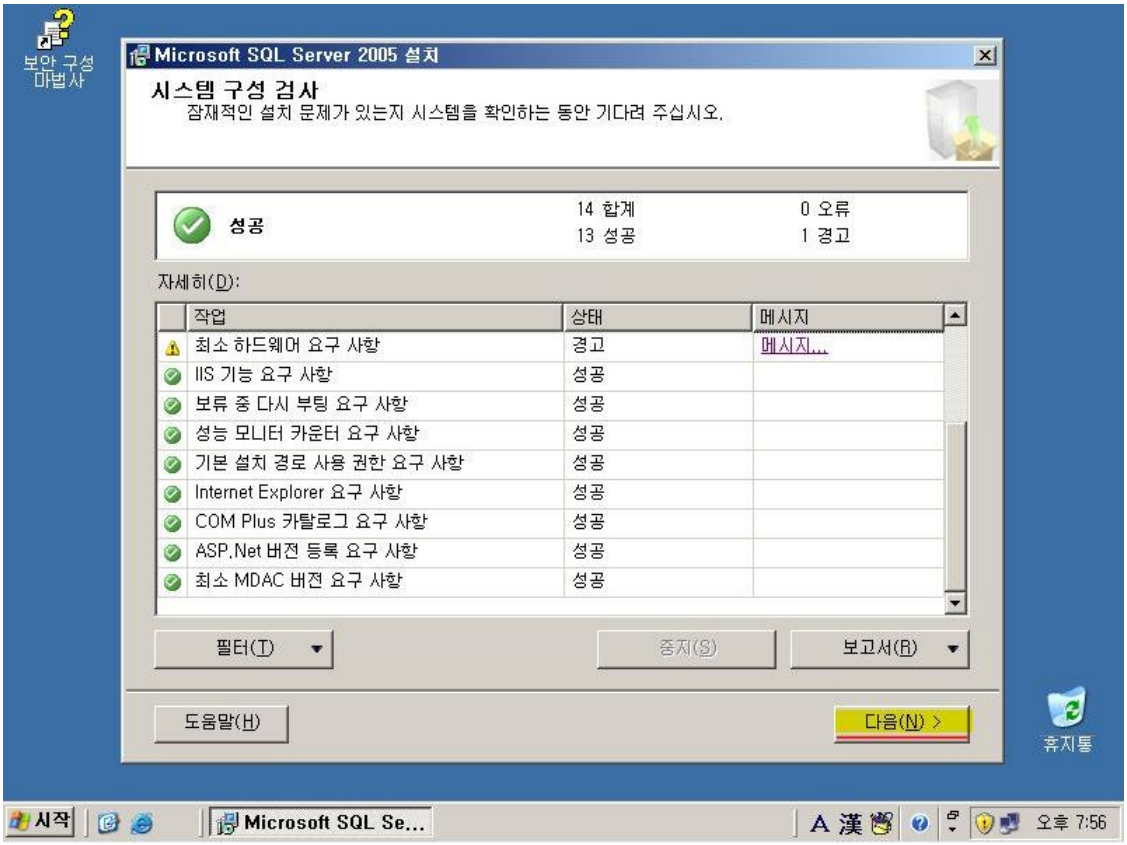
4. 다음



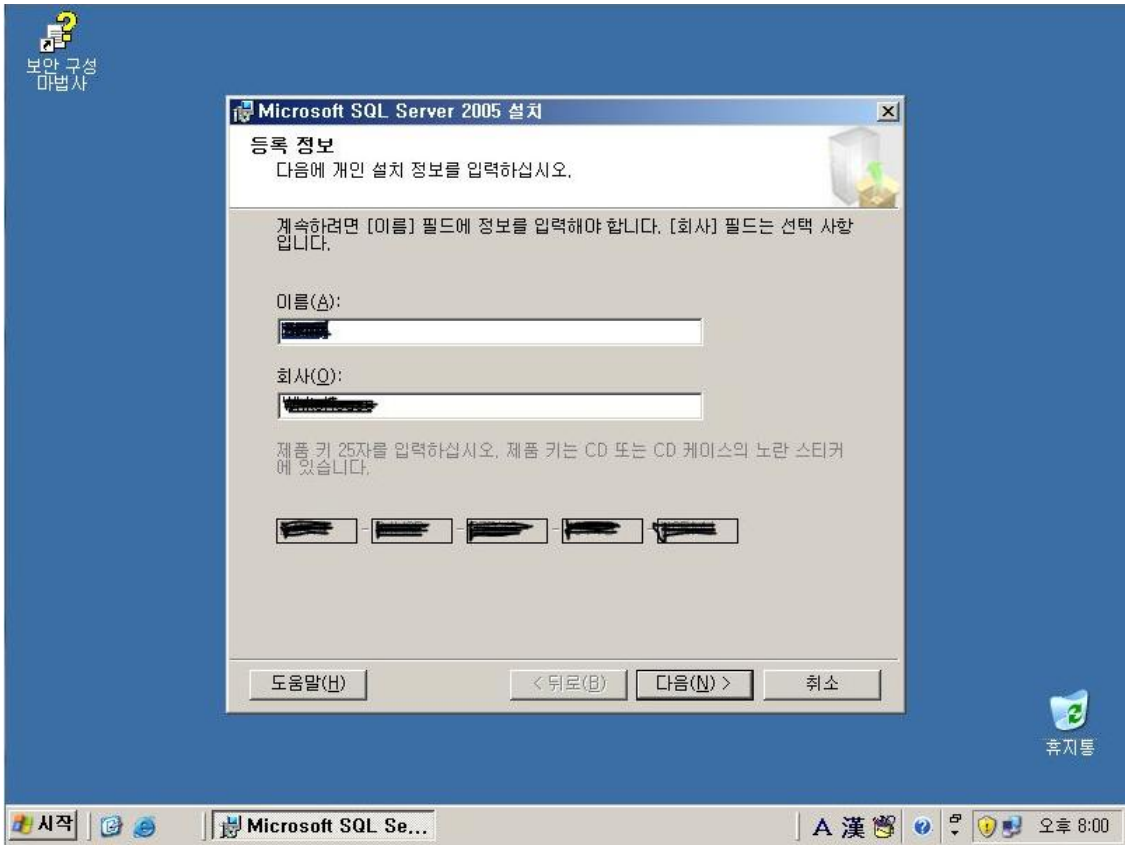
5. Microsoft SQL Server 설치 마법사 시작 화면 – 다음



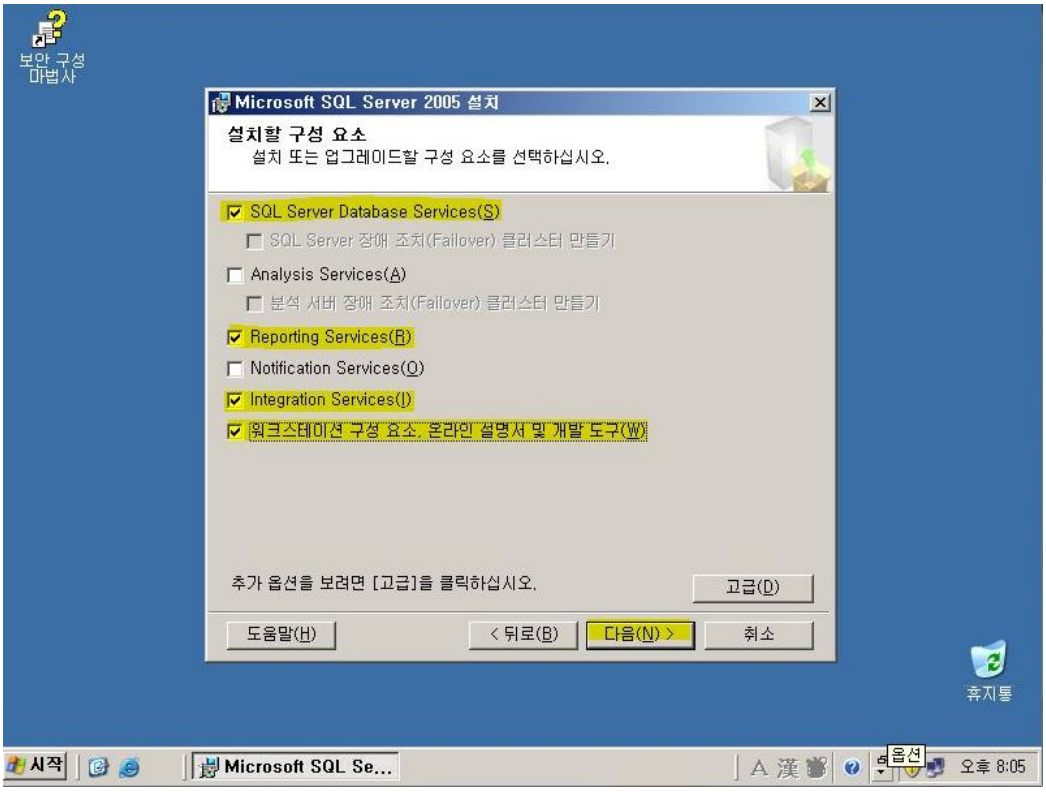
6. 시스템 구성 검사 화면 – 다음



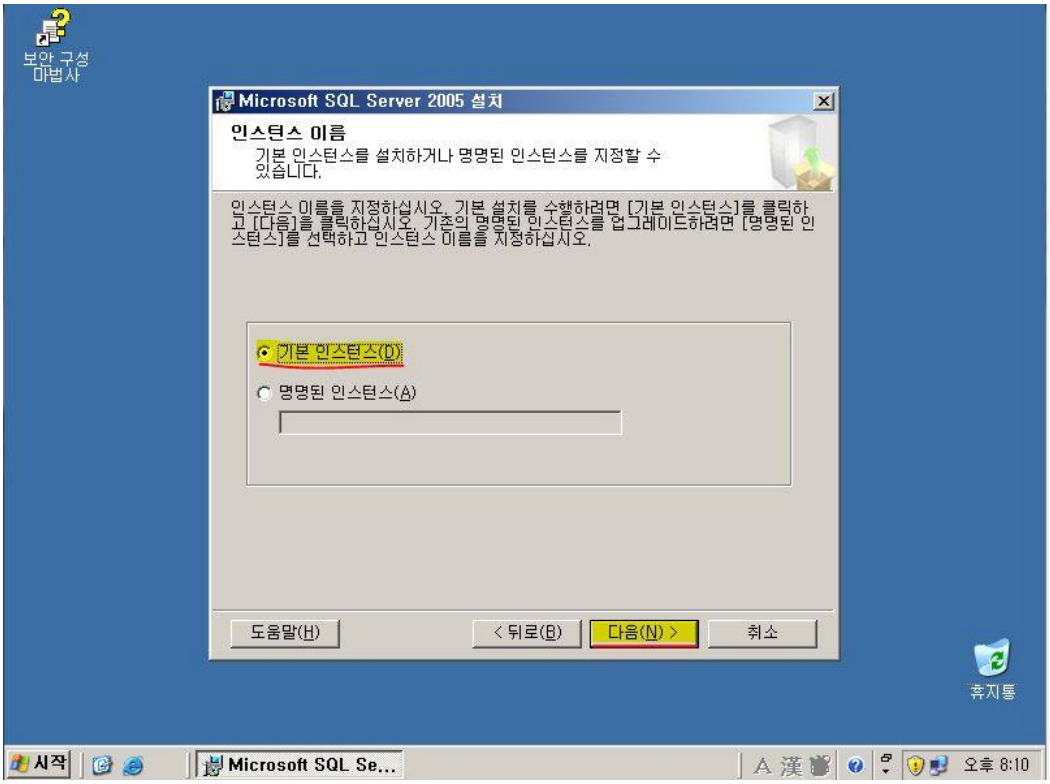
7. 등록 정보 입력 후 다음



8. 설치 구성 요서 선택 - SQL Server Database Services(S), Reporting Services(R), Integration Services(I), 워크스테이션 구성 요소, 온라인 설명서 및 개발 도구(W) 선택 후 다음

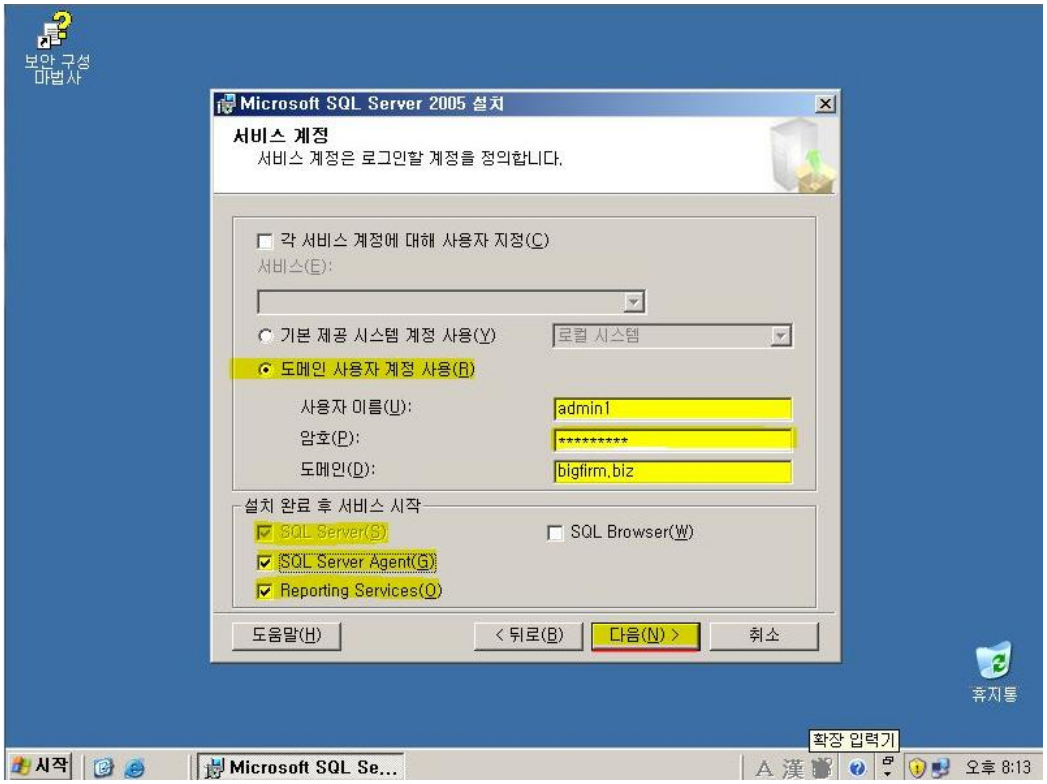


9. 기본 인스턴스 선택 후 다음

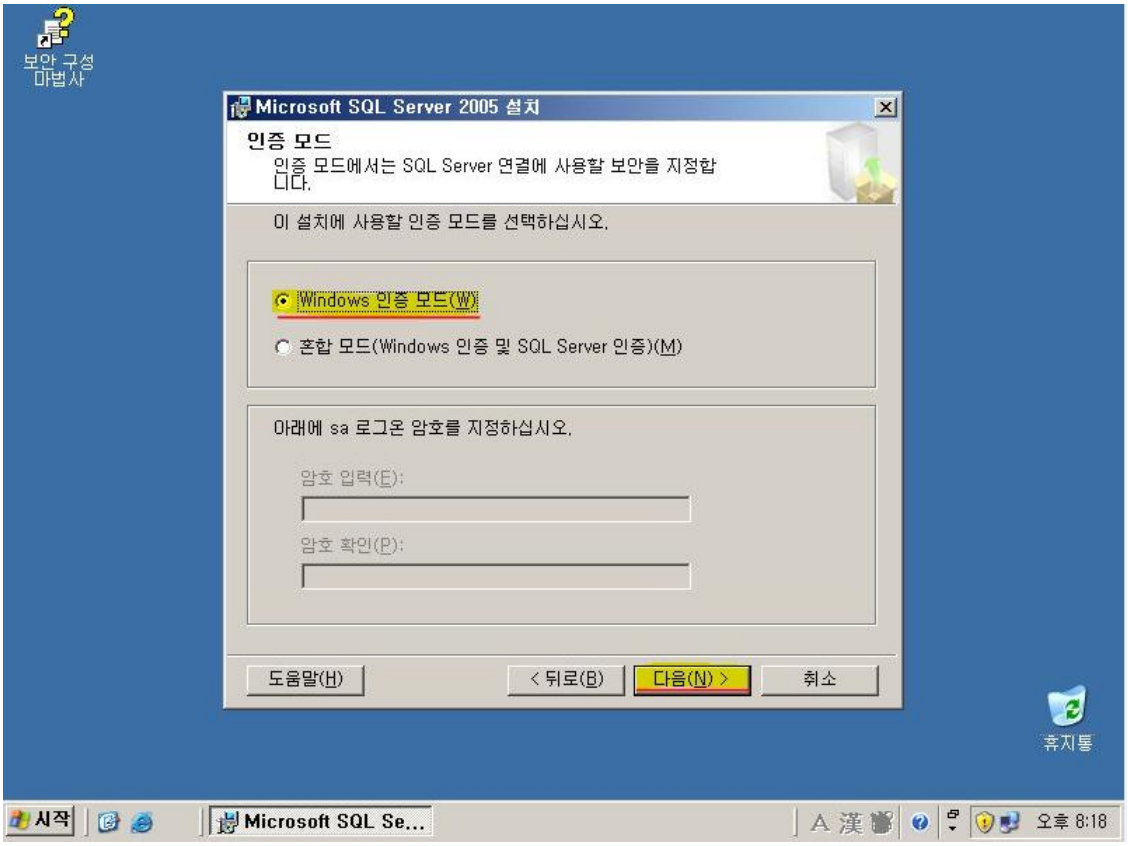


10. 서비스 계정 등록

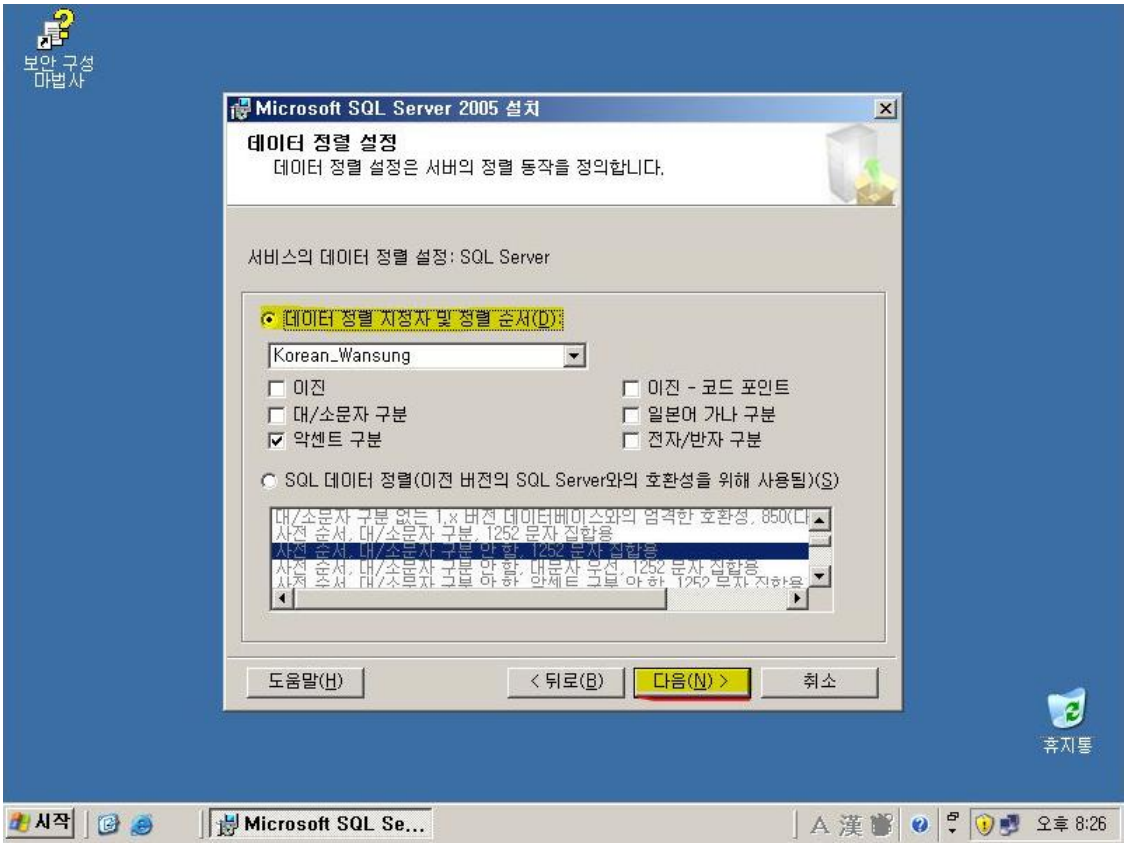
- 도메인 사용자 계정 사용에 체크 ,사용자 이름, 암호, 도메인 입력
- 설치 완료 후 서비스 시작에서 SQL Server, SQL Server Agent, Reporting Services 체크 후 다음



11. Windows 인증 모드(W) 선택 후 다음 (Windows 인증 모드가 혼합 모드 보다 보안상 안전함)

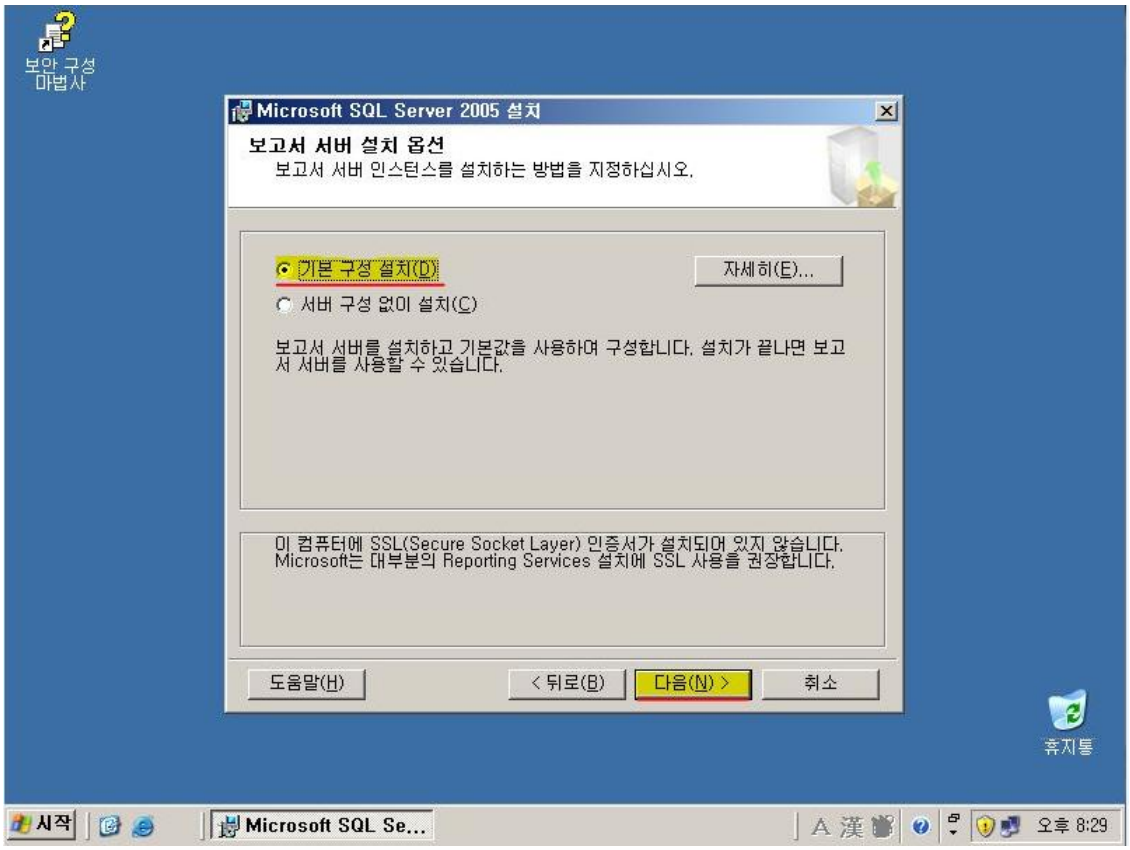


12. 데이터 정렬 설정 – (대/소문자 구분 체크 해제) 다음

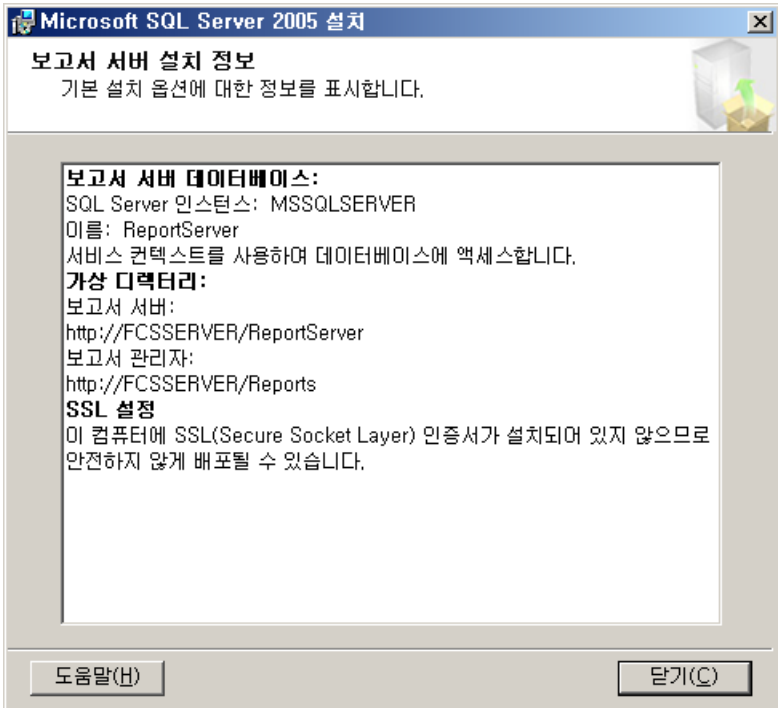


13. 보고서 서버 설치 옵션 – 기본 구성 설치(D) 선택 후 다음

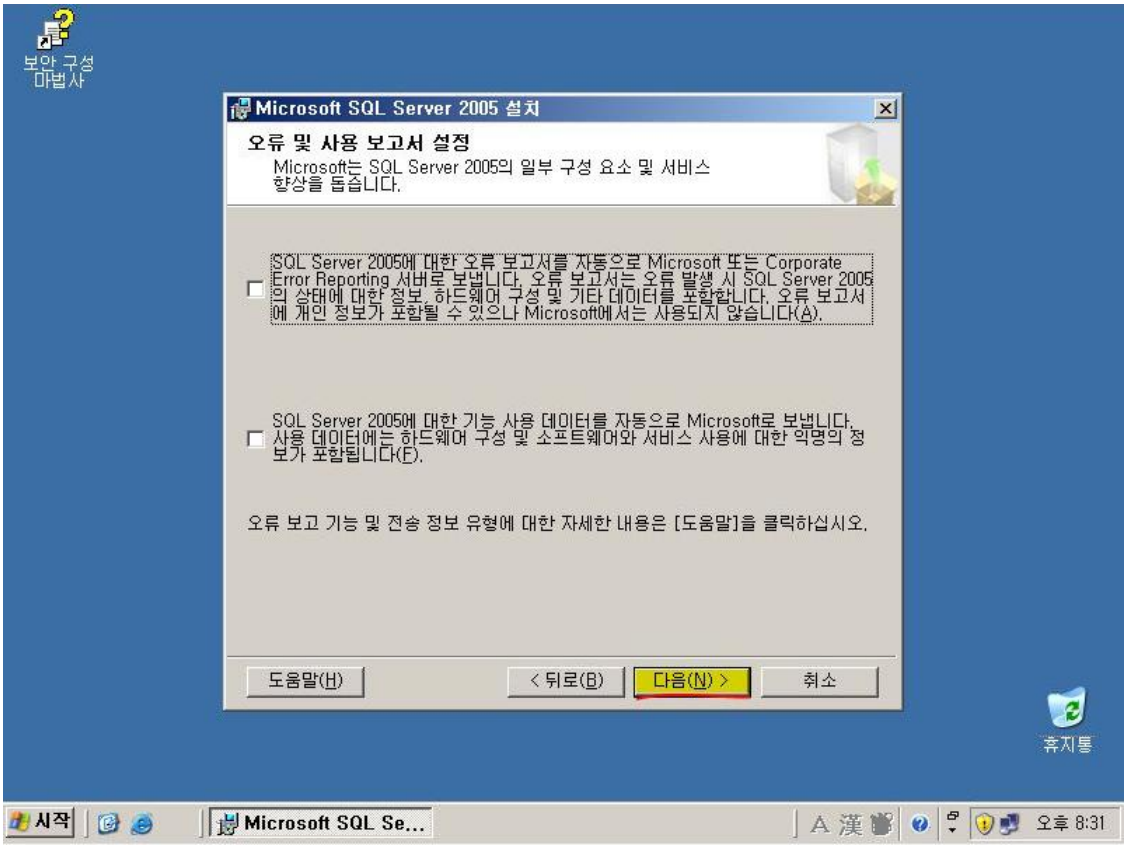
참고 : "자세히" 버튼을 누르면 설치 정보를 볼 수 있다.



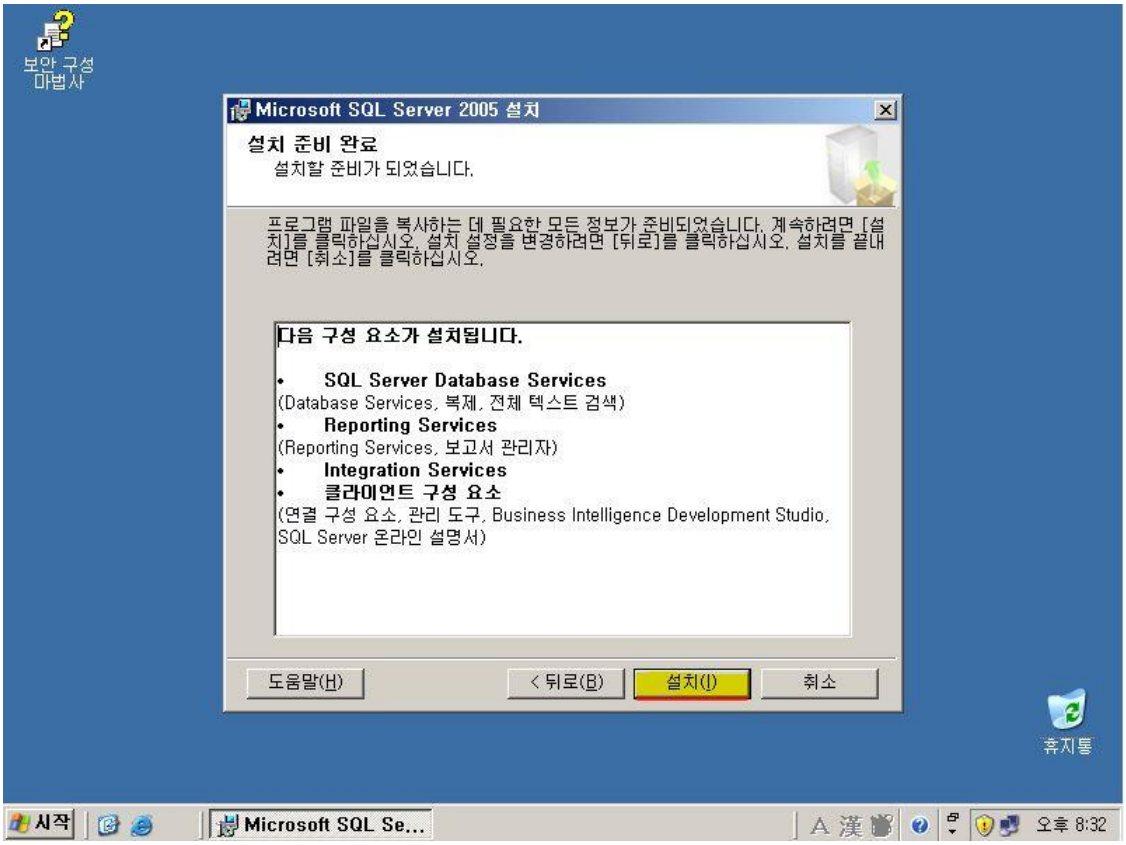
* "자세히(E)" 버튼을 눌렀을 때의 화면



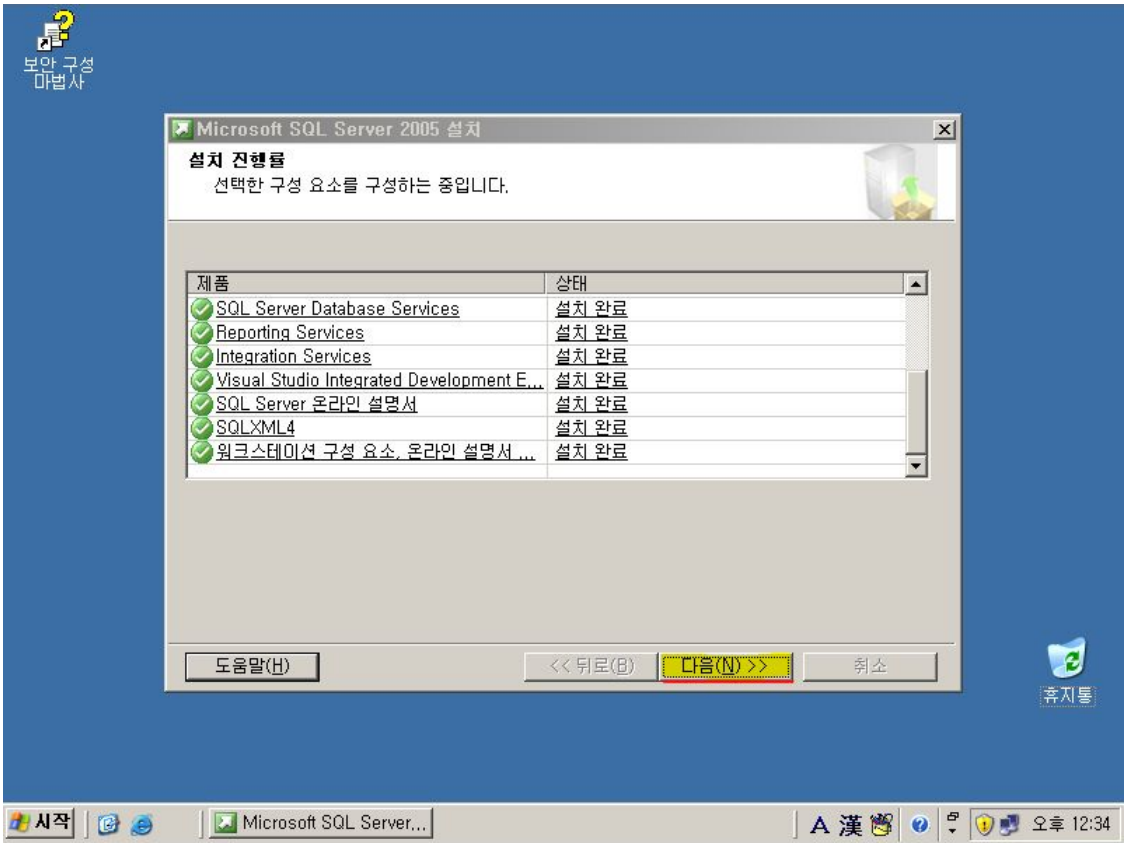
14. 오류 및 사용 보고서 설정 – 다음



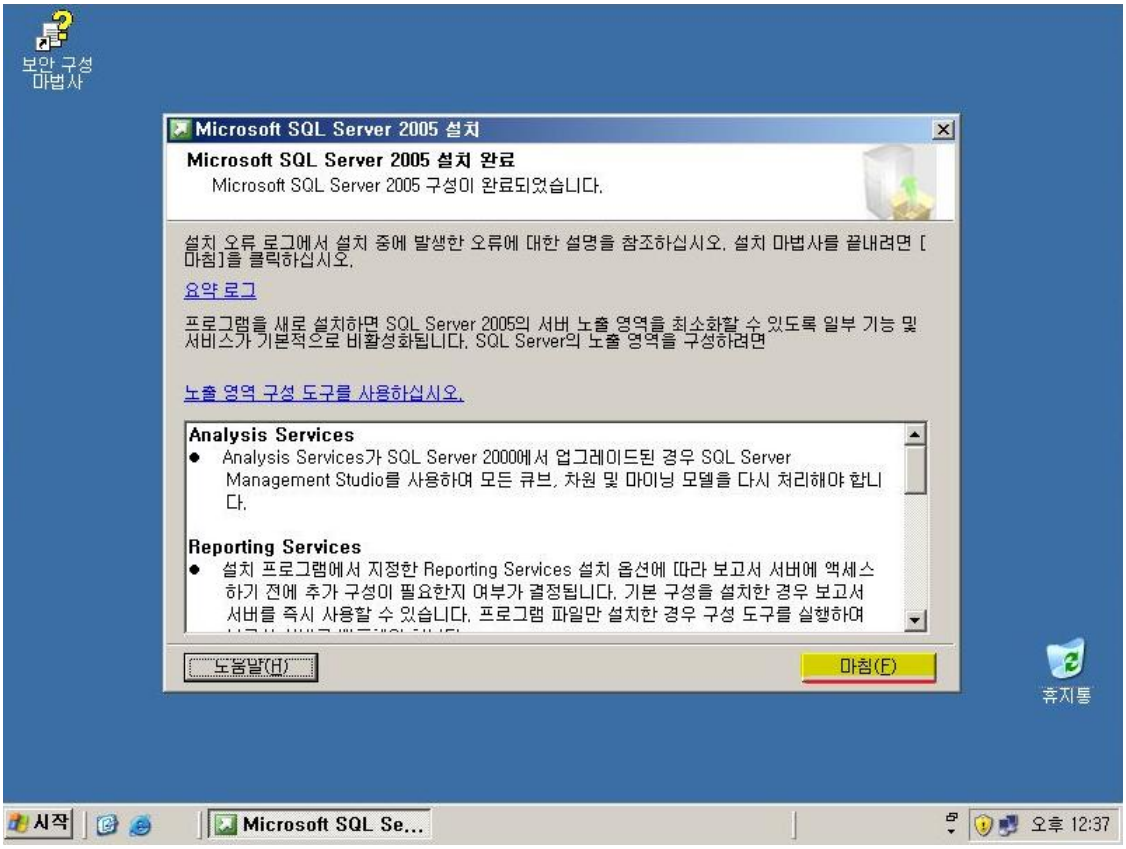
15. 설치



16. 설치 완료 – 다음



17. 마침



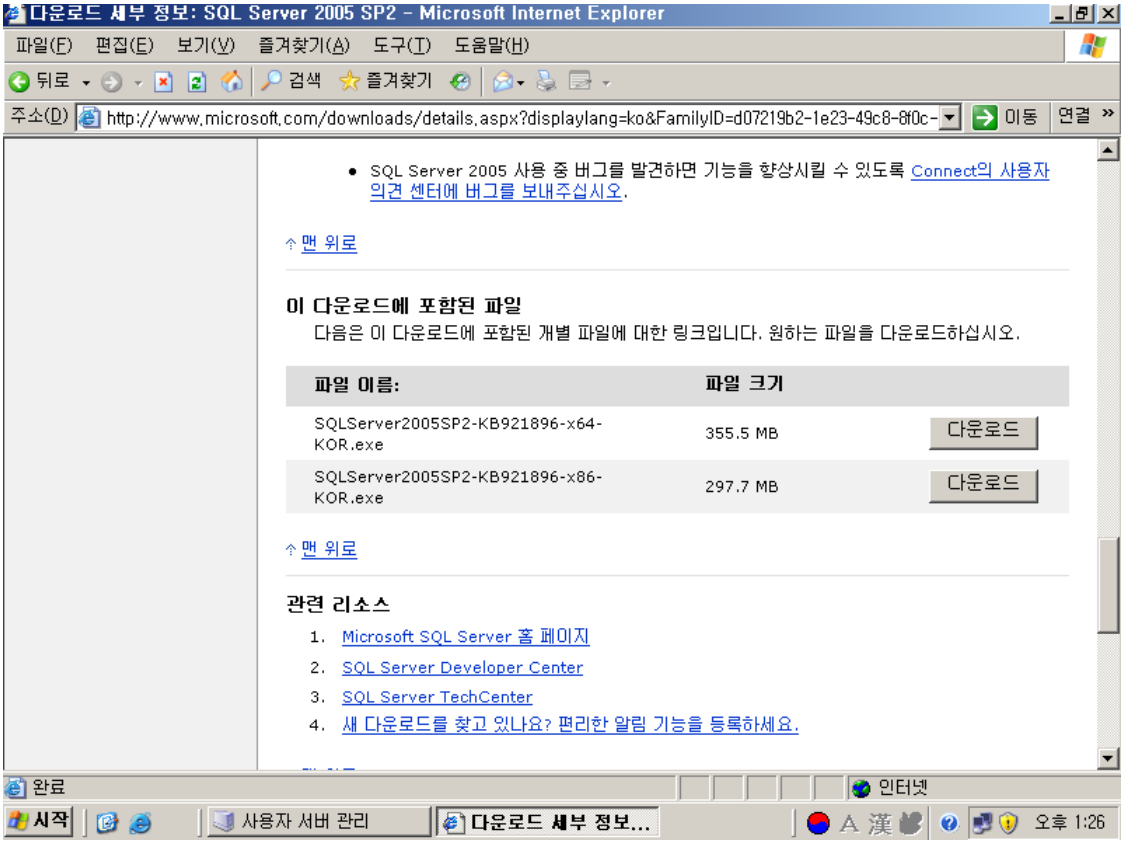
4.4. SQL Server 2005 Service Pack 설치

SQL Server 2005 SP2 또는 SP1을 설치합니다.

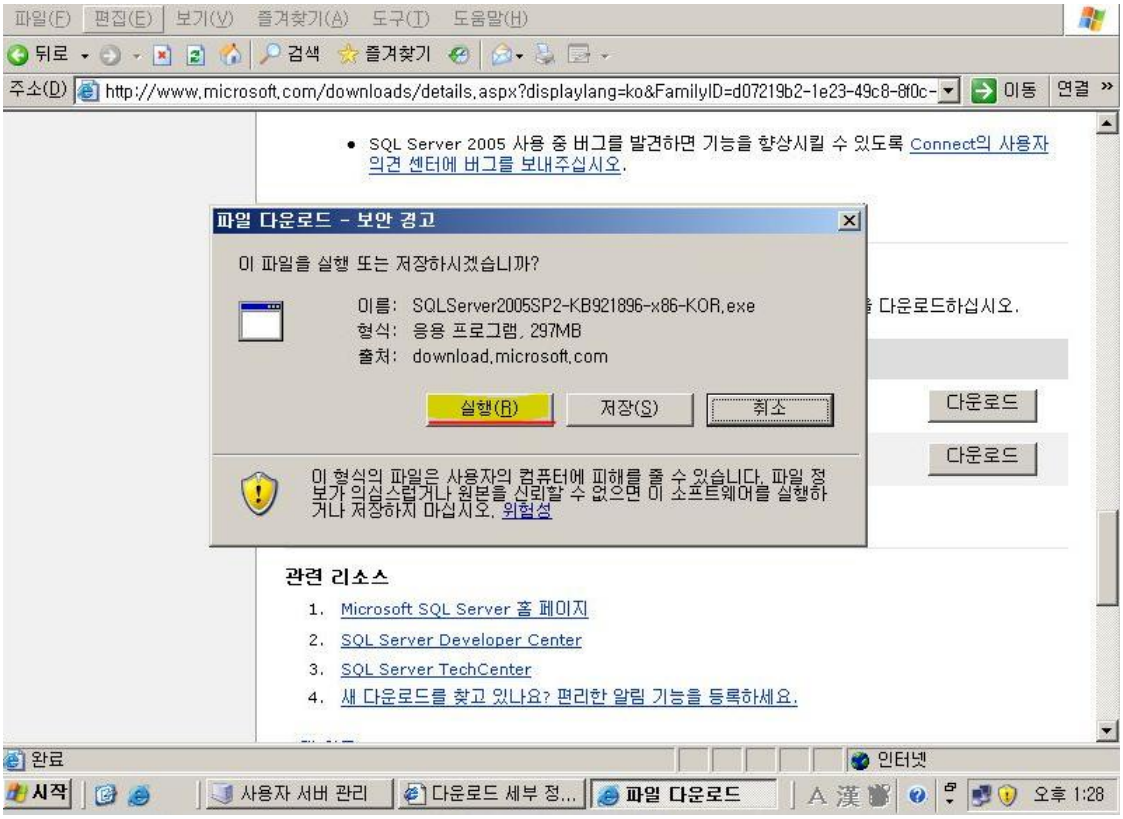
- SQL Server 2005 SP2 다운로드 경로 : http://go.microsoft.com/fwlink/?LinkID=84823
- SQL Server 2005 SP1 다운로드 경로 : http://go.microsoft.com/fwlink/?LinkId=77417

