

Exchange 서버에 SSL&TLS 통신 사용시 문제 될 수 있는 부분을 정리

본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다.

[고객센터]
한국기업보안. 유서트 기술팀



아래 내용은 Exchange 서버에 SSL&TLS 통신 사용 시 문제 될 수 있는 부분을 정리 하였습니다.

또한 첨부 드린 파일은 Autodiscover기능을 사용 할 경우 발생 할 수 있는 인증 실패에 대한 내용을 **파일 첨부** 드렸습니다

1. Exchange 와일드 카드 인증서 적용 가능 여부

Exchange 에 등록 된 도메인이 와일드카드 인증서로 지원이 가능하면 적용이 가능합니다.

예) autodiscover.ucert.co.kr, mail.ucert.co.kr, netbios.ucert.co.kr

2. Exchange SSL통신 메커니즘

- ① SMTPS POP3S IMAP4 등의 SSL 보안 통신을 지원 합니다.
- ② 1번의 기능을 자체 서명 인증 구성으로 위 내용을 지원 하지만 아래와 같은 문제점이 발생 됩니다.
- ③ PKI 암호화의 특성상 공개되는 키(공개키)의 신뢰성을 확인 할 수 없습니다.
- ④ 3번과 같은 이유로 외부 서비스 시 Exchange ActiveSync와 Outlook Anywhere를 사용 할 수 없습니다.

아래와 같은 기능을 사용 시 공용 CA에서 서명된 인증서를 사용 하셔야 합니다.

- A. POP3 및 IMAP4 클라이언트의 Exchange 액세스
- B. Outlook Web Access
- C. 외부에서 Outlook 사용
- D. Exchange ActiveSync
- E. 자동 검색
- F. 도메인 보안

Exchange 2007 에서 Autodiscover 서비스 구성을 통해서 쉽게 Outlook 프로필을 자동으로 구성하실 수 있음은 아실 겁니다.



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

하지만 사설인증서를 통해서 인증서 서비스를 구현할 경우 인증서 주체이름 때문에 Outlook 프로필 구성 후 사용자 인증에 실패하는 사례가 몇몇 있었습니다.

예시 환경)

Exchange 2007 Server

통합 Exchange FQDN : mail.msexchange.com

Outlook Anywhere 연결주소 : proxy.msexchange.com

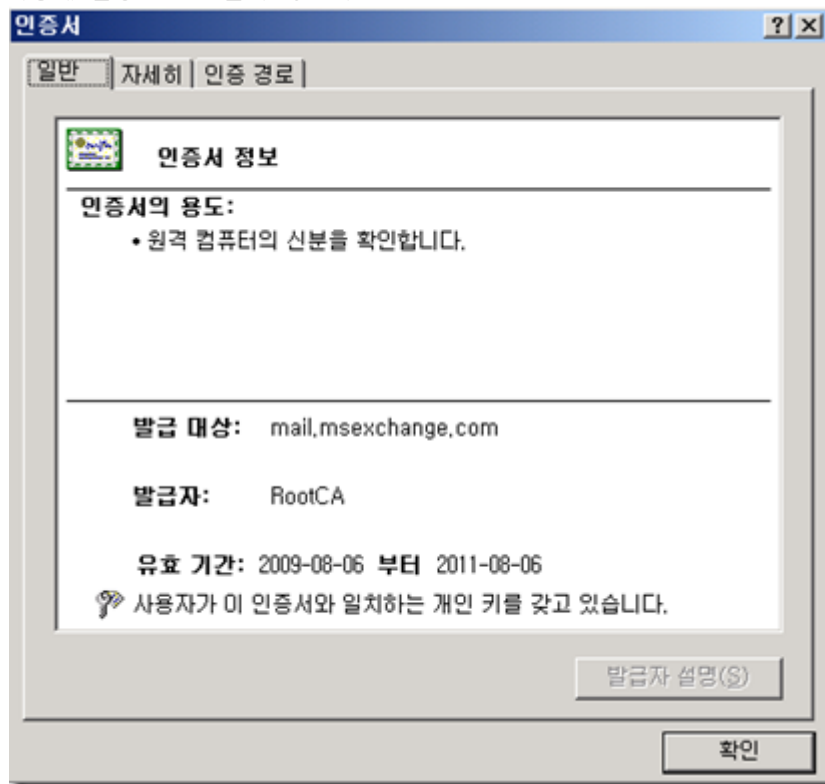
Autodiscover 를 통한 프로필 구성시 인증에 실패하는 경우는 이렇습니다

결론부터 말씀 드리면 CAS 서버의 IIS 웹사이트 바인딩 된 인증서의 주체이름과 Outlook 프로필 생성시 설정되는 Outlook Anywhere 연결설정에서 msstd:인증서 주체이름 값이 서로 다를 경우 로그인에 실패합니다.