SQL Server 2005 SP2 설치 절차

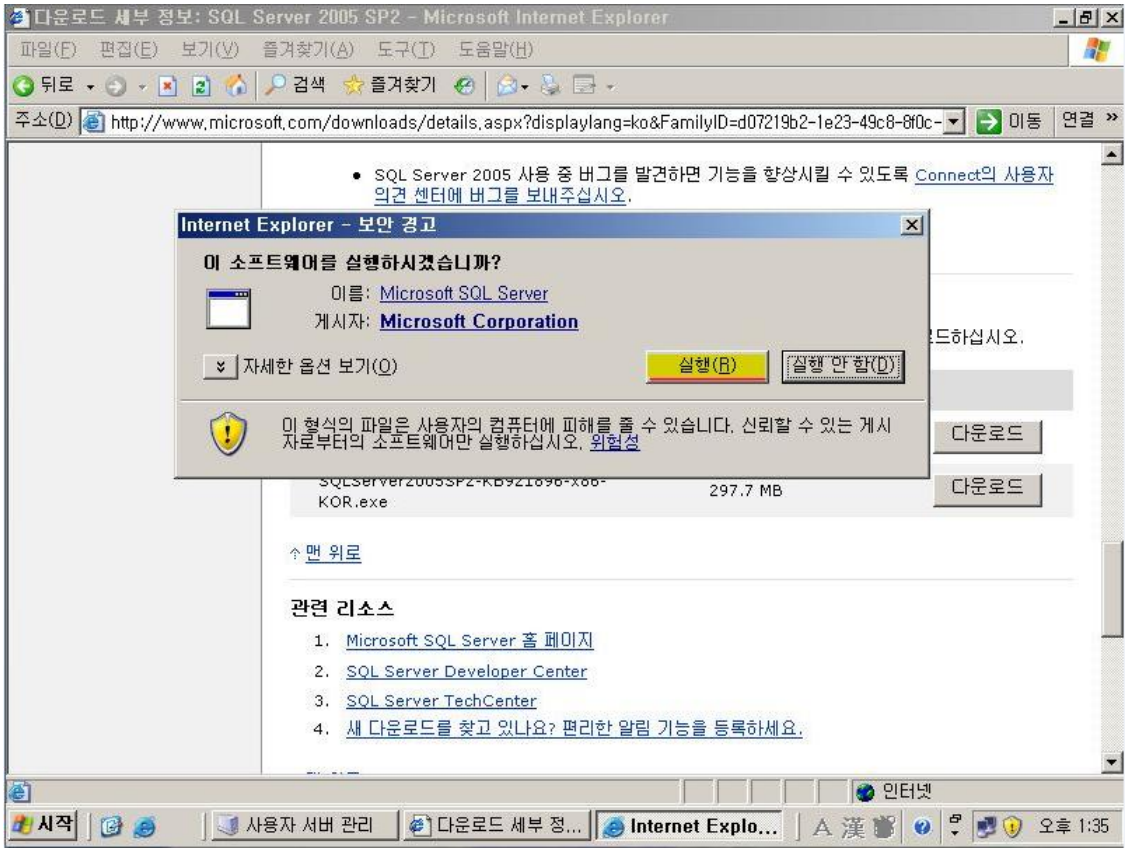
1. SQL Server 2005 SP2 다운로드



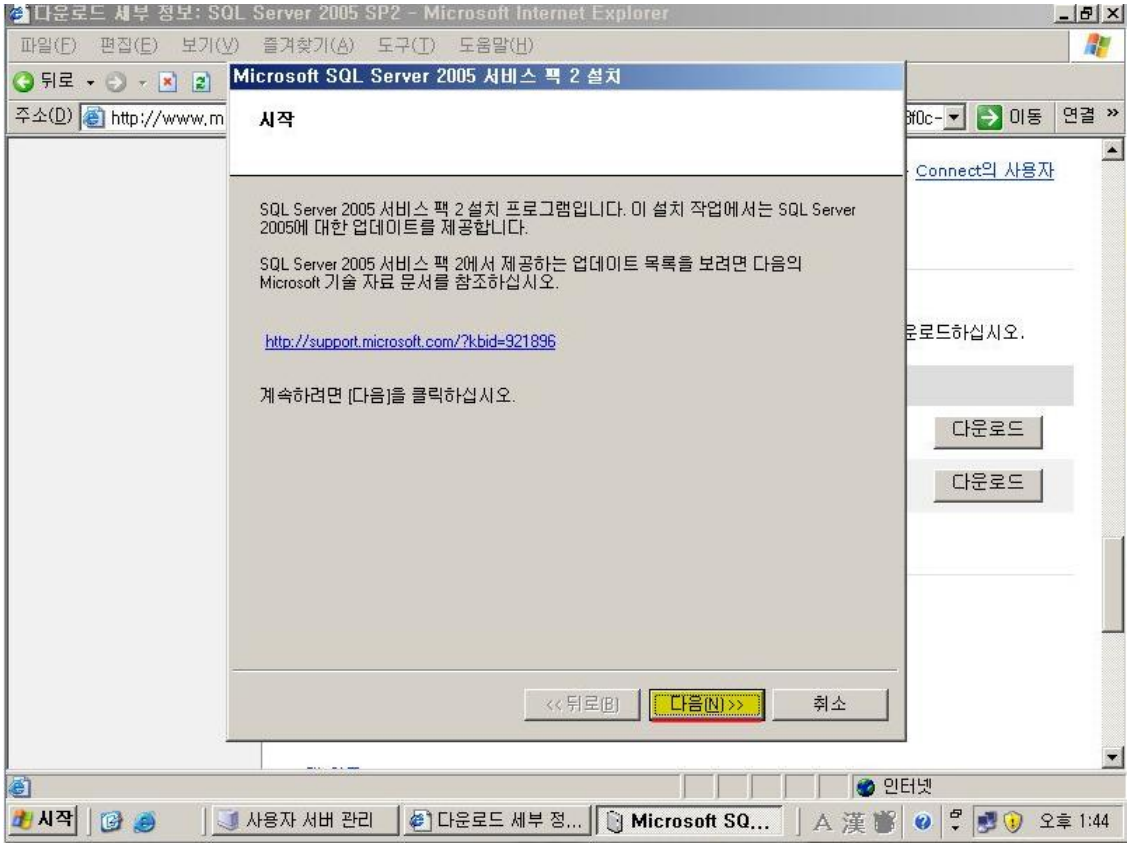
2. 실행 또는 저장 선택



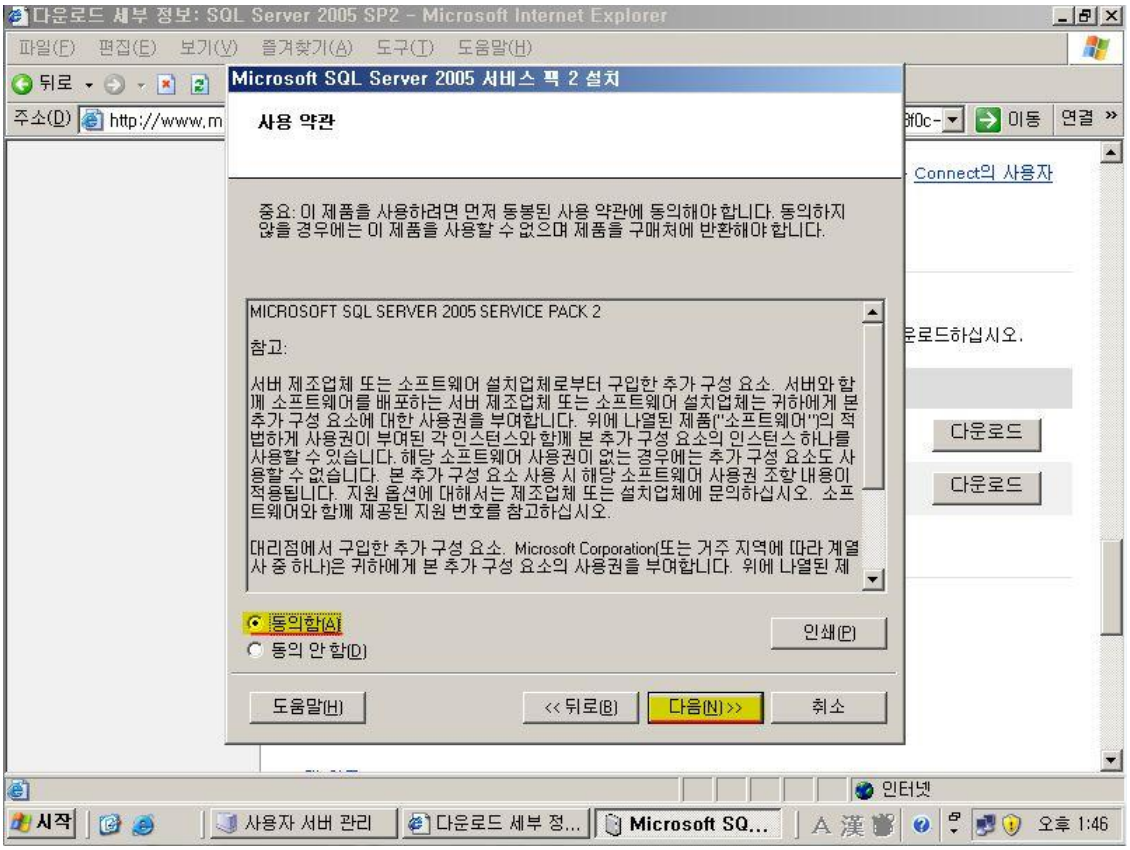
3. 실행



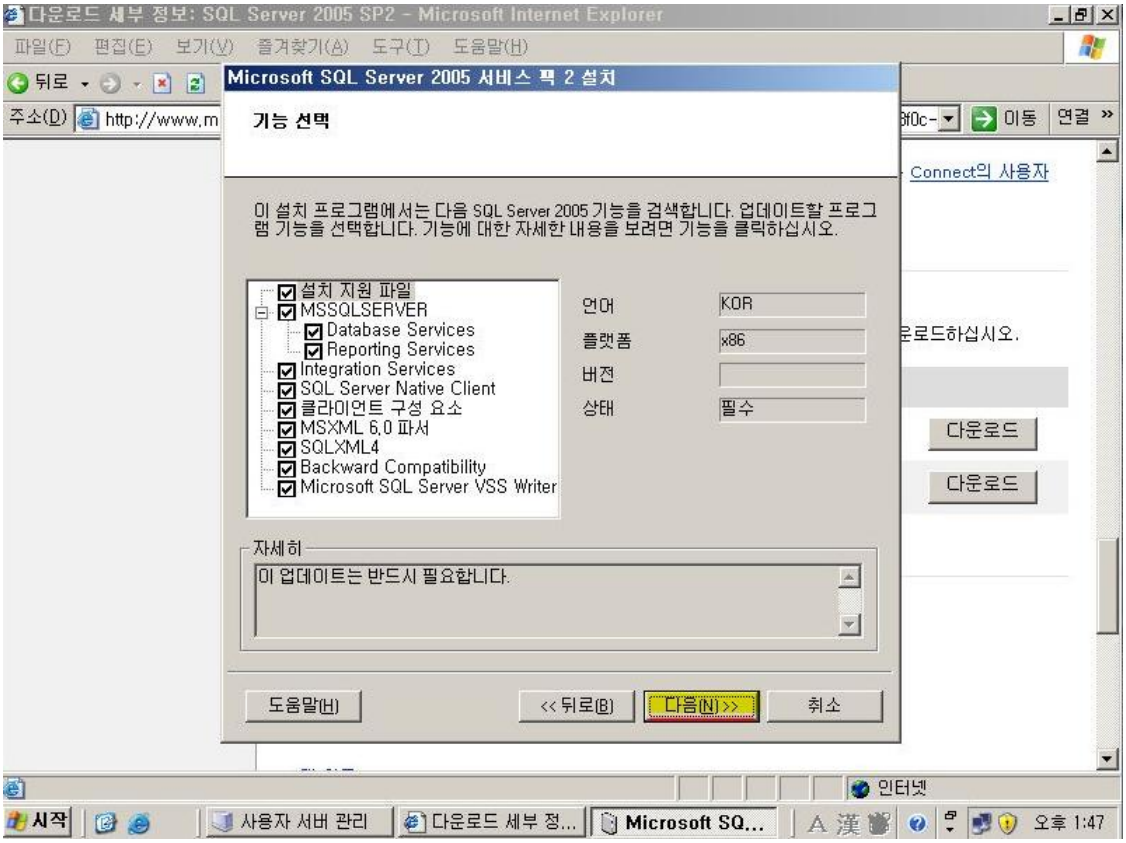
4. 설치 시작 – 다음



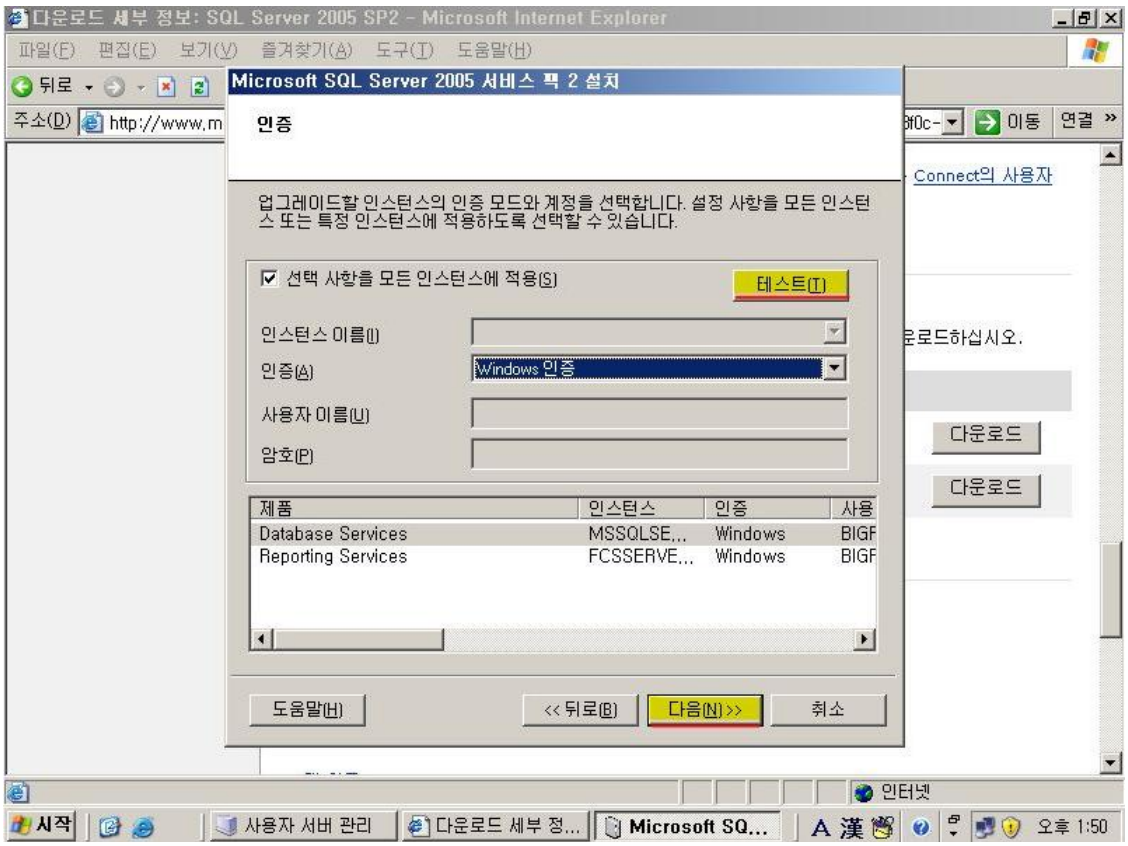
5. 사용 약관 – 동의함(A) 선택 후 다음



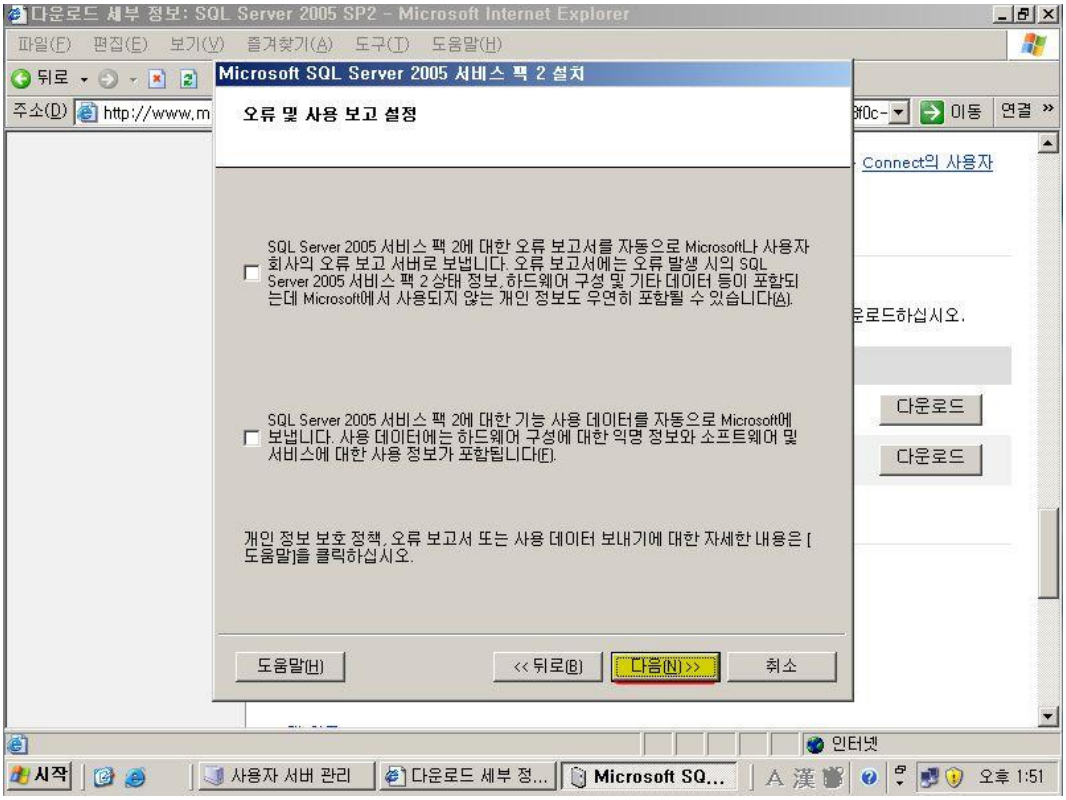
6. 다음



7. 테스트 클릭 후 다음

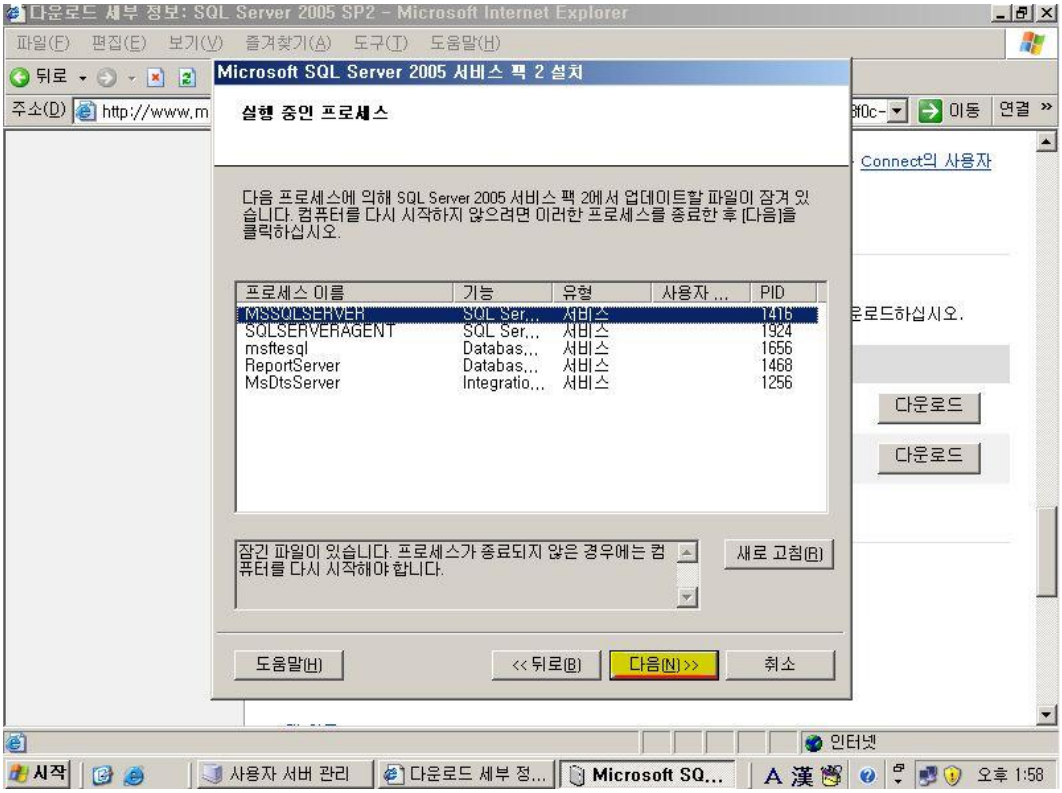


8. 오류 및 사용 보고 설정 – 다음

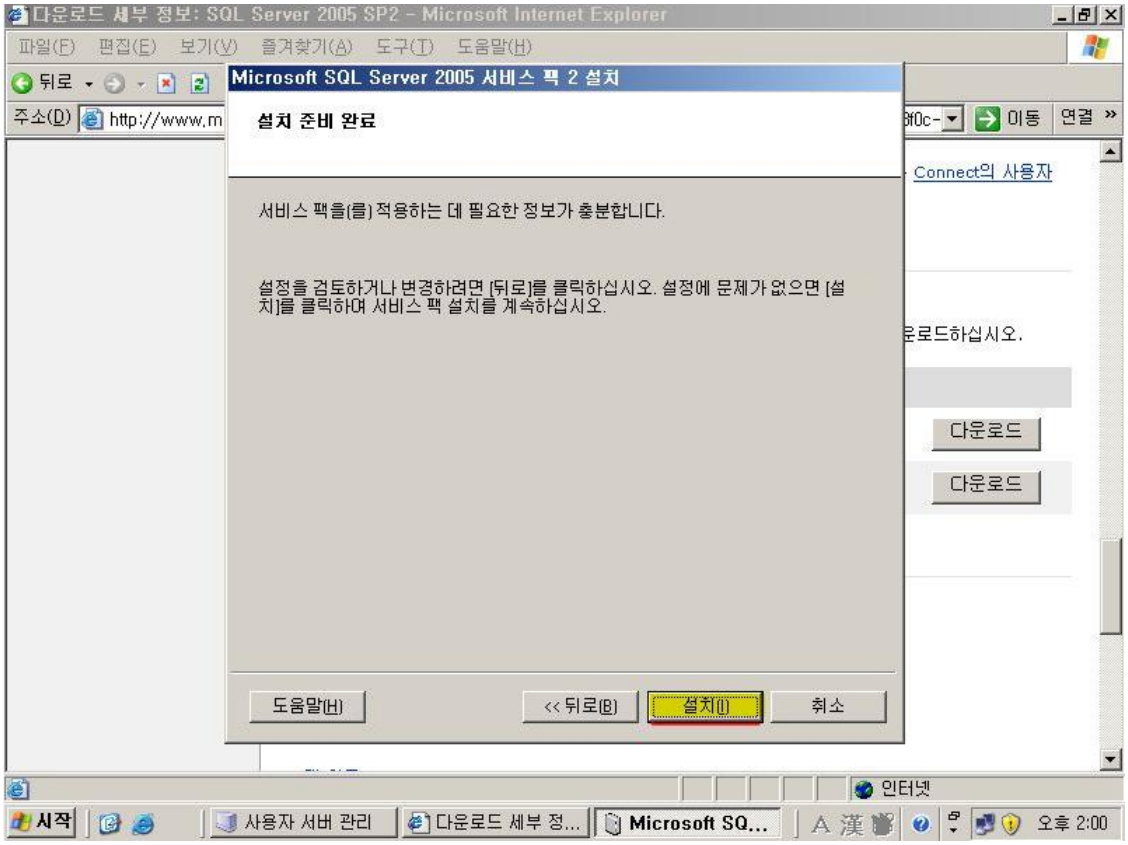


9. 실행 중인 프로세스 – 다음

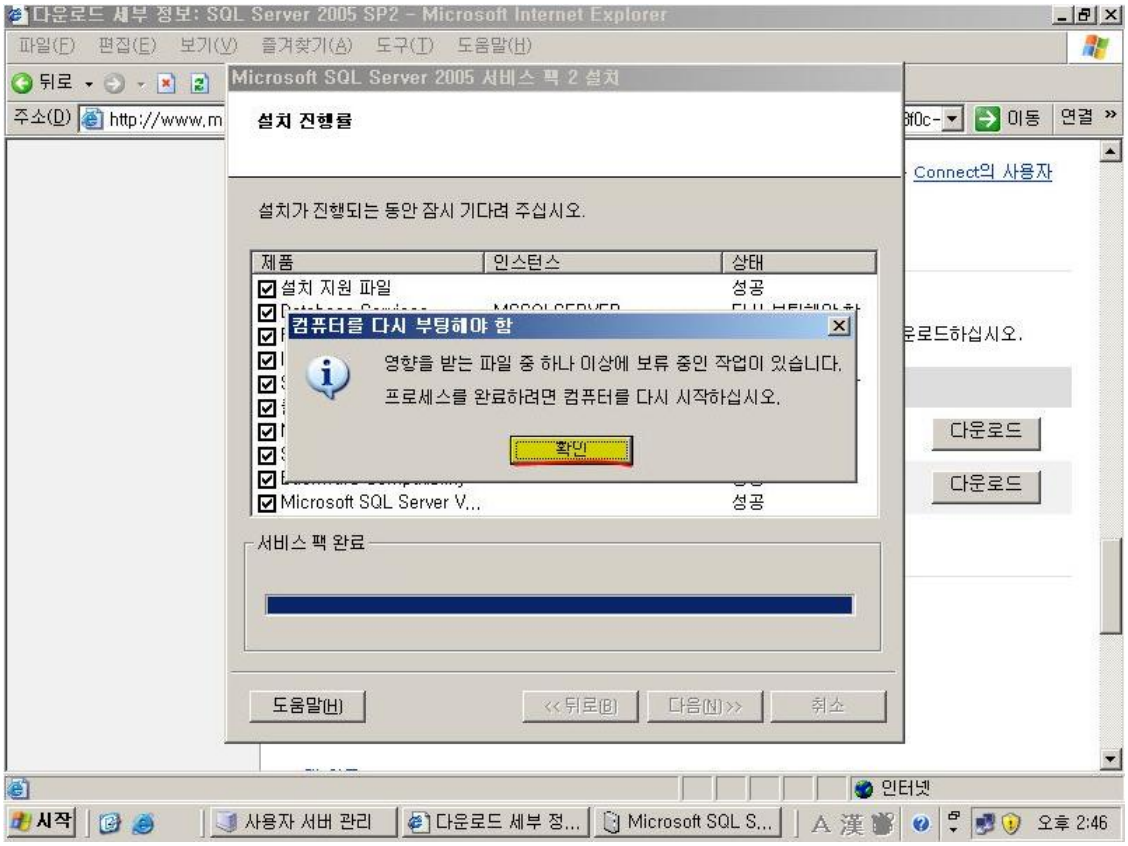
참고 : 실행 중인 프로세스를 멈추고 설치를 진행하면, 설치 완료 후 컴퓨터를 재 부팅 해야 합니다. 그냥 다음을 눌러 설치를 계속 진행하고, 재 부팅하겠습니다.



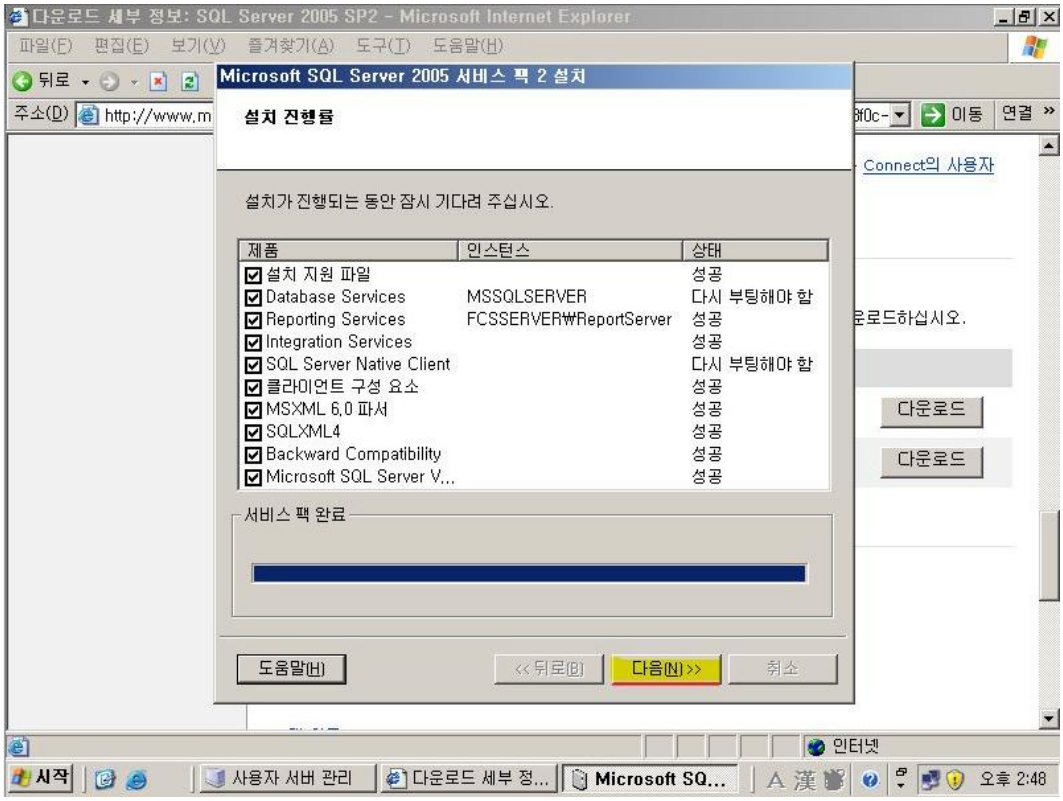
10. 설치 준비 완료 – 설치



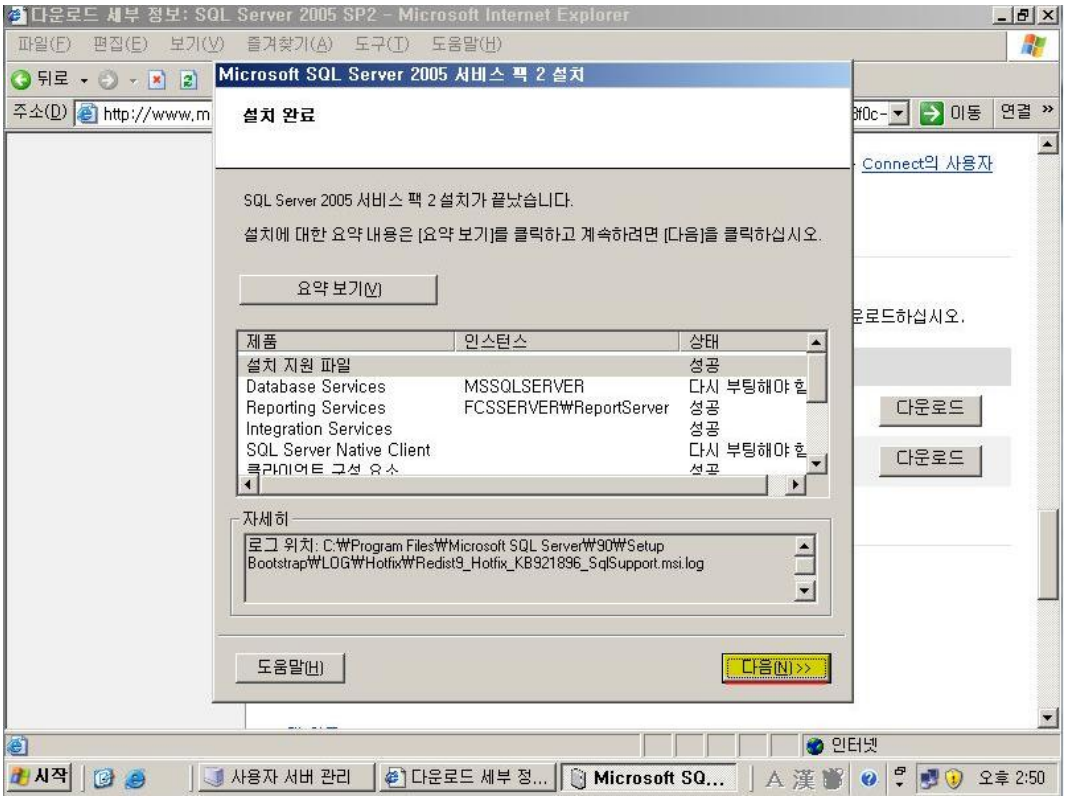
11. 컴퓨터를 재 부팅해야 한다는 메시지 – 확인



12. 다음



13. 설치 완료 – 다음



14. 재 부팅해서 설치를 완료한다.

4.5. MMC 3.0 설치

MMC 3.0 다운로드 경로 : http://go.microsoft.com/fwlink/?linkid=77419

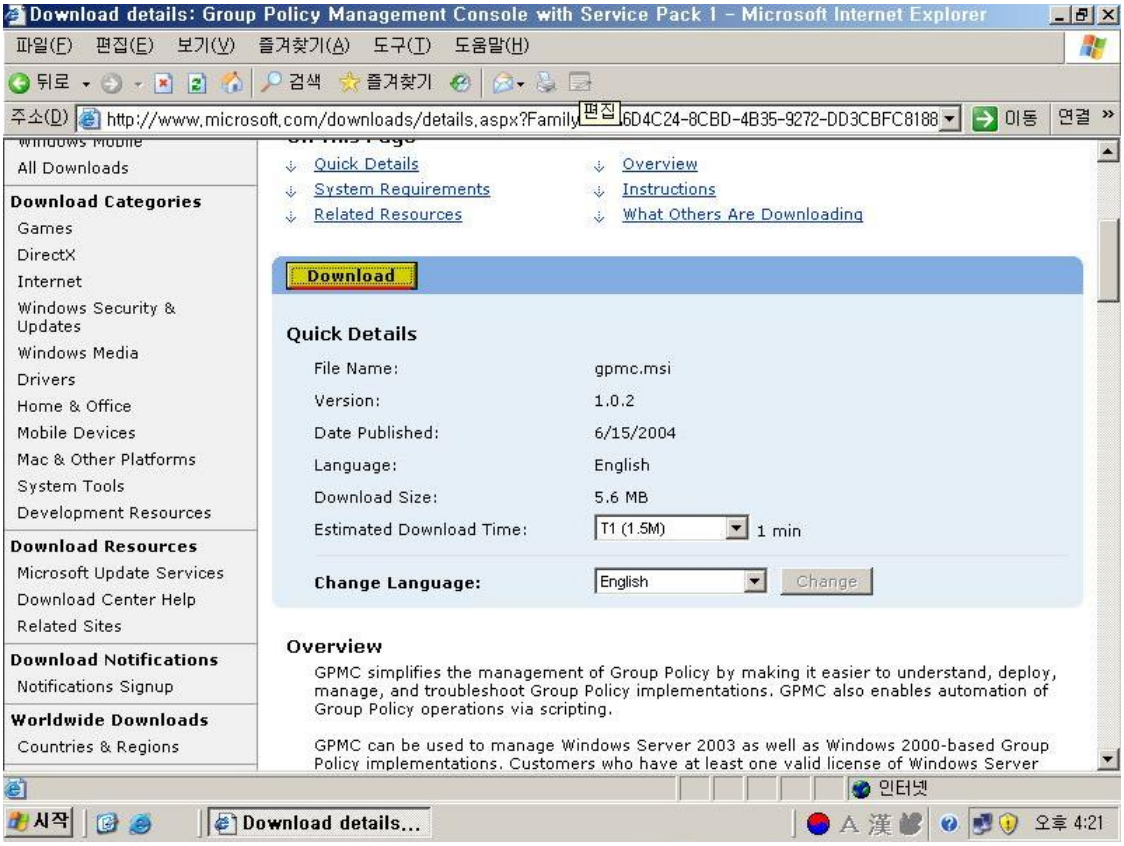
참고 : 운영체제로 Windows 2003 R2를 사용하는 경우 MMC 3.0 설치가 필요 없습니다.
Windows 2003 R2에는 MMC 3.0이 기본 포함 되어 있습니다.

4.6. GPMC SP1 설치

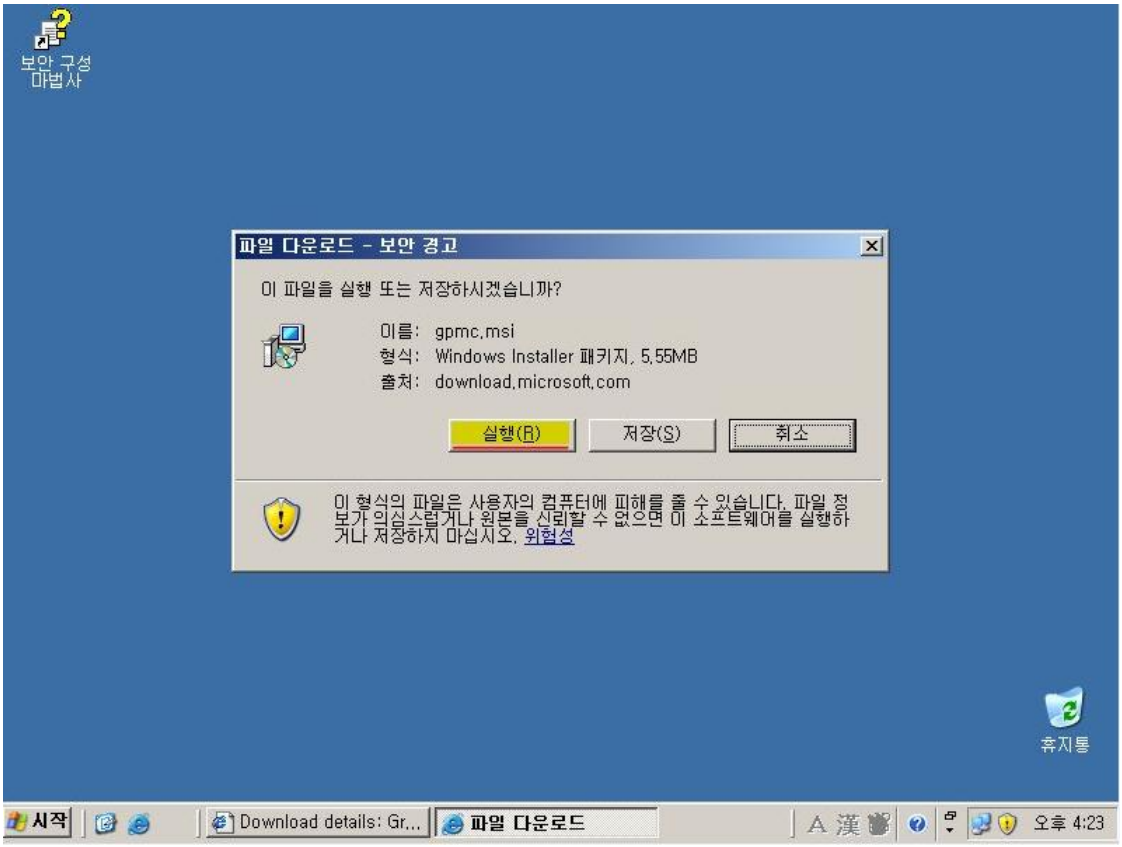
GPMC SP1 다운로드 경로 : http://go.microsoft.com/fwlink/?linkid=77421

참고 : GPMC SP1 설치를 위해서는 MSXML4 SP2가 필요합니다.
GPMC SP1은 현재 한글 버전을 지원하지 않기 때문에 GPMC SP1을 설치하기 위해서는
MSXML4 SP2 영문 버전을 설치해야 합니다.
MSXML4 SP2 영문 버전은 GPMC SP1 영문판 설치 시 다운로드 및 설치 할 수 있습니다.

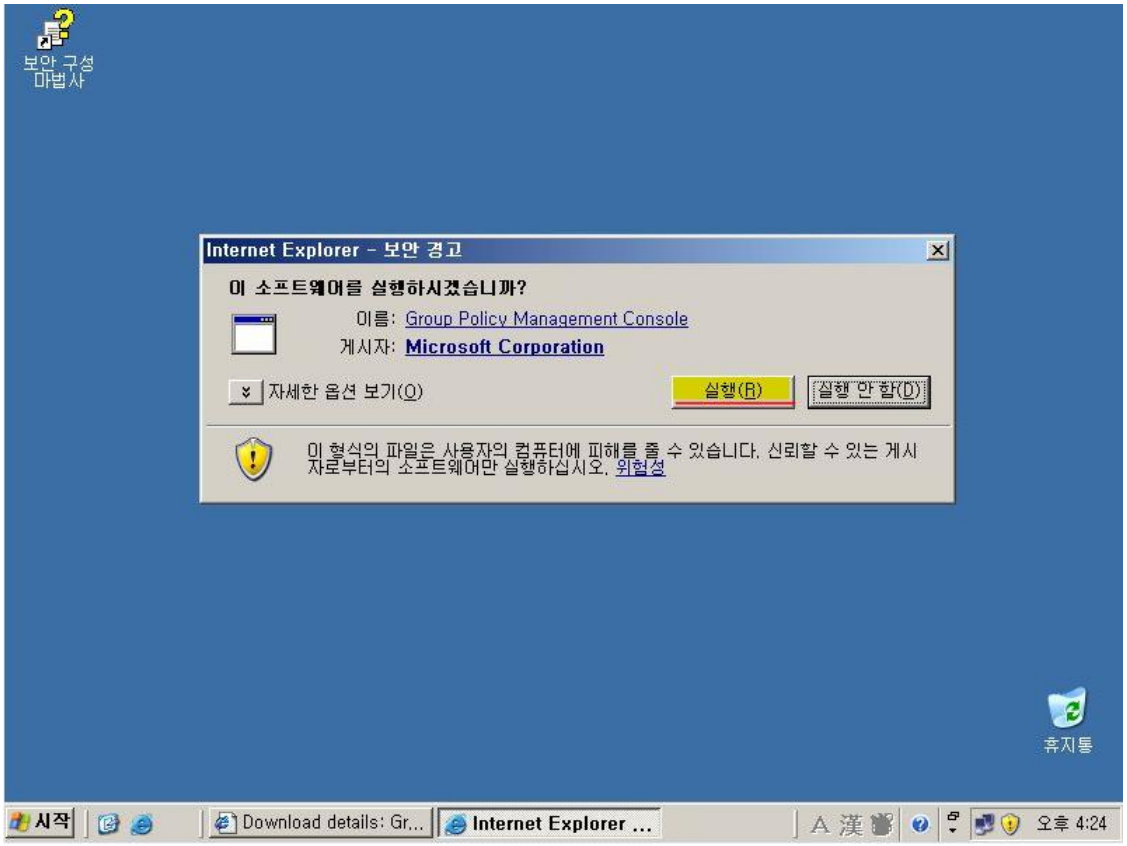
1. 다운로드



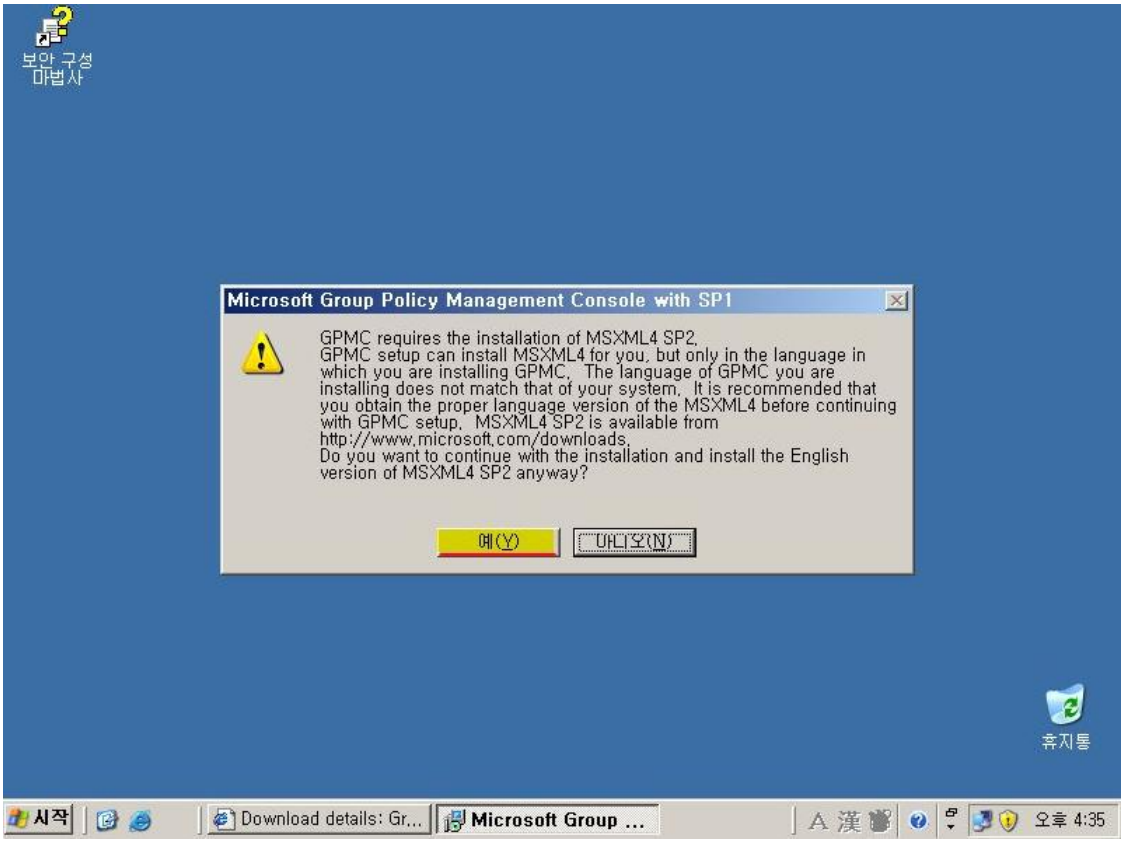
2. 실행 또는 저장


보안 구성 마법사
파일 다운로드 - 보안 경고
이 파일을 실행 또는 저장하시겠습니까?
이름: gpmc.msi
형식: Windows Installer 패키지, 5.55MB
출처: download.microsoft.com
실행(R)
저장(S)
취소
이 형식의 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 파일 정보가 의심스럽거나 원본을 신뢰할 수 없으면 이 소프트웨어를 실행하거나 저장하지 마십시오. 위험성
휴지통
시작
Download details: Gr...
파일 다운로드
오후 4:23

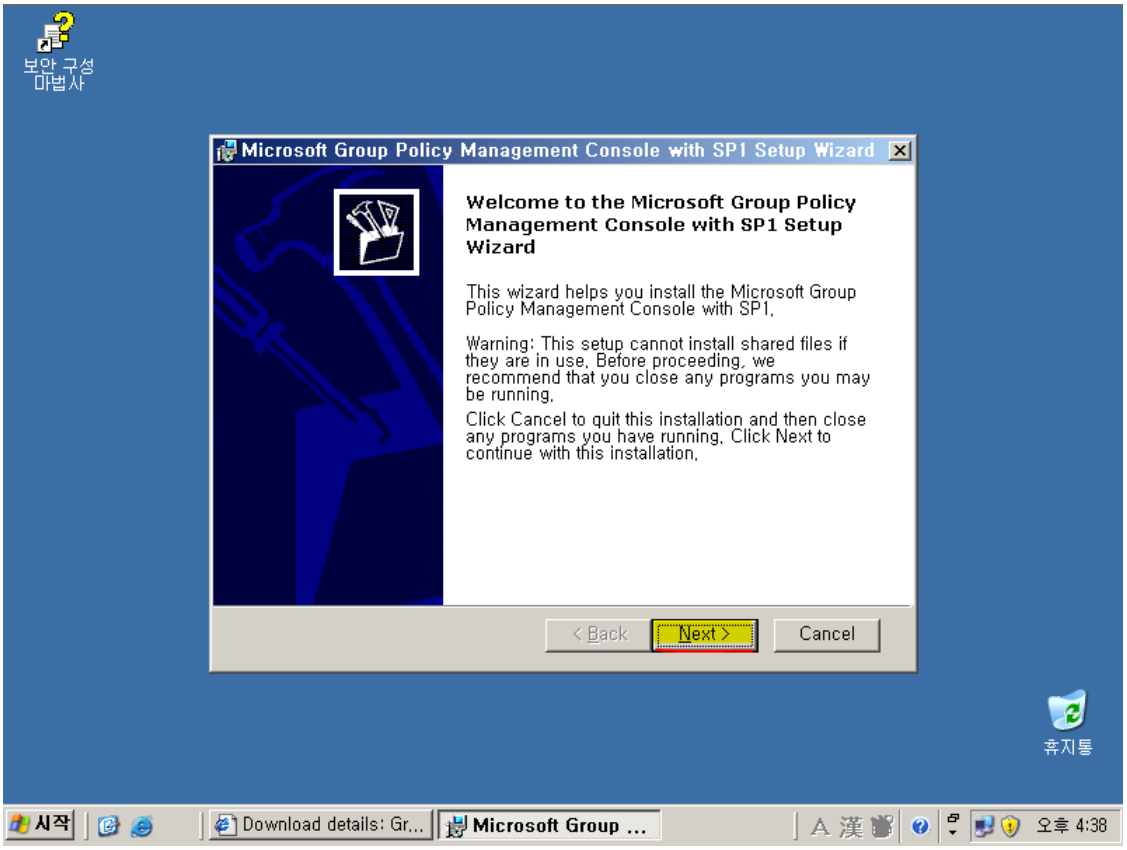
3. 실행


보안 구성 마법사
Internet Explorer - 보안 경고
이 소프트웨어를 실행하시겠습니까?
이름: Group Policy Management Console
게시자: Microsoft Corporation
자세한 옵션 보기(O)
실행(R)
실행 안 함(D)
이 형식의 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 신뢰할 수 있는 게시자로부터의 소프트웨어만 실행하십시오. 위험성
휴지통
시작
Download details: Gr...
Internet Explorer ...
오후 4:24

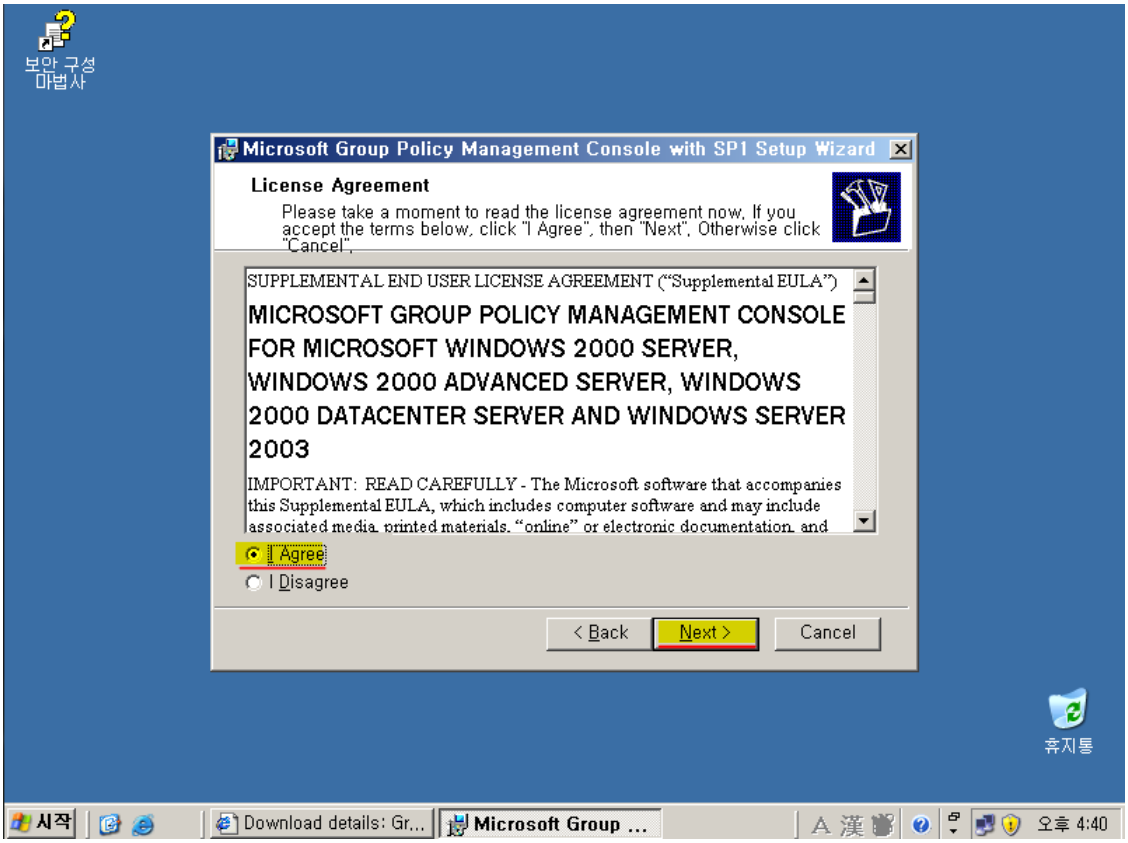
4. MSXML4 SP2가 필요하다는 메시지. ("예" 버튼을 눌러 계속 진행)



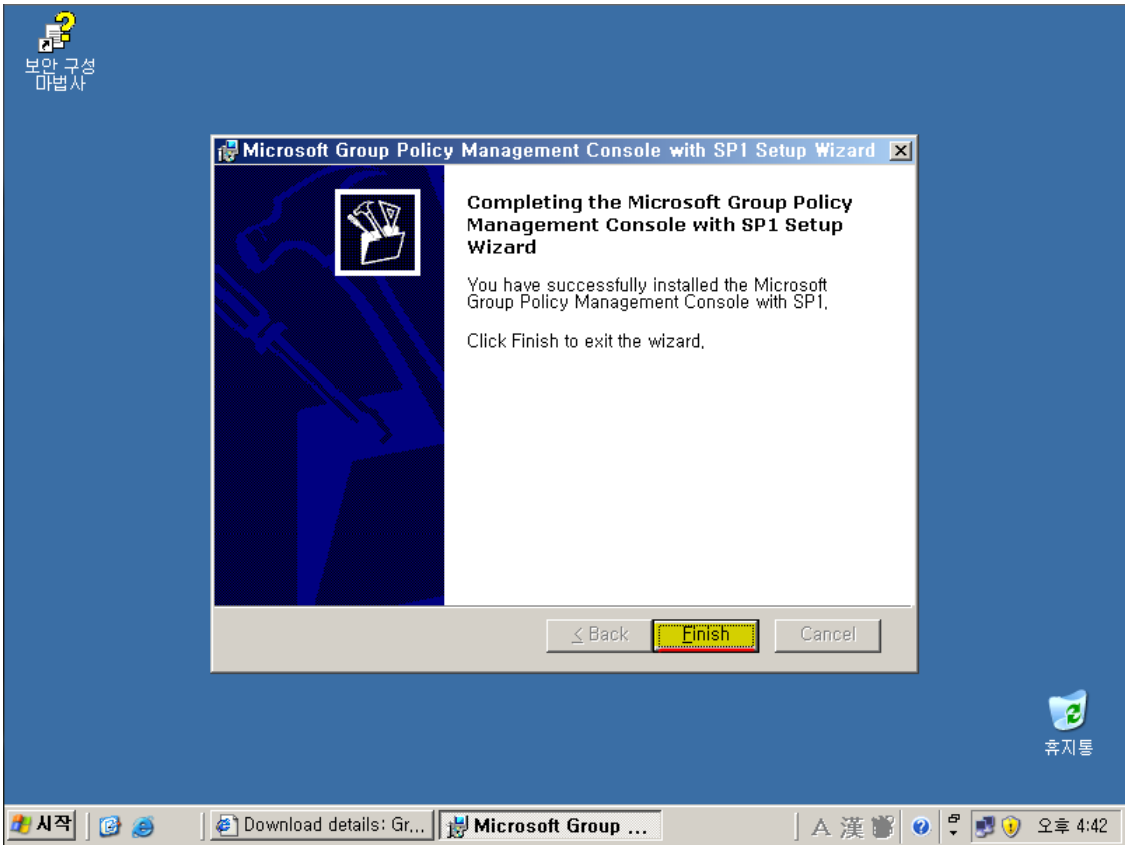
5. 설치 시작 – Next 선택



6. 사용 약관(License Agreement) – "I Agree" 선택 후 Next



7. 설치 완료 – Finish



4.7. WSUS SP1 설치

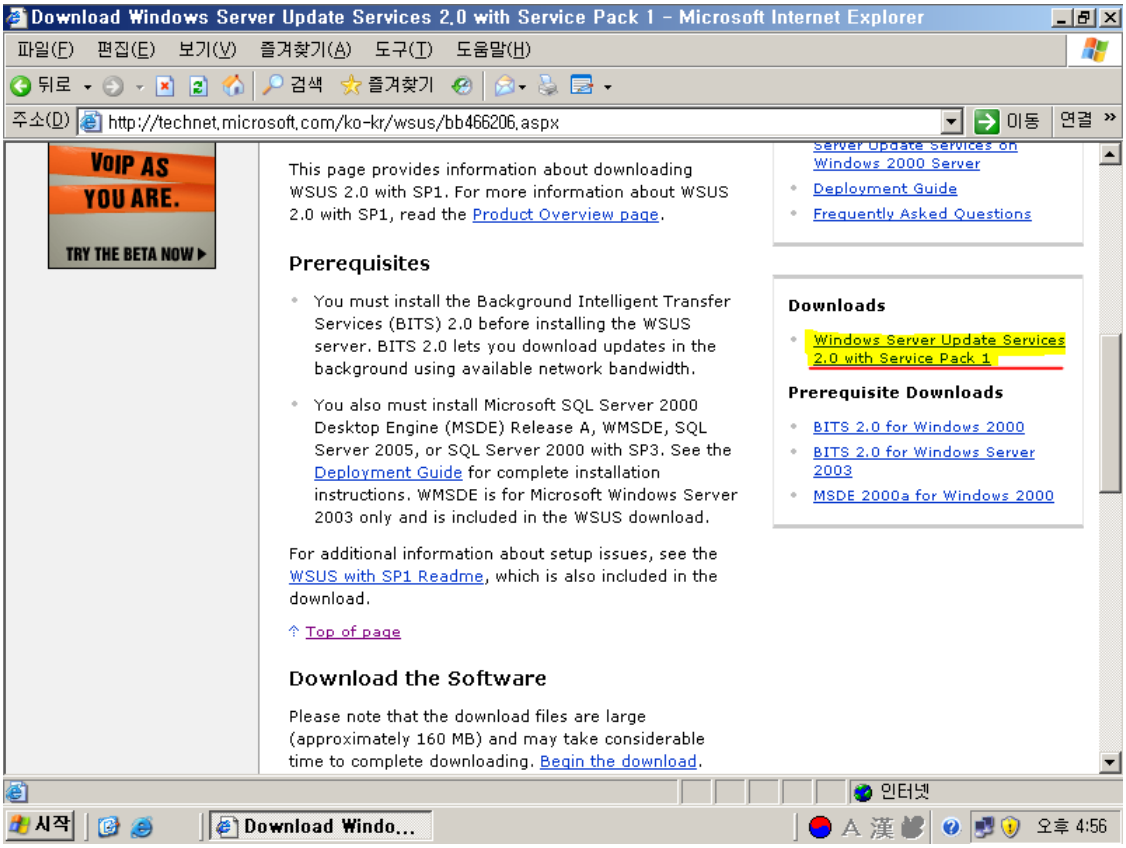
Forefront Client Security는 클라이언트 컴퓨터에 에이전트를 배포 및 정의 업데이트에 WSUS를 사용합니다.
WSUS는 아래의 경로에서 다운받으시면 됩니다.

WSUS SP1 다운로드 경로 : http://go.microsoft.com/fwlink/?linkid=77418

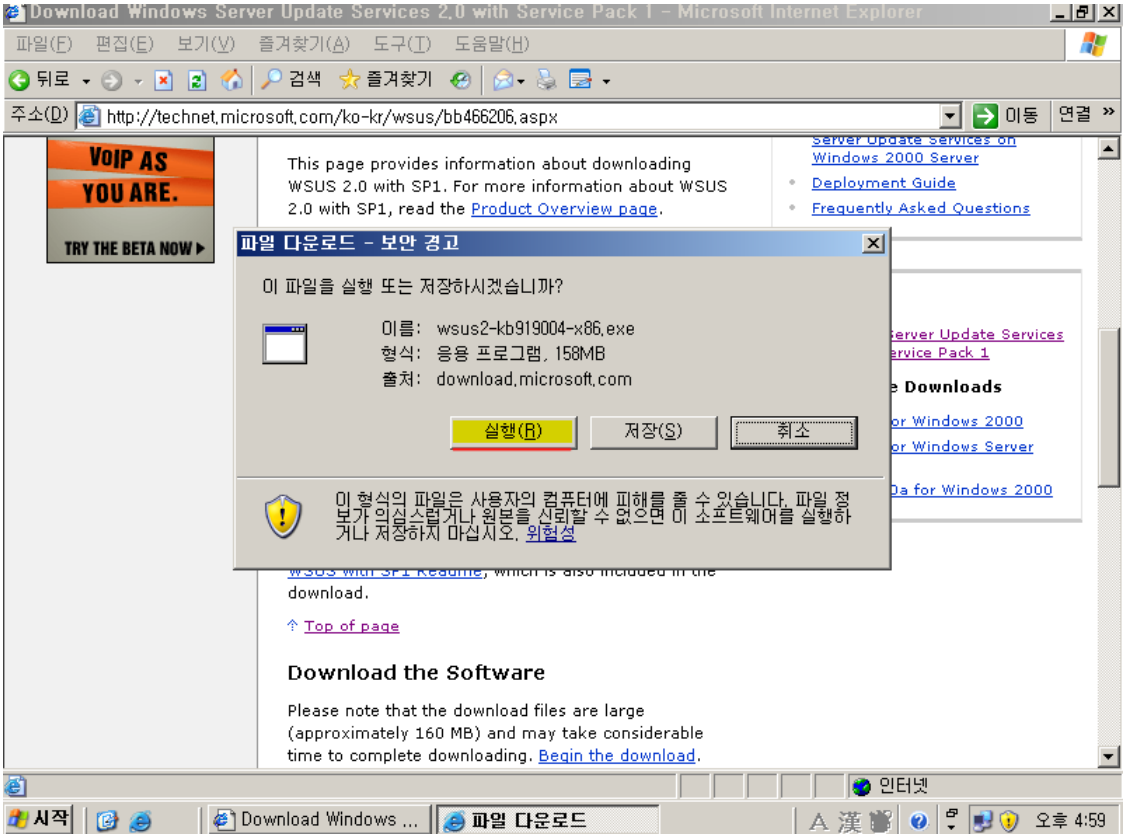
*주의 : 이전 단계인 SQL Server 2005 설치가 우선되어야 한다

WSUS SP1 설치 절차

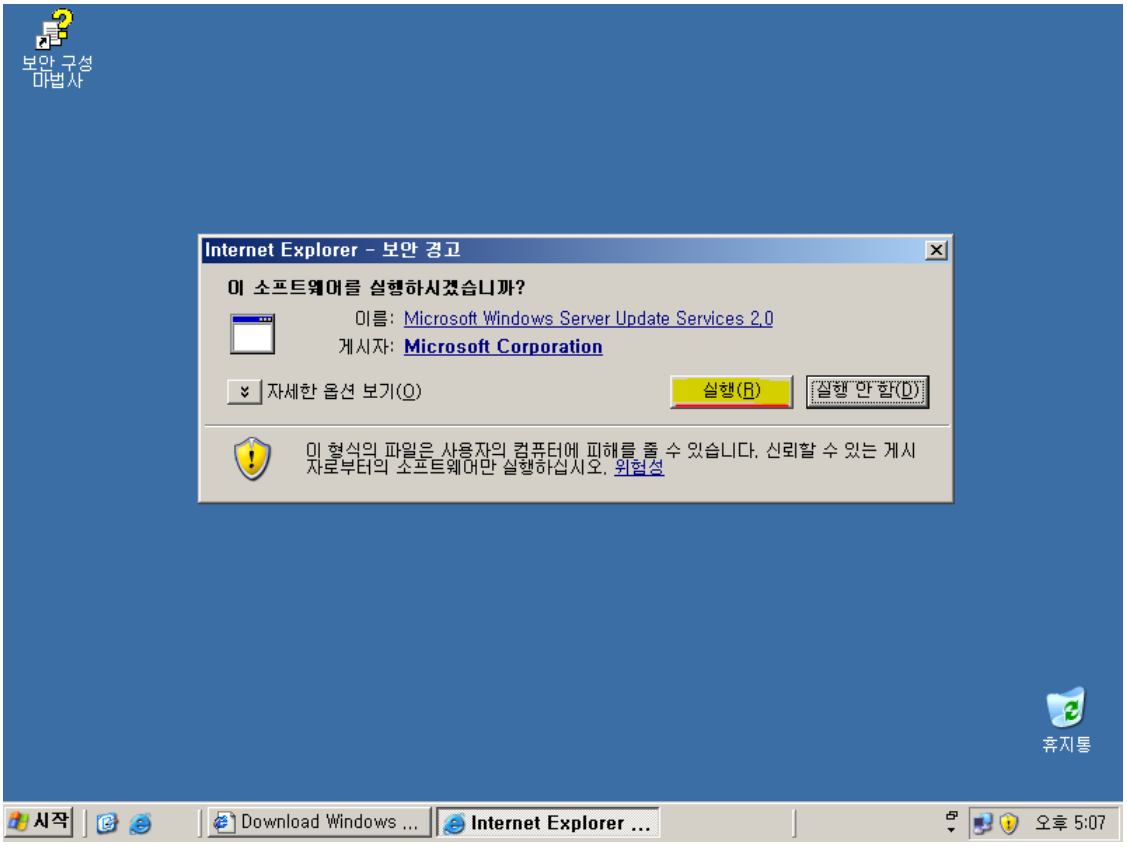
1. WSUS SP1 다운로드



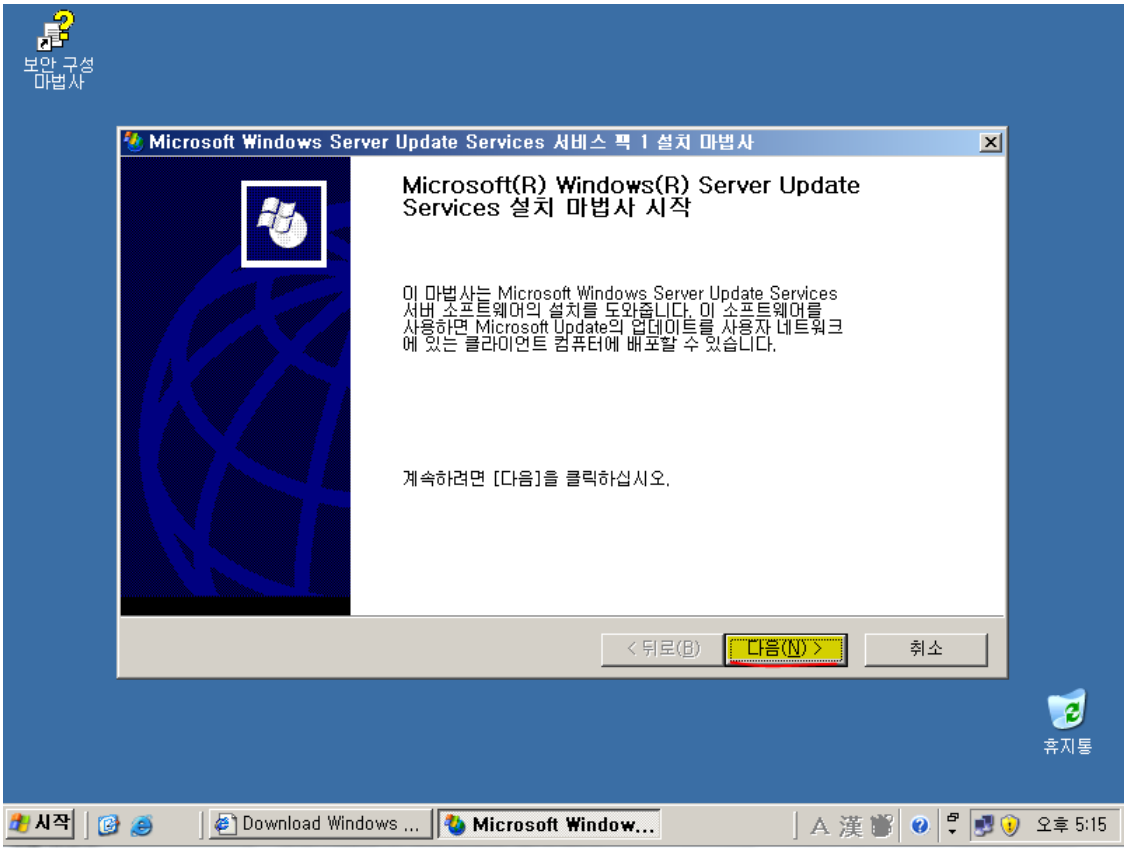
2. 실행 (또는 저장) 선택



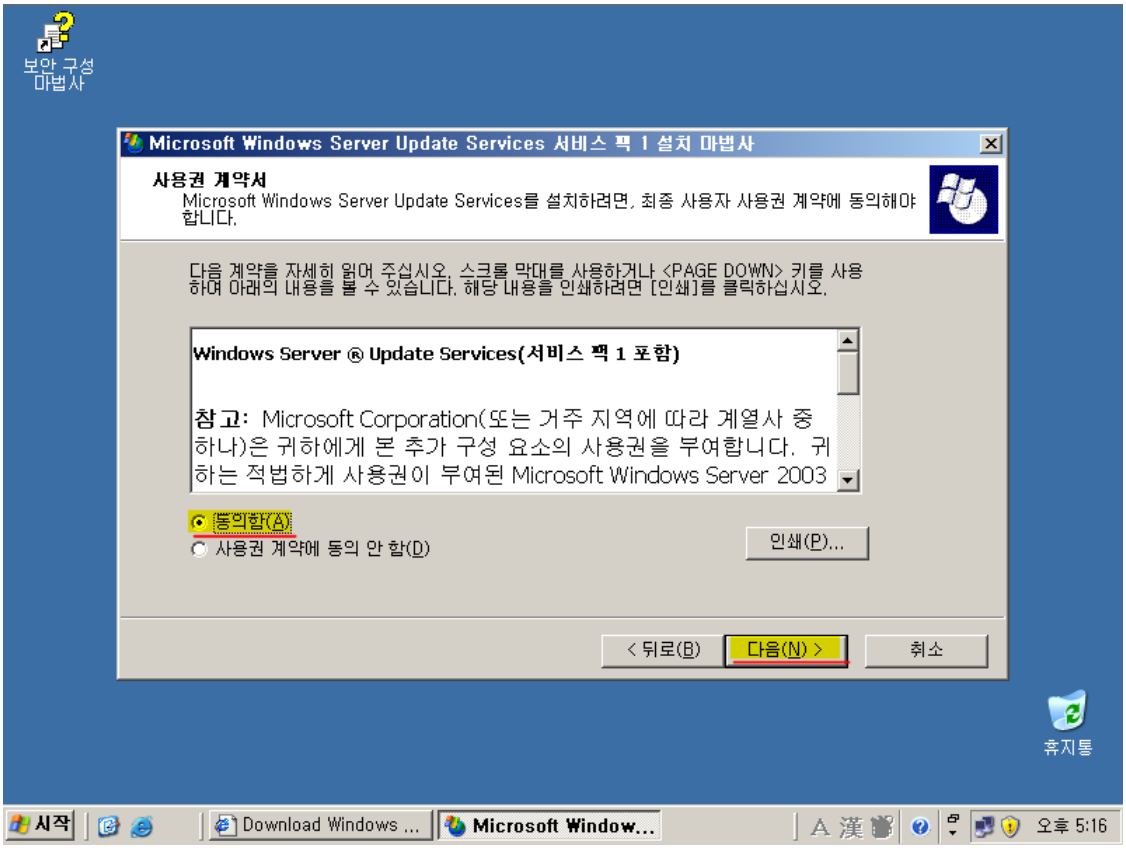
3. 실행



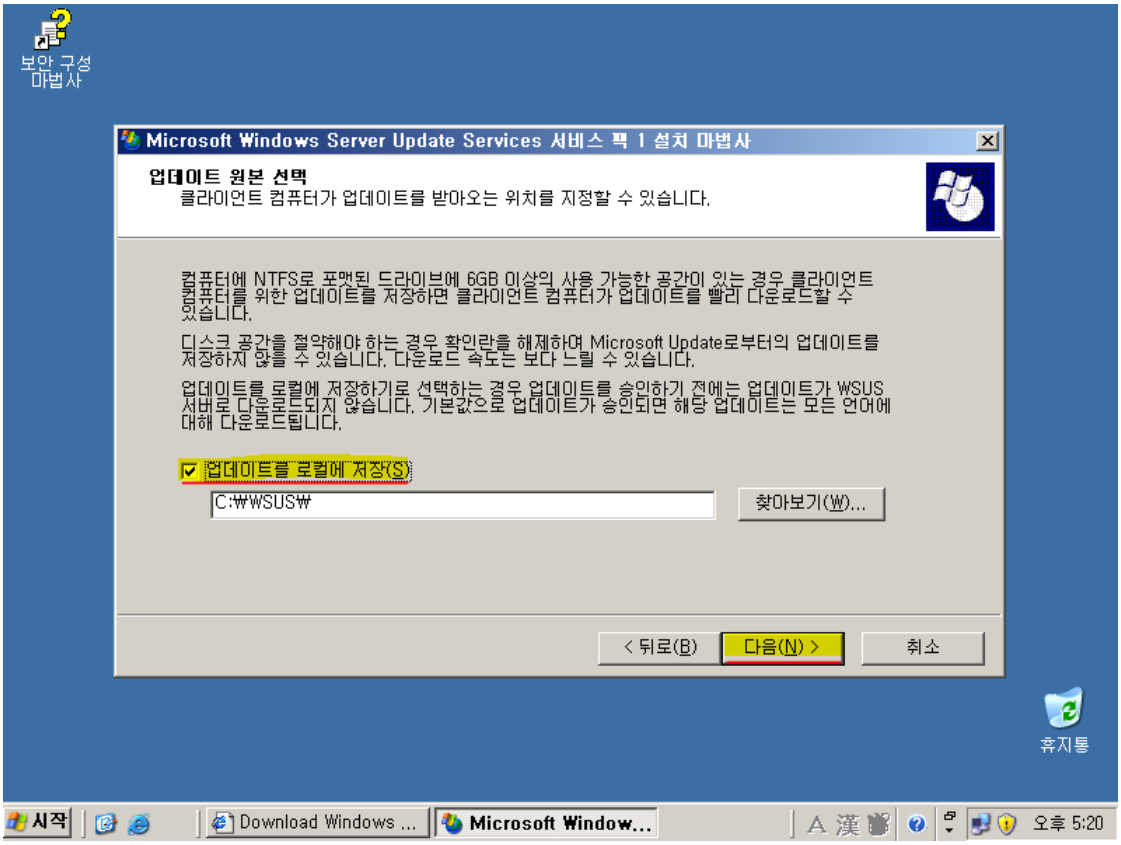
4. 설치 시작 – 다음



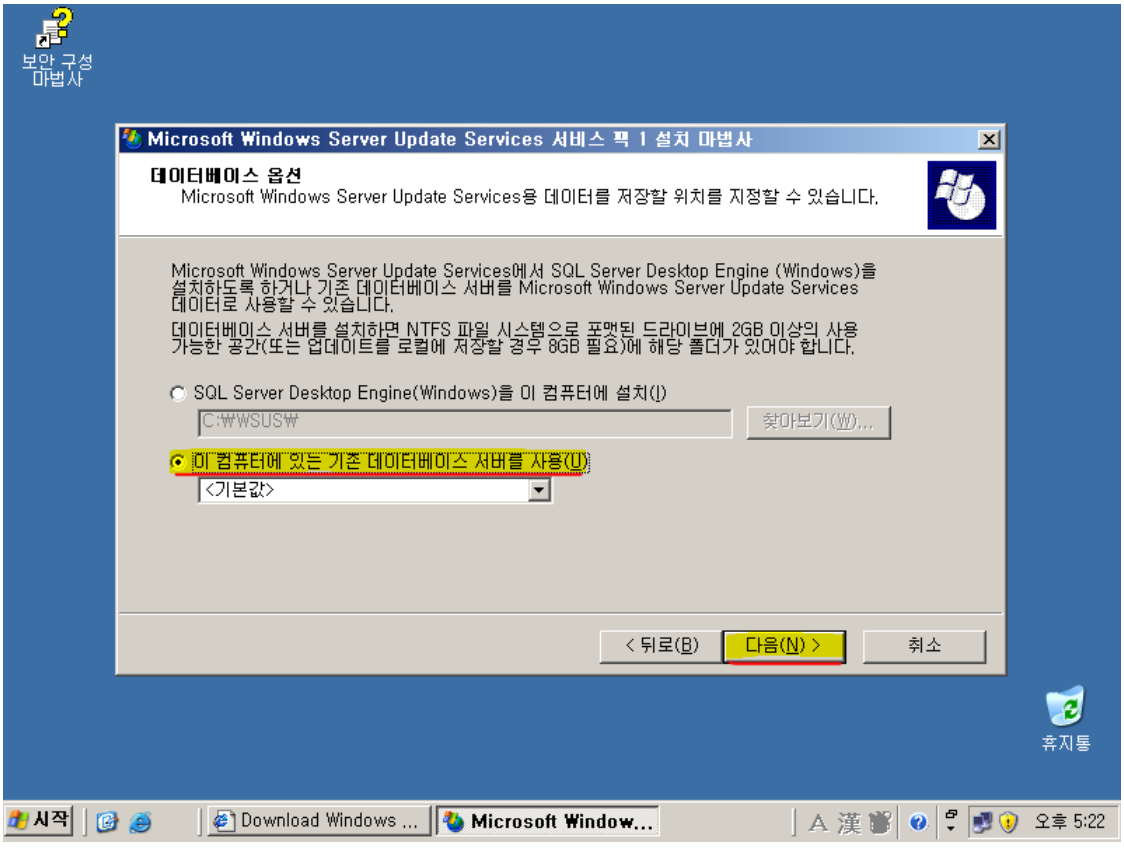
5. 사용권 계약서 – 동의함 선택 후 다음



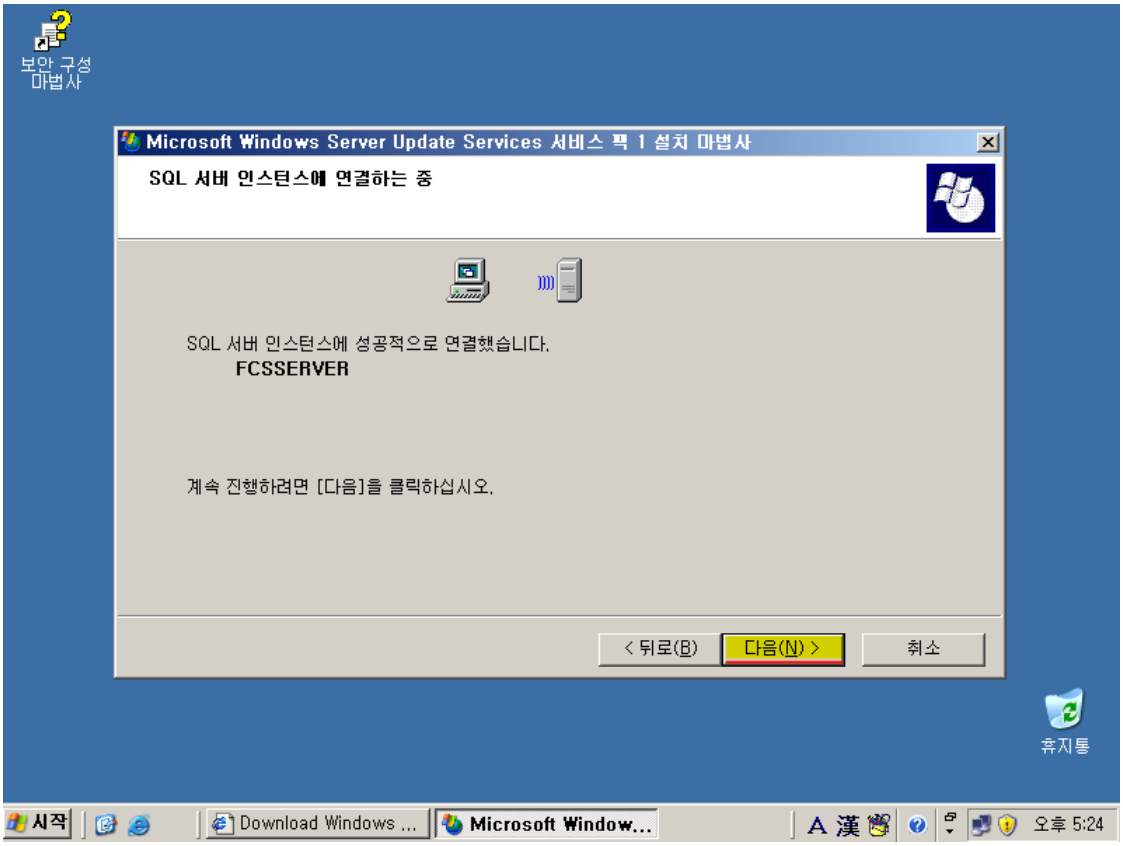
6. "업데이트를 로컬에 저장(S)" 체크 후 다음



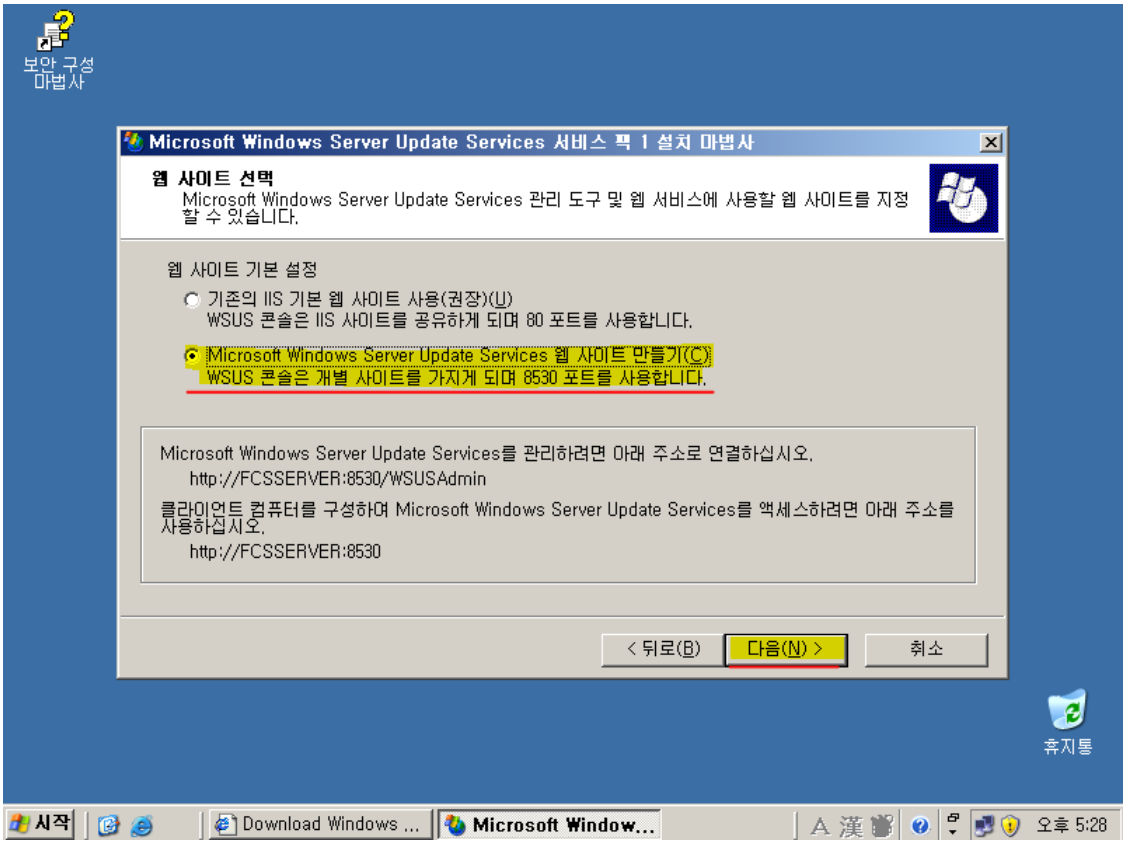
7. "이 컴퓨터에 있는 기존 데이터베이스 서버를 사용(U)" 선택 후 다음



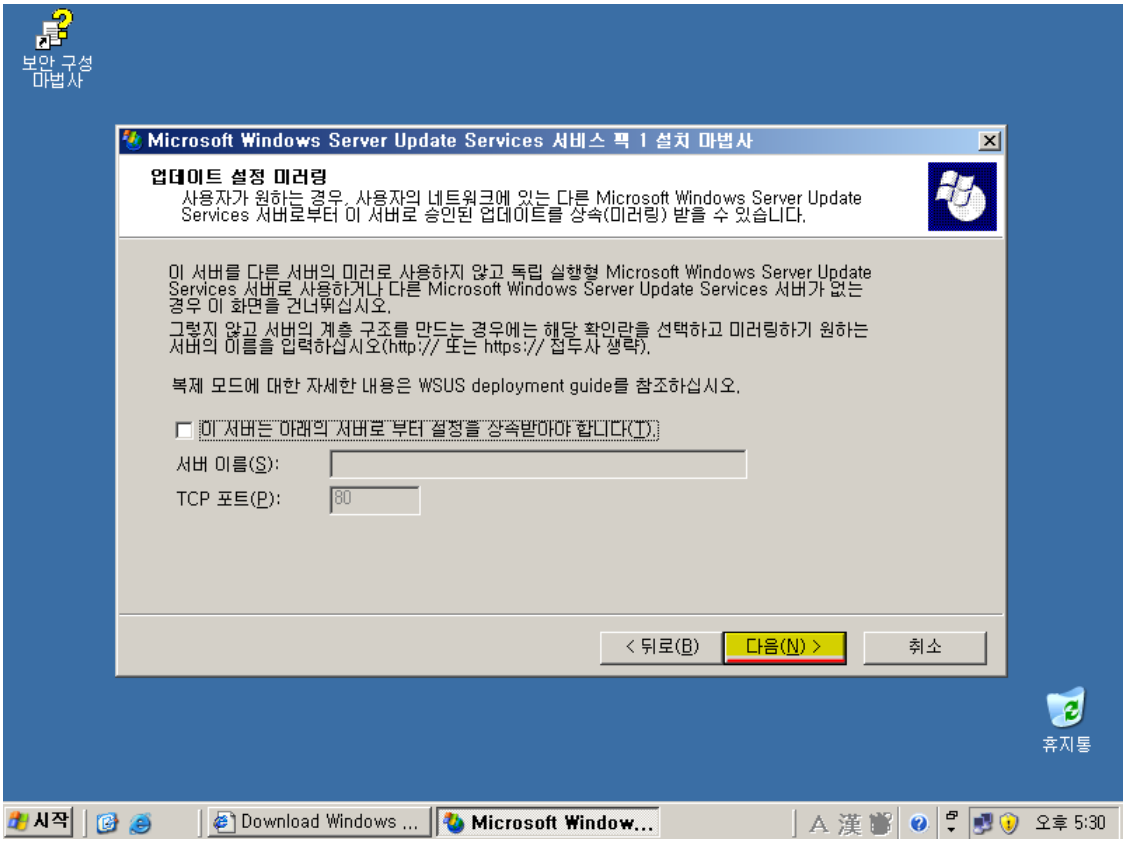
8. SQL 서버 인스턴스에 연결 – 다음



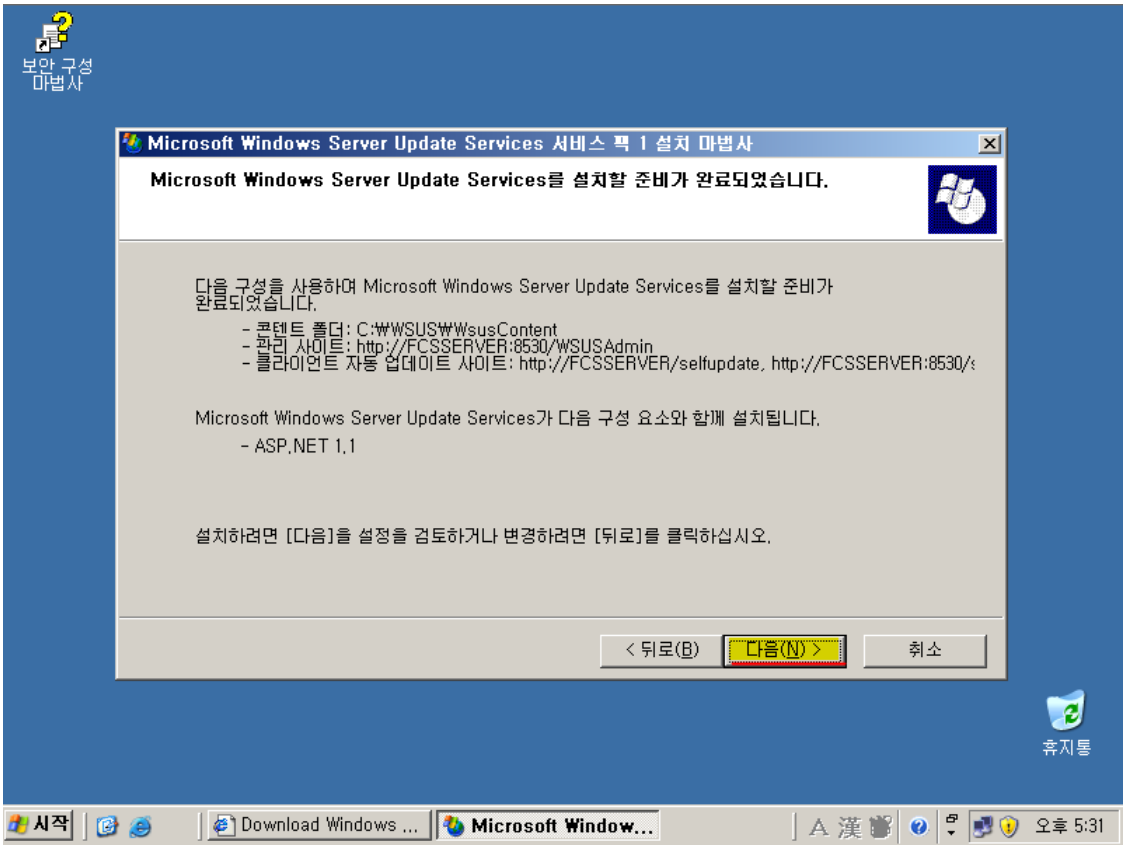
9. 웹 사이트 선택 – Microsoft Windows Server Update Services 웹 사이트 만들기(C) 선택



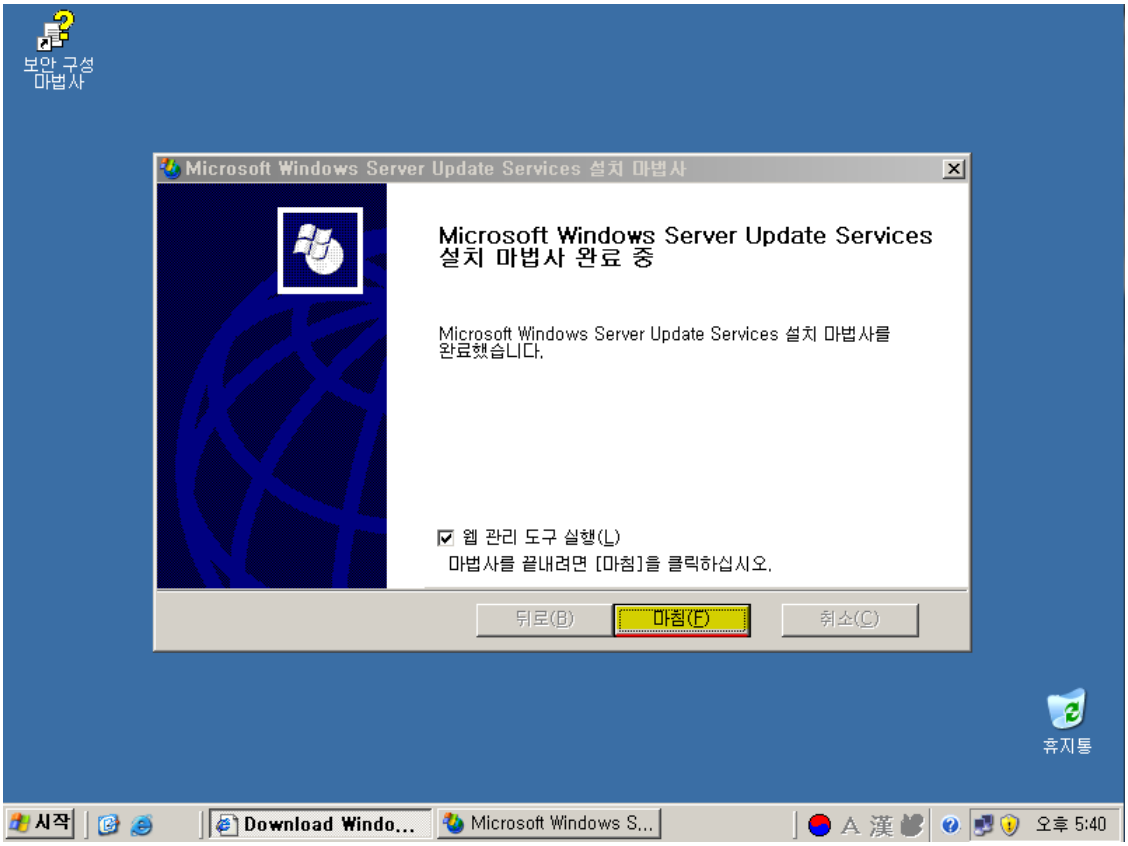
10. 업데이트 설정 미러링 – 체크 없이 다음



11. 설치 준비 완료 – 다음



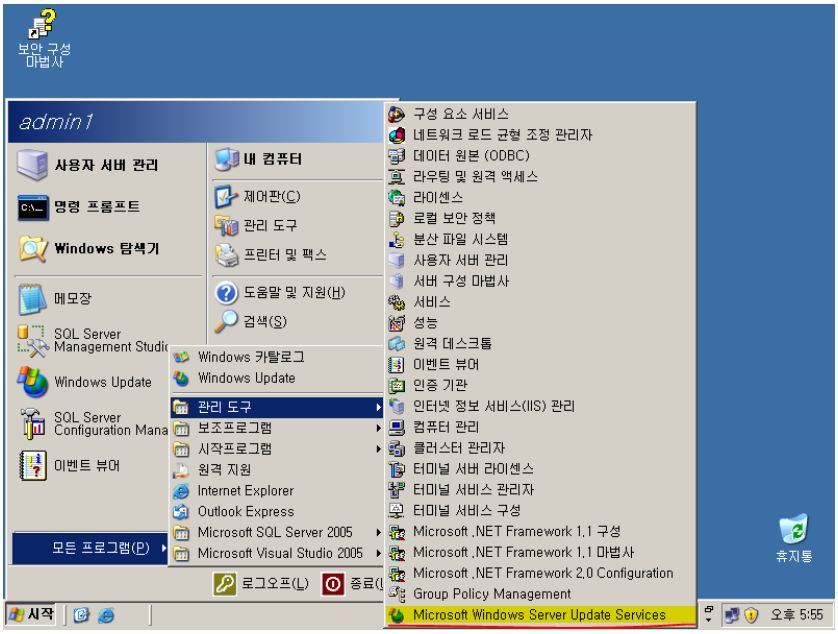
12. 설치 완료 – 마침



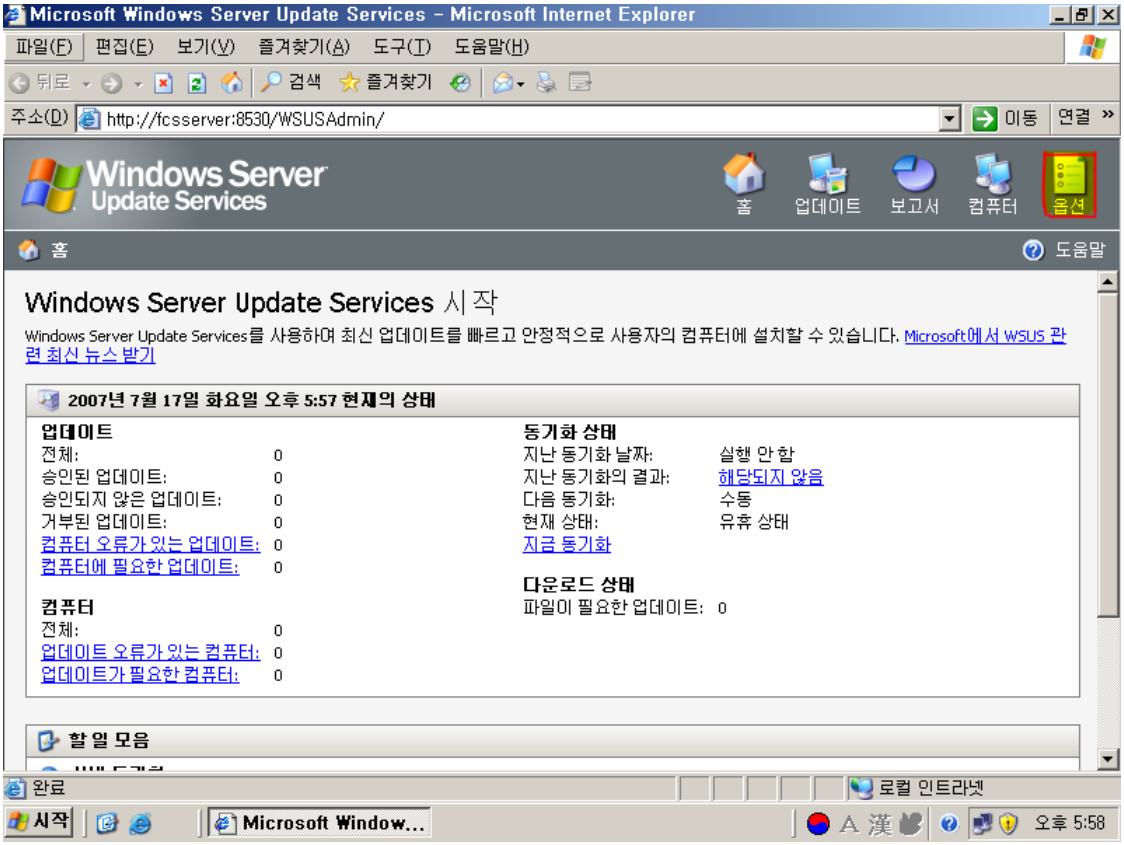
4.8. WSUS SP1 구성 및 동기화

Forefront Client Security를 설치하기 전에 WSUS를 구성하고 동기화해야 합니다.

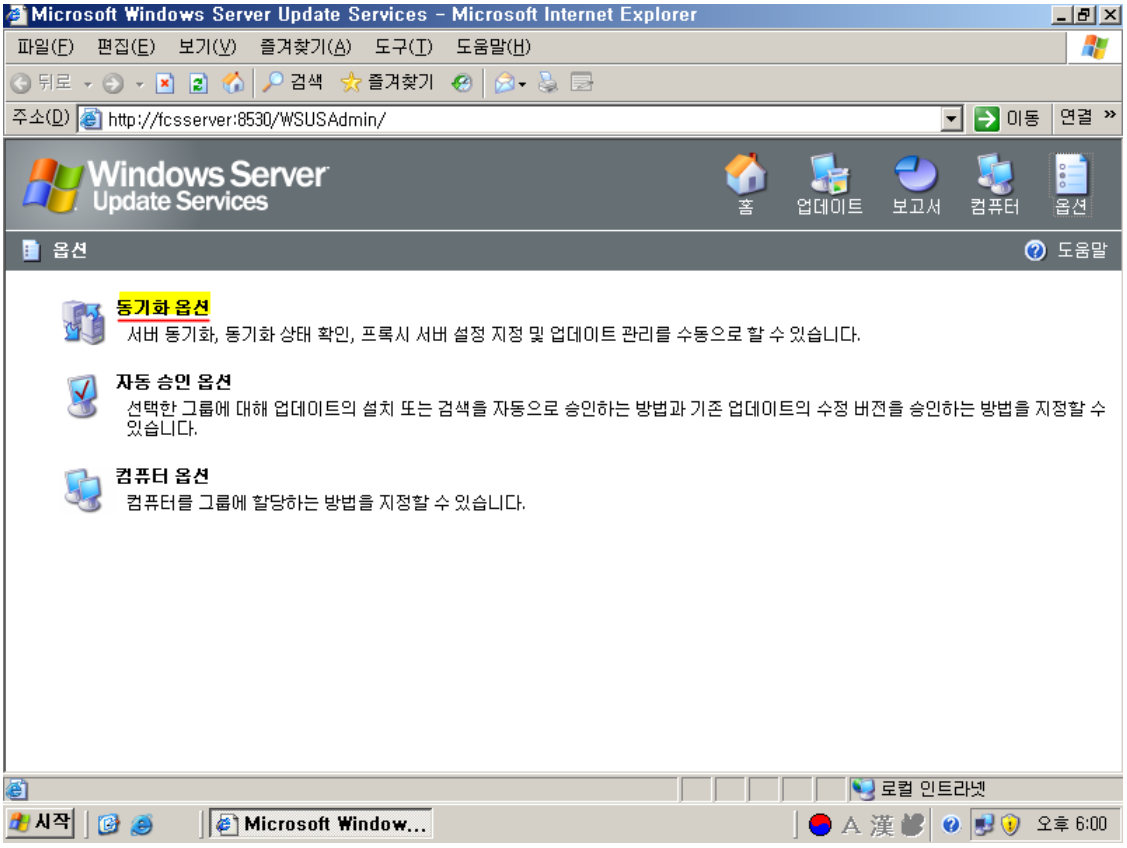
1. WSUS 콘솔 실행



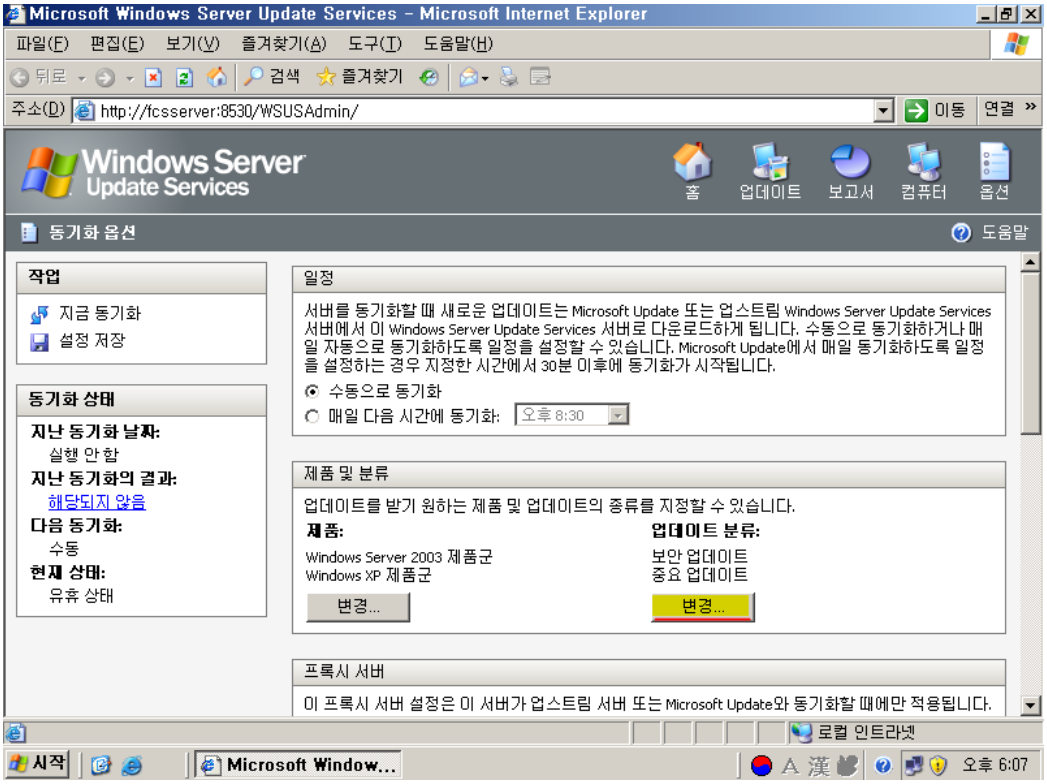
2. 옵션 선택



3. 동기화 옵션 선택

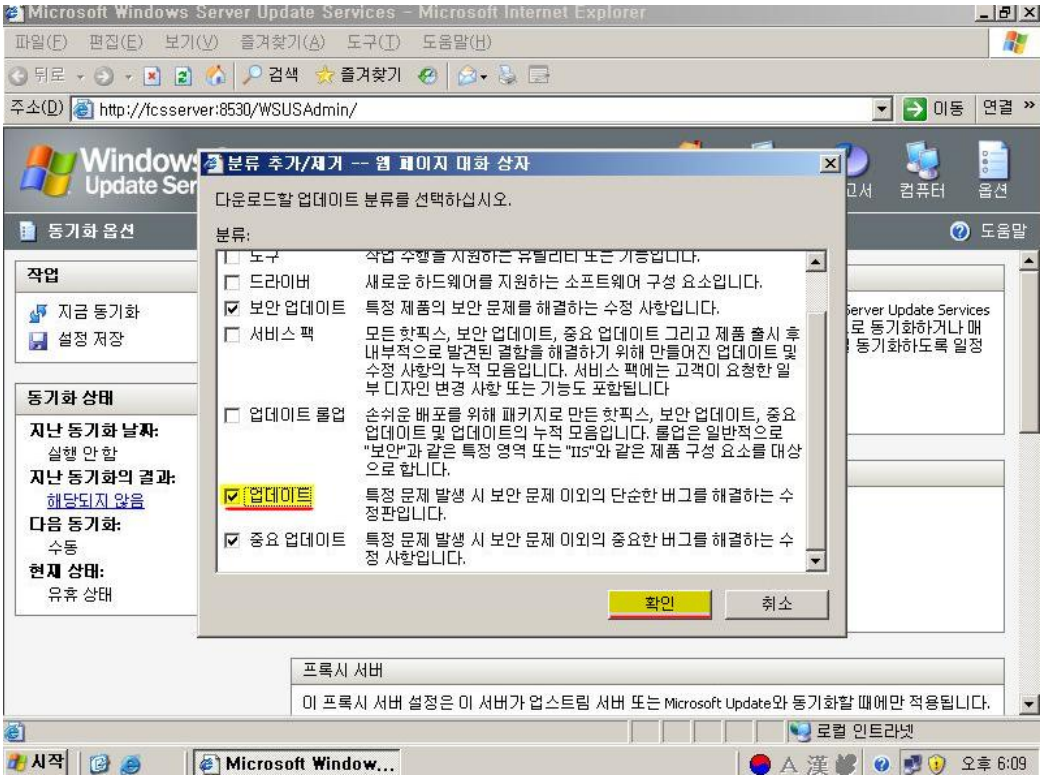


4. 업데이트 분류 에서 "변경..." 버튼 클릭

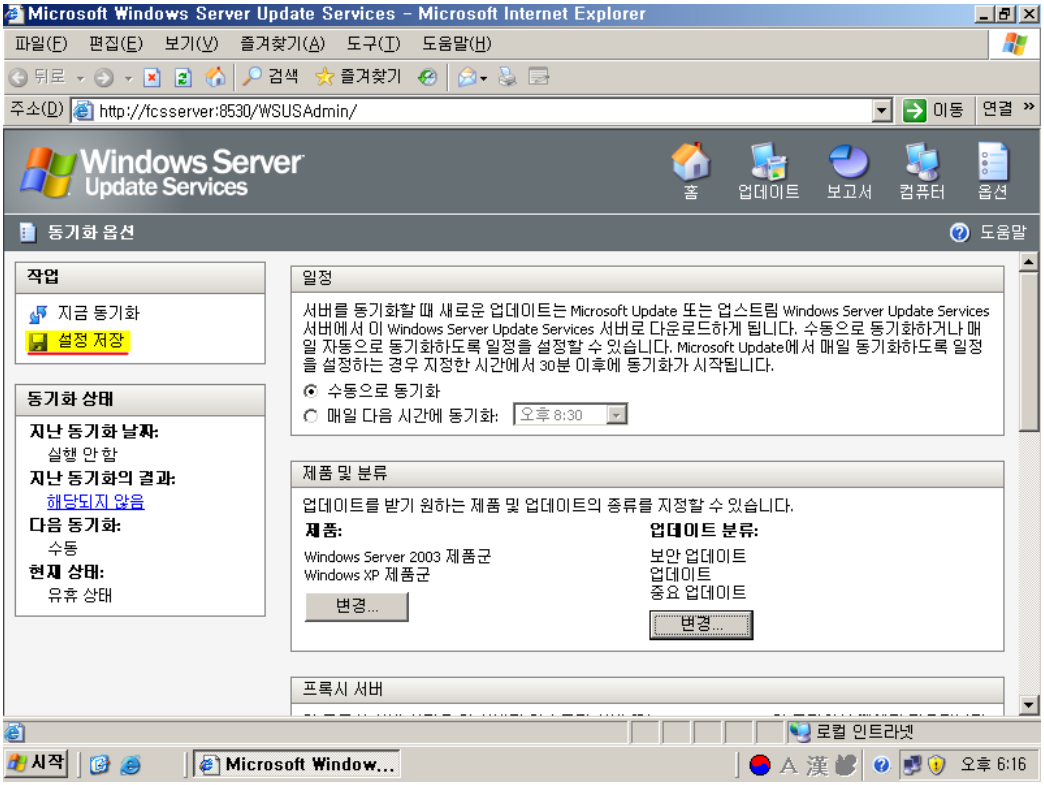


5. "업데이트" 항목에 체크 후 확인

참고 : 이 설정을 통해 WSUS에서 Client Security의 클라이언트 구성 요소를 다운로드 합니다. Client Security 정의 업데이트는 Client Security의 배포 서버 구성 요소를 설치하면 동기화 옵션으로 자동 선택됩니다.