이 부분을 이제부터 자세히 풀어서 설명 드리겠습니다

1. CAS 서버의 /Autodiscover 가상 디렉토리가 위치하는 IIS 의 기본웹사이트에서 인증서를 확인해보면 CAS 서버의 FQDN 이 대상임을 확인하실 수 있습니다.

이렇게 설정하는 분들이 많으시죠.



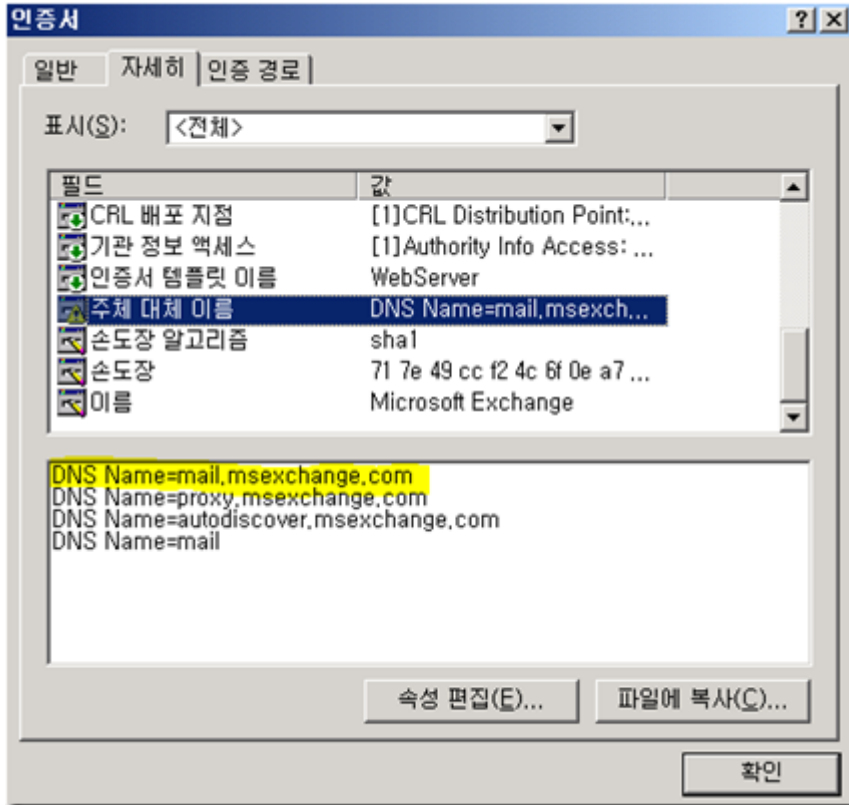
또한 자세히 탭을 통해서 주체대체이름, 혹은 SAN(Subject Alternative Name)이라고 부르는 값도 확인합니다.

제일 앞에 오는 이름은 New-ExchangeCertificate 명령을 통한 인증서 요청 파일 생성시 제일 앞에 입력한 이름이며 이 이름이 곧 주체이름으로 포함됨을 확인할 수 있습니다.