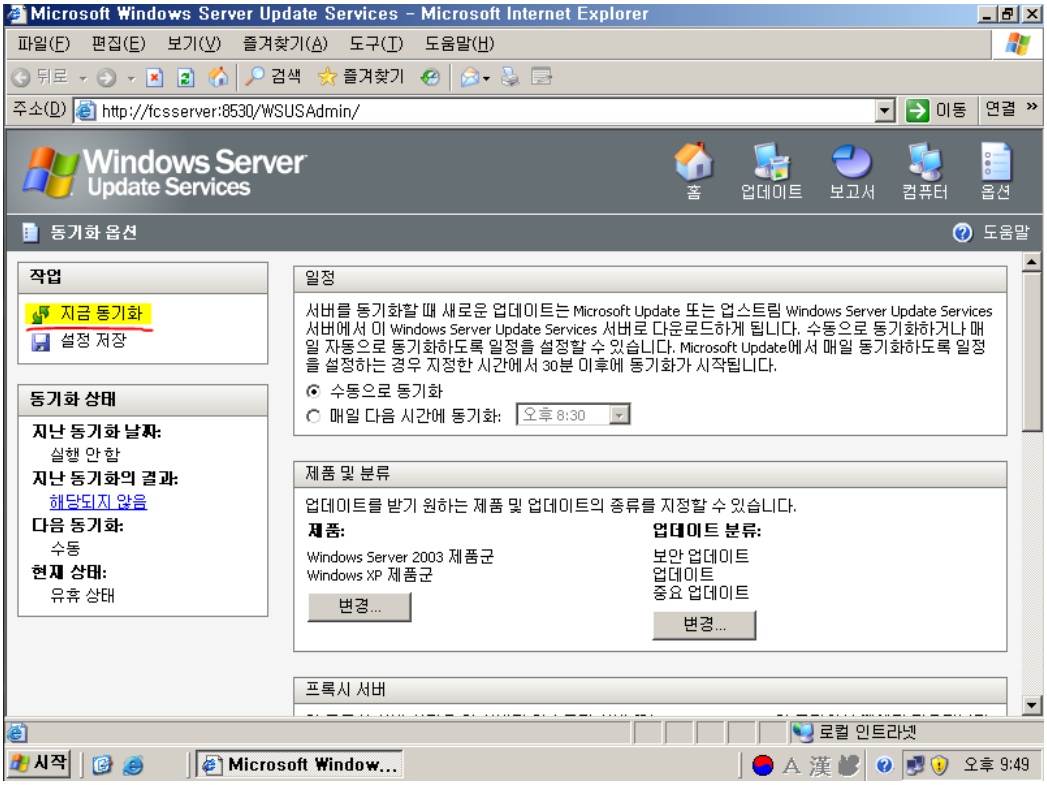


6. "설정 저장" 클릭

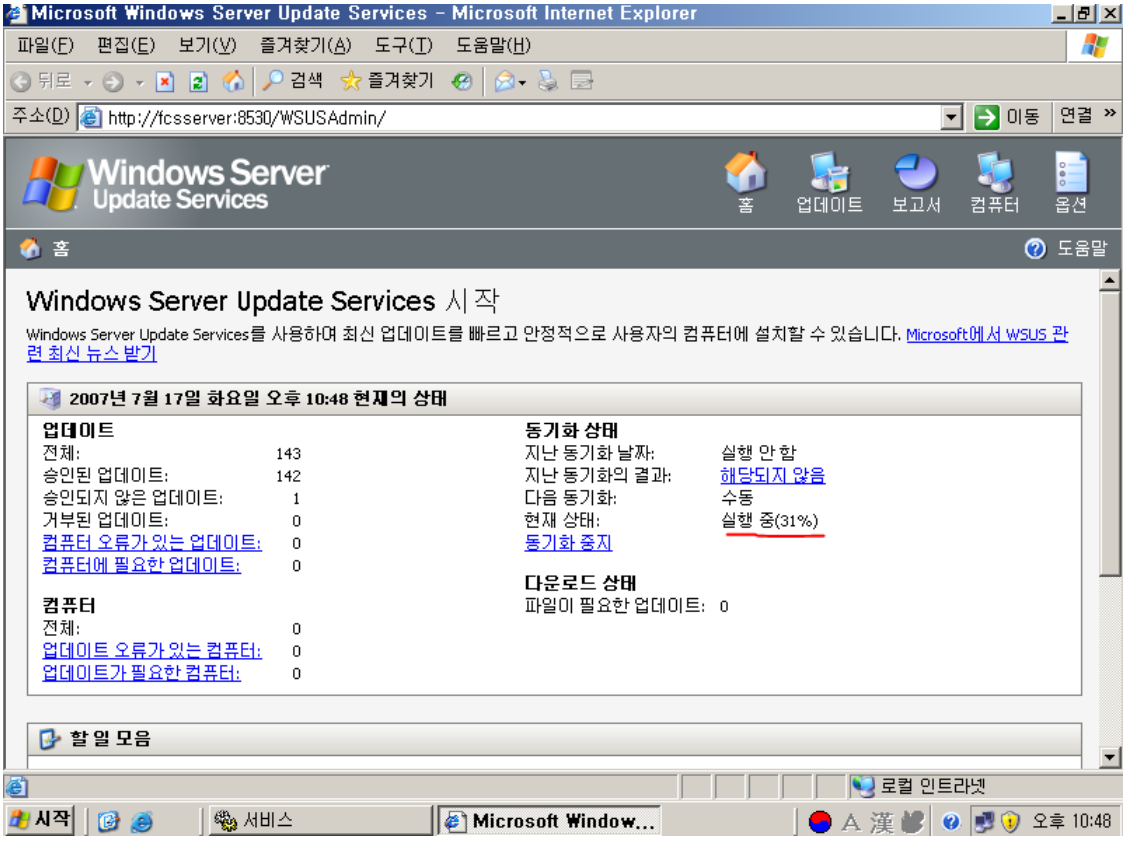


7. 동기화를 시작하려면 "지금 동기화" 클릭

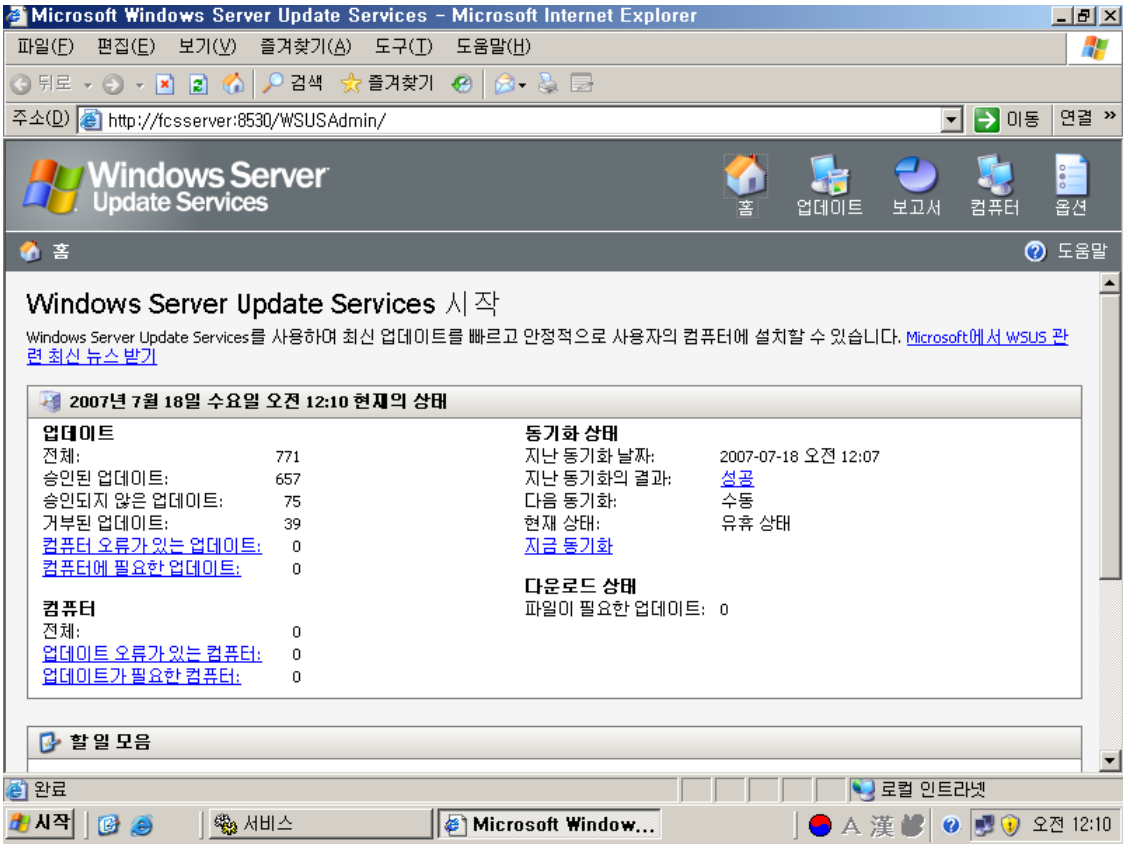
참고 : WSUS 서버를 처음 동기화하는 경우 몇 시간이 소요될 수 있습니다.



8. 동기화 진행 중 화면



9. 동기화 완료

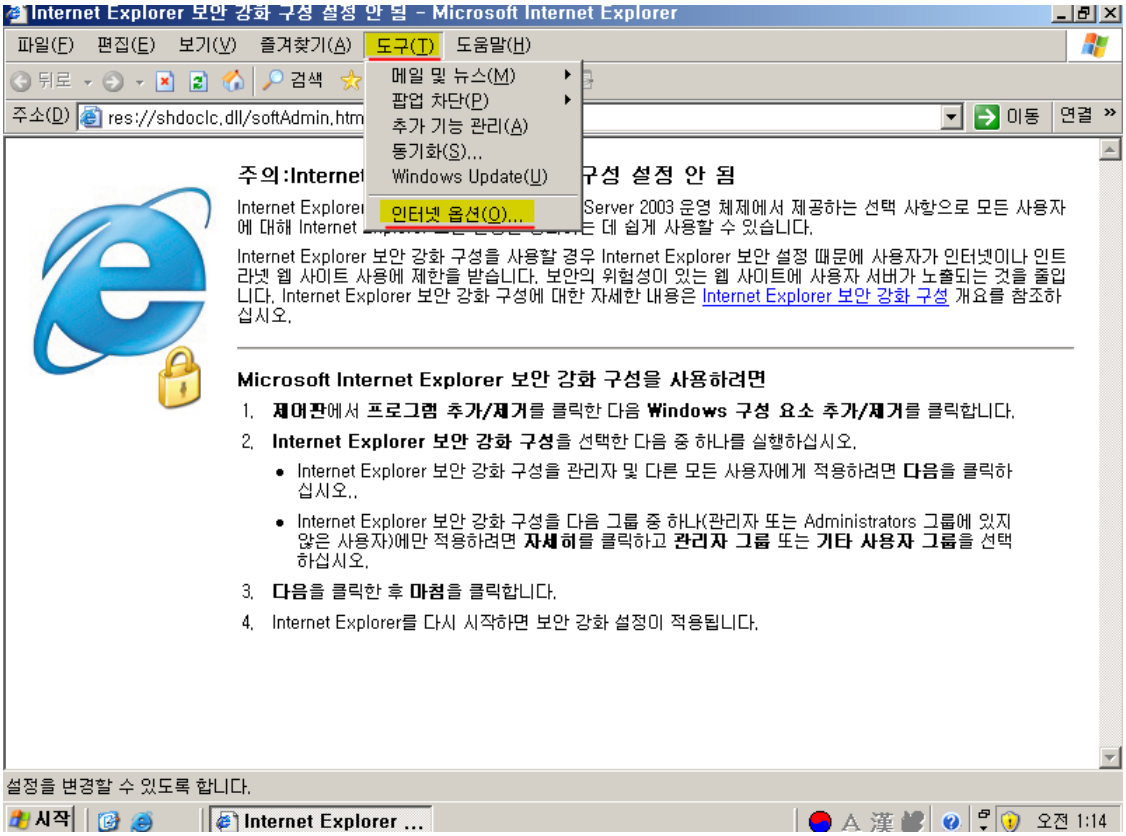


4.9. Internet Explorer의 로컬 인트라넷 영역에 보고 서버 사이트 추가

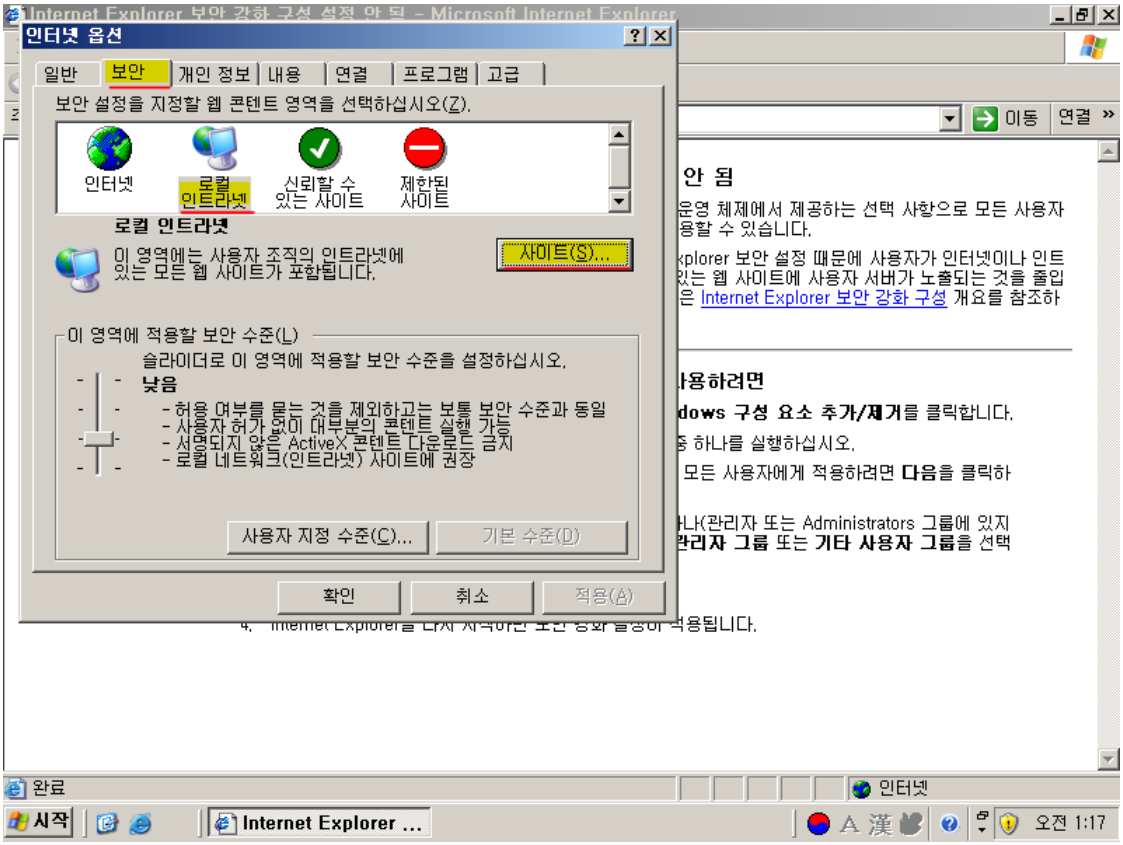
SQL Server Reporting Services를 올바르게 작동하려면 Client Security 서버의 로컬 인트라넷 영역에 보고 서버 사이트를 추가해야 합니다.

참고 : Internet Explorer는 로컬 인트라넷 영역에 대해 2개의 다른 사이트 목록을 유지해야 합니다. 향상된 보안 구성을 사용하는 경우에는 하나의 목록이 적용되고, 향상된 보안 구성을 사용하지 않는 경우에는 다른 목록이 적용됩니다. 로컬 인트라넷 영역에 웹 페이지를 추가하는 경우, 현재 적용이 가능한 한 목록에만 해당 웹 페이지를 추가합니다.

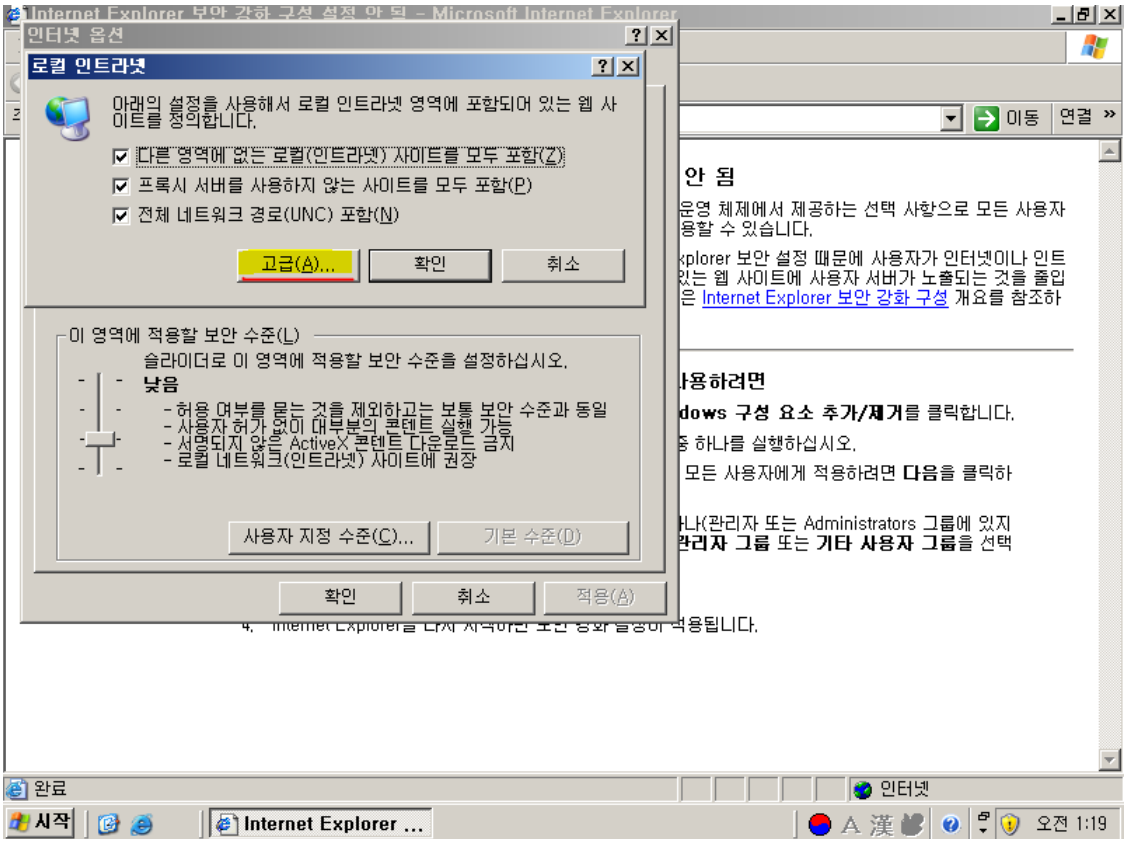
1. Internet Explorer의 도구 메뉴 – 인터넷 옵션



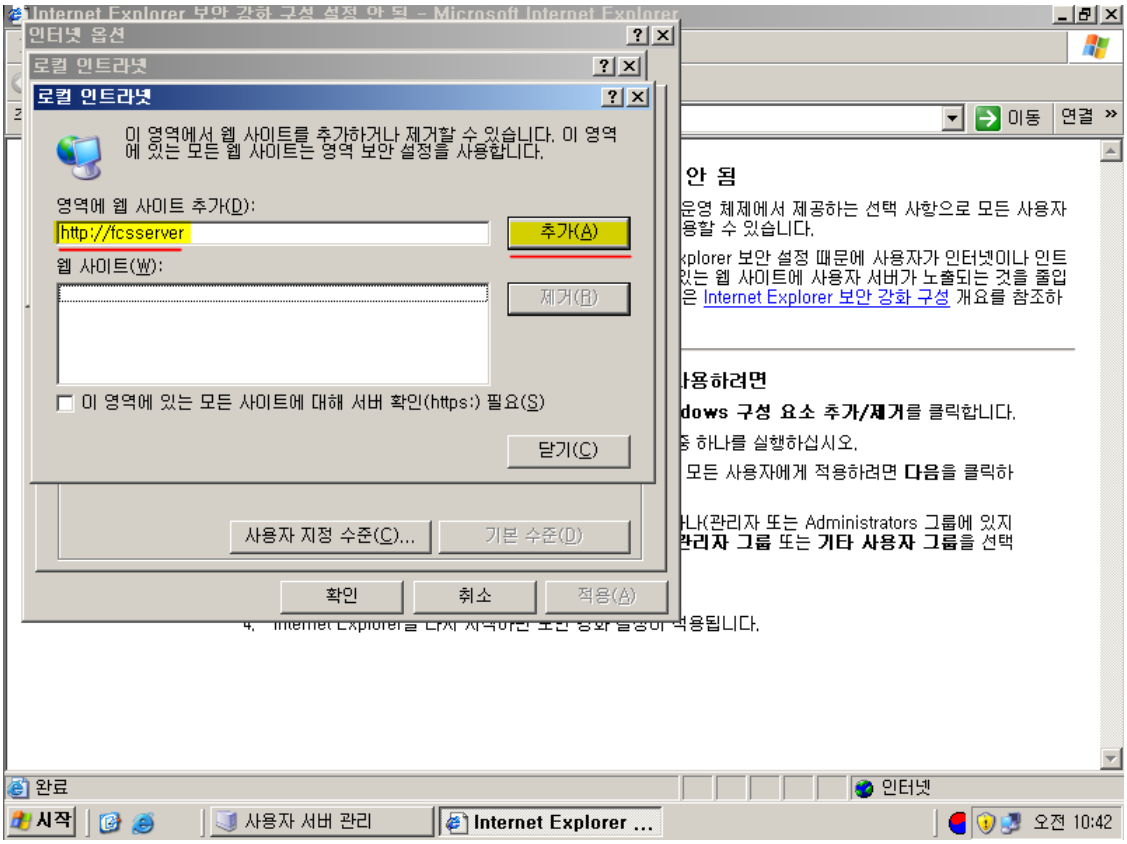
2. "보안" 탭 – "로컬 인트라넷" 영역 – "사이트" 버튼 클릭



3. "고급" 버튼 클릭



4. "영역에 웹 사이트 추가" 상자에 SQL Server Reporting Services 사이트의 URL 입력 후 "추가" 버튼 클릭



5. 단일 서버 토폴로지에 Client Security 설치 및 구성

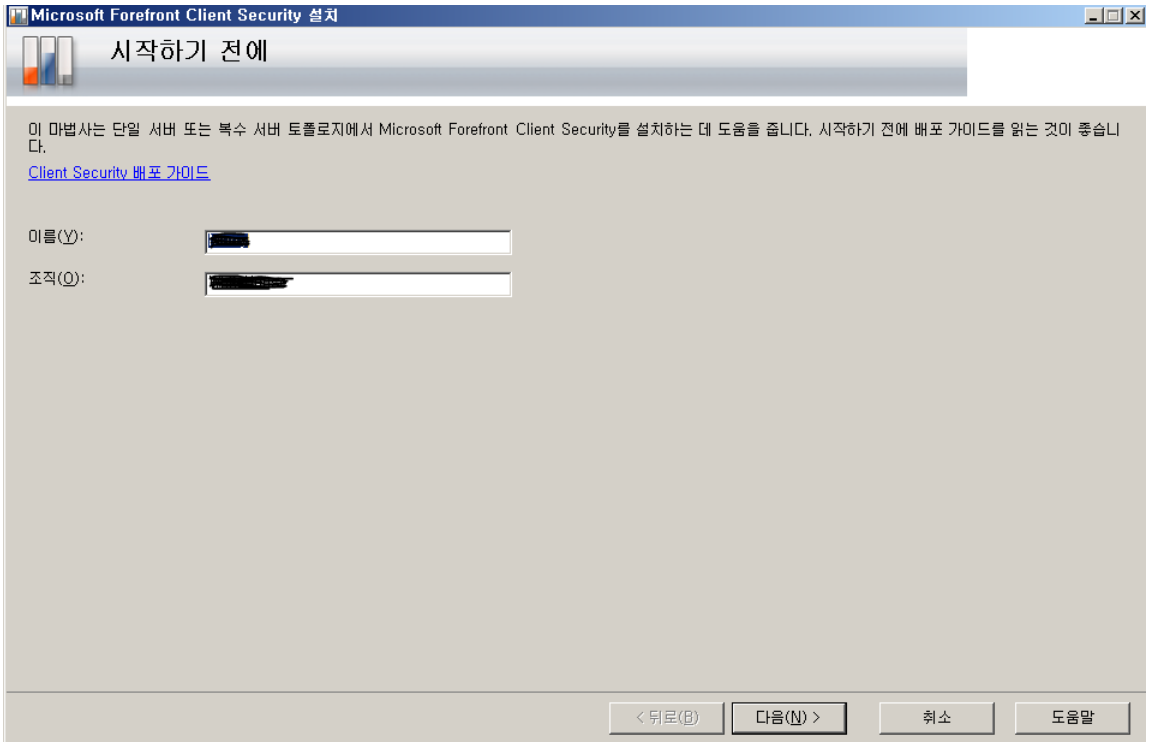
5.1. Forefront Client Security 설치

1. 로컬 관리자 권한이 있는 계정을 사용하여 Client Security를 설치할 서버에 로그인

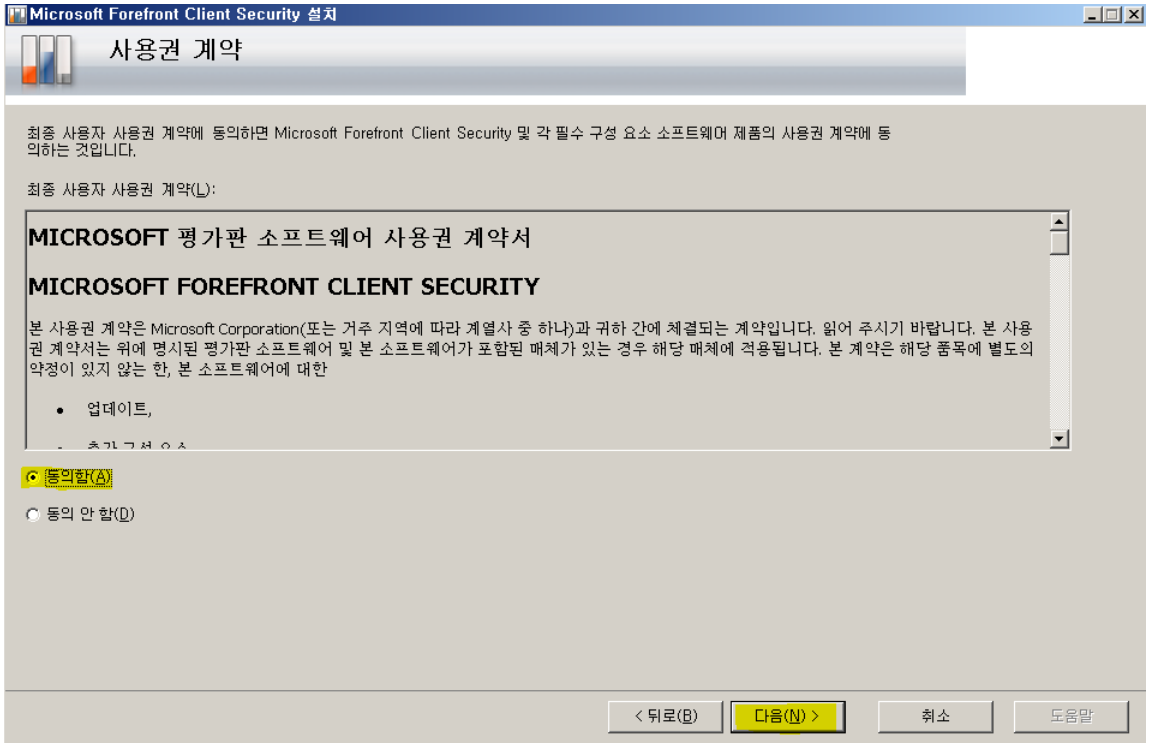
2. Microsoft Forefront Client Security 설치 씨디 삽입.

3. Forefront Client Security 첫 화면 – "설치 마법사 실행" 클릭

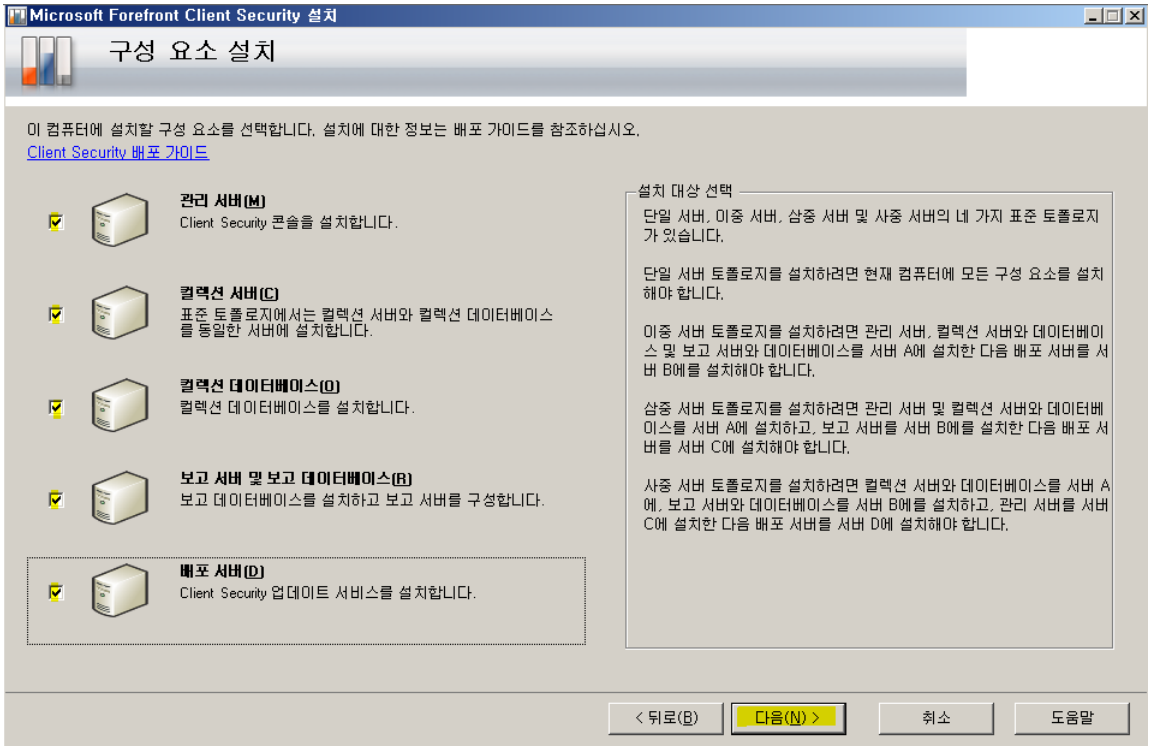
2. 이름과 조직 입력(컴퓨터의 사용자와 조직이 기본으로 나타남)



3. 사용권 계약 – "동의함" 선택 후 다음



4. 모두 체크 후 다음



5. 컬렉션 서버 설정

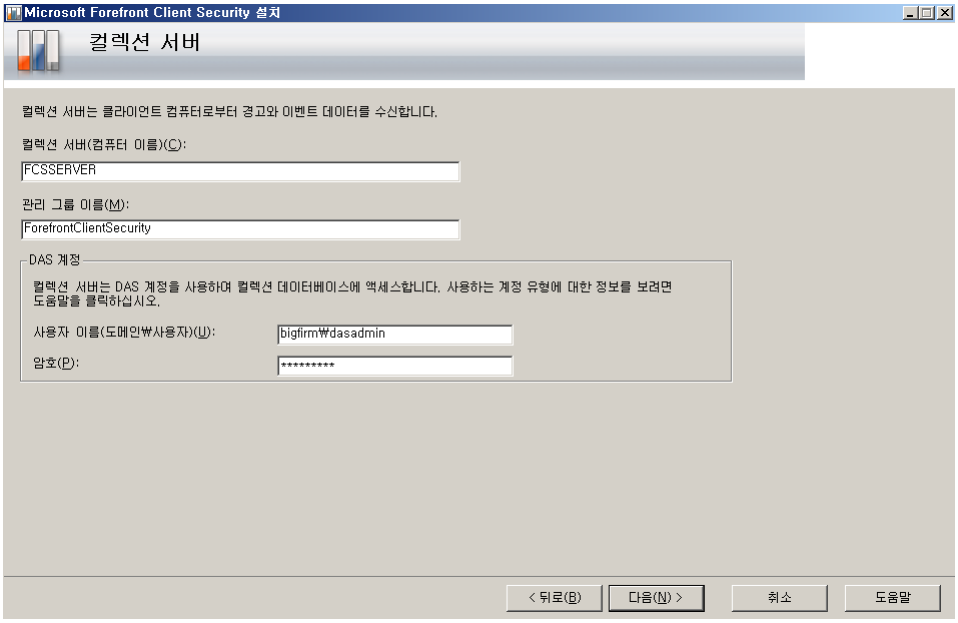
a. 컬렉션 서버(컴퓨터 이름)(C) : 현재 컴퓨터 이름 (기본값으로 들어가 있음)

b. 관리 그룹 이름 : 원하는 이름 입력 (기본값 : ForefrontClientSecurity)

주의 : 이름에 공백을 포함시켜서는 안됨.

c. DAS 계정 : DAS 계정의 사용자 이름과 암호 입력

주의 : 작업 계정에 DAS 계정을 다시 사용할 경우, 로컬 관리자 권한을 부여해야 함 (Client Security는 설치 중 DAS 계정에 권한을 자동으로 부여)

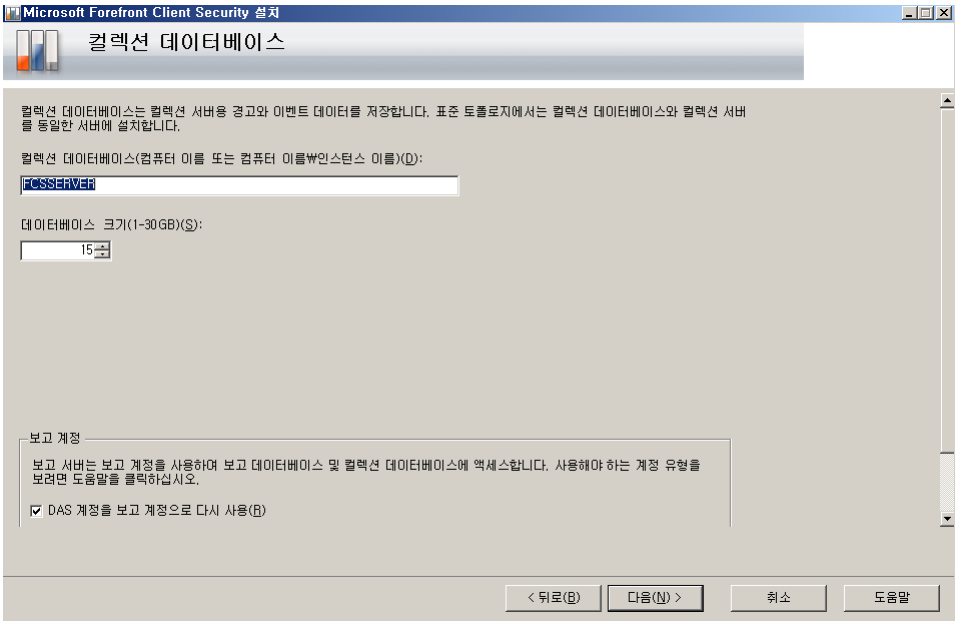


6. 컬렉션 데이터베이스

a. 컬렉션 데이터베이스 이름 : 현재 컴퓨터의 이름 입력 (기본값으로 들어가 있음)

b. 데이터베이스 크기 : 원하는 값 입력 (기본값 : 15Gb)

c. 보고 계정 – DAS 계정을 보고 계정으로 다시 사용(R) 체크

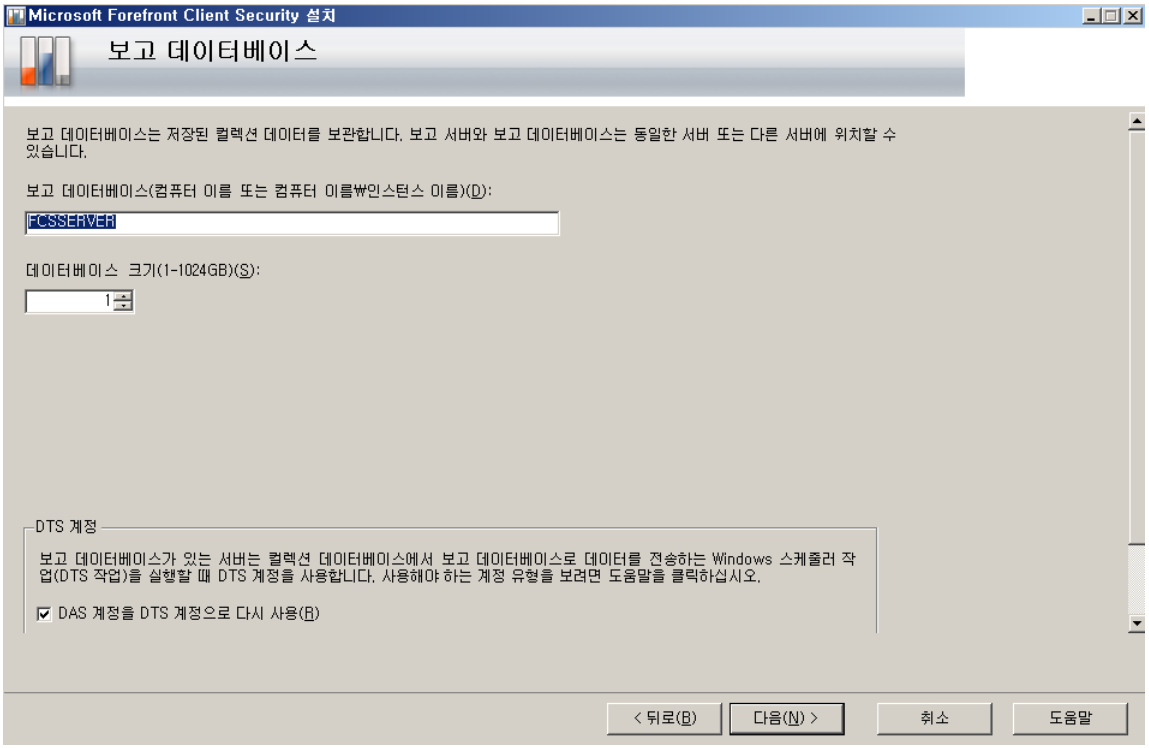


7. 보고 데이터베이스

a. 보고 데이터베이스 이름 – 현재 컴퓨터의 이름 입력 (기본값으로 들어가 있음)

b. 데이터베이스 크기 : 원하는 값 입력 (기본값 : 1Gb)

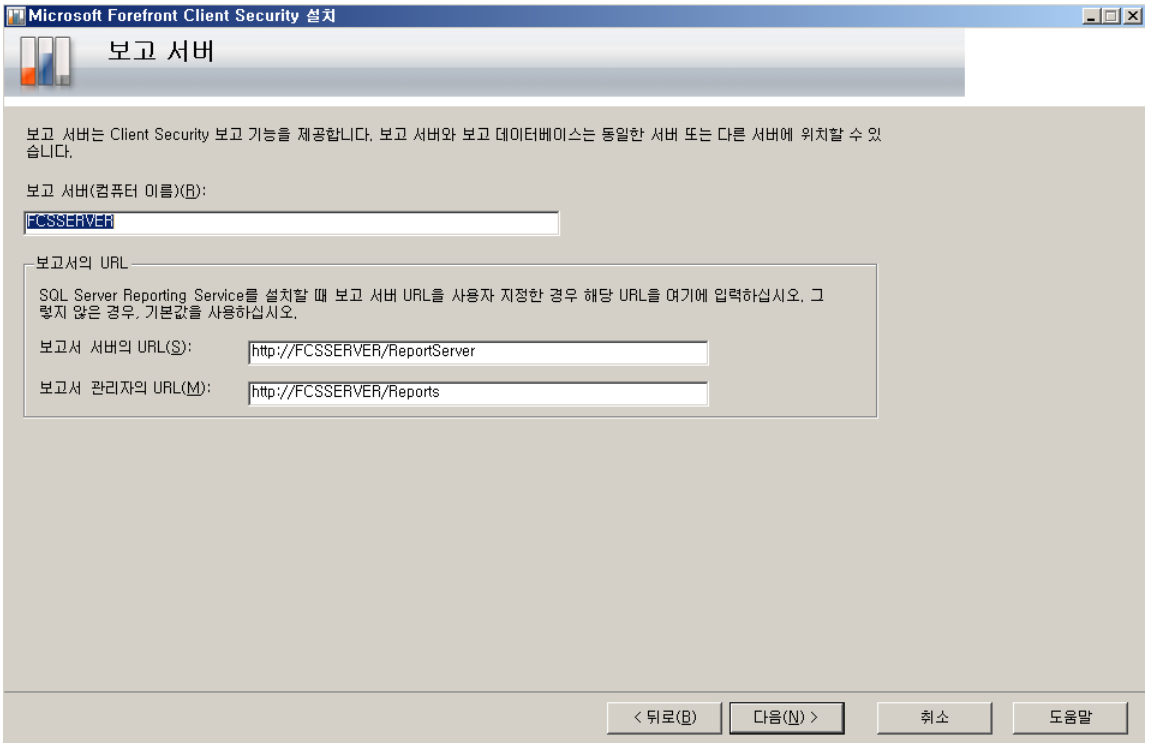
c. DTS 계정 – DAS 계정을 보고 계정으로 다시 사용(R) 체크



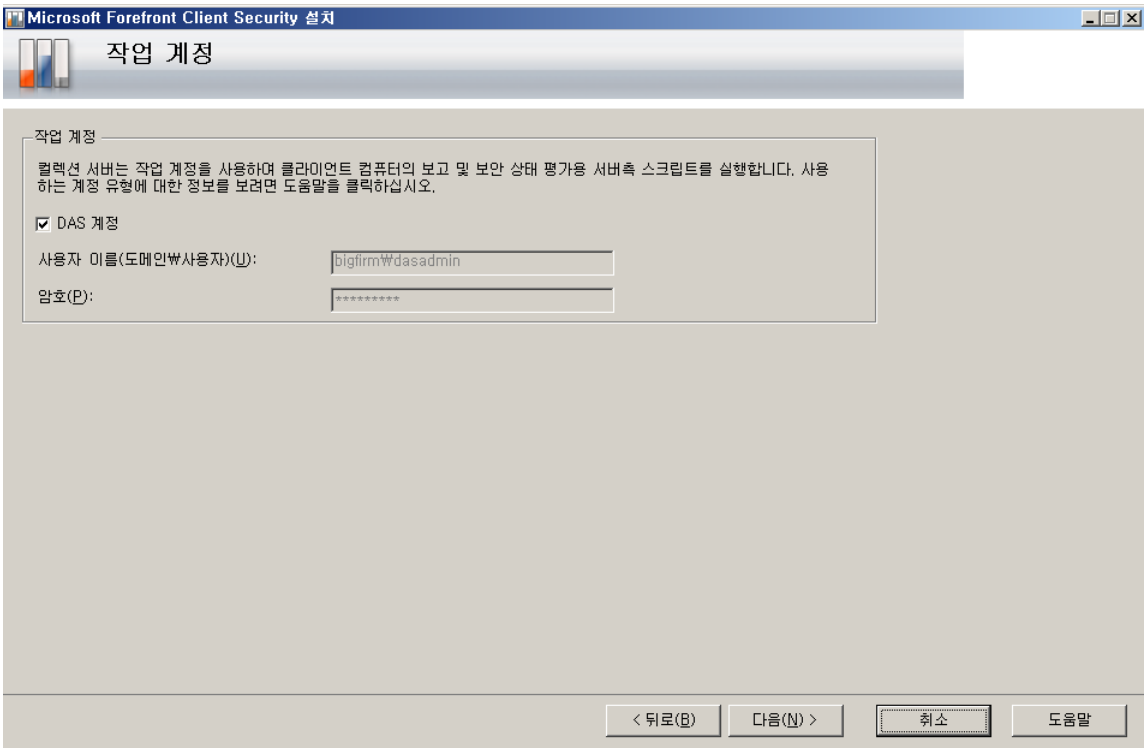
8. 보고 서버

a. 보고 서버 이름 – 현재 컴퓨터의 이름 입력 (기본값으로 들어가 있음)

b. 보고서 서버의 URL 및 보고서 관리자의 URL – SQL Server Reporting Services 설치 시 지정한 URL 입력.

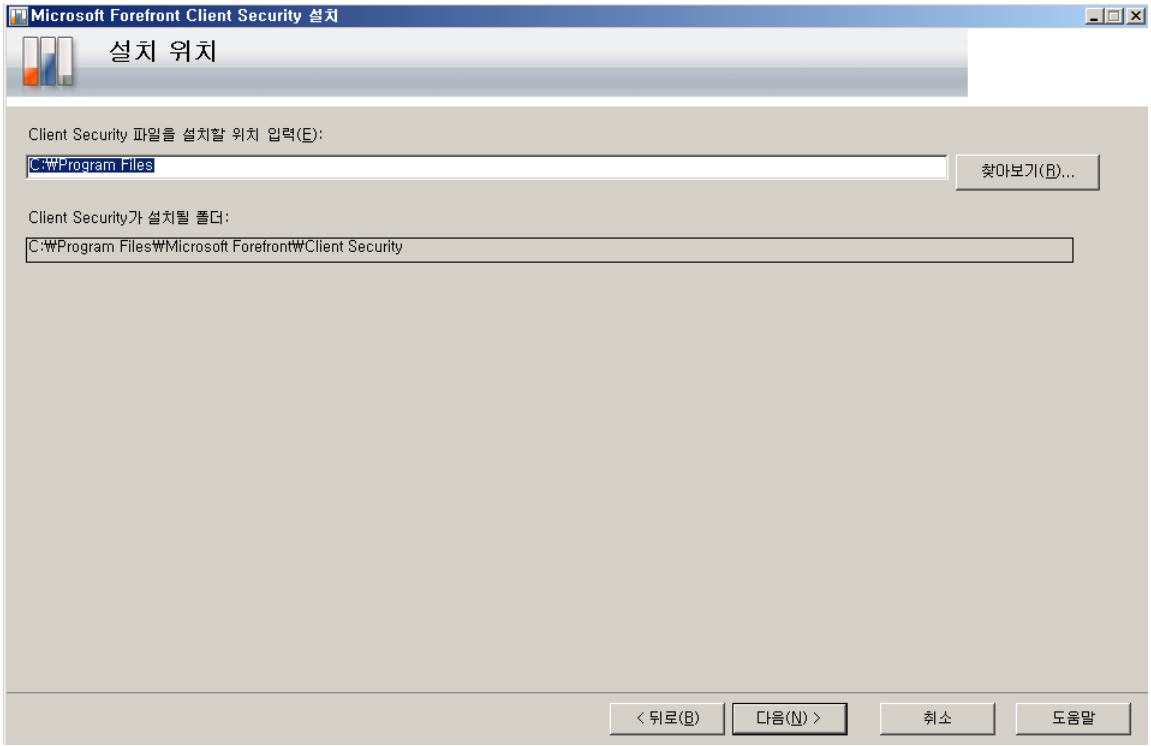


9. 작업 계정 – DAS 계정 사용 권장



10. 설치 위치 – 기본값 사용(C:₩Program Files₩Microsoft Forefront₩Client Security)

참고 : "찾아보기(R)" 버튼을 눌러 설치 위치를 바꿀 수 있음.