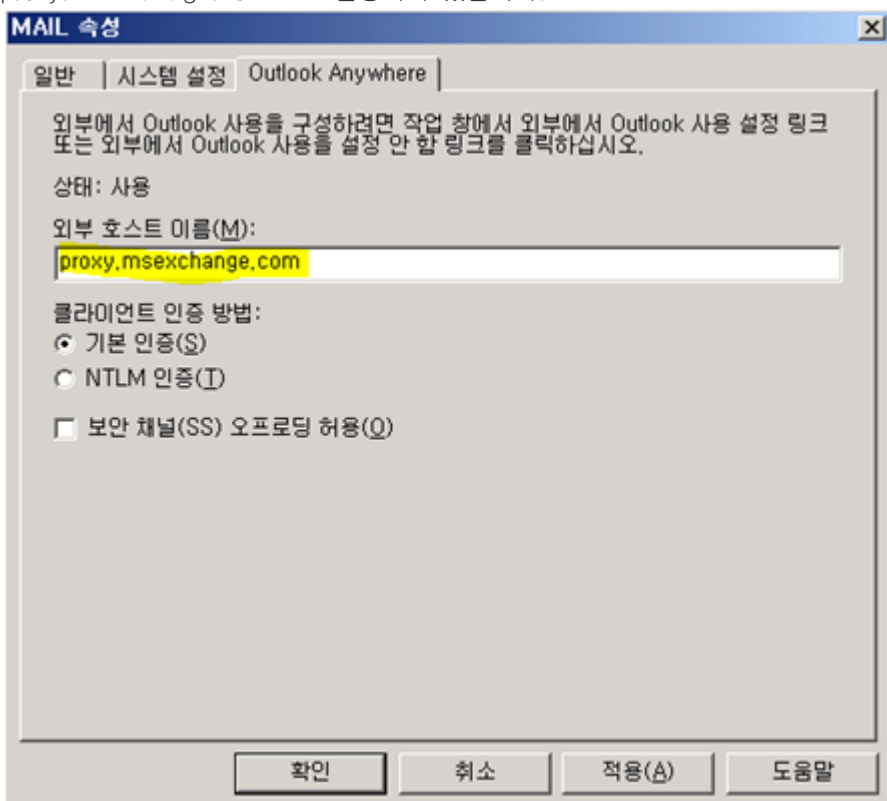
그 뒤의 이름들은 주체이름이 외에 인증서를 통해서 신뢰하는 도메인 이름들이 포함되어 있습니다.



(아래 예의 인증서는 4 개의 DNS 이름을 통한 연결에 대하여 신뢰하게 됩니다)



2. Exchange 관리콘솔에서 서버 구성 > 클라이언트 액세스 > 클라이언트 액세스 서버의 속성 > Outlook Anywhere 탭에서 구성된 외부 호스트이름을 확인합니다.
 이 이름이 실제적으로 외부 Outlook 클라이언트에서 Exchange 프록시 정보로 설정되는 URL 정보이며 여기서는 proxy.msexchange.com 으로 설정되어 있습니다.



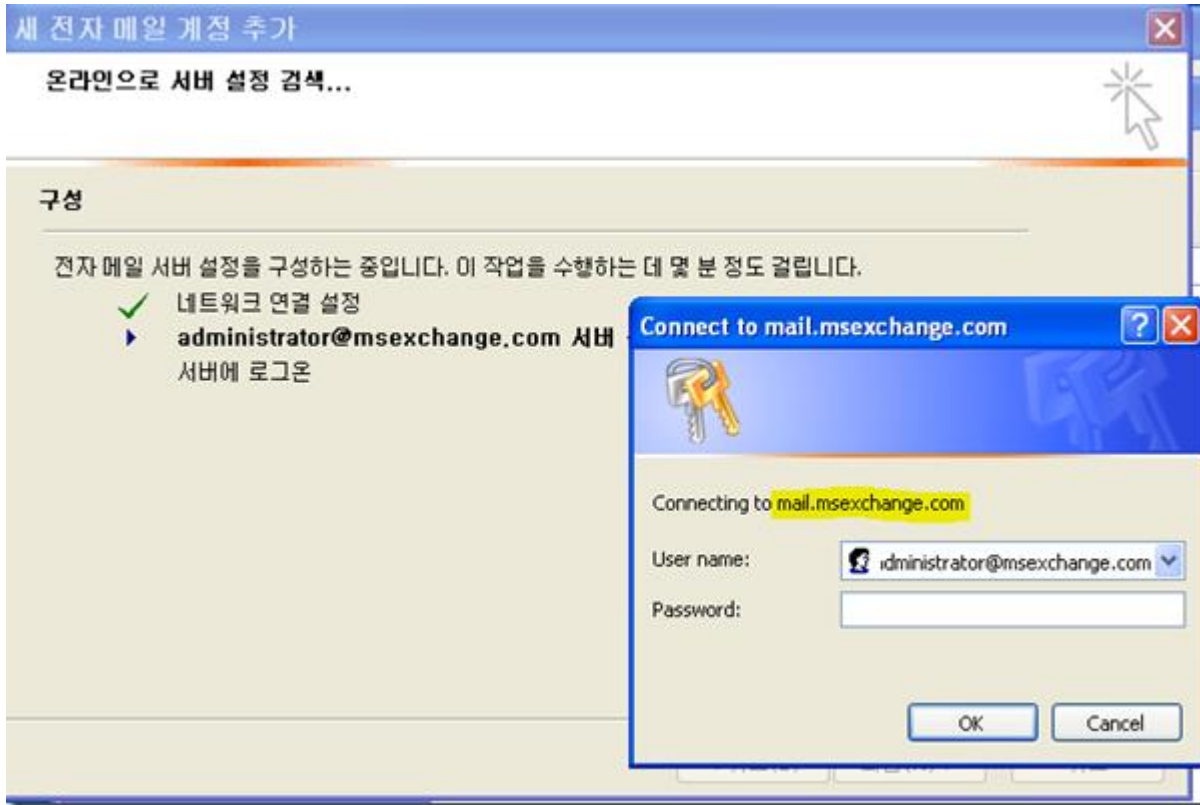
본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
 주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