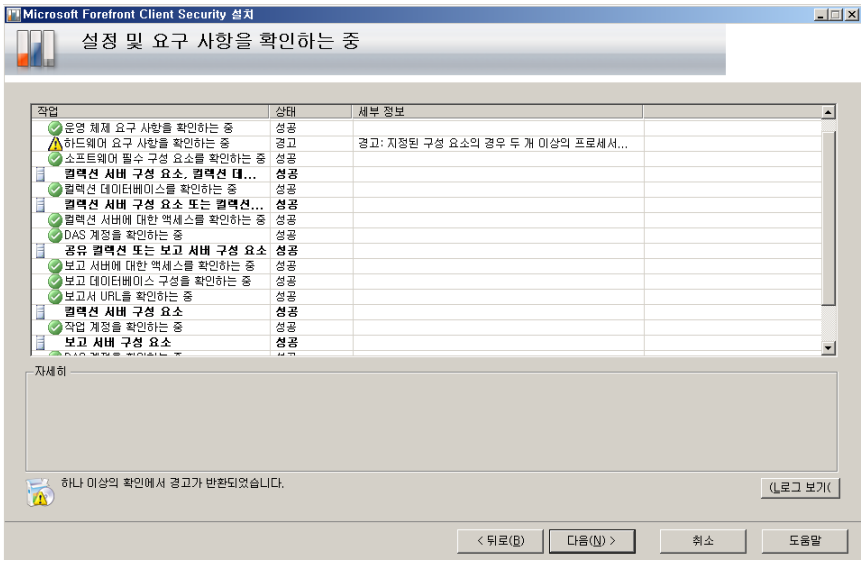
11. 설정 및 요구 사항을 확인 하는 중

*참고 : 오류가 발생하면 Client Security 설치를 계속할 수 없습니다.

경고나 오류가 발생하는 경우에는 다음 리소스에서 자세한 내용을 참조하십시오.

*설치 로그 파일 ("로그 보기" 클릭) - 설치 로그 파일에 대한 자세한 내용은 Client Security 문제 해결 가이드에서 로그 파일(http://go.microsoft.com/fwlink/?LinkId=82466)(영문)을 참조하십시오.

*Client Security 문제 해결 가이드의 설치 문제 해결 (http://go.microsoft.com/fwlink/?LinkId=82442)(영문)을 참조하십시오.



12. 설치 마법사 완료

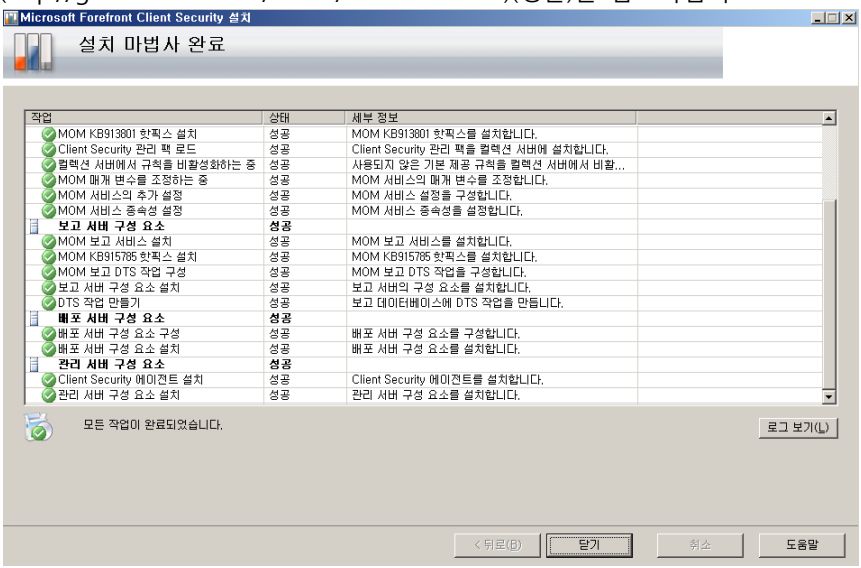
*참고 : Client Security를 성공적으로 설치했는지 확인한 다음 닫기를 클릭합니다.

오류가 발생하면 Client Security 설치를 계속할 수 없습니다.

경고나 오류가 발생하는 경우에는 다음 리소스에서 자세한 내용을 참조하십시오.

*설치 로그 파일 ("로그 보기" 클릭). 설치 로그 파일에 대한 자세한 내용은 Client Security 문제 해결 가이드에서 로그 파일(http://go.microsoft.com/fwlink/?LinkId=82466)(영문)을 참조하십시오.

*Client Security 문제 해결 가이드의 설치 문제 해결 (http://go.microsoft.com/fwlink/?LinkId=82442)(영문)을 참조하십시오.

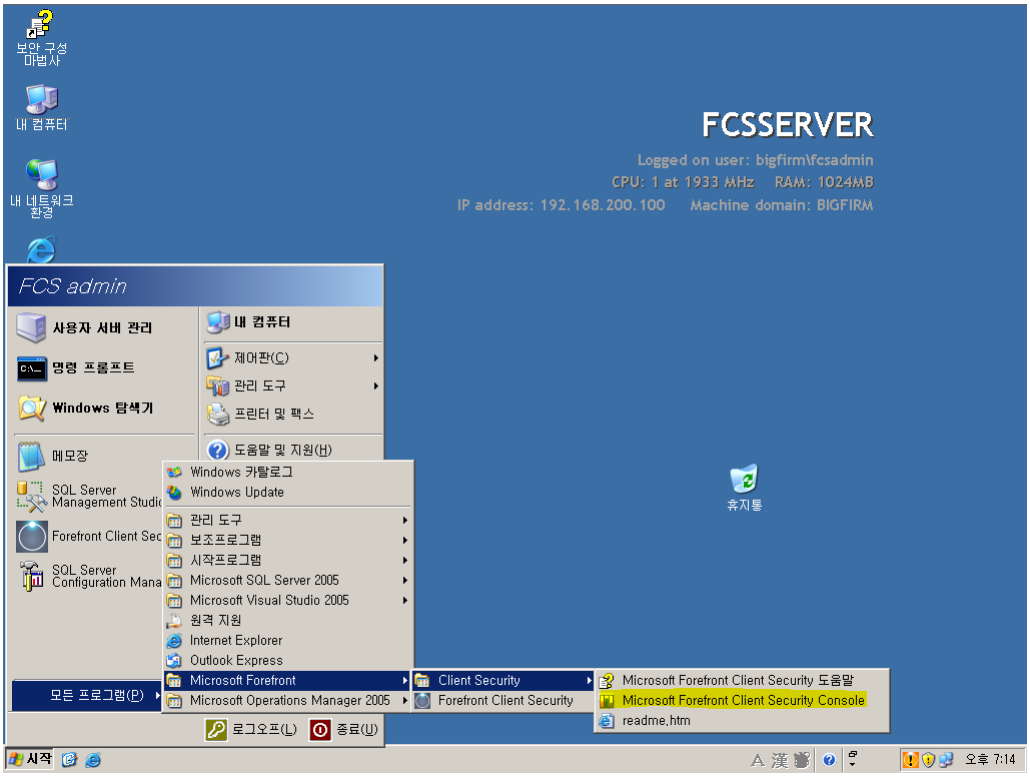


5.2. Forefront Client Security 구성

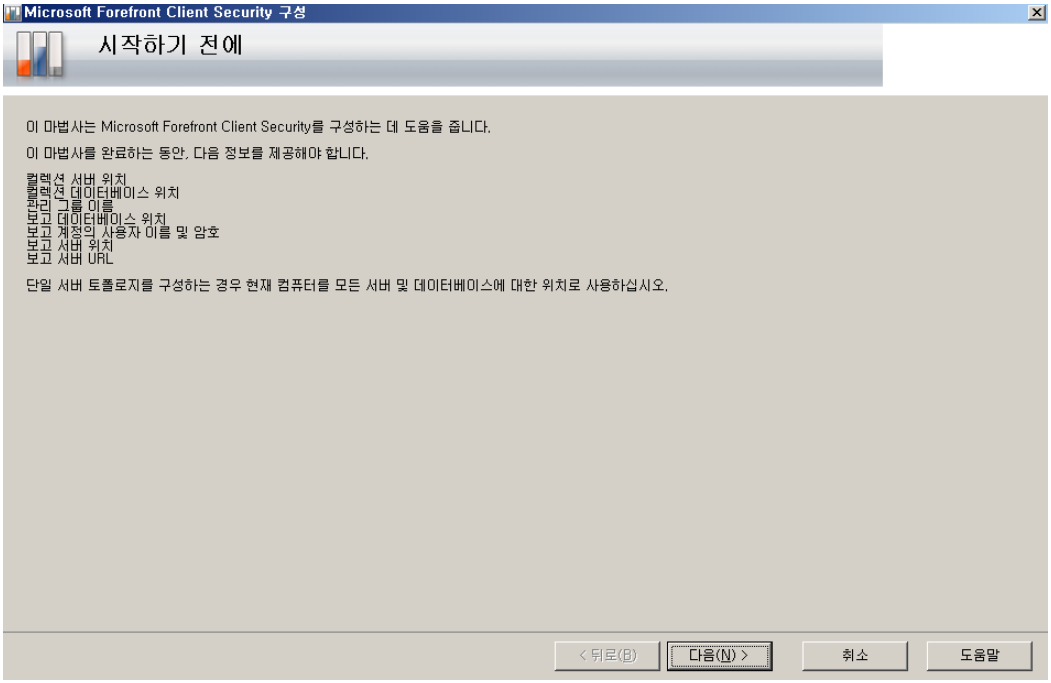
Client Security를 구성하려면 구성 마법사를 실행해야 합니다. 마법사는 Client Security 콘솔을 처음으로 열 때 자동으로 실행 됩니다.

1. Forefront Client Security 콘솔 실행

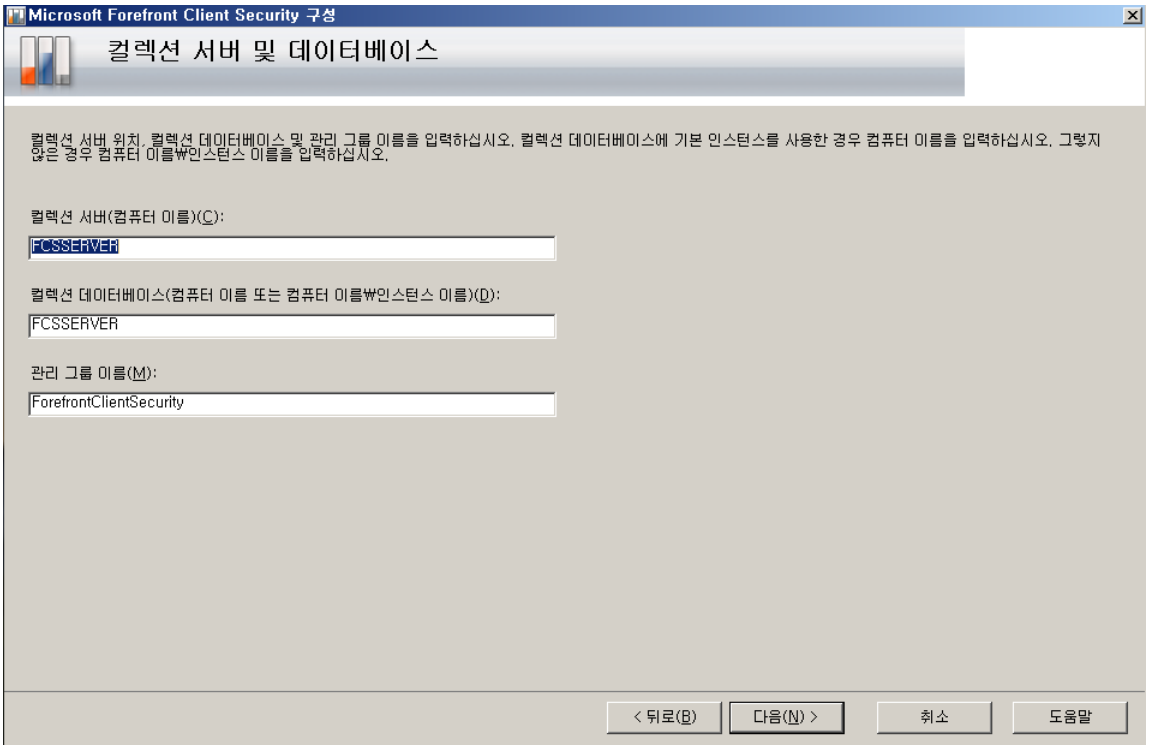
(시작-모든 프로그램 - Microsoft Forefront - Client Security – Microsoft Forefront Client Security Console)



2. "다음" 버튼 클릭



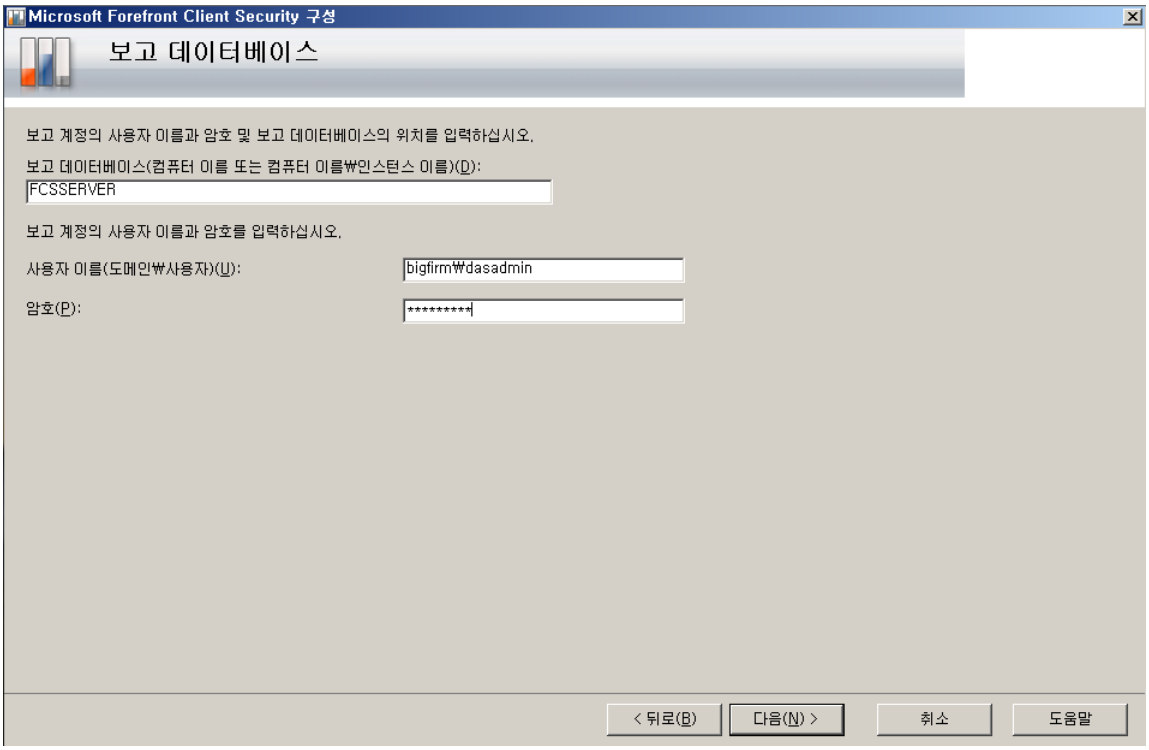
3. 컬렉션 서버 및 데이터베이스 – 설치 시 기본값을 수정하지 않았다면 "다음" 버튼을 눌러 계속 진행한다. (수정하였다면, 그에 맞는 값을 넣도록 한다.)



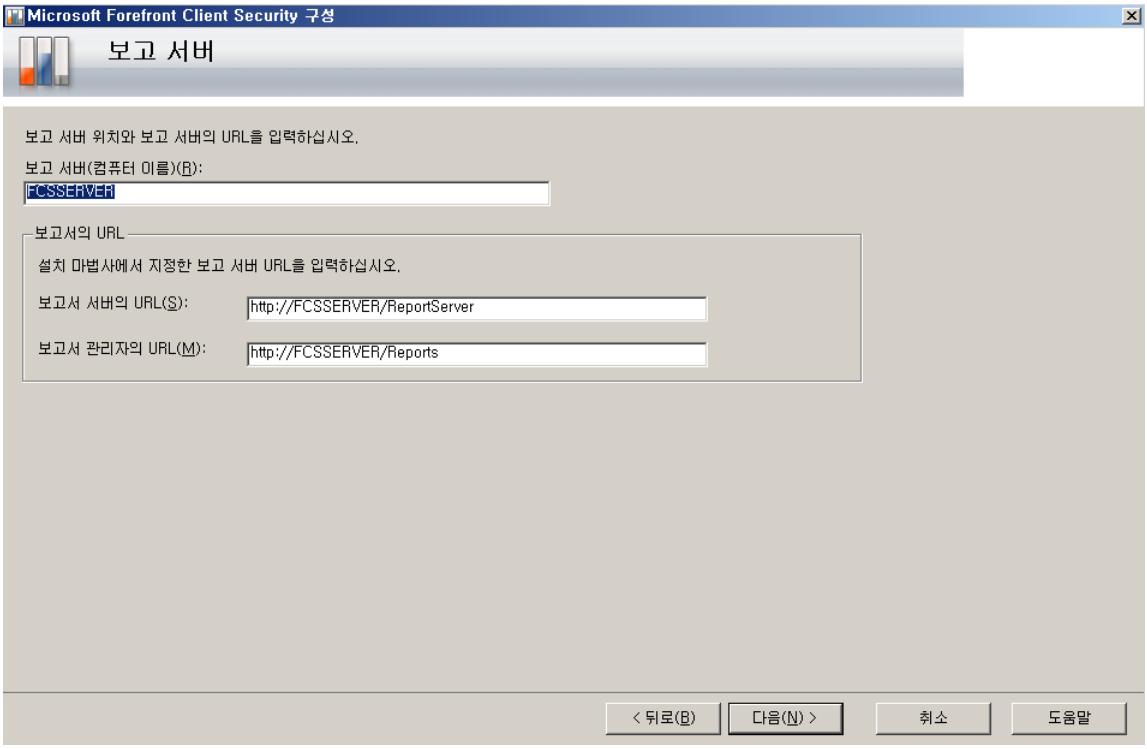
4. 보고 데이터베이스

a. 보고 데이터베이스 : 현재 컴퓨터 이름(기본 값)을 입력. (필요한 경우, SQL Server 인스턴스 입력)

b. 사용자 이름과 암호 : 보고 계정의 사용자 이름과 암호를 입력한다.



5. 보고 서버 - 설치 시 기본값을 수정하지 않았다면 "다음" 버튼을 눌러 계속 진행한다.
(수정하였다면, 그에 맞는 값을 넣도록 한다.)



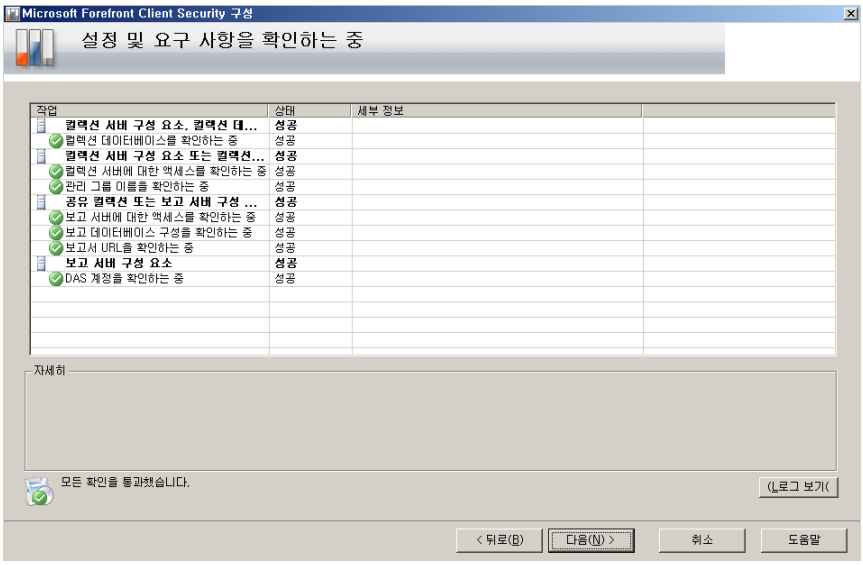
6. 설정 및 요구 사항을 확인 하는 중

*참고 : 오류가 발생하면 Client Security 구성을 계속할 수 없습니다.

경고나 오류가 발생하는 경우에는 다음 리소스에서 자세한 내용을 참조하십시오.

*구성 로그 파일 ("로그 보기" 클릭) - 구성 로그 파일에 대한 자세한 내용은 Client Security 문제 해결 가이드에서 로그 파일(http://go.microsoft.com/fwlink/?LinkId=82466)(영문)을 참조하십시오.

*Client Security 문제 해결 가이드의 설치 문제 해결 (http://go.microsoft.com/fwlink/?LinkId=82442)(영문)을 참조하십시오.



7. 구성 마법사 완료

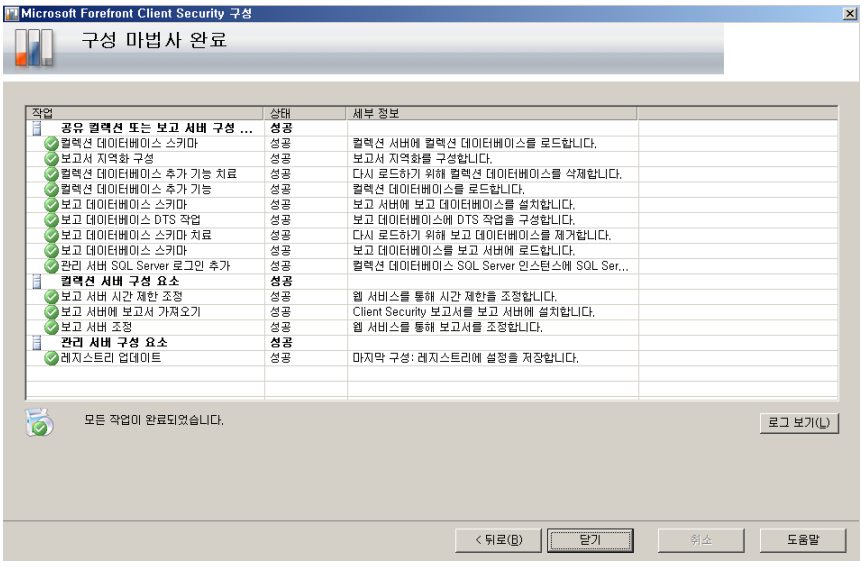
*참고 : Client Security를 성공적으로 구성했는지 확인한 다음 닫기를 클릭합니다.

오류가 발생하면 Client Security 구성을 계속할 수 없습니다.

경고나 오류가 발생하는 경우에는 다음 리소스에서 자세한 내용을 참조하십시오.

*구성 로그 파일 ("로그 보기" 클릭). 구성 로그 파일에 대한 자세한 내용은 Client Security 문제 해결 가이드에서 로그 파일(http://go.microsoft.com/fwlink/?LinkId=82466)(영문)을 참조하십시오.

*Client Security 문제 해결 가이드의 설치 문제 해결 (http://go.microsoft.com/fwlink/?LinkId=82442)(영문)을 참조하십시오.

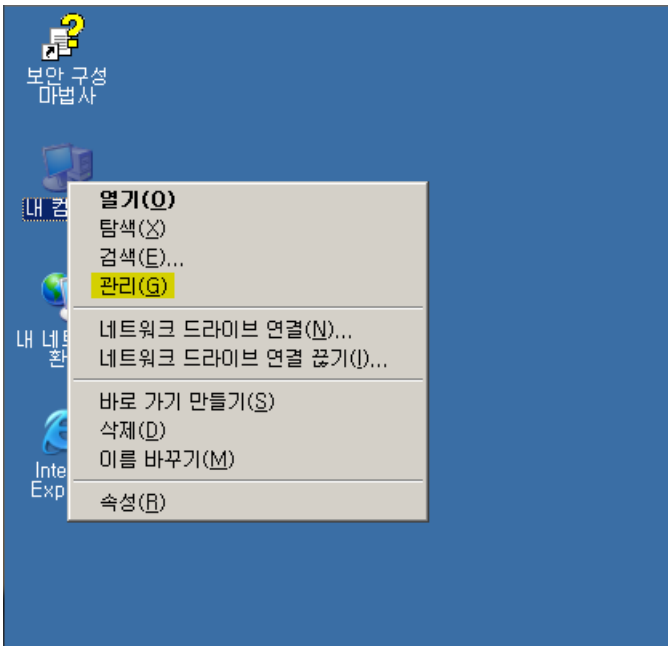


5.3. 서비스 계정에 대한 올바른 권한 부여

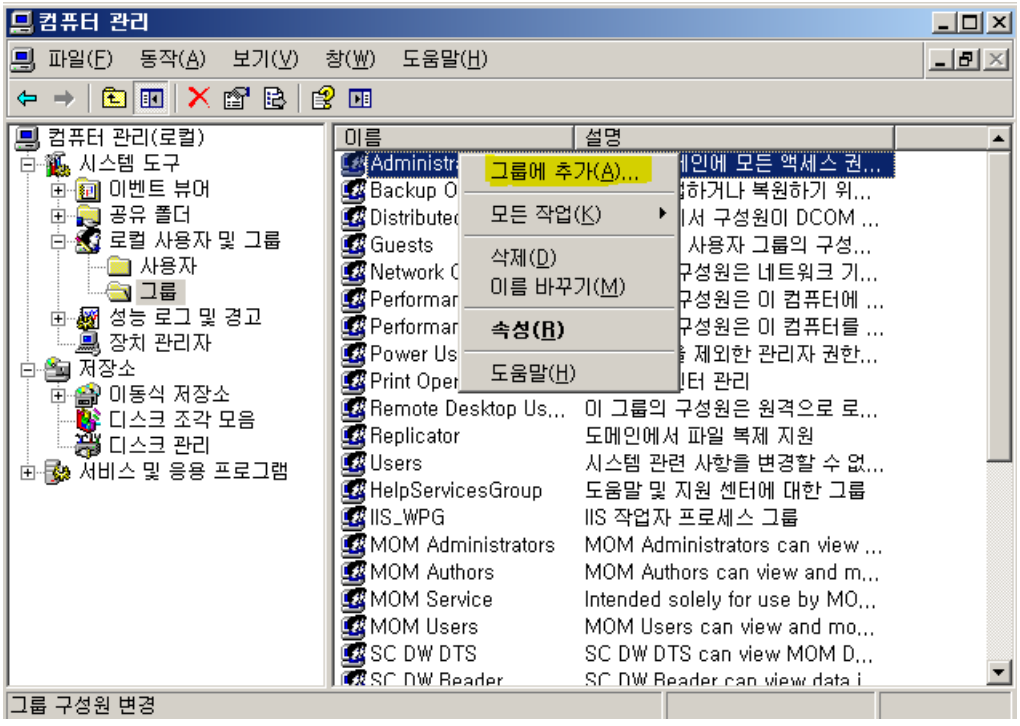
Client Security를 사용하기 전에 서비스 계정에 대한 추가 권한을 부여해야 한다.

1. Client Security 서버에서 관리자 그룹에 작업 계정을 추가한다.

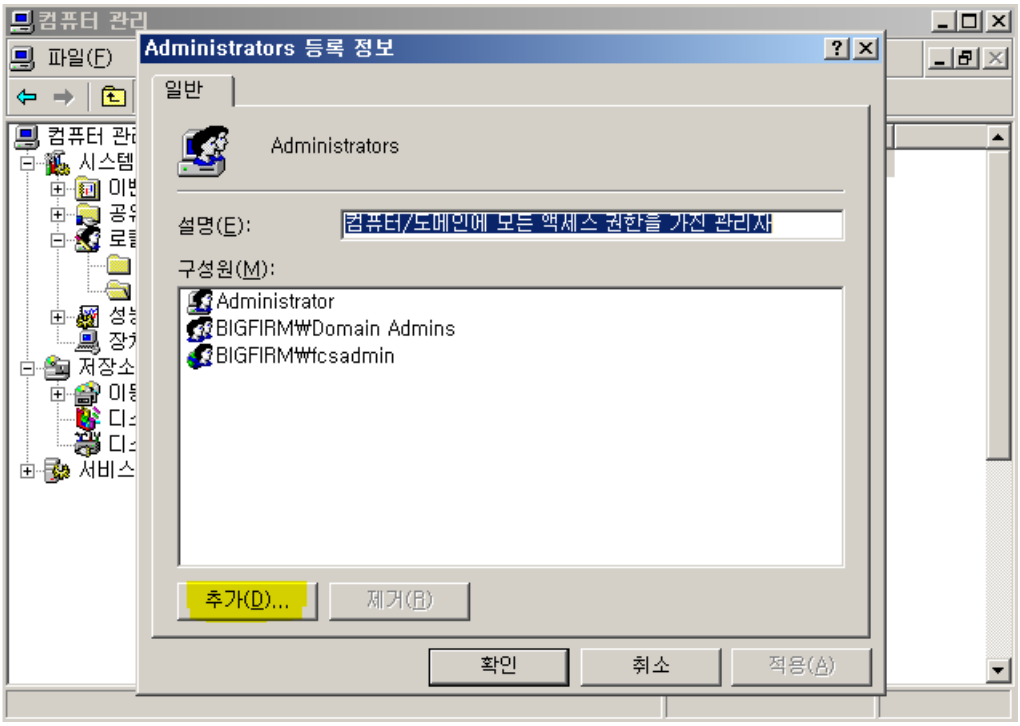
a. 내 컴퓨터 오른쪽 버튼 클릭 – 관리



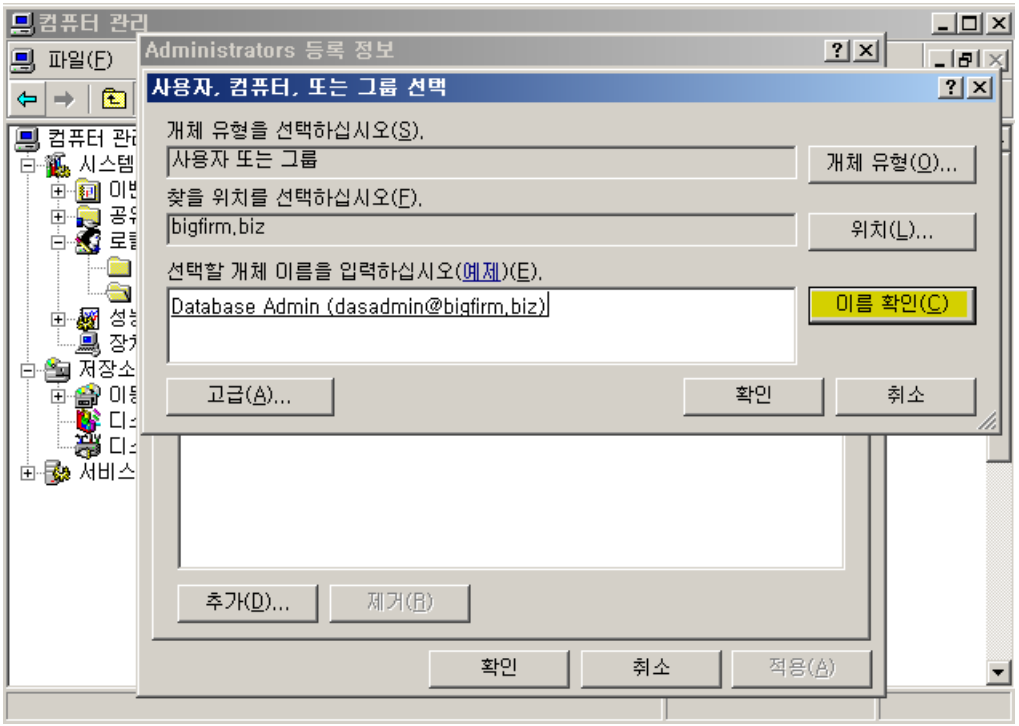
b. 로컬 사용자 그룹 – 그룹 – Administrators 오른쪽 버튼 클릭 – 그룹에 추가



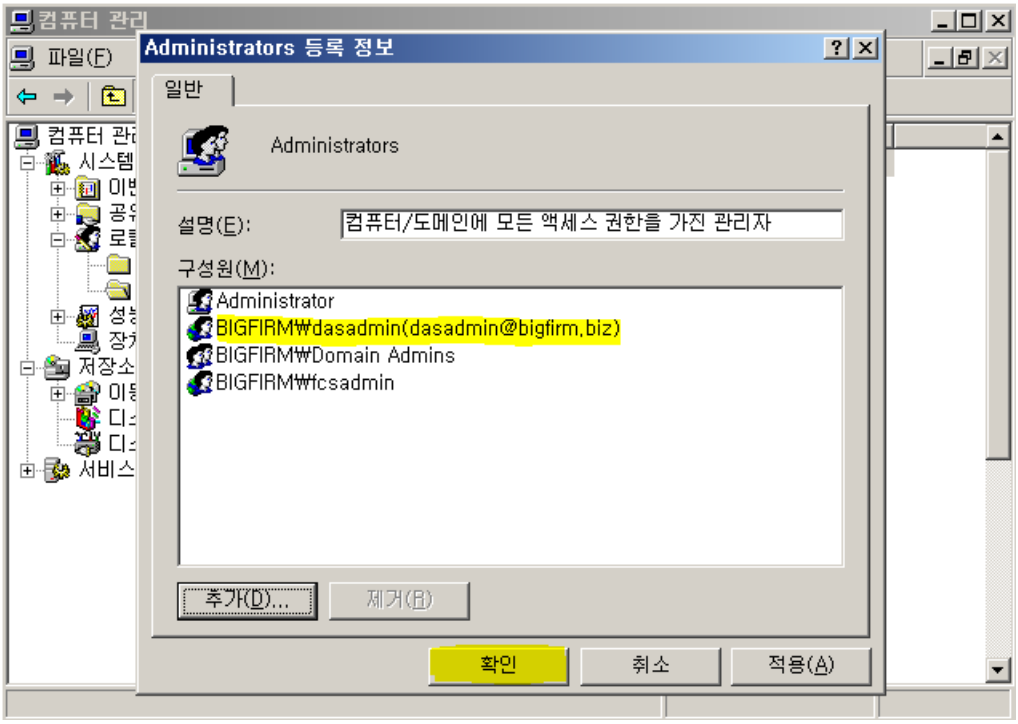
c. "추가" 버튼 클릭



d. 작업 계정 입력 후 "이름 확인(C)" 버튼 클릭 – 확인

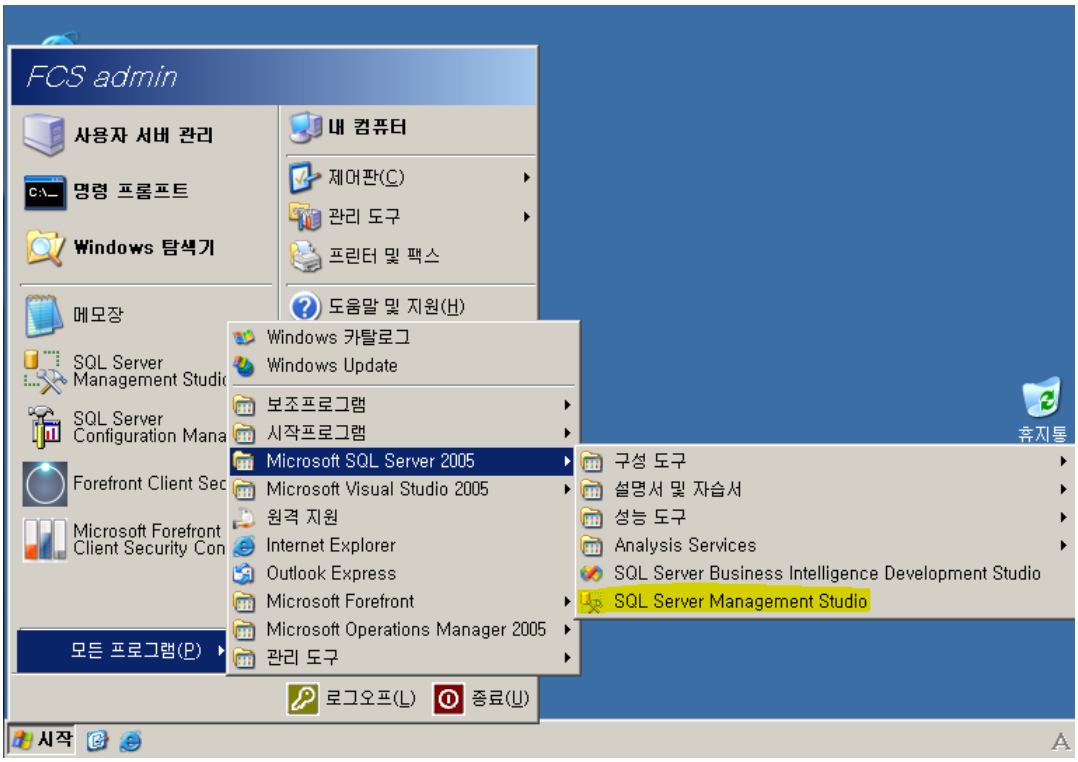


e. 계정 추가된 것 확인 후 "확인" 버튼을 눌러 창을 닫는다.



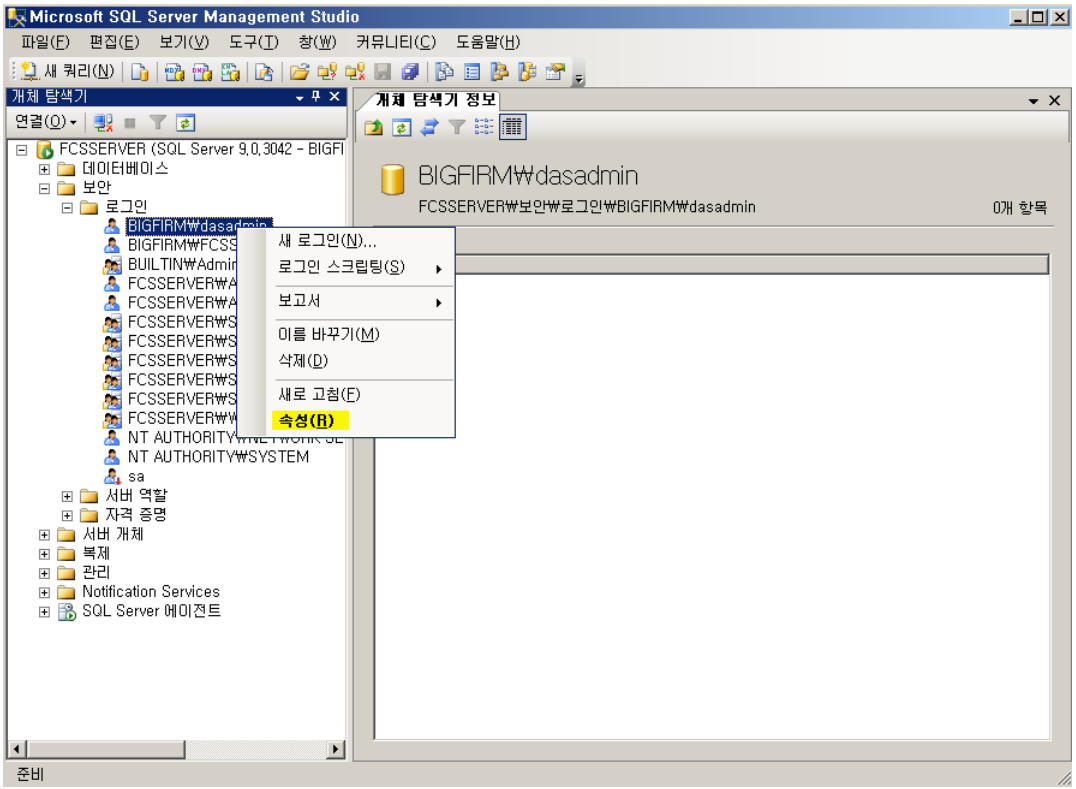
2. SystemCenterReporting 데이터베이스에 대한 db_owner 권한을 보고 계정에 부여한다.

a. 시작 – 모든 프로그램 – Microsoft SQL Server 2005 – SQL Server Management Studio

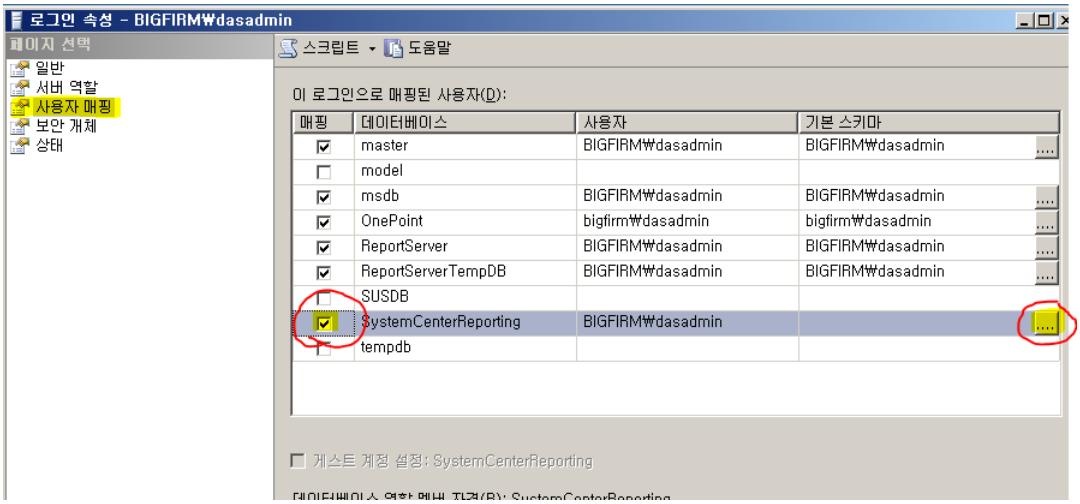


b. “연결” 버튼 클릭

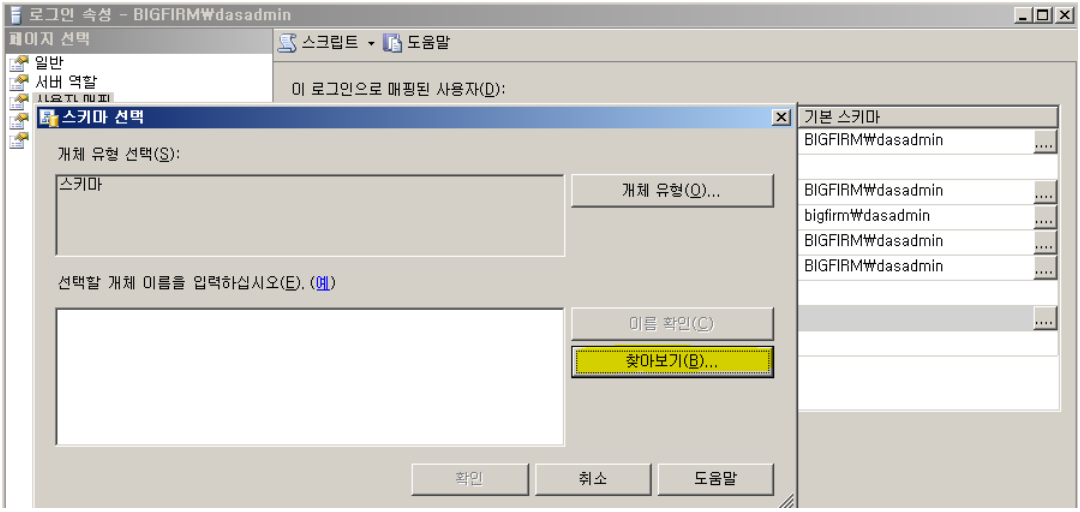
c. 보안 – 로그인 – 해당 보고 계정 오른쪽 클릭 – 속성



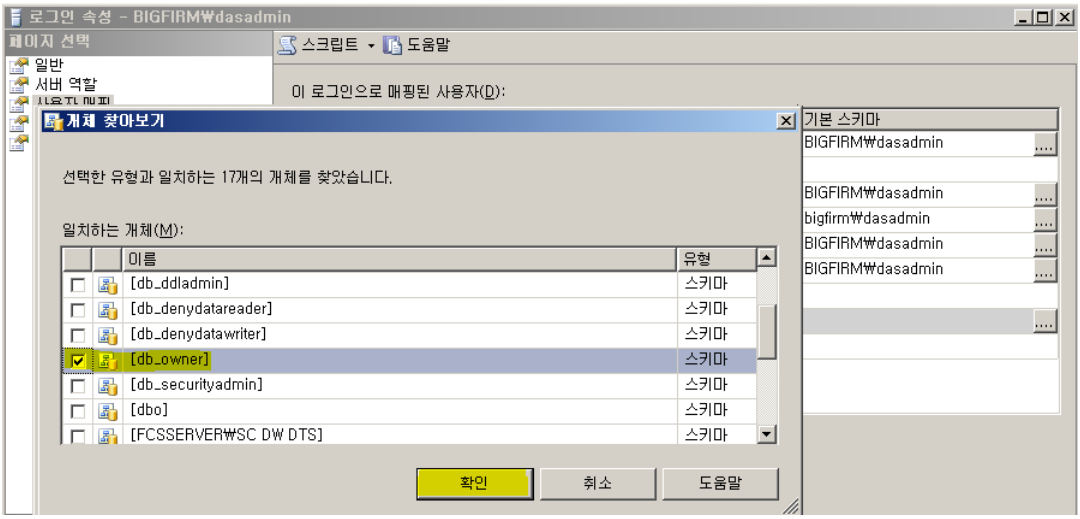
d. 사용자 매핑 – SystemCenterReporting 체크 – 찾기(....) 버튼 클릭



e. "찾아보기(B)" 버튼 클릭



f. db_owner 체크 후 확인



g. 차례대로 확인을 눌러 창을 모두 닫는다.

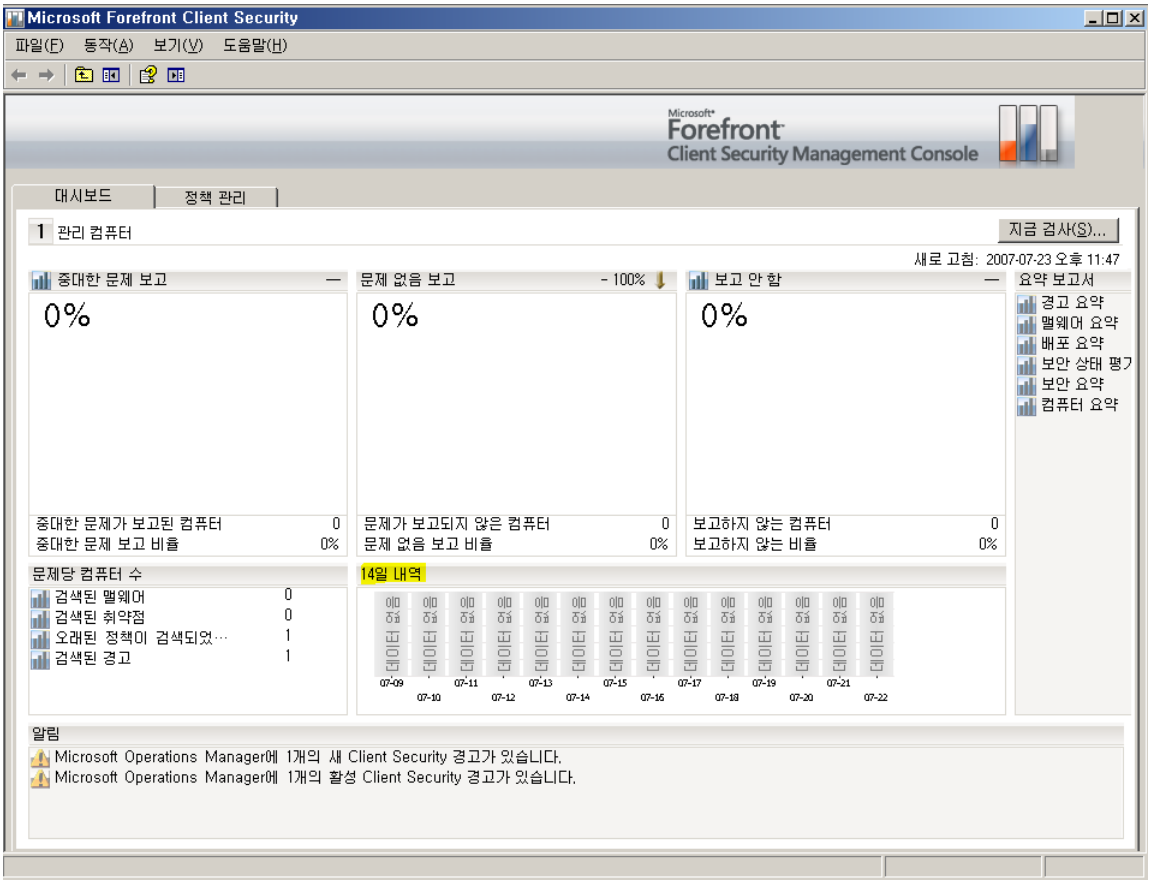
3. DAS 계정 및 작업 계정에 서로 다른 계정을 사용한 경우, OnePoint 데이터베이스에 대한 db_owner권한을 작업 계정에 부여해야 한다. (위 작업과 동일하게 하면 된다.)

4. DAS 계정 및 보고 계정에 서로 다른 계정을 사용한 경우, OnePoint 데이터베이스에 대한 db_owner권한을 작업 계정에 부여해야 한다. (위 작업과 동일하게 하면 된다.)

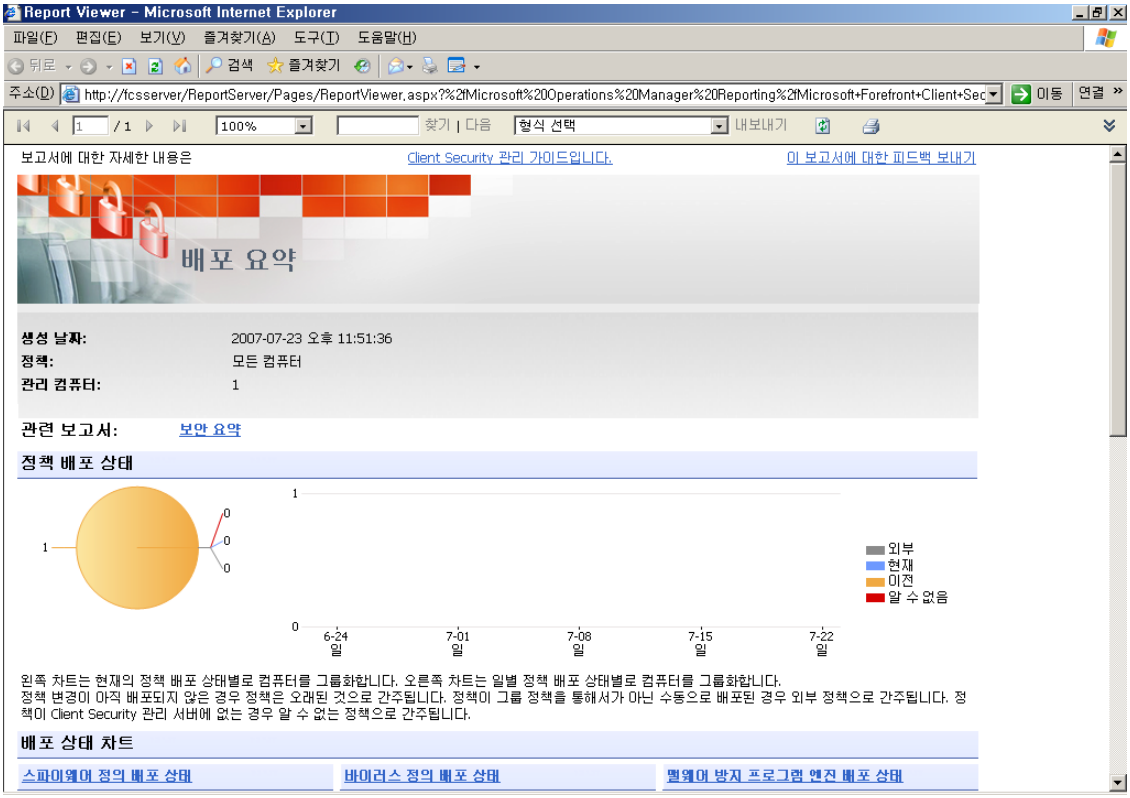
5.4. Client Security 설치 확인

서버에 Client Security를 설치 및 구성한 후에는 Client Security를 클라이언트 컴퓨터에 배포하기 전에 설치를 확인하는 것이 좋습니다.
성공적으로 설치했는지 확인하려면 다음을 수행하십시오.

*Client Security 콘솔을 엽니다. 콘솔에서 14일 내역 차트를 포함한 모든 데이터를 볼 수 있는지 확인합니다.



*콘솔에서 보고서를 엽니다. 보고서의 모든 데이터를 볼 수 있는지 확인하십시오.



*Client Security에서 생성한 설치 및 구성 로그를 확인합니다. 자세한 내용은 Client Security 문제 해결 가이드에서 로그 파일(http://go.microsoft.com/fwlink/?LinkId=82466)(영문)을 참고하십시오.

6. Forefront Client Security 배포

6.1. 개요

*중요 : WSUS를 배포 서버로 사용하는 경우, Client Security 정책이 배포된 컴퓨터는 Client Security의 클라이언트 구성요소를 자동으로 받게 됩니다.

컴퓨터	작업	단계
모든 컴퓨터	하드웨어 및 소프트웨어 요구 사항을 확인합니다.	Client Security를 클라이언트 컴퓨터에 배포하기 전에 이러한 컴퓨터가 하드웨어 및 소프트웨어 요구 사항을 만족하는지 확인해야 합니다. 경우에 따라 Client Security를 배포하기 전에 컴퓨터 업데이트를 배포해야 할 수 있습니다.
	네트워크 배포를 준비합니다.	컬렉션 서버와 클라이언트 컴퓨터 사이에 방화벽이 있는 경우 네트워크 포트를 열어야 할 수도 있습니다. 클라이언트 컴퓨터는 동일한 포리스트에 있는 트러스트되는 도메인 집합에 속해야 합니다. 클라이언트 컴퓨터는 조직 구성 단위 또는 보안 그룹에 속해 있는 것이 좋습니다. 정책 생성 및 배포를 위한 적절한 권한이 있는지 확인합니다.
배포 서버	WSUS의 클라이언트 구성 요소를 승인합니다.	Client Security를 배포하기 전에 WSUS에 있는 Client Security의 클라이언트 구성 요소를 승인해야 합니다. 배포 서버에서 WSUS 콘솔을 엽니다. **업데이트** 페이지에서 **Microsoft Forefront Client Security 클라이언트 업데이트**를 선택하고 **설치하도록 승인**을 클릭합니다.
관리 서버	자동 업데이트를 구성합니다.	클라이언트 컴퓨터가 배포 서버에서 Client Security 업데이트를 다운로드하도록 자동 업데이트를 구성해야 합니다. 이를 위해 GPMC(Group Policy Management Console)에서 정책을 편집 및 배포할 수 있습니다. 클라이언트 컴퓨터 구성과 함께 관리 서버에서 자동 업데이트를 구성해야 합니다.
	클라이언트 컴퓨터에 Client Security를 배포합니다.	Client Security를 클라이언트 컴퓨터에 배포하려면 Client Security 정책을 해당 컴퓨터에 배포해야 합니다. 정책이 있는 모든 컴퓨터는 Client Security의 클라이언트 구성 요소를 자동으로 받게 됩니다. 정책을 배포하려면 관리 서버에서 Client Security 콘솔을 열고 정책을 만들어 배포합니다.
	Client Security 배포를 확인합니다.	Client Security를 설치 및 구성하고 정책 및 클라이언트 컴퓨터를 배포하면 설치가 완료됩니다. 설치를 완료한 후에는 보고서를 통해 Client Security가 제대로 실행되고 있는지 확인할 수 있습니다.

6.2. 네트워크 배포 준비

클라이언트 컴퓨터에 Client Security를 배포하기 전에 다음 사항을 확인해야 합니다.
* Client Security 서버가 있는 도메인과 양방향 신뢰되는 하나 이상의 도메인에 클라이언트 컴퓨터가 속하는지 여부
* 적절한 네트워크 포트가 열려 있는지 여부

6.2.1. 트러스트된 도메인의 클라이언트 컴퓨터

모든 클라이언트 컴퓨터가 하나의 도메인 또는 여러 도메인의 집합에 있어야 합니다. 그러한 도메인은 Client Security 서버가 있는 도메인과 양방향 신뢰되어야 합니다.
*참고
트러스트된 도메인에 속하지 않는 클라이언트 컴퓨터에 Client Security를 배포할 수도 있습니다. 예를 들어 직원의 가정용 컴퓨터에 Client Security를 설치할 수 있습니다. 그러나 Client Security가 트러스트된 도메인에 속하지 않는 컴퓨터에 설치된 경우 기능이 제한됩니다. 이러한 컴퓨터는 Client Security 서버에 보고할 수 없으며 해당 컴퓨터에 Clieyt Security 정책을 배포할 수 없습니다.
클라이언트 컴퓨터는 조직 구성 단위 또는 보안 그룹에 속해 있는 것이 좋습니다. 그러나 Client Security 정책은 전체 도메인에 직접 배포할 수 있습니다. 레지스트리 파일을 사용하여 Client Security 정책을 배포할 수도 있습니다.

6.2.2. Client Security 구성 요소를 위한 포트 사용법

다음 표에는 Client Security 서버와 클라이언트 컴퓨터 간의 통신에 사용되는 네트워크 포트 및 프로토콜이 나열되어 있습니다. 사용하는 방화벽의 유형과 위치에 따라 이러한 포트를 열어야 할 수 있습니다.
*참고
그룹 정책, DNS(Domain Name System) 및 기타 표준 기술에 사용되는 포트는 이러한 포트에 포함되지 않습니다. Microsoft 서버 제품이 사용하는 포트 목록은 주요 Microsoft 서버 제품이 사용하는 네트워크 포트(http://go.microsoft.com/fwlink/?LinkId=86643)(영문)를 참조하십시오.

컴퓨터	연결	포트(프로토콜)
클라이언트 컴퓨터	연결 서버	1270(TCP 및 UDP)
클라이언트 컴퓨터	배포 서버	80(TCP) 또는 8530(TCP) 또는 사용자 지정

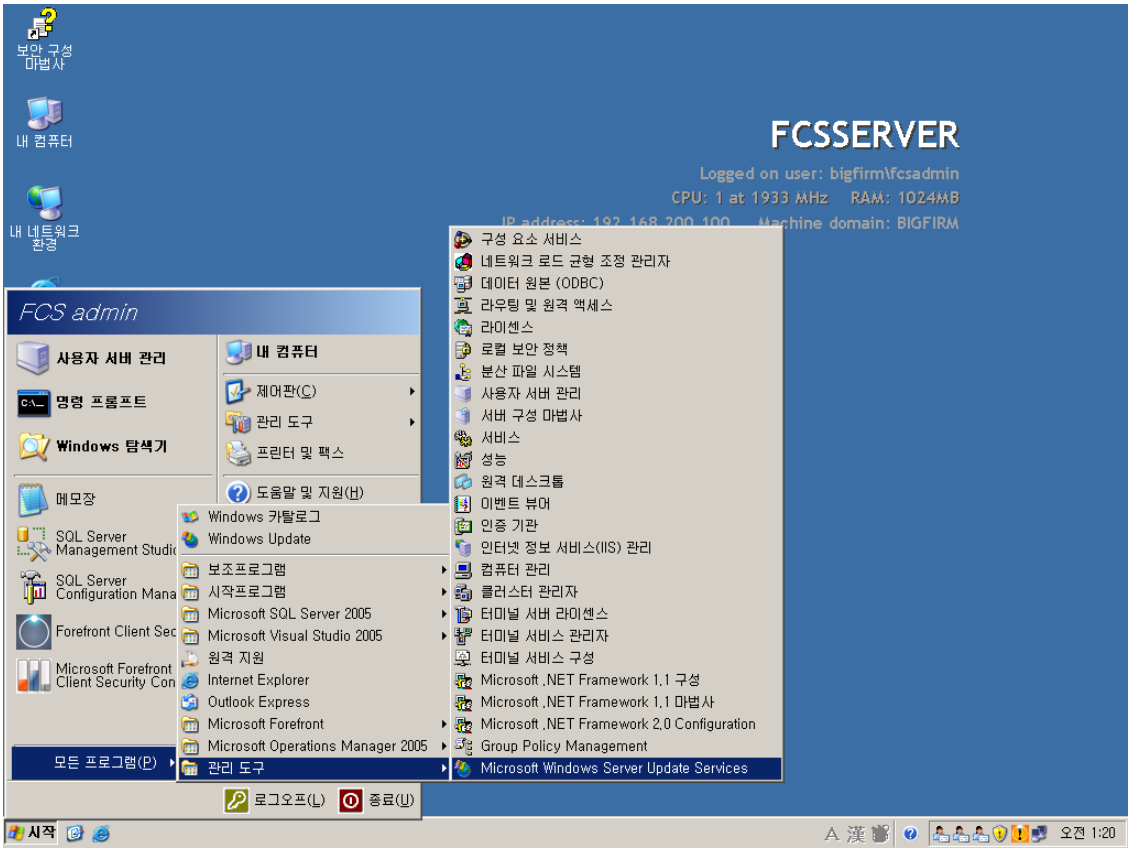
6.2.3. Windows 방화벽에서 포트 열기

그룹 정책으로 포트를 여는 방법은 Microsoft Windows XP 서비스 팩 2를 위한 Windows 방화벽 설정 배포(http://go.microsoft.com/fwlink/?LinkId=86644)(영문)를 참조하십시오.
포트를 수동으로 열려면 다음 절차를 따르십시오.

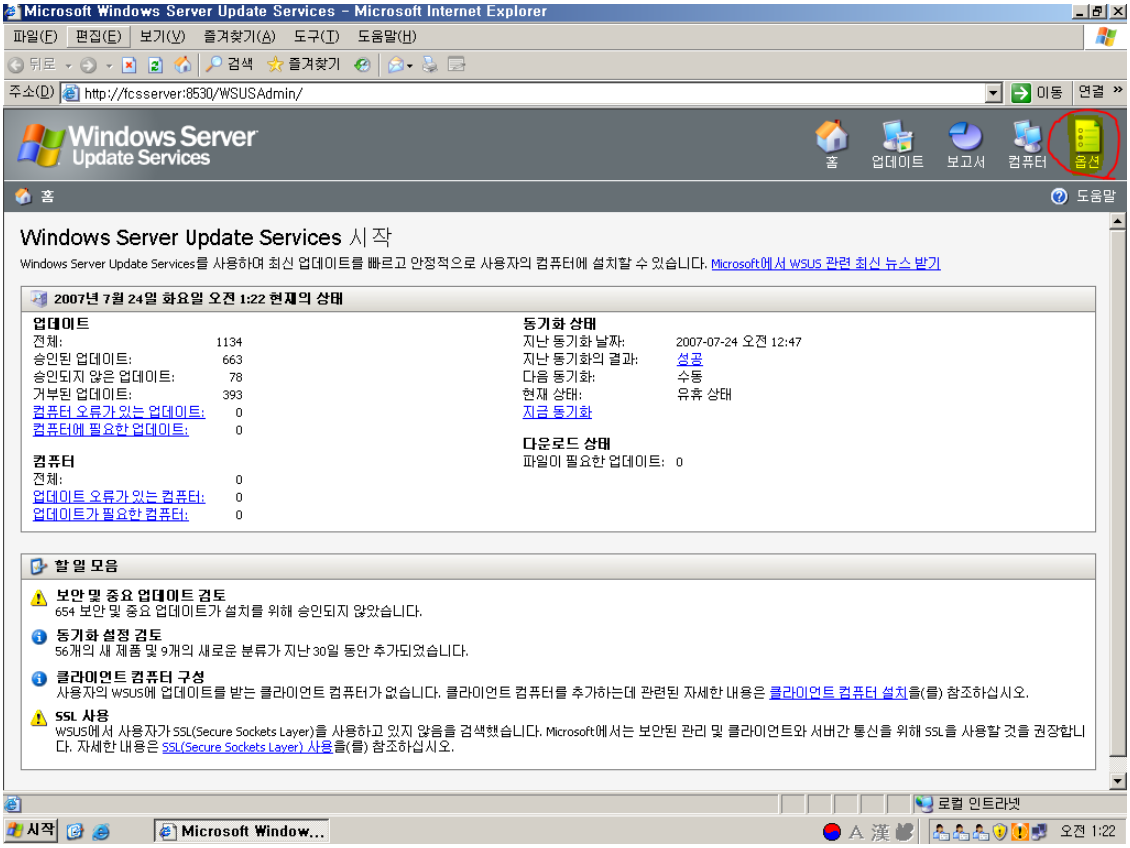
Windows 방화벽의 포트를 열려면
1. 시작, 제어판을 차례로 클릭한 다음 Windows 방화벽을 두 번 클릭합니다.
2. 예외 탭을 클릭한 다음 포트 추가를 클릭합니다.
3. 이름 상자에 새 포트 이름을 입력합니다.
4. 포트 번호 상자에 포트 번호를 입력합니다.
5. TCP 또는 UDP를 선택합니다.

6.3. WSUS의 클라이언트 구성 요소 승인
Client Security를 배포하기 전에 WSUS에서 관련 클라이언트 구성 요소를 승인해야 합니다. 또한 정의 업데이트 외에 업데이트를 동기화하도록 WSUS를 구성했는지 확인해야 합니다.

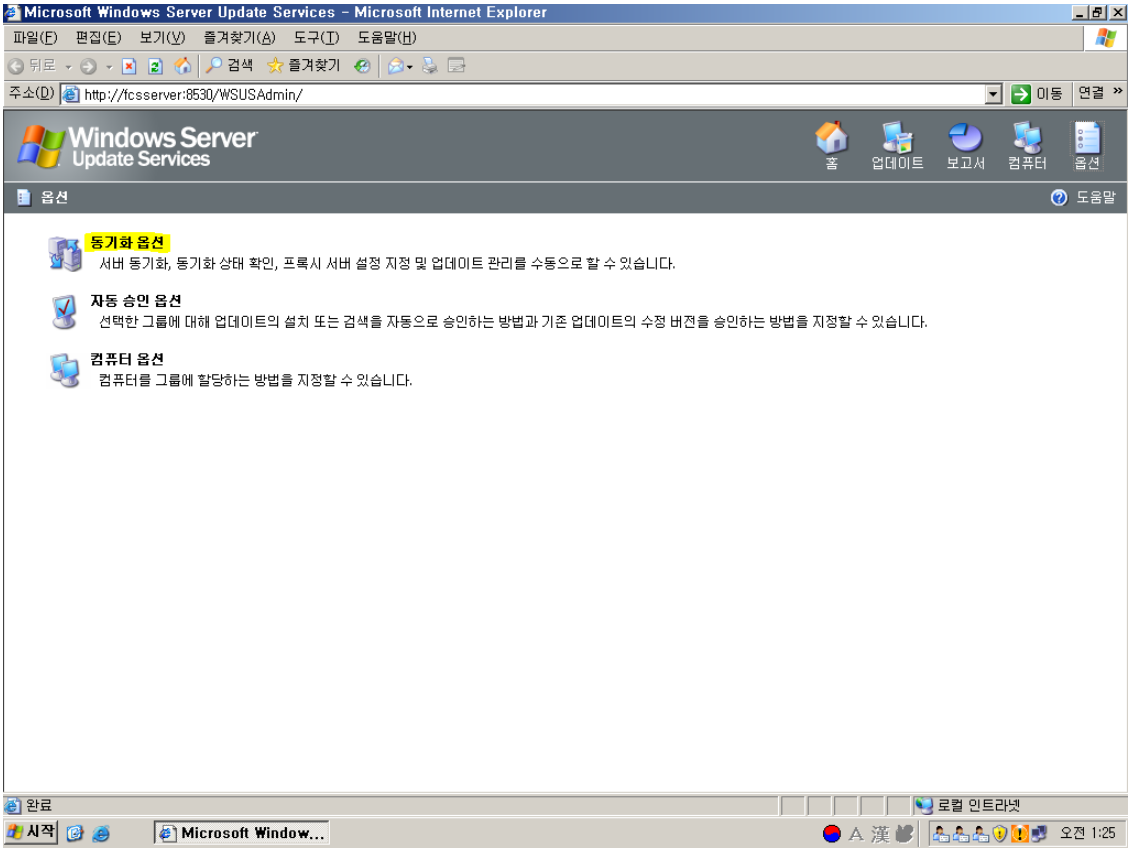
WSUS에서 클라이언트 구성 요소 승인 절차
1. 시작 – 모든 프로그램 – 관리 도구 – Microsoft Windows Server Update Service



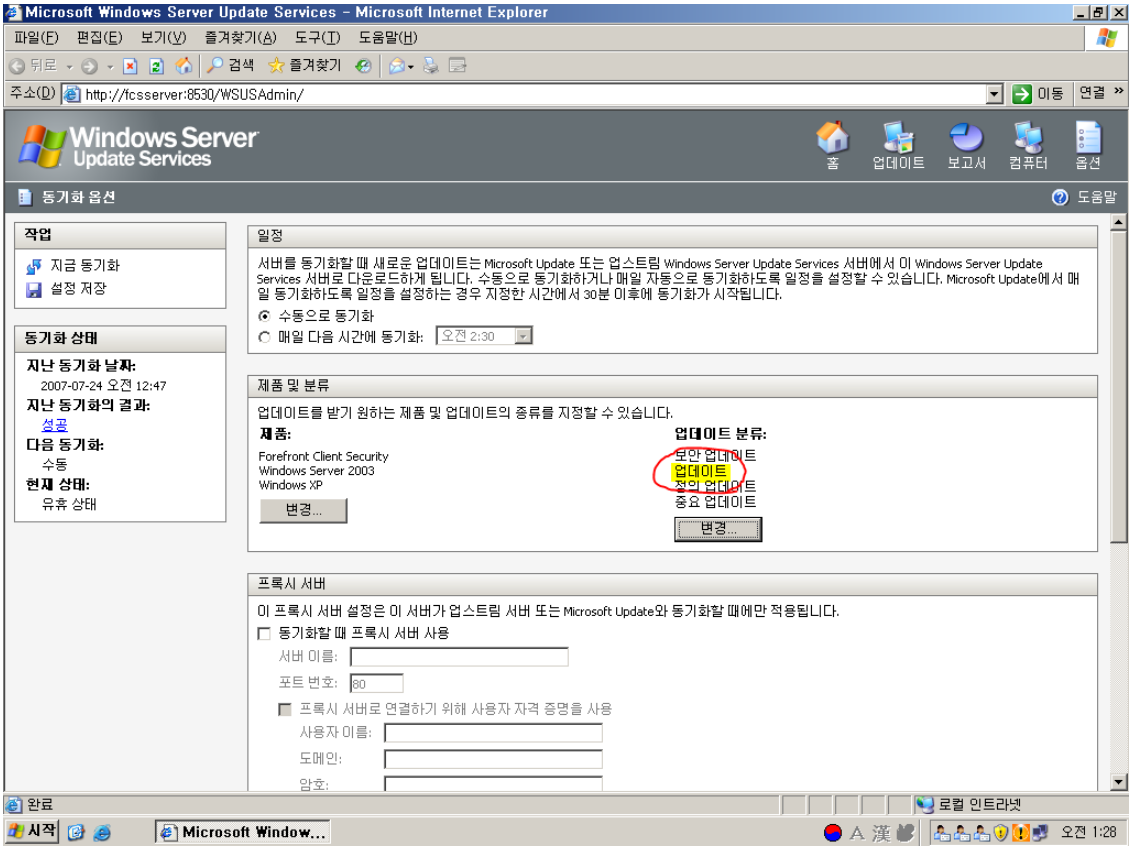
2. 옵션


Microsoft Windows Server Update Services - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
주소(D) http://fcsserver:8530/WSUSAdmin/
Windows Server Update Services
홈 업데이트 보고서 컴퓨터 옵션
홈
도움말
Windows Server Update Services 시작
Windows Server Update Services를 사용하여 최신 업데이트를 빠르고 안정적으로 사용자의 컴퓨터에 설치할 수 있습니다. Microsoft에서 WSUS 관련 최신 뉴스 받기
2007년 7월 24일 화요일 오전 1:22 현재의 상태
업데이트
전체: 1134
승인된 업데이트: 663
승인되지 않은 업데이트: 78
거부된 업데이트: 393
컴퓨터 오류가 있는 업데이트: 0
컴퓨터에 필요한 업데이트: 0
컴퓨터
전체: 0
업데이트 오류가 있는 컴퓨터: 0
업데이트가 필요한 컴퓨터: 0
동기화 상태
지난 동기화 날짜: 2007-07-24 오전 12:47
지난 동기화의 결과: 성공
다음 동기화: 수동
현재 상태: 유휴 상태
지금 동기화
다운로드 상태
파일이 필요한 업데이트: 0
할 일 모음
보안 및 중요 업데이트 검토
654 보안 및 중요 업데이트가 설치를 위해 승인되지 않았습니다.
동기화 설정 검토
56개의 새 제품 및 9개의 새로운 분류가 지난 30일 동안 추가되었습니다.
클라이언트 컴퓨터 구성
사용자의 WSUS에 업데이트를 받는 클라이언트 컴퓨터가 없습니다. 클라이언트 컴퓨터를 추가하는데 관련된 자세한 내용은 클라이언트 컴퓨터 설치을(를) 참조하십시오.
SSL 사용
WSUS에서 사용자가 SSL(Secure Sockets Layer)을 사용하고 있지 않음을 검색했습니다. Microsoft에서는 보안된 관리 및 클라이언트와 서버간 통신을 위해 SSL을 사용할 것을 권장합니다. 자세한 내용은 SSL(Secure Sockets Layer) 사용을(를) 참조하십시오.
로컬 인트라넷
시작
Microsoft Window...
오전 1:22

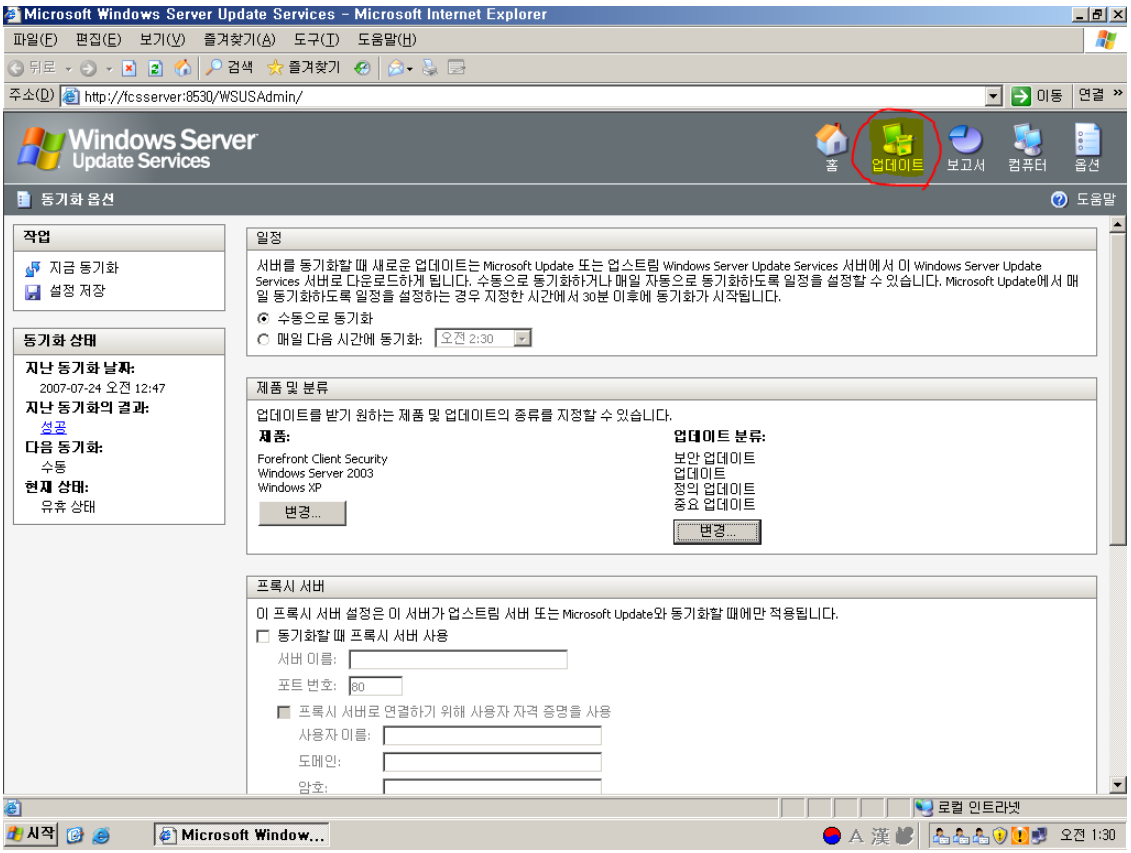
3. 동기화 옵션


Microsoft Windows Server Update Services - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
주소(D) http://fcsserver:8530/WSUSAdmin/
Windows Server Update Services
홈 업데이트 보고서 컴퓨터 옵션
옵션
도움말
동기화 옵션
서버 동기화, 동기화 상태 확인, 프록시 서버 설정 지정 및 업데이트 관리를 수동으로 할 수 있습니다.
자동 승인 옵션
선택한 그룹에 대해 업데이트의 설치 또는 검색을 자동으로 승인하는 방법과 기존 업데이트의 수정 버전을 승인하는 방법을 지정할 수 있습니다.
컴퓨터 옵션
컴퓨터를 그룹에 할당하는 방법을 지정할 수 있습니다.
완료
로컬 인트라넷
시작
Microsoft Window...
오전 1:25

4. 업데이트 분류에 "업데이트" 선택되어 있는지 확인



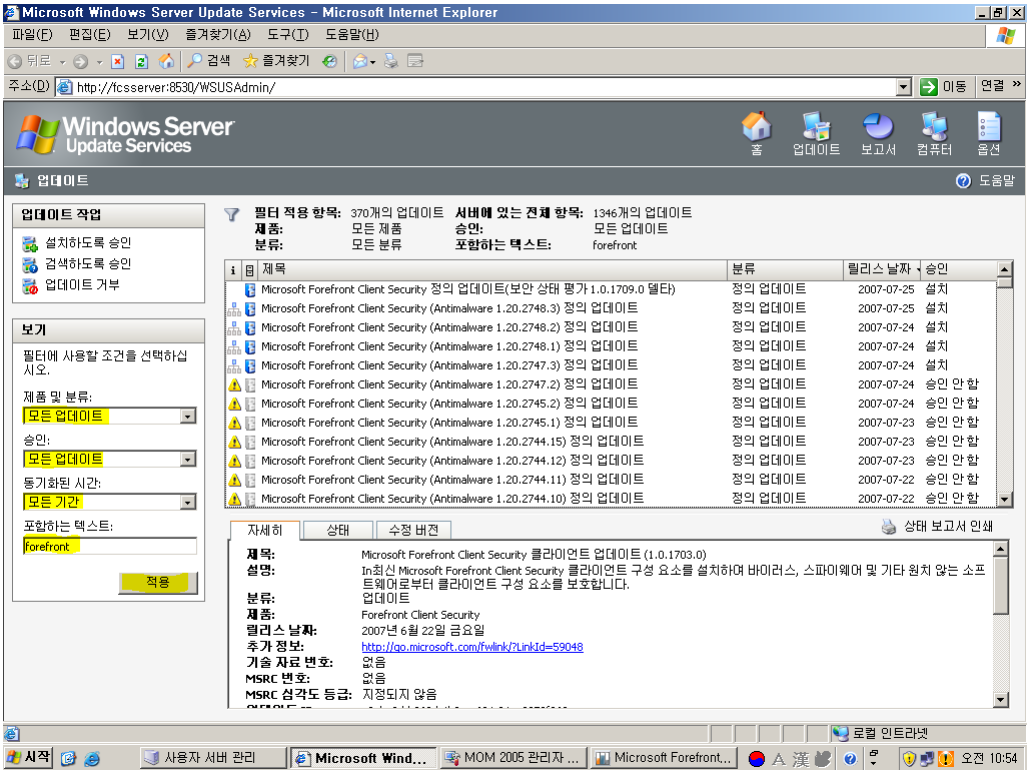
5. 상단 메뉴에서 "업데이트" 클릭



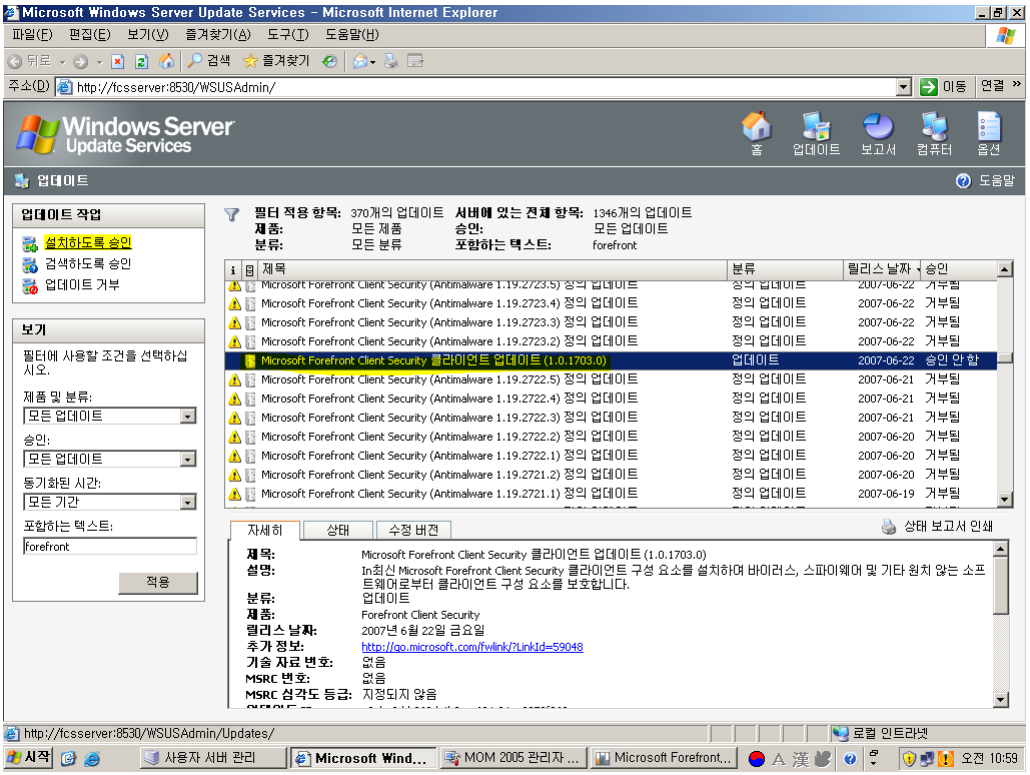
6. 좌측 '보기' 창에서

제품 및 분류 : 모든 업데이트 ,승인 : 모든 업데이트

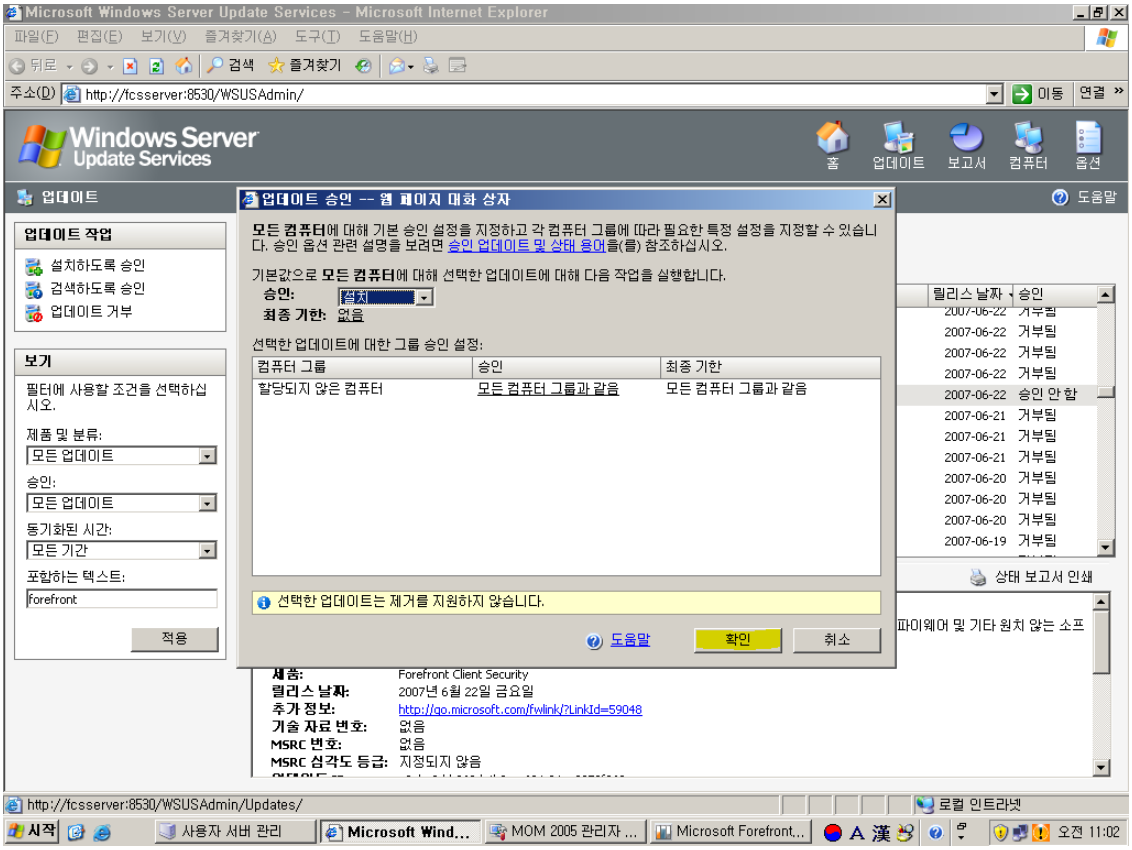
동기화된 시간 : 모든 기간 ,포함하는 텍스트 : forefront 입력 후 적용 버튼 클릭



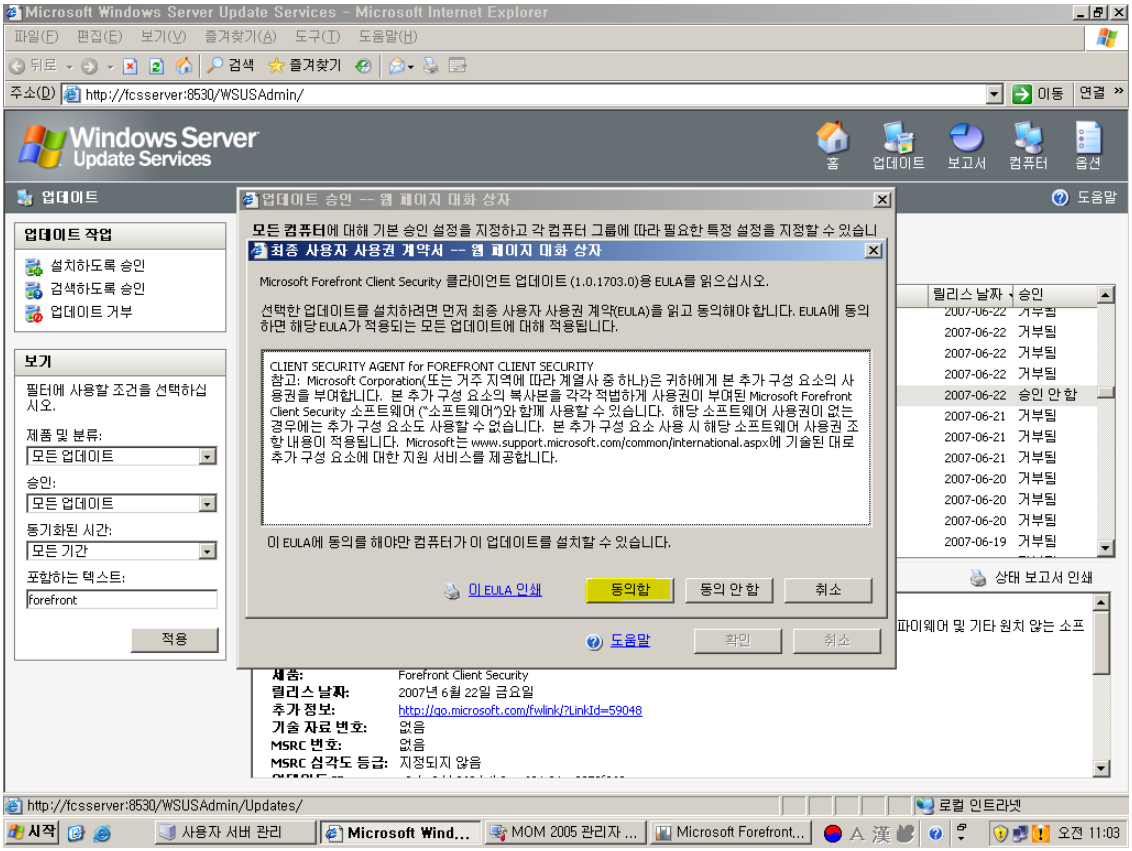
7. 우측 목록에서 "Microsoft Forefront Client Security 클라이언트 업데이트" 선택 후 좌측 업데이트 작업 창에서 "설치하도록 승인" 클릭



8. 업데이트 승인 창에서 승인 선택을 설치로 선택하고 확인 버튼 클릭



9. 최종 사용자 사용권 계약서 – "동의함" 버튼 클릭



6.4. 자동 업데이트 구성

클라이언트 컴퓨터가 배포 서버에서 업데이트를 다운로드 하도록 하려면 클라이언트 컴퓨터의 자동 업데이트가 WSUS 서버로 지정되도록 클라이언트 컴퓨터를 구성해야 합니다. 이 구성은 그룹 정책을 사용하여 수행할 수 있습니다.

*중요

표준 클라이언트 컴퓨터와 함께 관리 서버의 자동 업데이트도 WSUS 서버로 지정되도록 구성해야 합니다. 이를 수행하지 않으면 보고서가 올바르게 표시되지 않습니다.

WSUS에 대한 그룹 정책 설정을 구성할 때는 사용자 환경에 적합한 Active Directory 디렉터리 서비스 컨테이너에 연결된 그룹 정책 개체(GPO)를 사용해야 합니다.

클라이언트 컴퓨터를 설치한 후 몇 분 정도 지나면 WSUS 콘솔의 컴퓨터 페이지에 해당 이름이 나타납니다. Active Directory에 기반한 GPO로 구성된 클라이언트 컴퓨터의 경우 그룹 정책을 새로 고친 후(즉, 클라이언트 컴퓨터에 새 설정을 적용한 후) 20분 정도 걸립니다. 기본적으로 그룹 정책은 90분마다(0~30분 임의 차감) 백그라운드에서 새로 고쳐집니다.

Notes:

* 그룹 정책을 더 빨리 새로 고치려면 클라이언트 컴퓨터의 명령 프롬프트로 이동하여 gpupdate /force를 입력합니다.

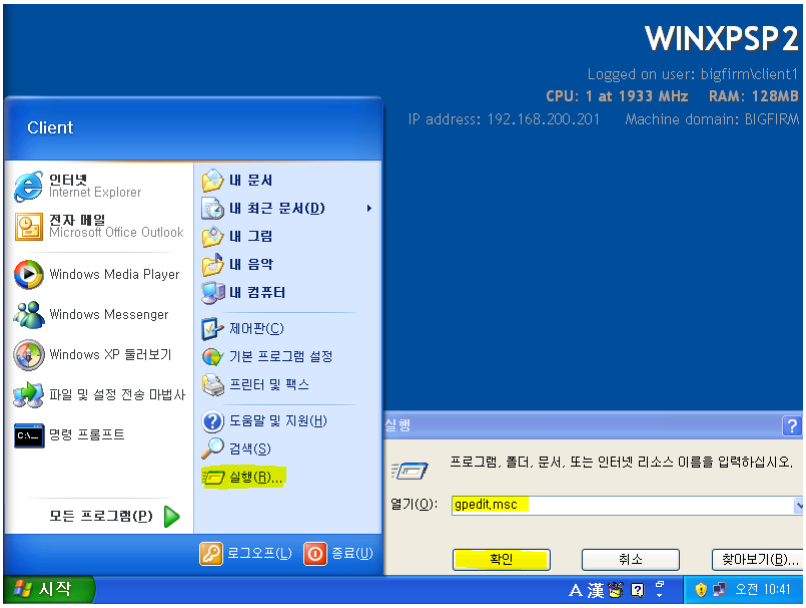
* 클라이언트 컴퓨터가 WSUS 서버와 즉시 동기화하도록 하려면 클라이언트 컴퓨터의 명령 프롬프트로 이동하여 wuauclt.exe /detectnow를 입력합니다.

자동 업데이트 구성에 대한 자세한 내용은 그룹 정책을 사용하여 클라이언트 구성(http://go.microsoft.com/fwlink/?LinkID=85860)(영문)을 참조하십시오.

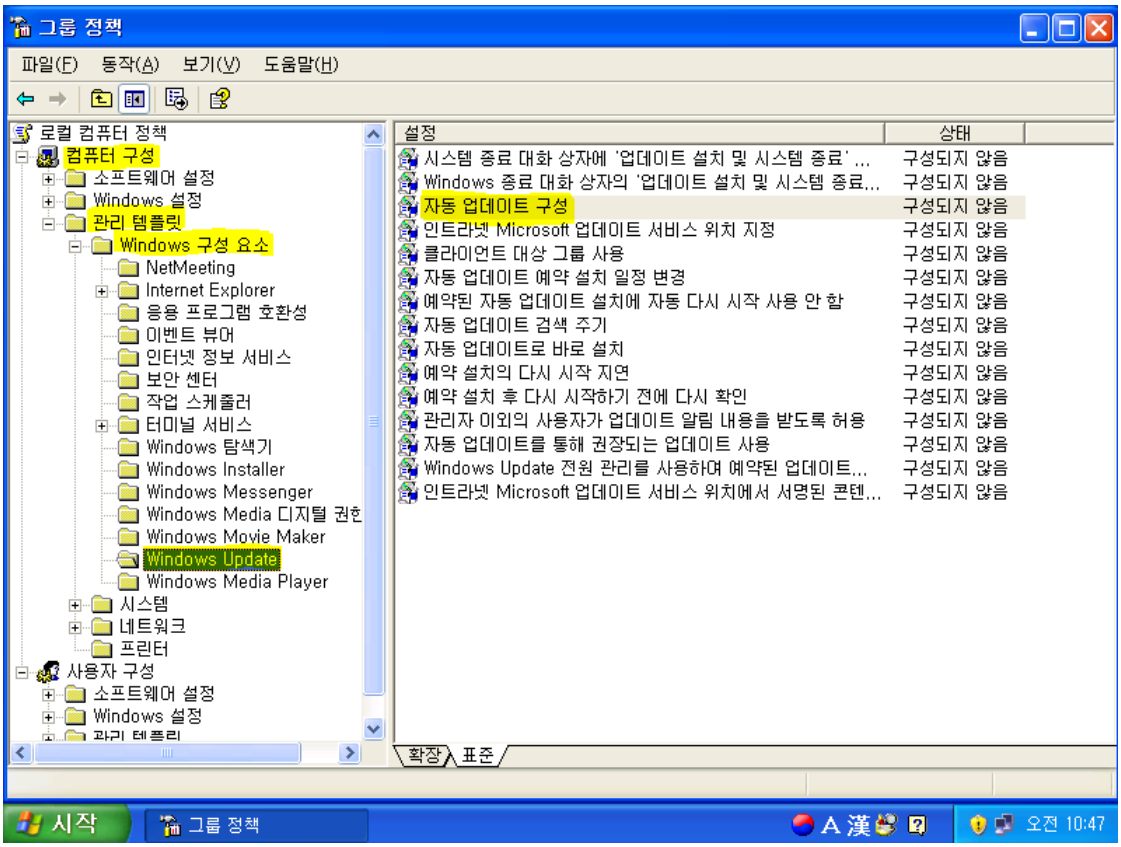
1. Client PC 자동 업데이트 구성 절차

Client PC에서 로컬 그룹 정책 편집기를 사용하여 WSUS 서버로부터 업데이트 받도록 수정하는 절차를 설명합니다. (Client PC는 XP를 운영체제로 사용하고 있다고 가정합니다.)