3. 이제 Outlook Anywhere 를 통하여 자동 프로필을 구성해보면 됩니다.

Autodiscover 서비스에 의해 자동으로 프로필 구성을 시도하며 도중에 CAS 서버를 대상으로 하는 로그인 창이 나타나며 사용자 이름과 패스워드를 입력하도록 요구합니다.

하지만 더 이상 진행되지 않고 계속해서 인증 창만 나타나는 문제를 발생시키게 됩니다.



4. 이번에는 Autodiscover 서비스를 통한 자동 프로필 구성이 아닌 수동(Manually) 으로 Outlook 프로필을 구성해보겠습니다



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

새 전자 메일 계정 추가

Microsoft Exchange 설정
필요한 정보를 입력하여 Microsoft Exchange에 연결할 수 있습니다.

Microsoft Exchange Server의 이름을 입력하십시오. 자세한 내용은 시스템 관리자에게 문의하십시오.

Microsoft Exchange Server(E):

☐ 캐시된 Exchange 모드 사용(C)

관리자가 설정한 사서함의 이름을 입력하십시오. 사서함 이름은 일반적으로 사용자의 이름을 사용합니다.

사용자 이름(U):

Microsoft Exchange

일반 고급 보안 연결 원격 메일

연결

오프라인으로 작업 중 Microsoft Exchange 사용:

☒ LAN으로 연결(L)

☐ 전화선으로 연결(H)

☐ Internet Explorer 또는 타사의 전화 걸기 모뎀

다음 전화 접속 네트워크를 사용하여 연결

외부에서 Outlook 사용

☒ HTTP를 사용하여 Microsoft Exchange 연결

Microsoft Exchange 프록시 설정

HTTP 패킷에서 원격 프로시저 호출(RPC)을 중첩하여 인터넷에서 Microsoft Exchange와 통신할 수 있습니다. 사용하려는 프로토콜과 ID 확인 방법을 선택하십시오. 어떤 옵션을 선택해야 할지 모르는 경우 Exchange 관리자에게 문의하십시오.

연결 설정

Exchange용 프록시 서버 연결에 다음 URL 사용(U):

☒ SSL만 사용하여 연결(S)

☐ 인증서에 이 사용자 이름이 있는 프록시 서버에만 연결(P):

☒ 고속 네트워크에서 먼저 HTTP를 사용하여 연결한 다음, TCP/IP를 사용하여 연결(T)

☒ 저속 네트워크에서 먼저 HTTP를 사용하여 연결한 다음, TCP/IP를 사용하여 연결(W)

프록시 인증 설정

Exchange용 프록시 서버 연결 시 다음 인증 사용(A):

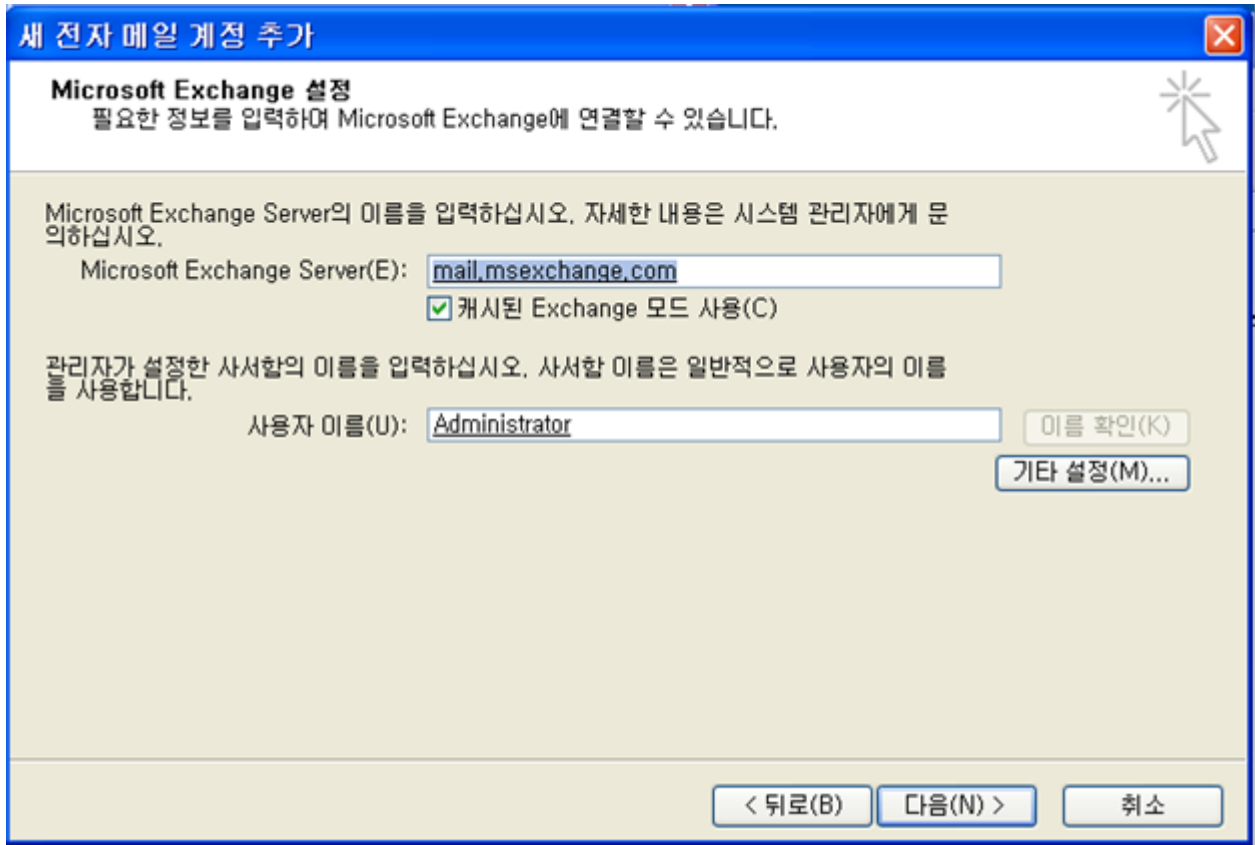
www.uccit.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

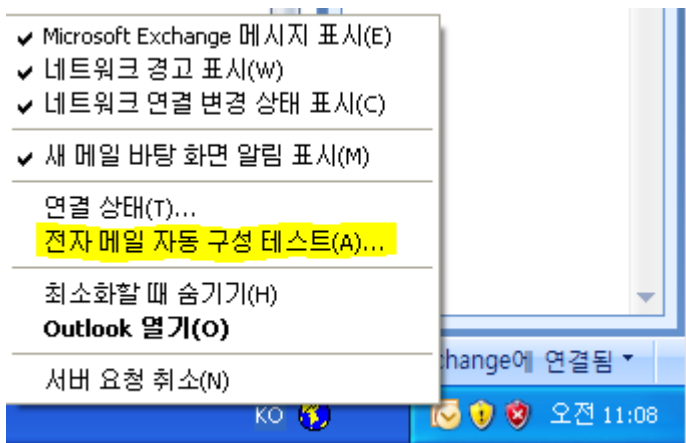
아래처럼 이름확인 과정에 성공하며 이때 정상적으로 Outlook 프로필이 구성되었습니다.



5. 위의 내용을 볼때 왜 Autodiscover 서비스를 통한 자동프로필을 구성시에만 인증이 실패하는 문제가 나타날까요?

하나씩 살펴보도록 하겠습니다

수동으로 프로필 구성된 Outlook Anywhere 연결을 열고 아래처럼 전자 메일 구성 테스트를 시도합니다.(Ctrl + 아이콘 클릭)



이 결과값은 Autodiscover 서비스에 의해 읽어오는 값입니다.

아래처럼 Exchange HTTP 연결을 보시면 Certificate Principal Name 이 msstd:proxy.msexchange.com 입니다.