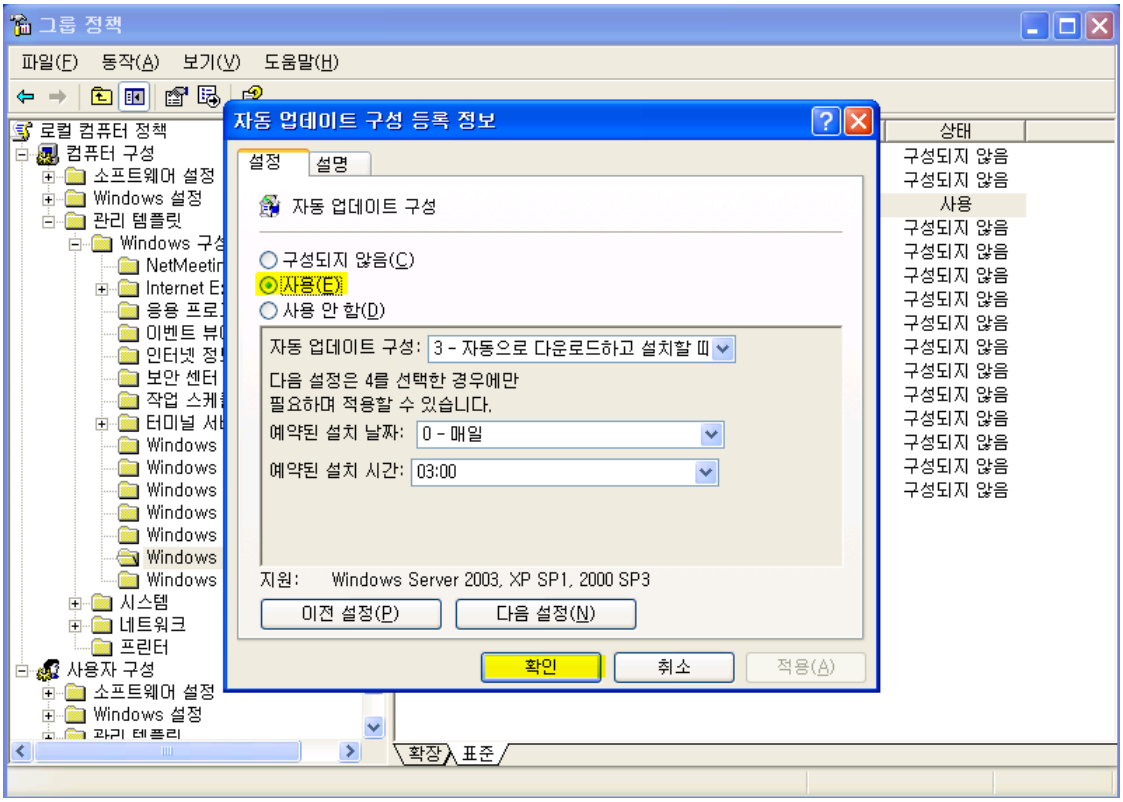
a. Client PC에서 시작 – 실행 – "gpedit.msc" 입력 후 "확인" 버튼 클릭



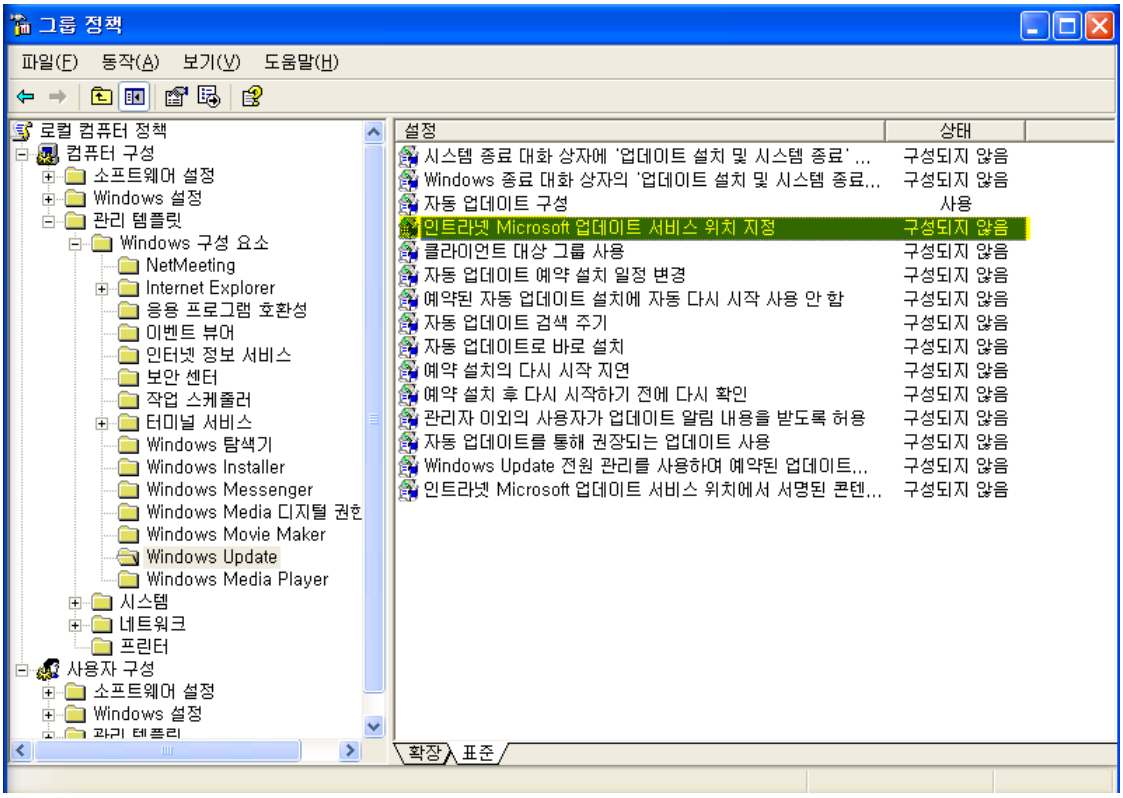
b. 그룹 정책 편집기 대화상자에서 컴퓨터 구성 – 관리 템플릿 – Windows 구성 요서 – Windows Update 로 들어간 후 우측 목록에서 "자동 업데이트 구성" 더블 클릭한다.



c. "사용" 에 체크 – "확인" 버튼 클릭

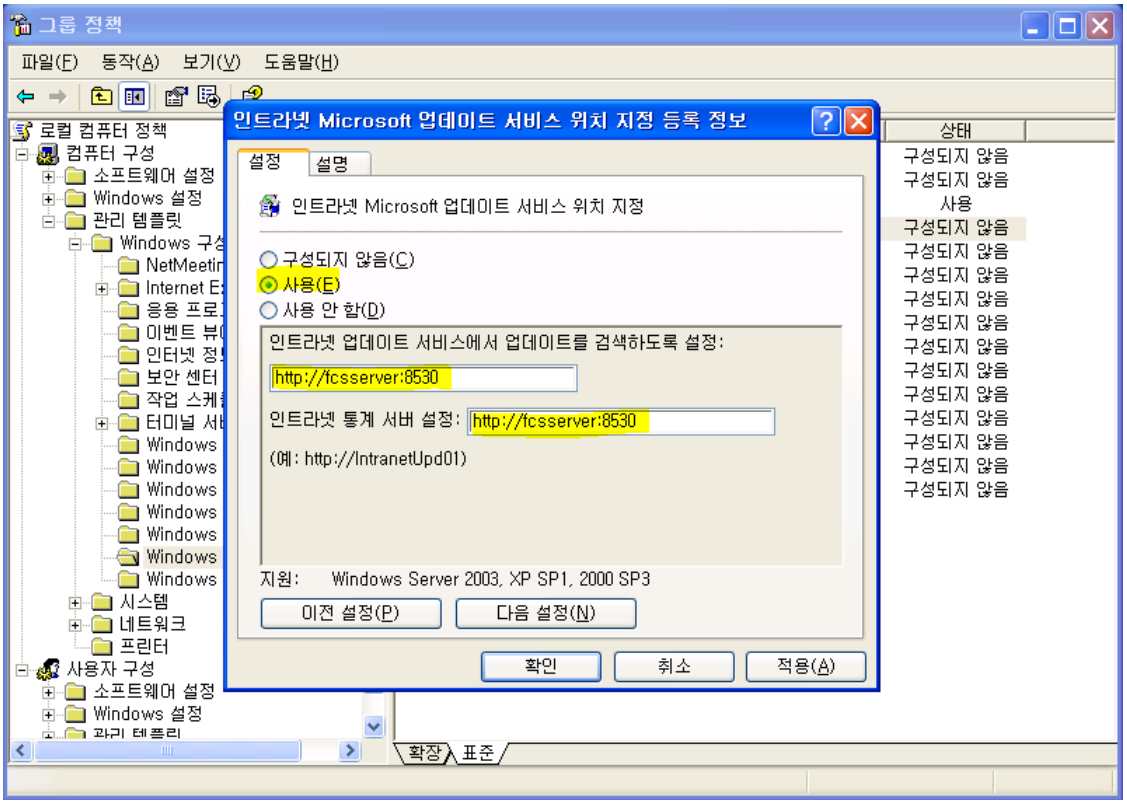


d. 우측 목록에서 "인트라넷 Microsoft 업데이트 서비스 위치 지정" 더블 클릭

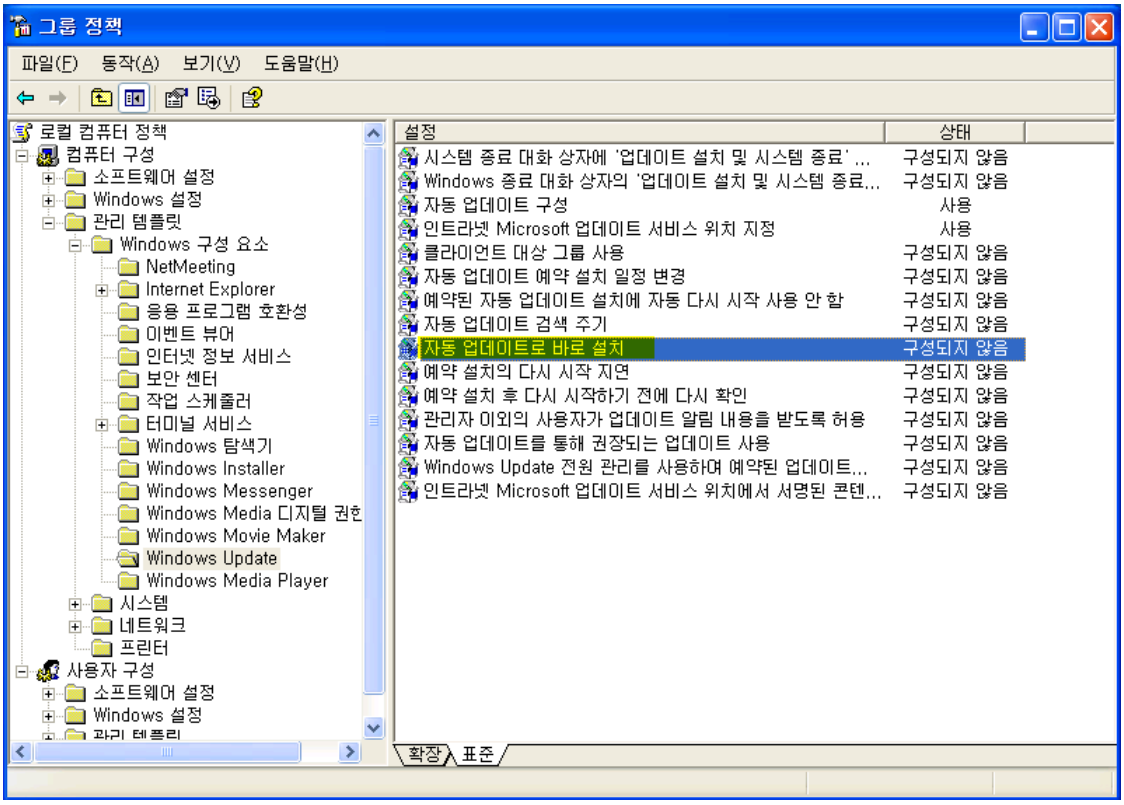


e. "사용"에 체크하고 "인트라넷 업데이트 서비스에서 업데이트를 검색하도록 설정" 입력 상자와 "인트라넷 통계 서버 설정" 입력 상자에 WSUS의 URL을 입력한 다음 "확인" 버튼 클릭.

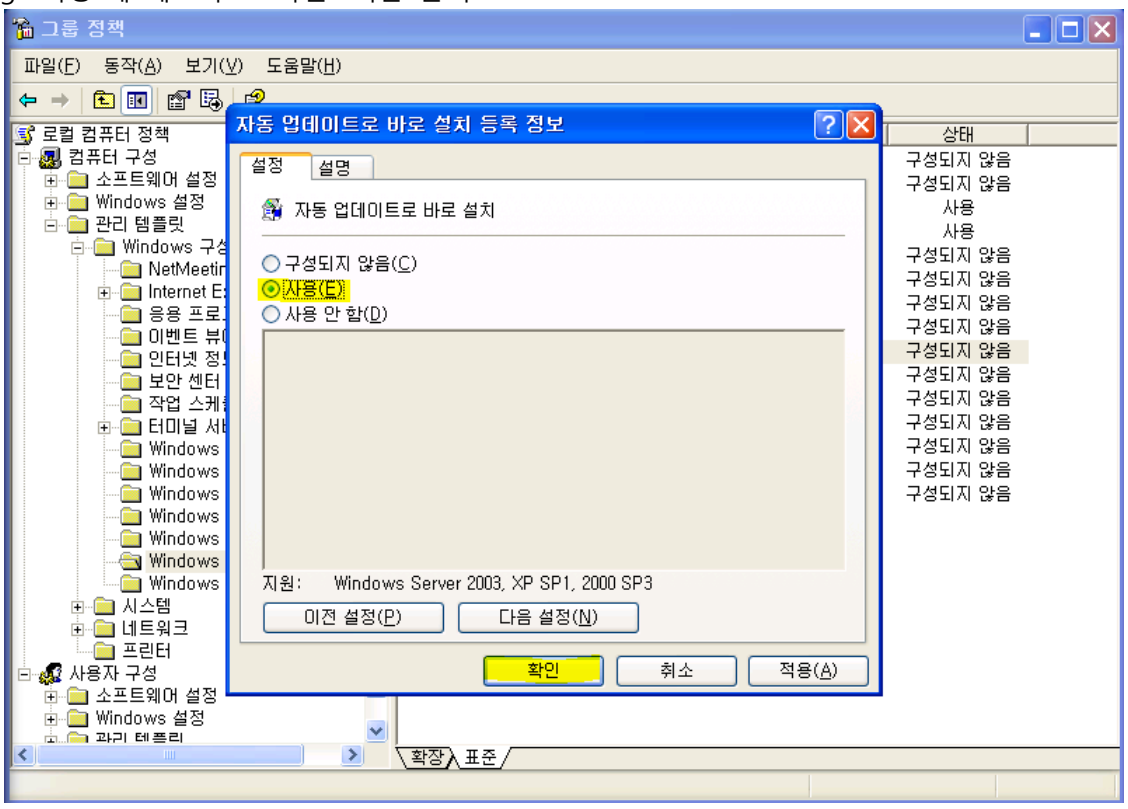
중요 : URL 뒤쪽에 포트 번호를 입력해야 한다. (ex : http://fcsserver:8530)



f. 우측 목록에서 "자동 업데이트로 바로 설치" 더블 클릭

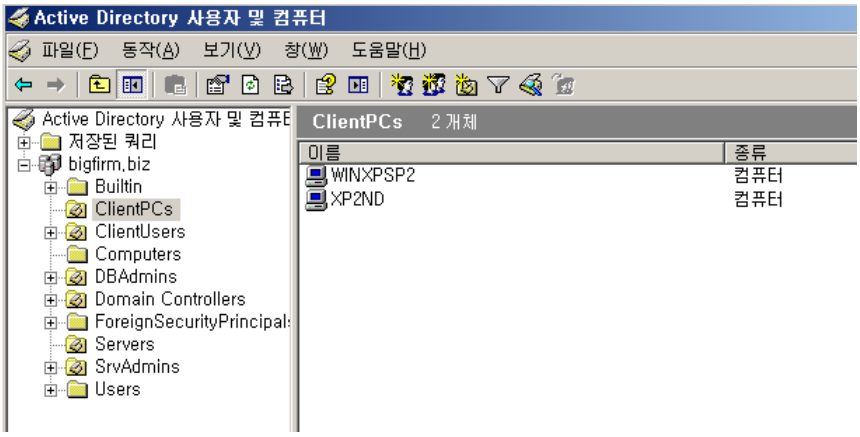


g. "사용"에 체크하고 "확인" 버튼 클릭

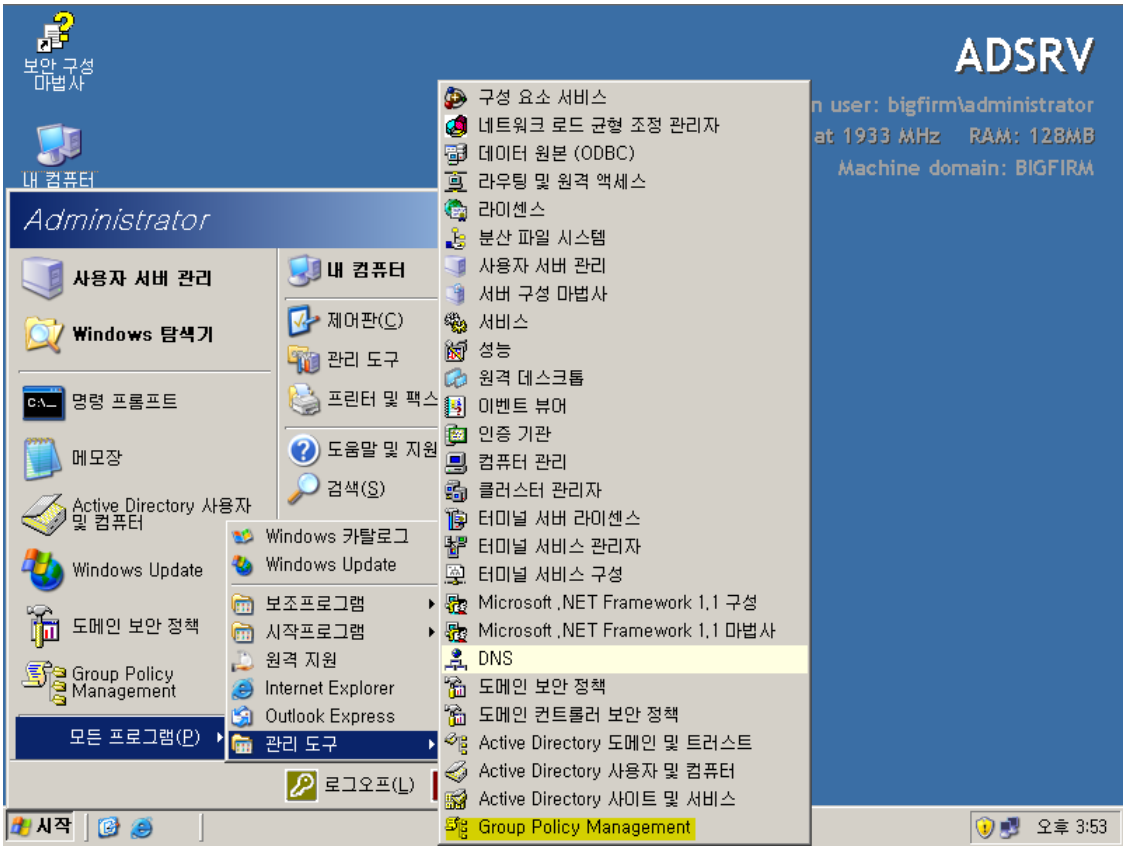


2. GPMC의 정책을 사용한 Client PC 자동 업데이트 구성 절차

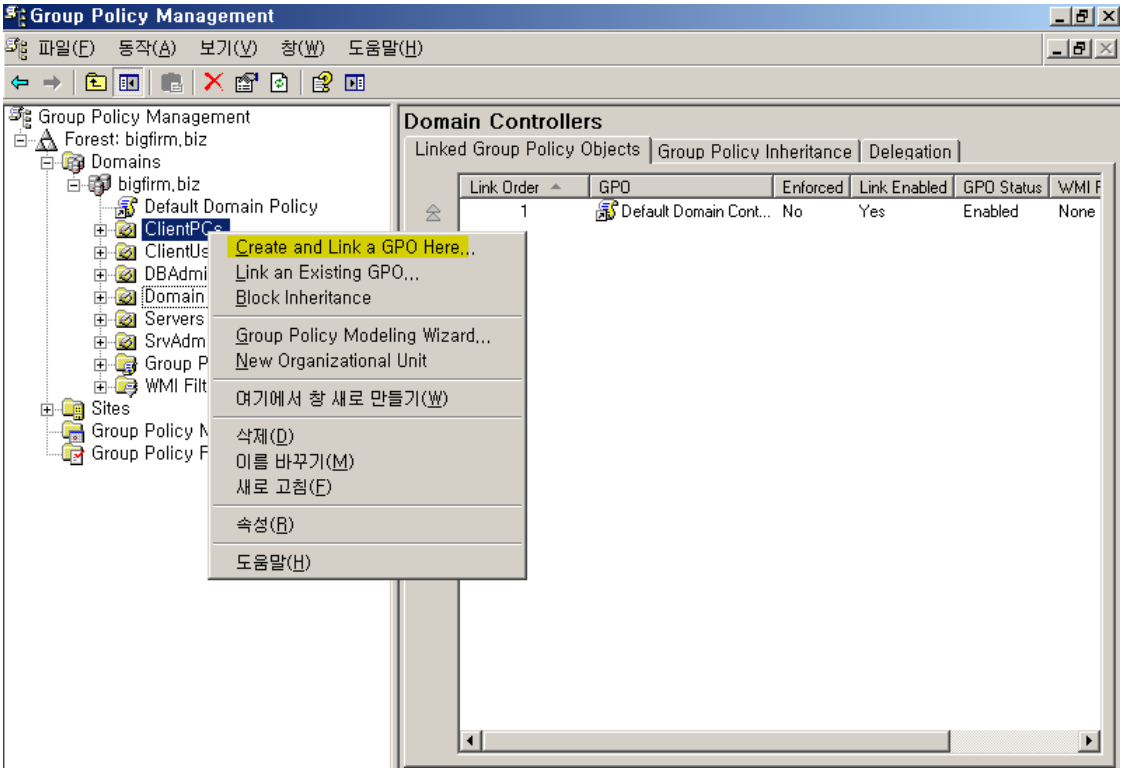
GPMC(Group Policy Management Console)를 사용하여 정책 적용을 통해서 Client PC들에게 자동 업데이트를 구성하는 예제를 보여드리겠습니다.
예제에서는 ClientPCs라는 OU에 정책을 적용해 보겠습니다. ClientPCs OU에는 두 대의 Client PC가 속해 있습니다.
참고 1. 이 작업은 도메인 관리자 권한을 가진 계정을 사용합니다.
참고 2. GPMC가 설치되어 있다고 가정합니다.



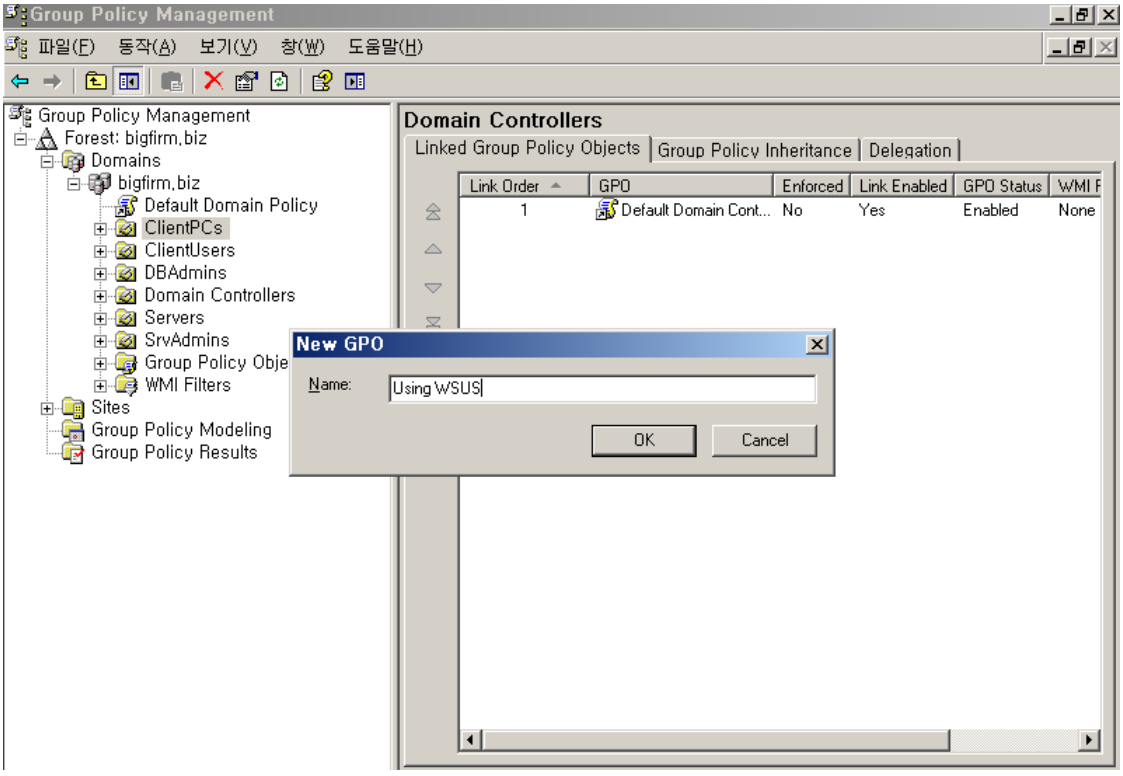
a. Active Directory Domain Controller에서 시작 – 모든 프로그램 – 관리도구 – Group Policy Management 선택



b. 적용하고자 하는 OU(여기서는 ClientPCs)를 오른쪽 버튼 클릭해서 "Create and Link GPO Here..." 선택

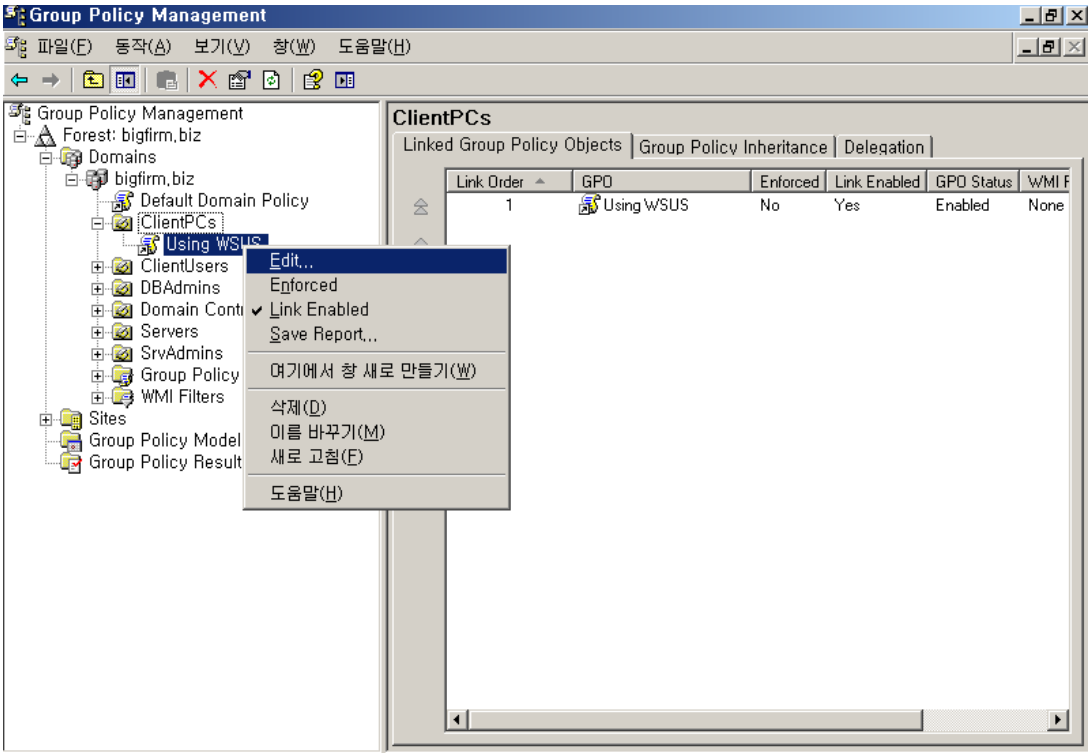


c. 그룹 정책 이름 입력(여기서는 "Using WSUS" 라고 하겠다.)

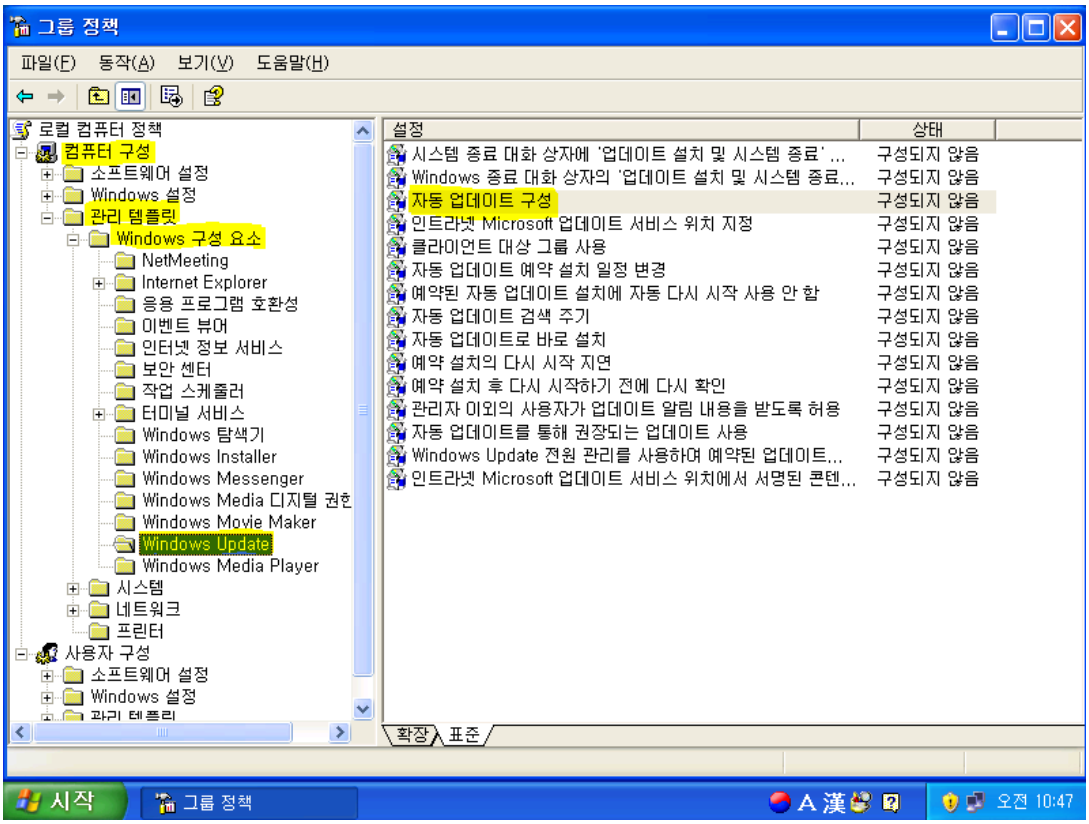


d. 입력한 GPO 오른쪽 버튼 클릭하고 "Edit..." 선택

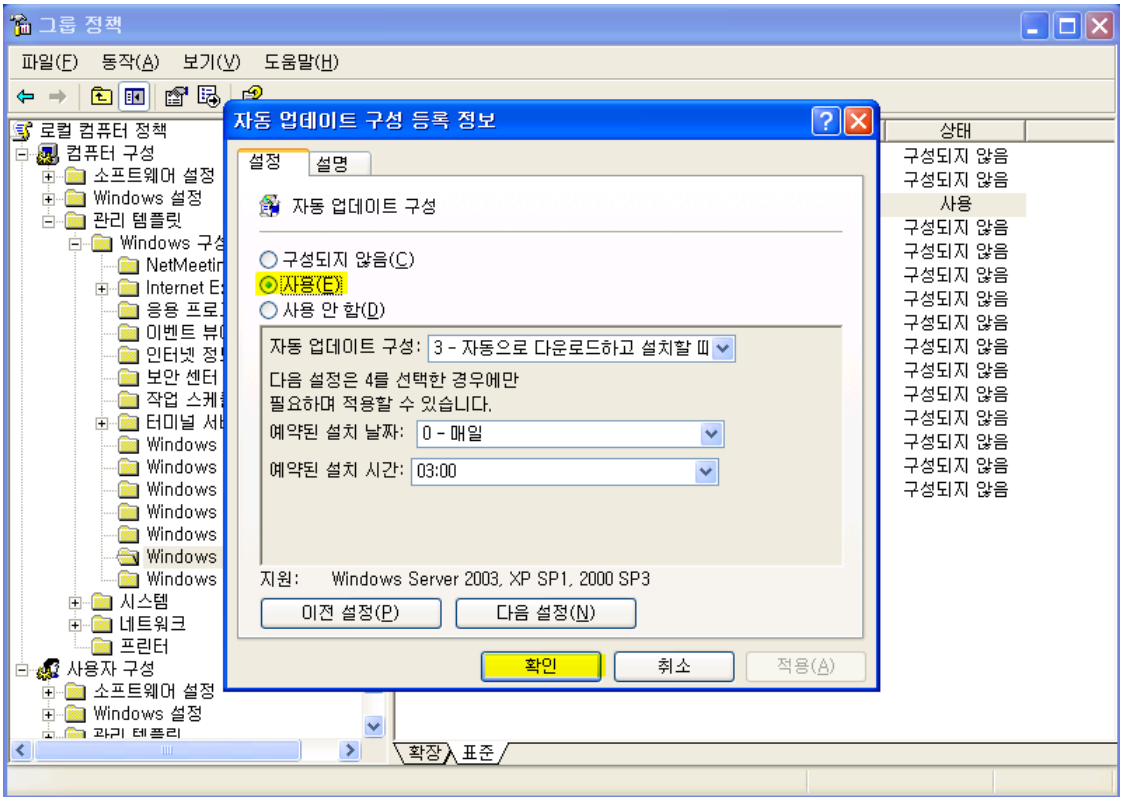
(그룹 정책 편집기 창이 뜬다. 이하의 작업은 개별 Client PC의 업데이트 설정작업과 동일함.)



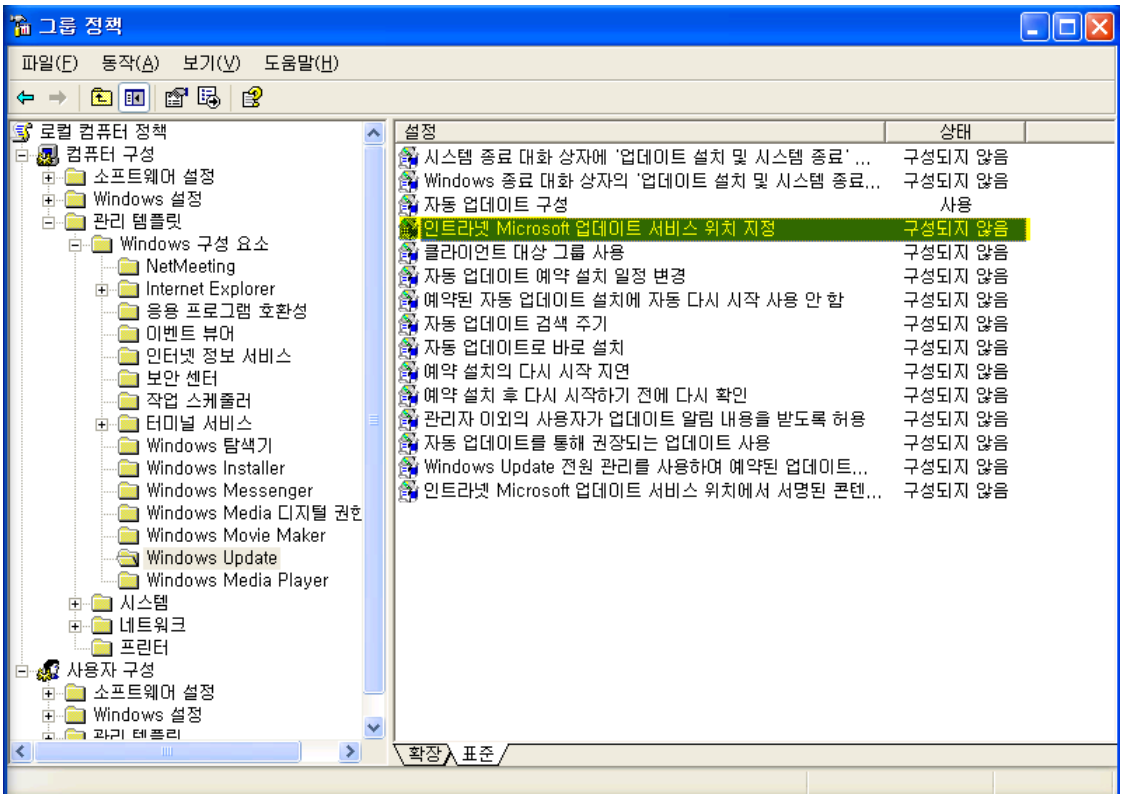
e. 그룹 정책 편집기 대화상자에서 컴퓨터 구성 – 관리 템플릿 – Windows 구성 요서 – Windows Update 로 들어간 후 우측 목록에서 "자동 업데이트 구성" 더블 클릭한다.



f. "사용" 에 체크 – "확인" 버튼 클릭

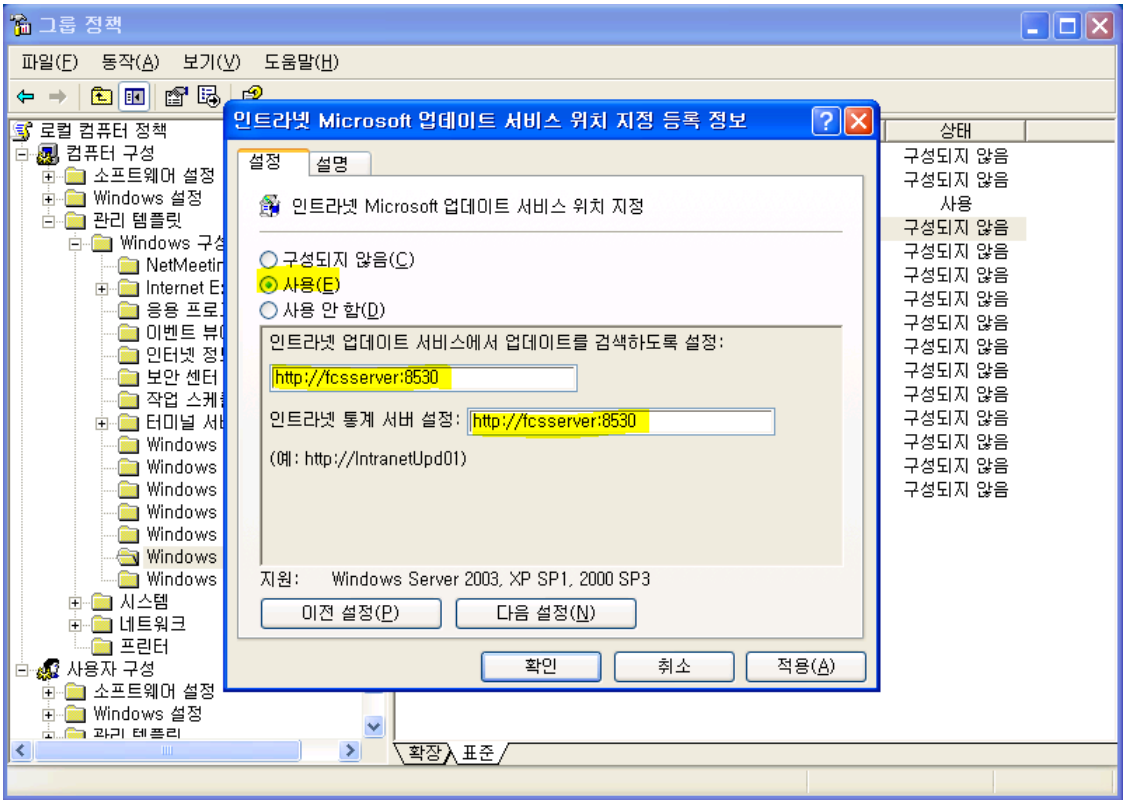


g. 우측 목록에서 "인트라넷 Microsoft 업데이트 서비스 위치 지정" 더블 클릭

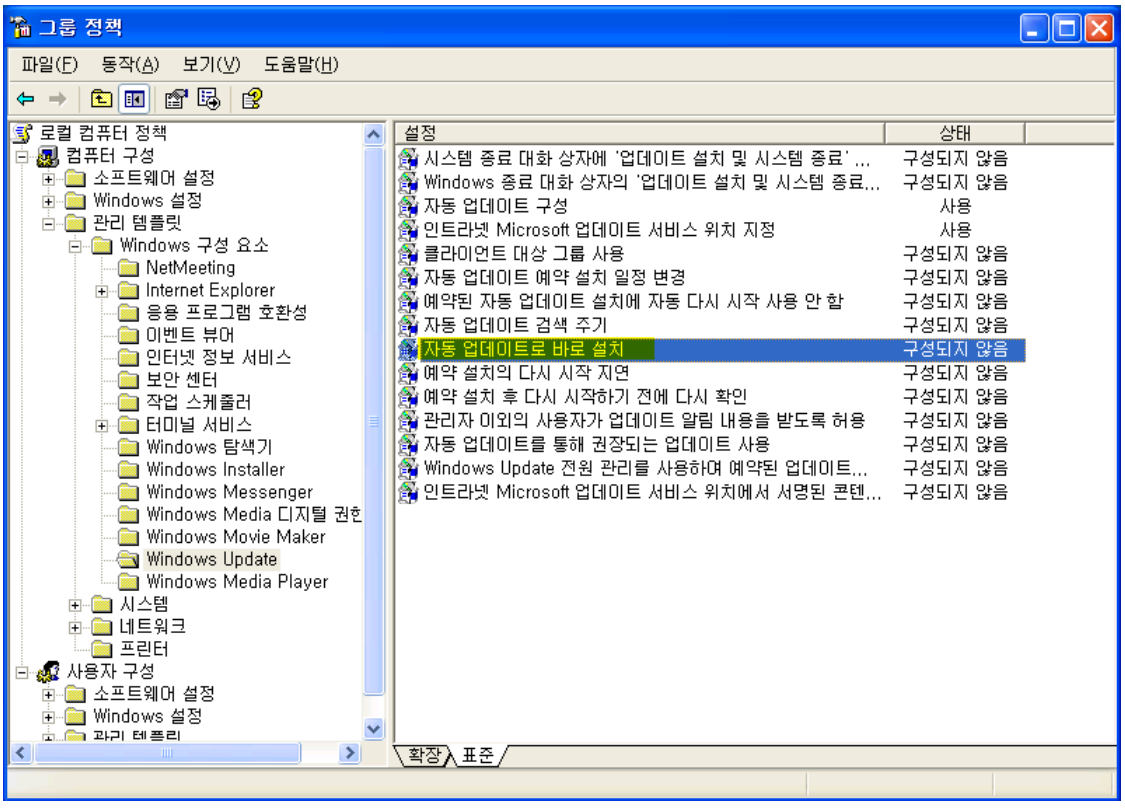


h. "사용"에 체크하고 "인트라넷 업데이트 서비스에서 업데이트를 검색하도록 설정" 입력 상자와 "인트라넷 통계 서버 설정" 입력 상자에 WSUS의 URL을 입력한 다음 "확인" 버튼 클릭.

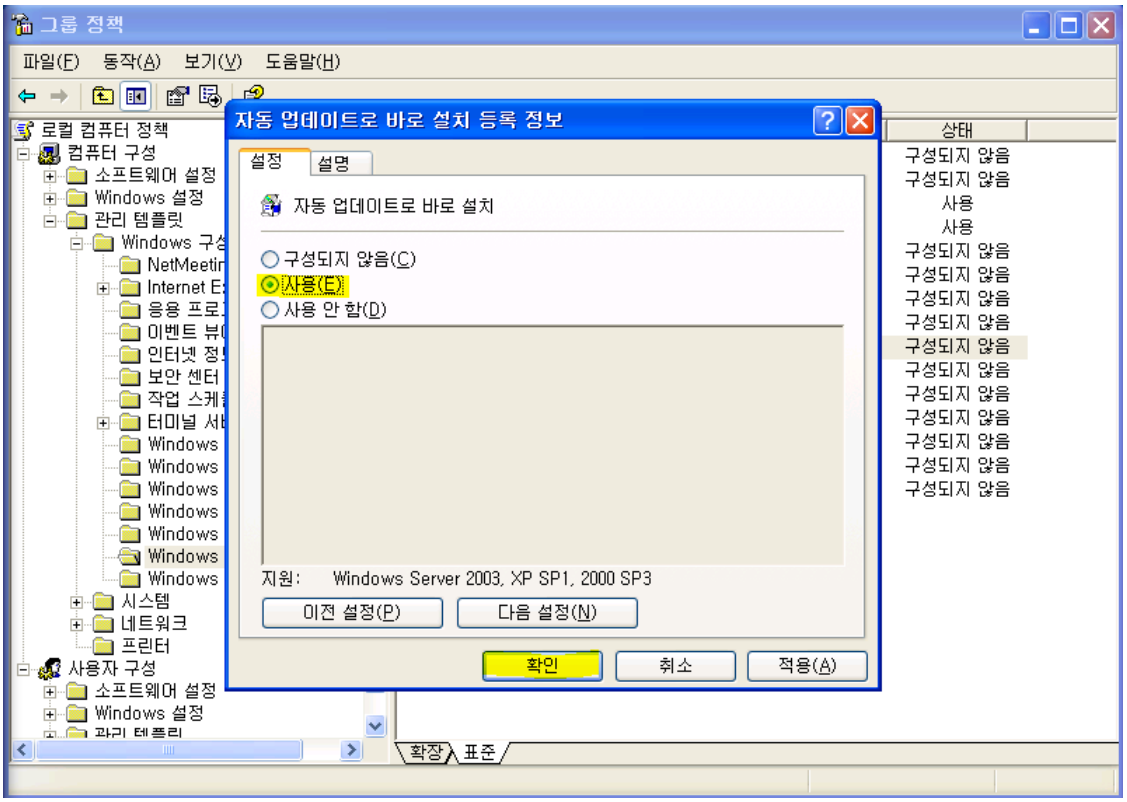
중요 : URL 뒤쪽에 포트 번호를 입력해야 한다.(ex : http://fcsserver:8530)



i. 우측 목록에서 "자동 업데이트로 바로 설치" 더블 클릭



j. "사용"에 체크하고 "확인" 버튼 클릭



6.5. 클라이언트 컴퓨터에 Client Security 배포

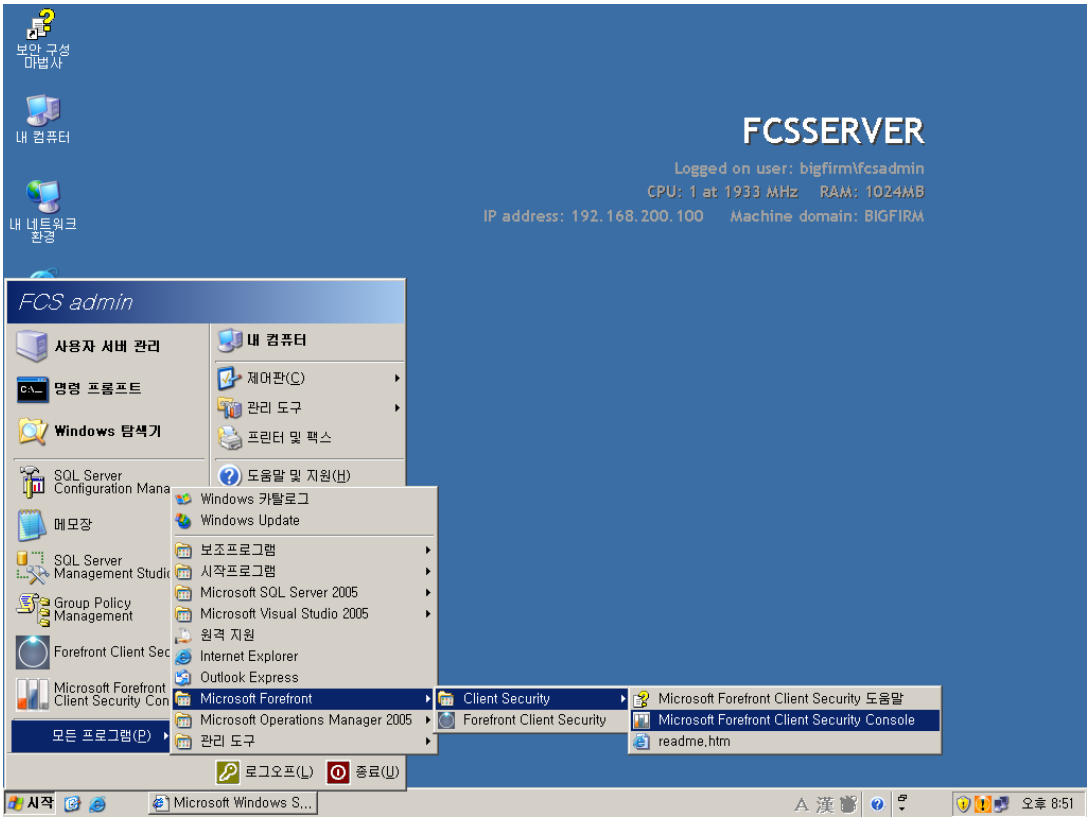
클라이언트 컴퓨터에 Client Security를 배포하려면 먼저 해당 컴퓨터에 정책을 배포해야 합니다. 정책이 배포되면 클라이언트 컴퓨터는 배포 서버에서 Client Security를 자동으로 다운로드 합니다. 클라이언트 컴퓨터에 대한 Client Security 정책 배포 방법을 결정할 때는 다음 사항을 염두에 두십시오.

*** 정책을 적용하려면 하나 이상의 대상 조직 구성 단위(OU), 보안 그룹 또는 GPO에 정책을 배포해야 합니다.**
*** 파일을 대상으로 배포하면 정책이 배포됨으로 표시됩니다. 그러나 아직 해당 클라이언트 컴퓨터에 정책을 적용해야 합니다. 정책을 적용할 때는 Client Security CD에 있는 fcspolicytool.exe 도구를 사용하는 것이 좋습니다.**

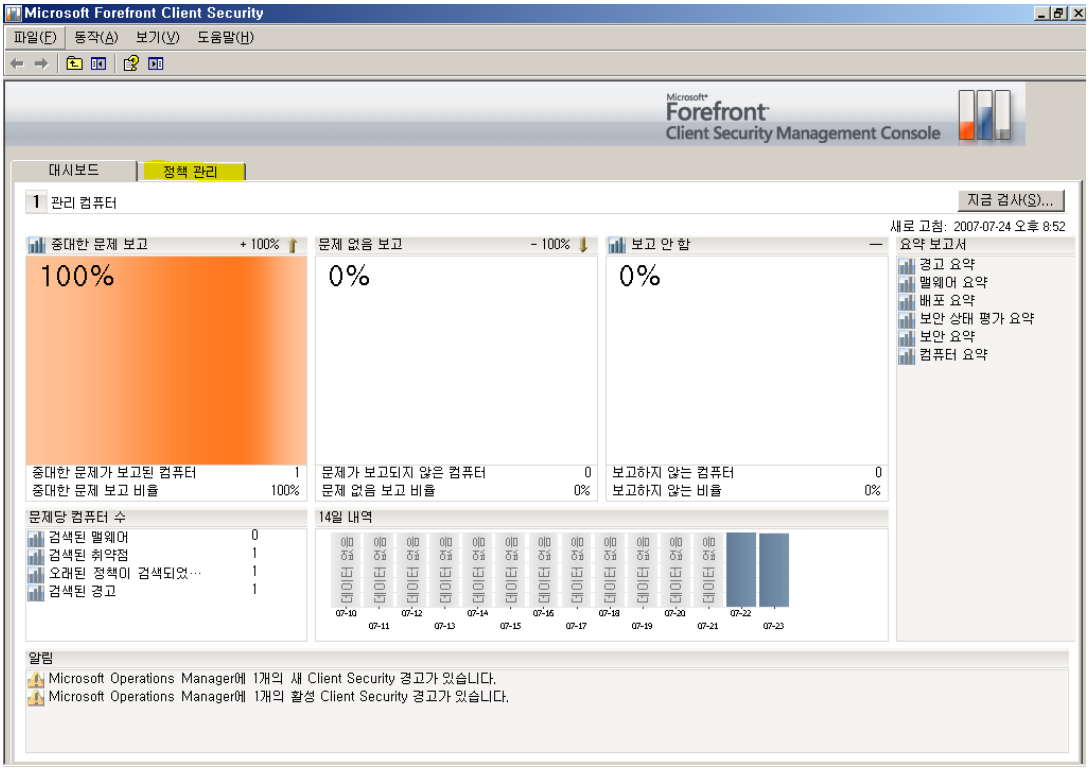
클라이언트 구성 요소가 배포된 후 클라이언트 컴퓨터가 데이터 보고를 시작하려면 MOM의 승인을 받아야 합니다. 클라이언트는 대개 한 시간 내에 자동으로 승인됩니다. 더 빨리 데이터를 보고하도록 하려면 클라이언트 컴퓨터를 수동으로 승인하면 됩니다. 자세한 단계는 이 항목의 뒷 부분에 나오는 MOM서버를 통해 클라이언트 승인을 참조하십시오.