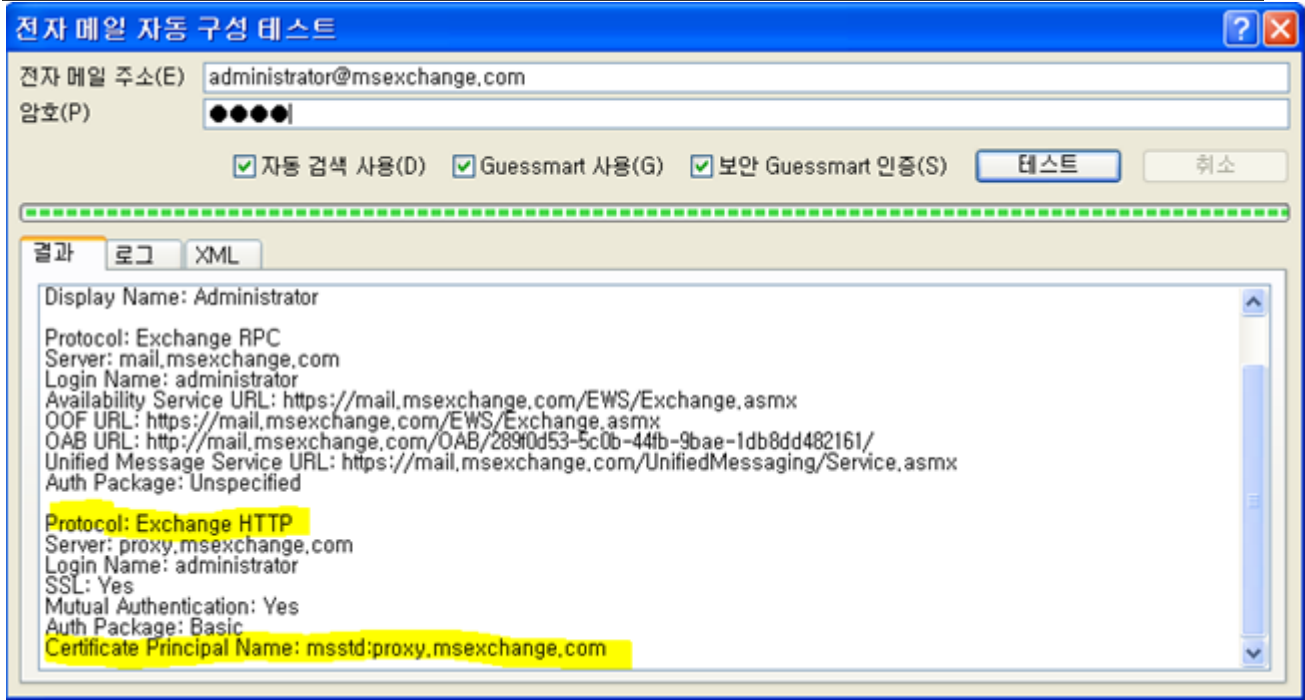
Certificate Principal name 은 우리말로 “인증서 주체 이름” 에 해당됩니다.



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

또한 이 값은 Autodiscover 서비스를 통해서 연결되는 값이며 Outlook 프로파일 구성시 설정되는 값이기도 합니다.



6. 이 글의 상단 부에 보시면 RPC Proxy 가 위치하는 IIS 웹사이트의인증서에 발급 대상에 mail.msexchange.com 으로 되어 있습니다. 즉 실제 인증서의 주체이름은 mail.msexchange.com 입니다.

하지만 클라이언트에서 보시면 클라이언트는 Autodiscover 서비스에 의해 인증서 주체이름을 proxy.msexchange.com 으로 가져왔습니다.

이는 곧 클라이언트에 설정되는 인증서 주체이름의 정보는 실제 서버에 바인딩된 인증서 주체이름과 일치하지 않는거죠...