6.5.1. 정책 생성

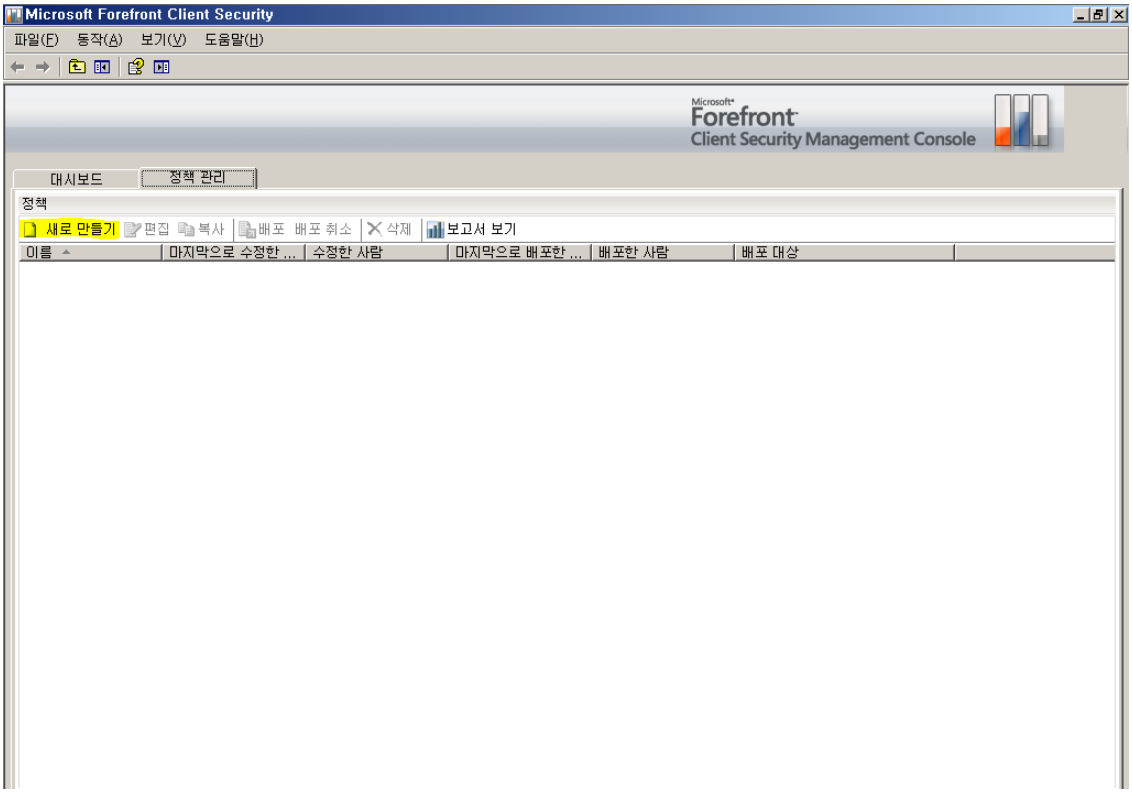
1. Forefront 서버에서 시작 – 모든 프로그램 – Microsoft Forefront – Client Security – Microsoft Forefront Client Security Console 클릭



2. "정책 관리" 탭 클릭

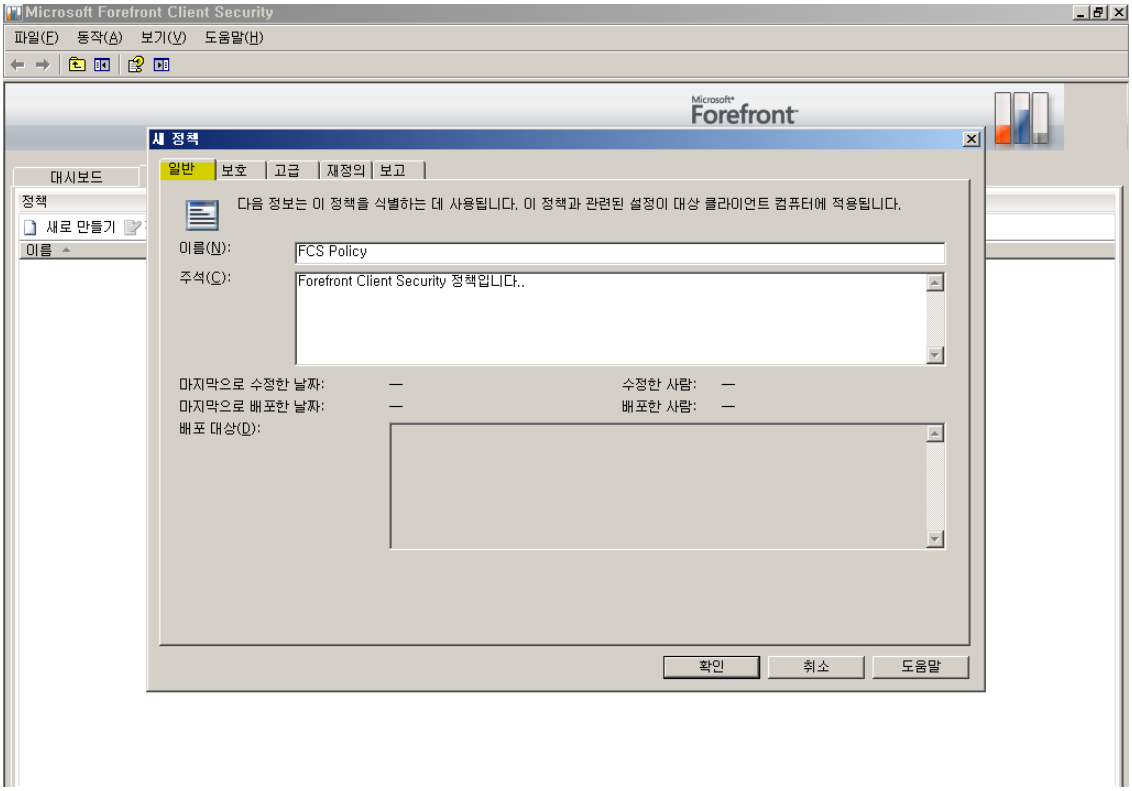


3. “새로 만들기” 클릭

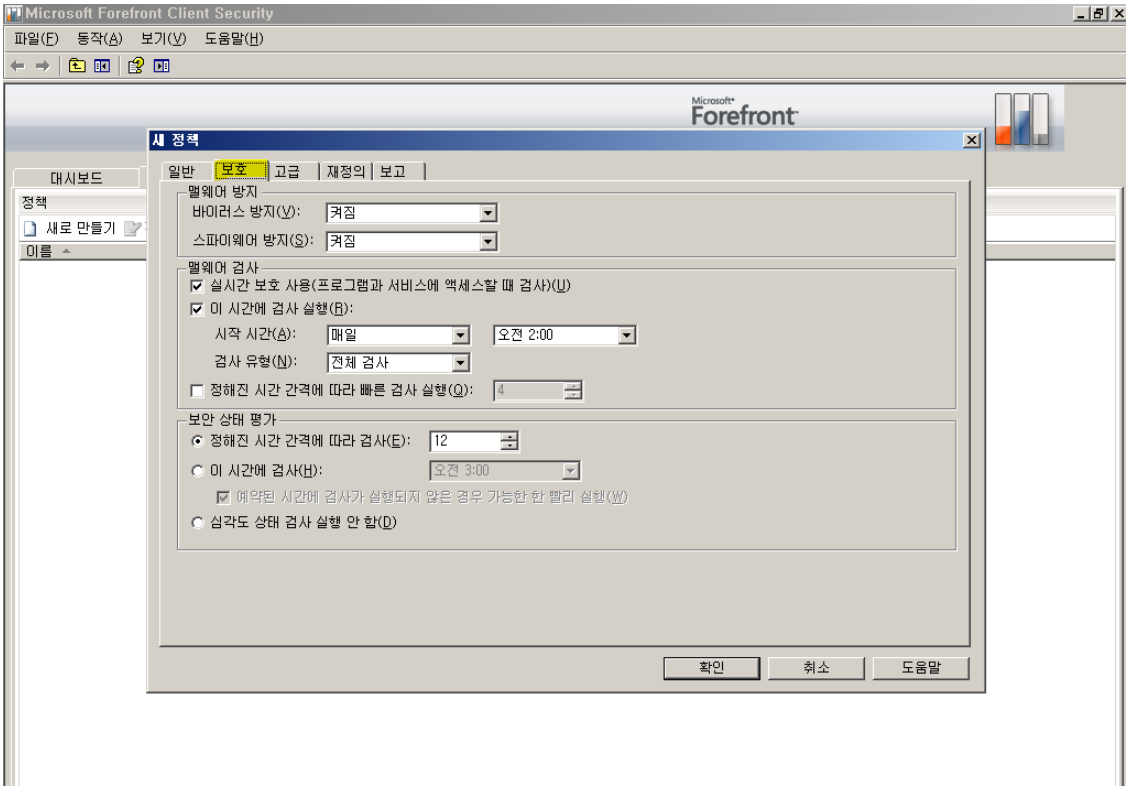


4. 새 정책

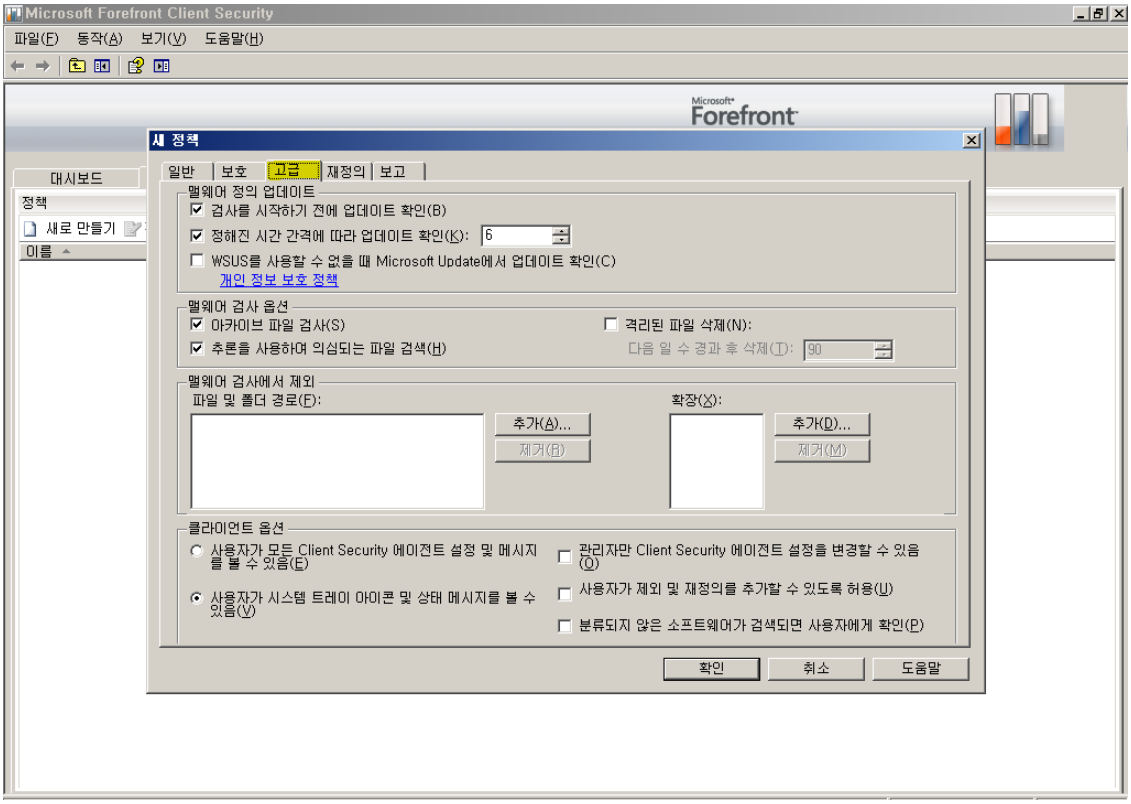
a. 일반 탭 – 정책 이름 과 설명을 입력한다.



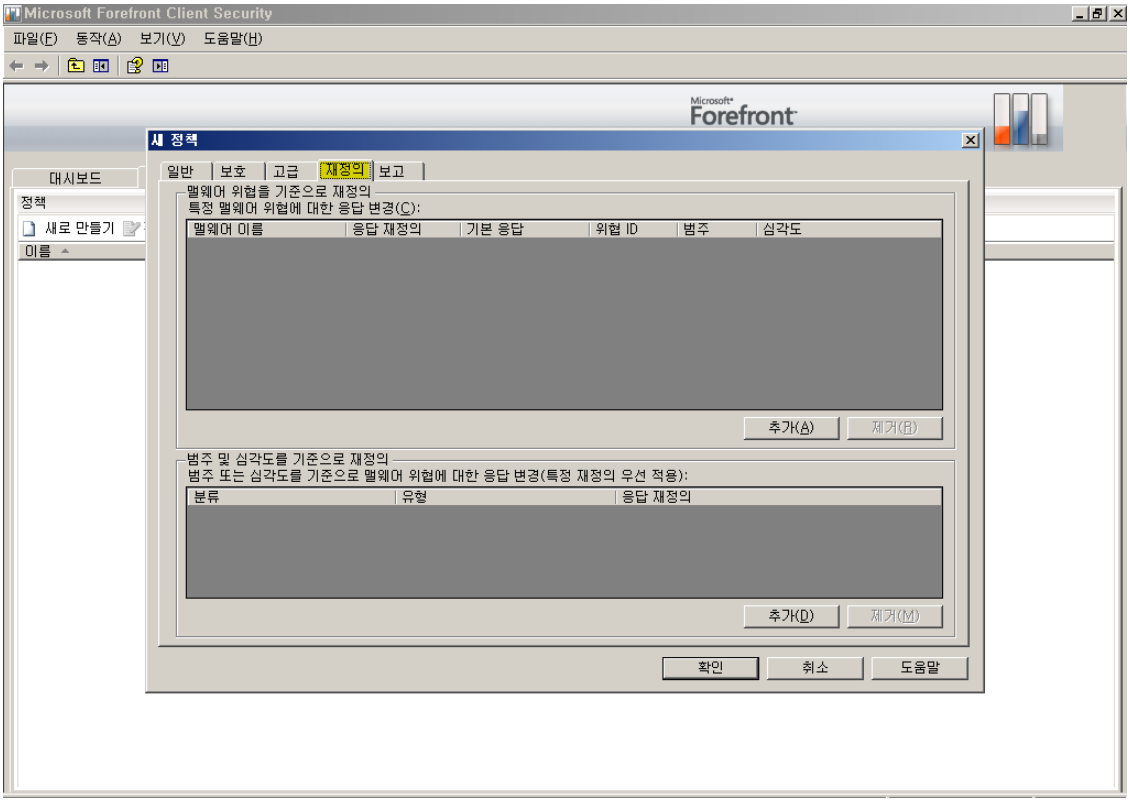
b. 보호 탭 – 바이러스 실시간 감시 및 보안 상태에 관한 설정을 한다.(기본 값 사용)



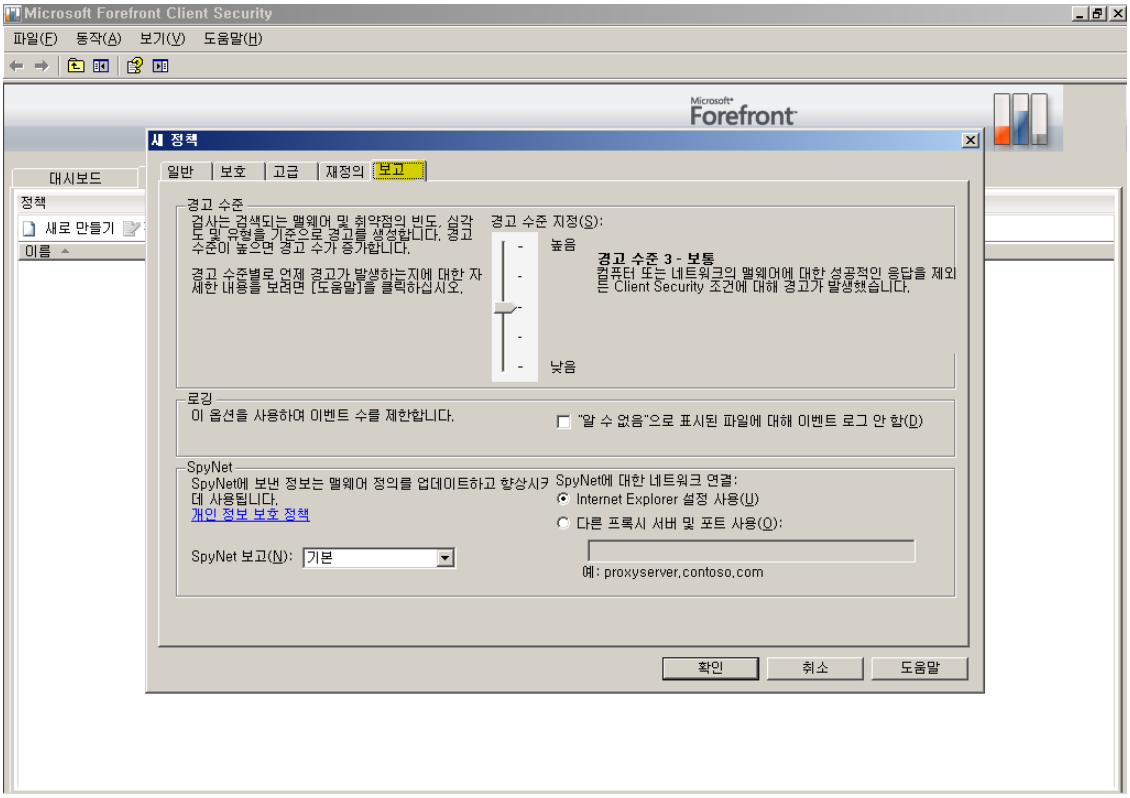
c. 고급 탭 – 악성 코드 정의 업데이트 및 검사 옵션을 설정할 수 있다. (기본 값 사용)



d. 재정의 탭 – 특정 악성 코드의 의협 및 범주에 따라 대응을 재정의할 수 있다.



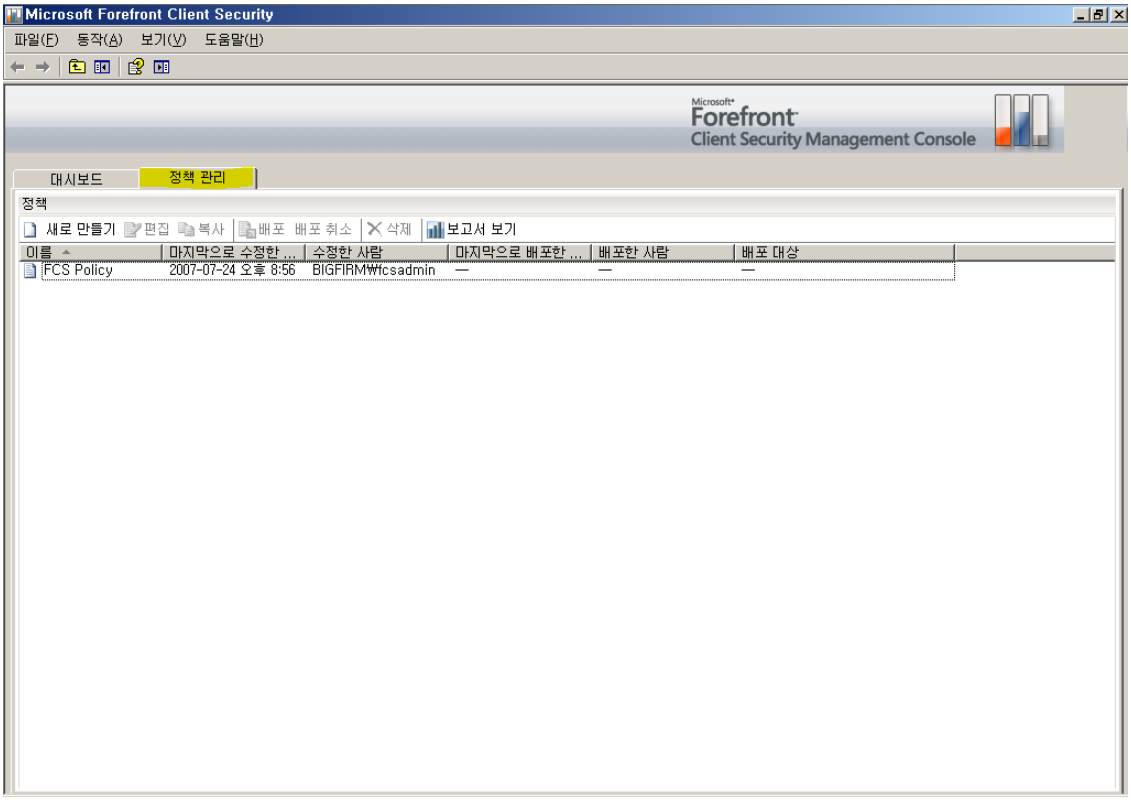
e. 보고 탭 – 보고와 관련된 설정을 할 수 있다. (기본 값 사용)



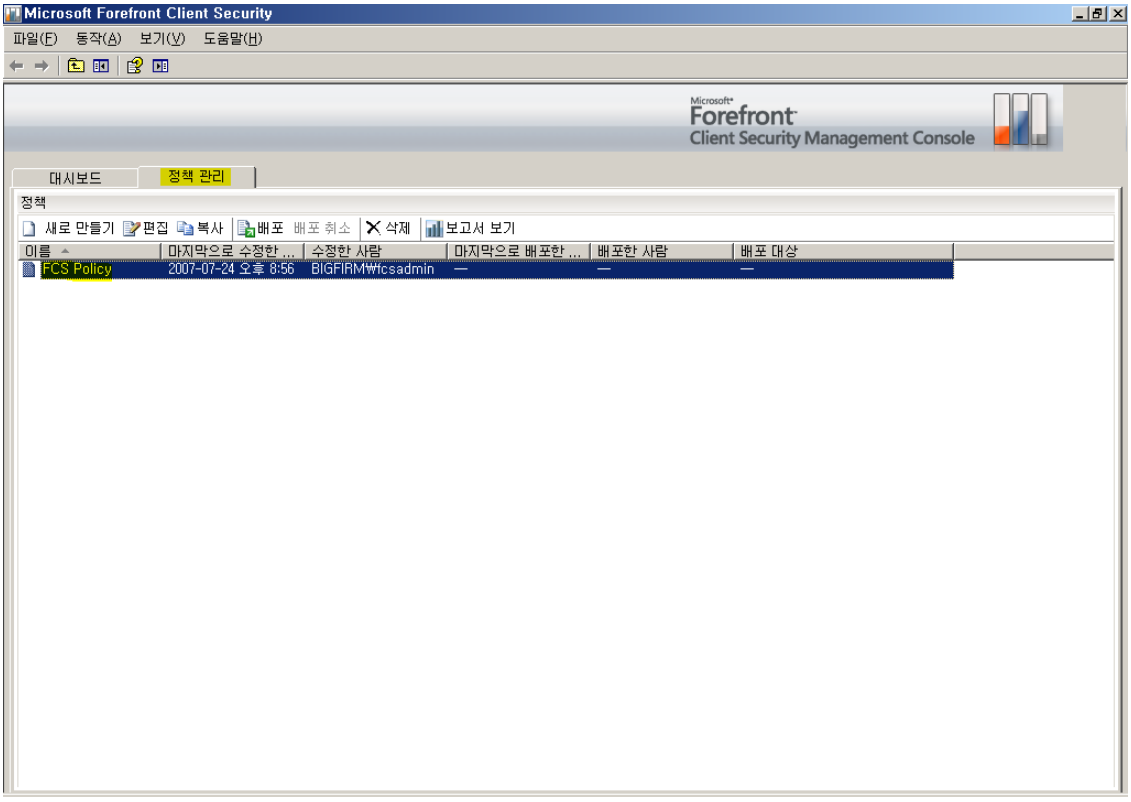
5. 확인을 눌러 정책을 저장한다.

6.5.2. 정책 배포

1. Client Security 콘솔 – 정책 관리

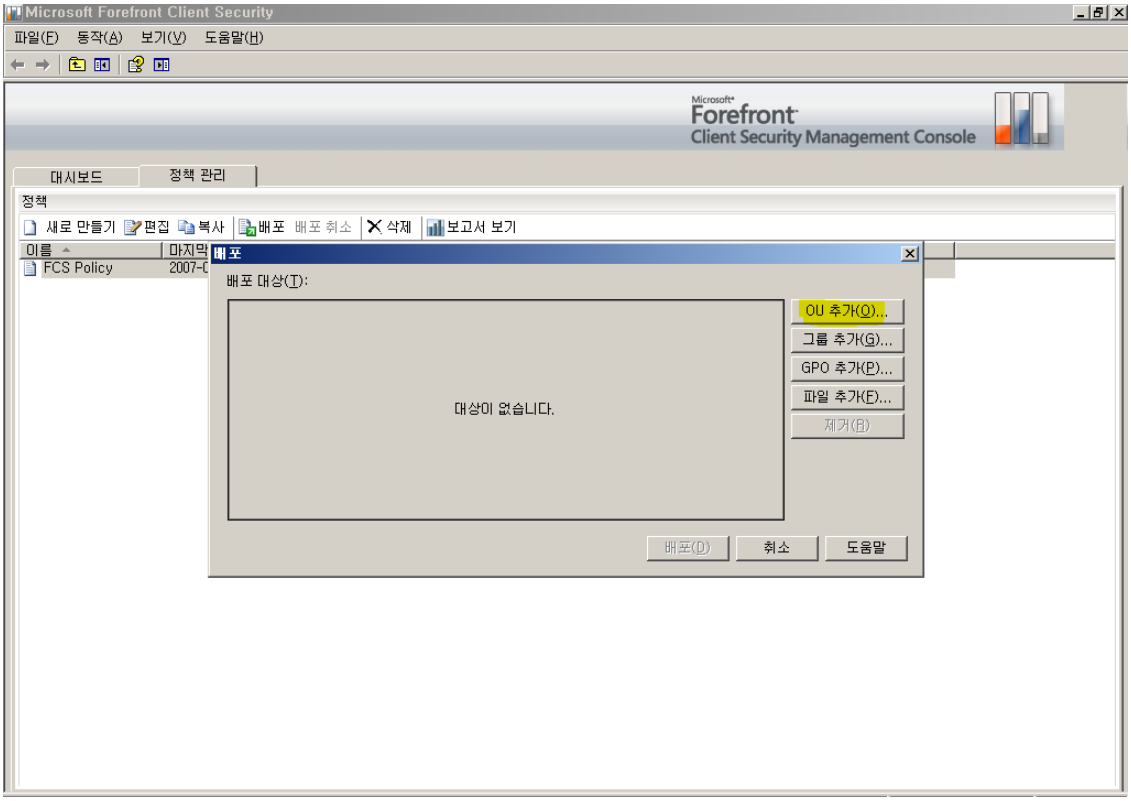


2. 배포할 정책을 선택하고 "배포" 클릭

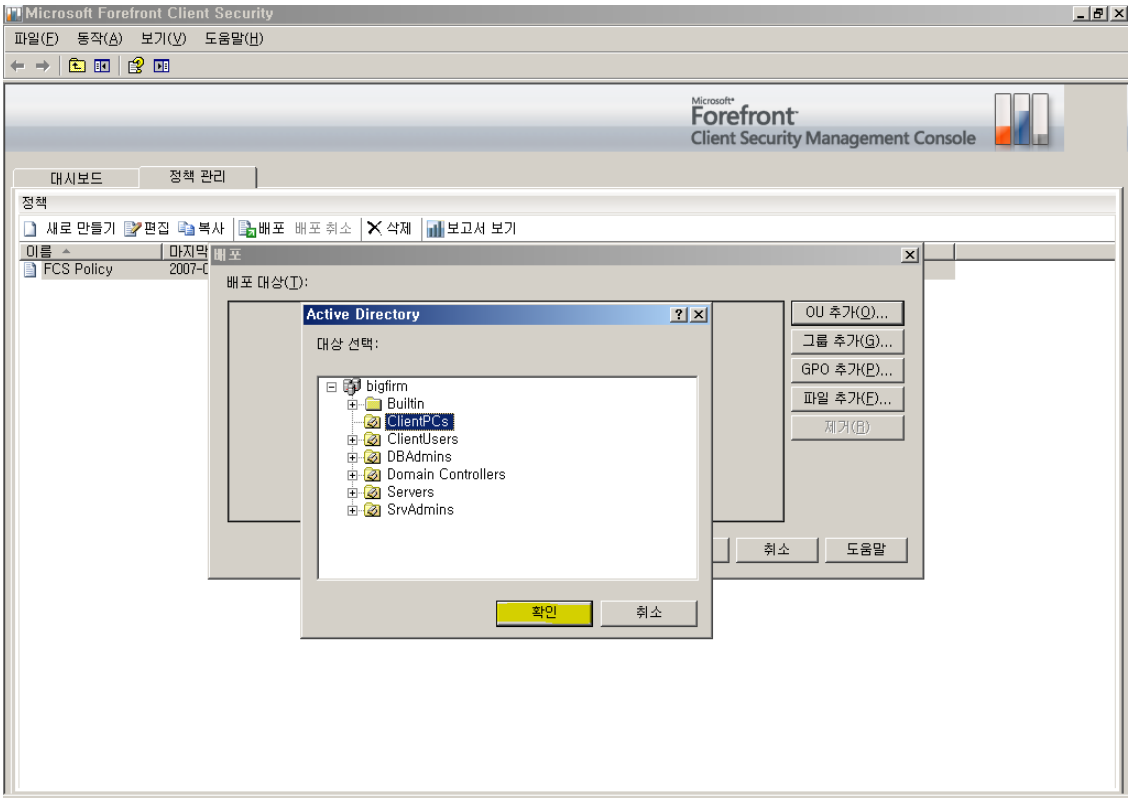


3. 배포 대화상자에서 배포할 대상을 선택 (OU에 배포한다고 가정)

a. "OU 추가(O)..." 버튼 클릭



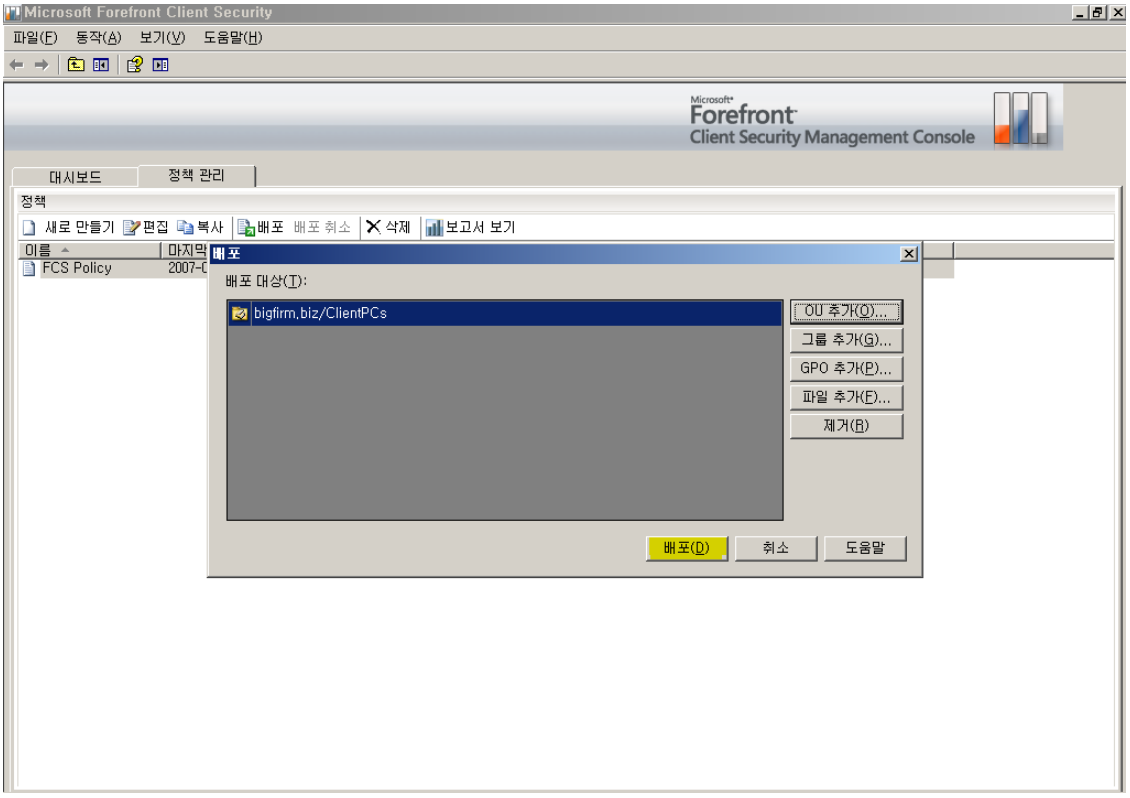
b. 대상 선택에서 도메인 혹은 원하는 OU 선택 후 확인



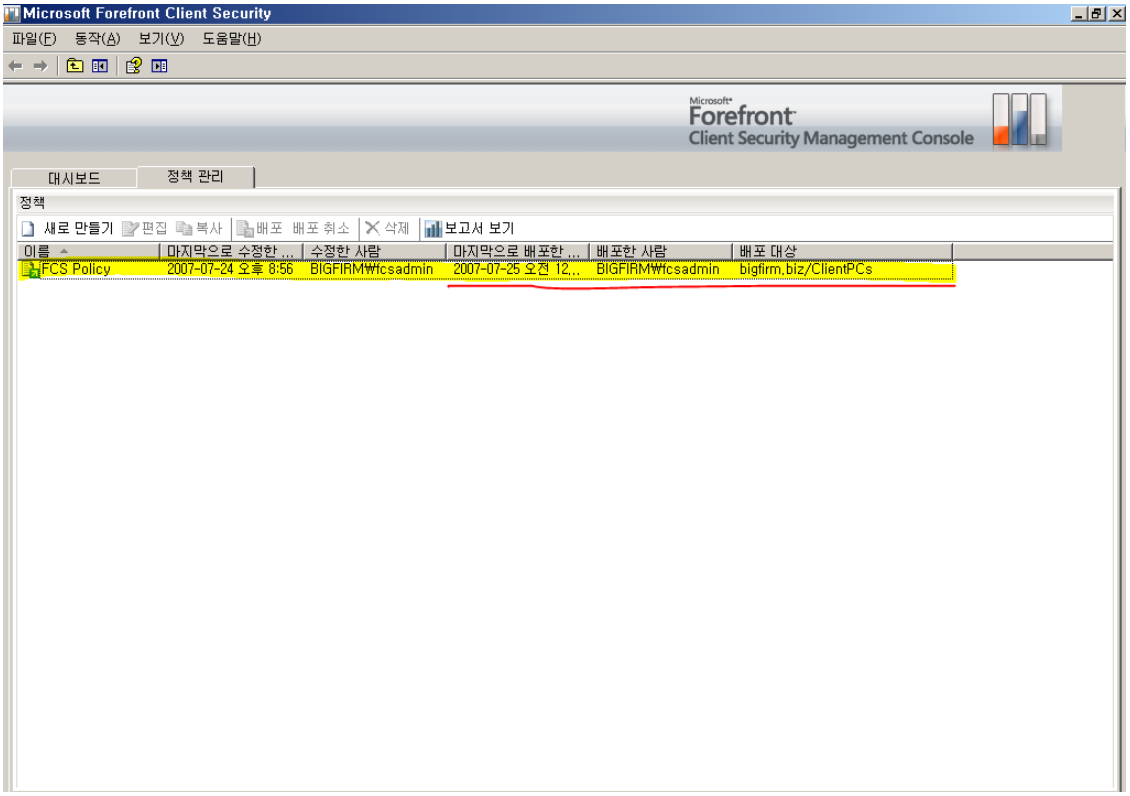
c. 배포 클릭

*주의 : 정책 배포 계정(Policy Deploy Role)에 적절한 권한이 없으면 배포에 실패합니다.

참고 문서 - Working with user roles(http://go.microsoft.com/fwlink/?linkid=86555)



d. 정상적으로 배포가 성공한 화면 (빨간 색 밑줄 친 부분)

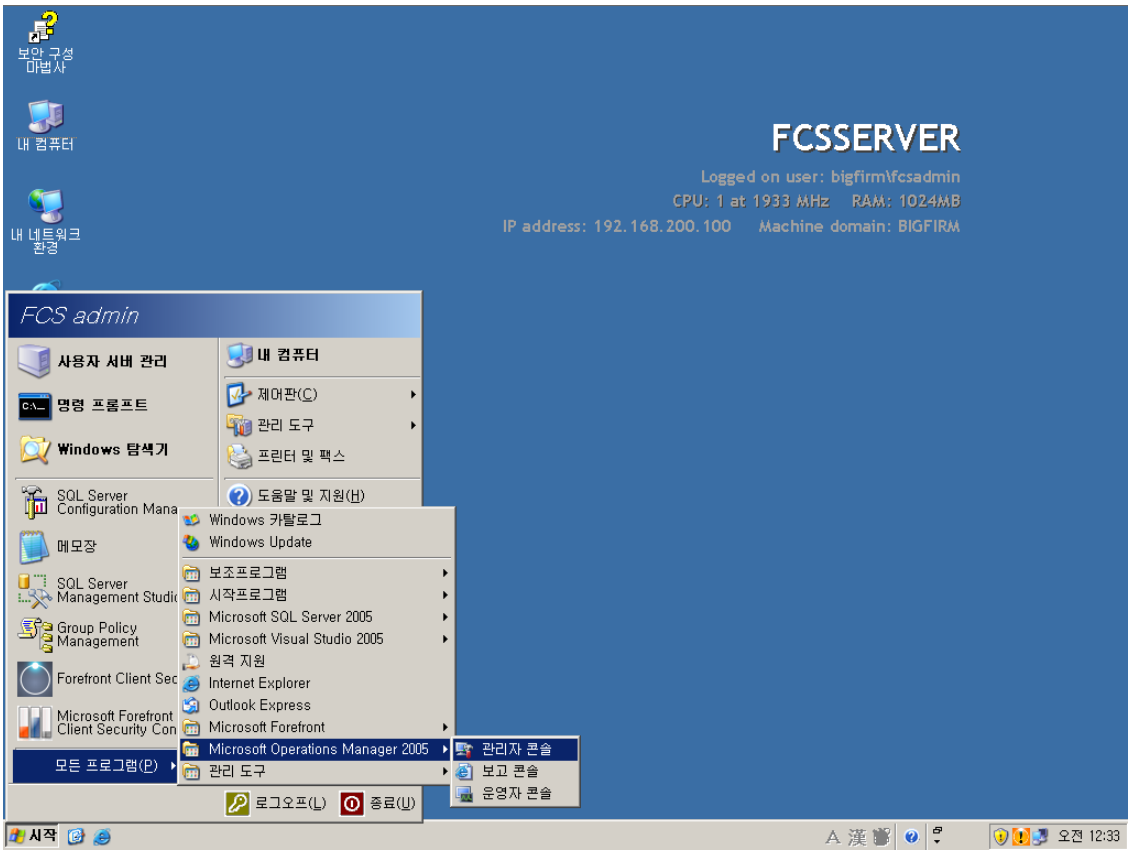


6.5.3. MOM 서버를 통해 클라이언트 승인

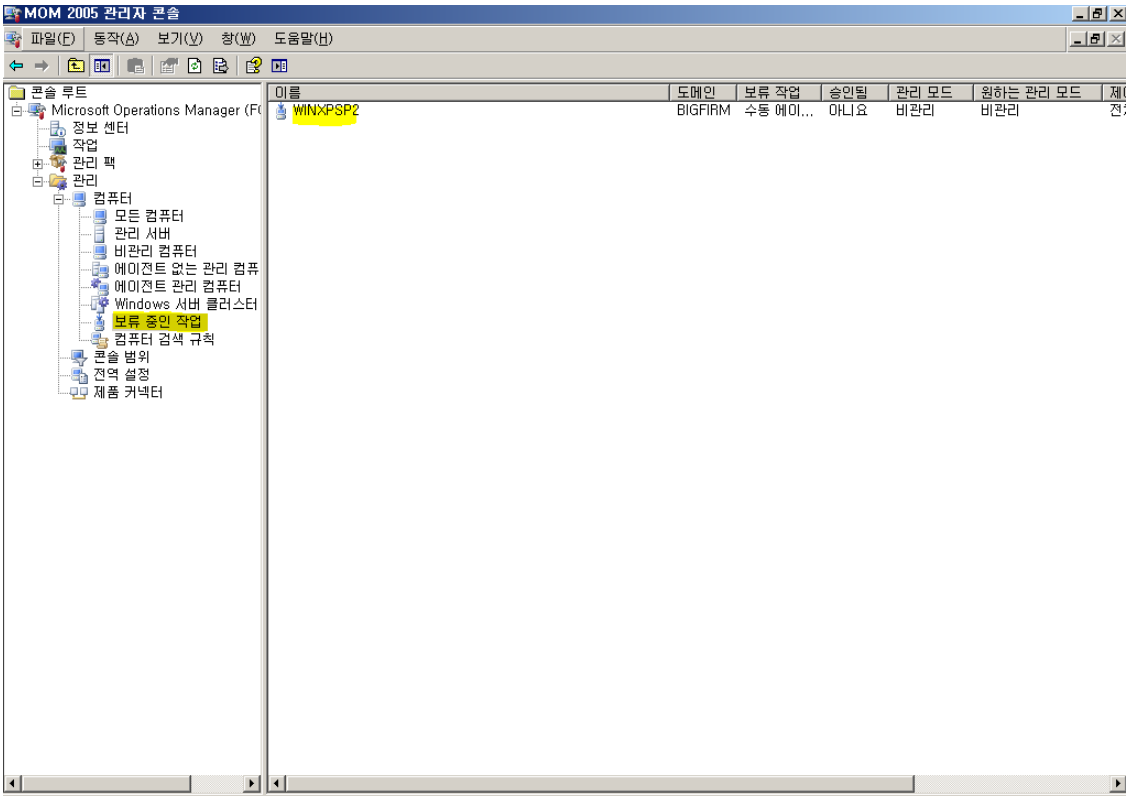
배포된 후 클라이언트는 대개 한 시간 내에 자동으로 승인됩니다. 이보다 더 빨리 데이터를 보고하도록 하려면 클라이언트 컴퓨터를 수동으로 승인하면 됩니다.

MOM 서버를 통한 클라이언트 수동 승인 절차

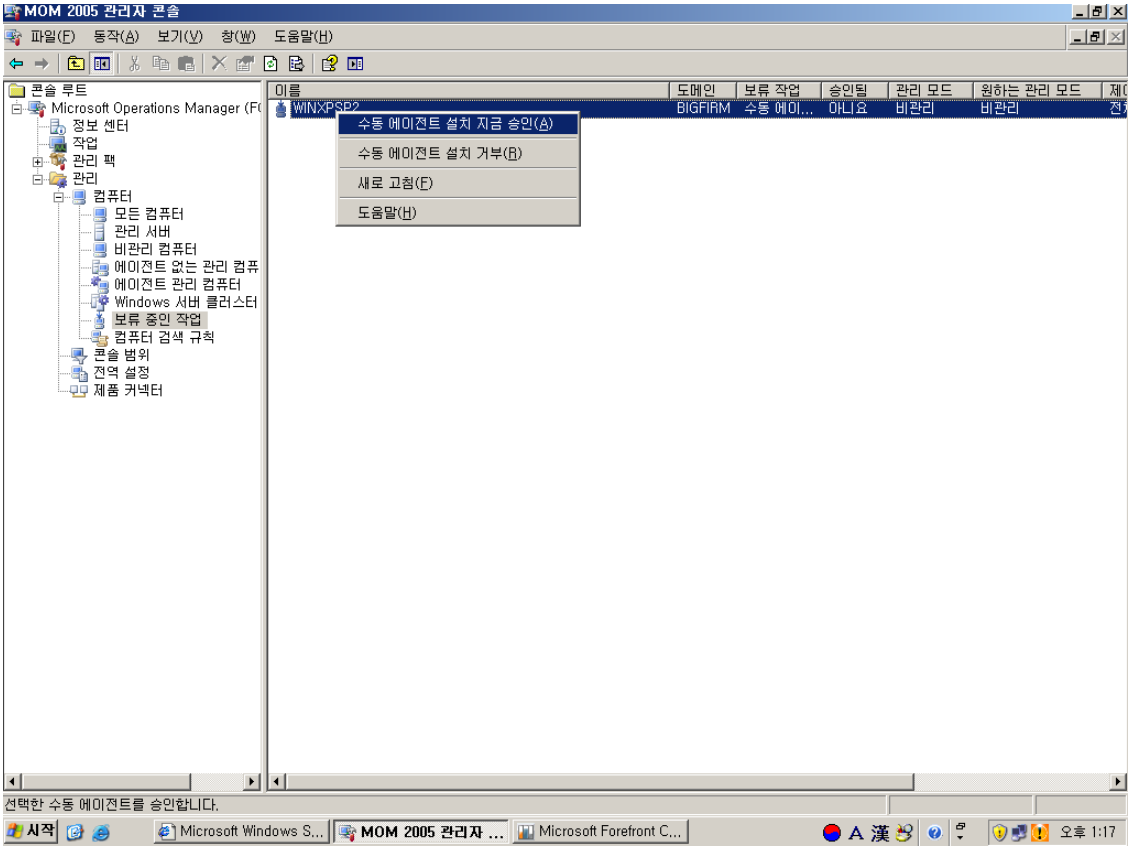
1. Forefront Client Security 관리 서버에서 시작 – 모든 프로그램 – Microsoft Operation Manager 2005 – 관리자 콘솔 클릭



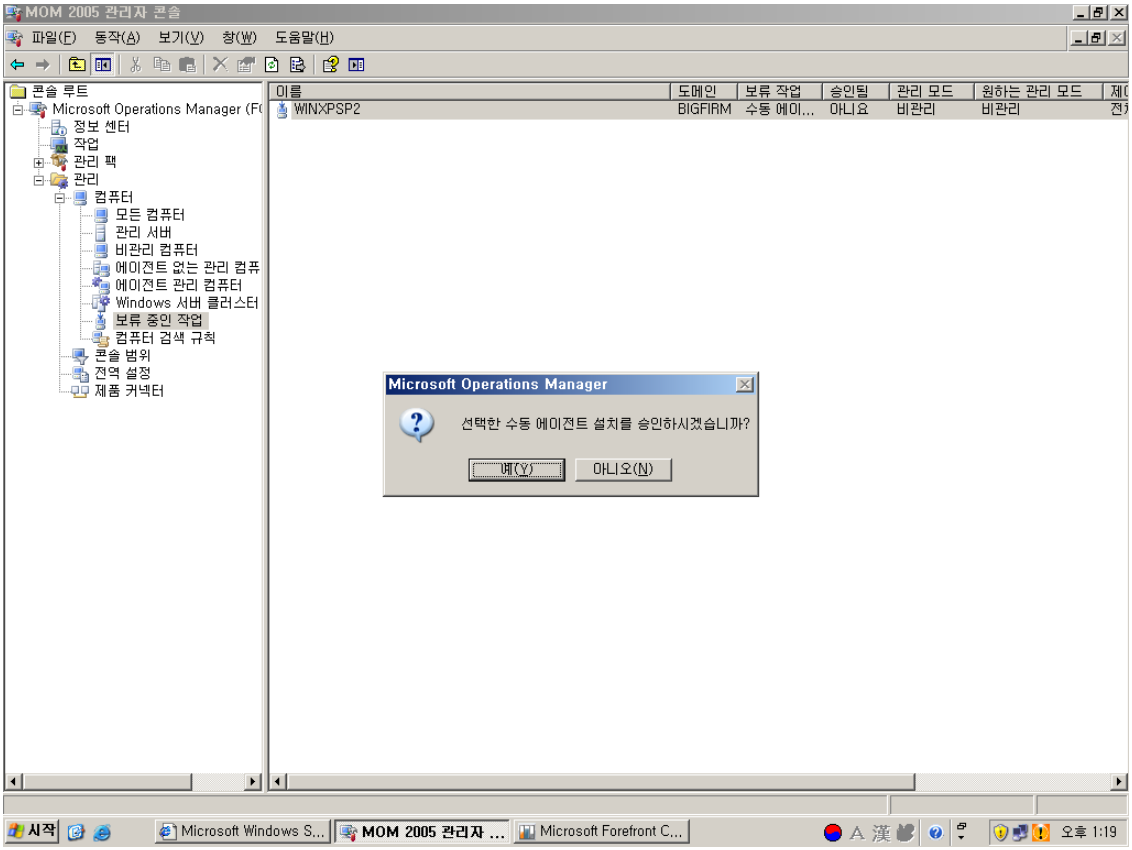
2. MOM 2005 관리자 콘솔의 콘솔 루트 – Microsoft Operations Manager – 관리 – 컴퓨터 – 보류 중인 작업 클릭 (우측 창에 보류 중인 PC가 보인다)



3. 보류 중인 컴퓨터 마우스 오른쪽 버튼 클릭 – "수동 에이전트 설치 지금 승인" 선택



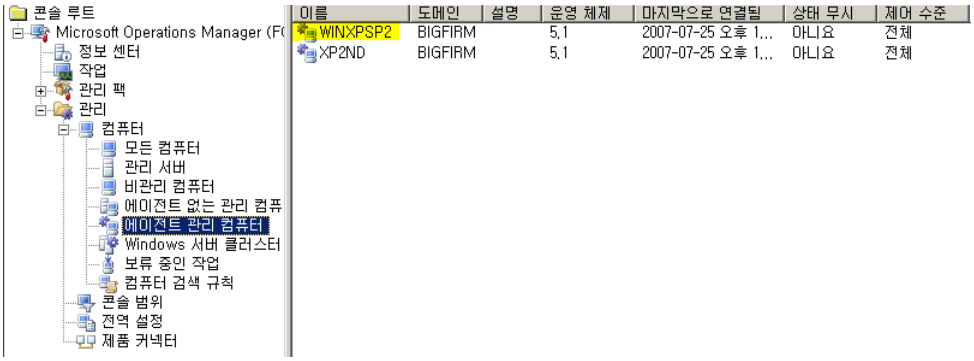
4. Microsoft Operations Manager 대화 상자에서 "예" 클릭 (대화창이 사라진다)



5. 보류 중인 작업 목록에서 사라지고, 에이전트 관리 컴퓨터 목록에 나타난다.

보류 중인 작업 목록 – 컴퓨터가 사라졌다.

에이전트 관리 컴퓨터 목록 – 보류 중이었던 PC가 넘어와있다.



6.6. Client Security 배포 확인

Client Security를 설치 및 구성하고 정책 및 클라이언트 컴퓨터를 배포하고 나면 설치가 완료됩니다. 설치를 완료한 후에는 보고서를 통해 Client Security가 제대로 실행되고 있는지 확인할 수 있습니다.

*중요
클라이언트 구성 요소의 배포를 확인하기 전에 정책이 배포되고 클라이언트 구성 요소가 배포되고 MOM에서 클라이언트 컴퓨터가 승인된 후 클라이언트 컴퓨터가 데이터 보고를 시작할 때까지 기다려야 합니다. 경우에 따라 클라이언트 컴퓨터를 수동으로 승인하고 정책 배포를 강제 설정하여 이러한 과정을 단축할 수 있습니다.

보고서 보기
Client Security 콘솔에는 네트워크의 상태 및 보안에 관한 다양한 보고서에 대한 링크가 포함되어 있습니다. 이러한 보고서를 통해 Client Security의 정책 배포, 검사 수행, 배포 정의 제공, 경고 및 이벤트 수집을 확인할 수 있습니다. Client Security 배포를 확인할 때 특히 중요한 다음과 같은 두 가지 보고서가 있습니다.
* 보안 요약 정책 배포 상태, 연결 상태, 맬웨어 및 보안 상태 평가 검사 결과를 표시합니다.
* 배포 요약 맬웨어 및 보안 상태 평가 검사에 대한 최신 정책 및 정의가 있는 컴퓨터 그룹을 표시합니다.

보고서를 보려면
1. Client Security 콘솔을 엽니다.
2. 대시보드 탭의 요약 보고서 영역에서 원하는 보고서를 클릭합니다.