Exchange 관리셸을 통해서 인증서 요청파일을 생성할때 -DomainName 다음부분에 나타나는 첫번째 이름이 바로 인증서 주체이름이 되는것입니다

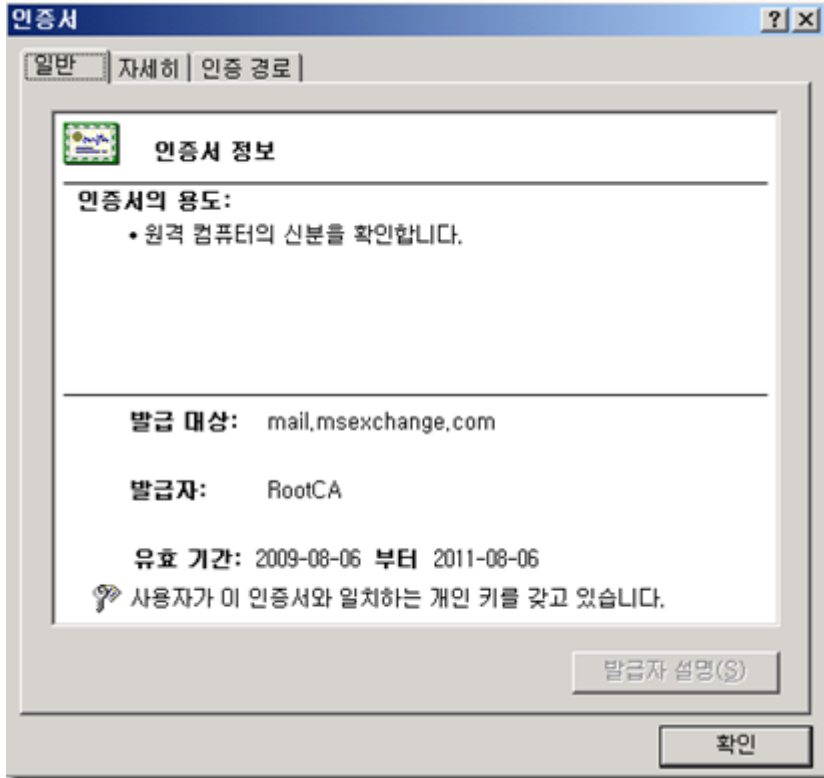
New-ExchangeCertificate -Generalrequest -DomainName



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

mail.msexchange.com,proxy.msexchange.com,autodiscover.msexchange.com,mail -Path C:\WCertreq.txt



7. 그럼 한가지 의문이 있을 수 있을 것입니다. 왜 수동으로 Outlook 프로필을 생성하면 정상적으로 로그인 가능한가 하는 것이겠죠?

수동으로 Outlook 프로필을 생성할때 Exchange 프록시 설정을 보면

아래 노란 부분의 “인증서에 이 사용자 이름이 있는 프록시 서버에만 연결” 옵션을 설정하지 않았습니다.

아래 의미는 Outlook Anywhere 연결시 인증서 주체이름여부는 Check 하지 않겠다는 의미입니다

UCERT
www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

Microsoft Exchange 프록시 설정

HTTP 패킷에서 원격 프로시저 호출(RPC)을 중첩하여 인터넷에서 Microsoft Exchange와 통신할 수 있습니다. 사용하려는 프로토콜과 ID 확인 방법을 선택하십시오. 어떤 옵션을 선택해야 할지 모르는 경우 Exchange 관리자에게 문의하십시오.

연결 설정

Exchange용 프록시 서버 연결에 다음 URL 사용(U):
 https://

☒ SSL만 사용하여 연결(S)
☐ 인증서에 이 사용자 이름이 있는 프록시 서버에만 연결(P):

☒ 고속 네트워크에서 먼저 HTTP를 사용하여 연결한 다음, TCP/IP를 사용하여 연결(T)
☒ 저속 네트워크에서 먼저 HTTP를 사용하여 연결한 다음, TCP/IP를 사용하여 연결(W)

프록시 인증 설정

Exchange용 프록시 서버 연결 시 다음 인증 사용(A):

만약 이 옵션이 설정한다면 이 옵션에 설정된 값은 실제 인증서 주체이름과 반드시 일치해야 함을 의미합니다.

왜냐면 이 옵션을 설정한다는 의미는 다시 말하면, 실제 인증서의 주체이름이 여기 정의된 값과 일치할 때만 연결한다는 의미이기 때문입니다.

(Autodiscover 서비스를 통한 Outlook 자동프로필 구성시 이 값이 기본적으로 Enable 되게 설정됩니다)

수동프로필 구성할 경우에도 아래처럼 “인증서에 이 사용자 이름이 있는 프록시 서버에만 연결” 값을 msstd:mail.msexchange.com, 실제 인증서 주체이름으로 넣어주시면 정상적으로 Outlook 로그인 하실 수 있습니다.

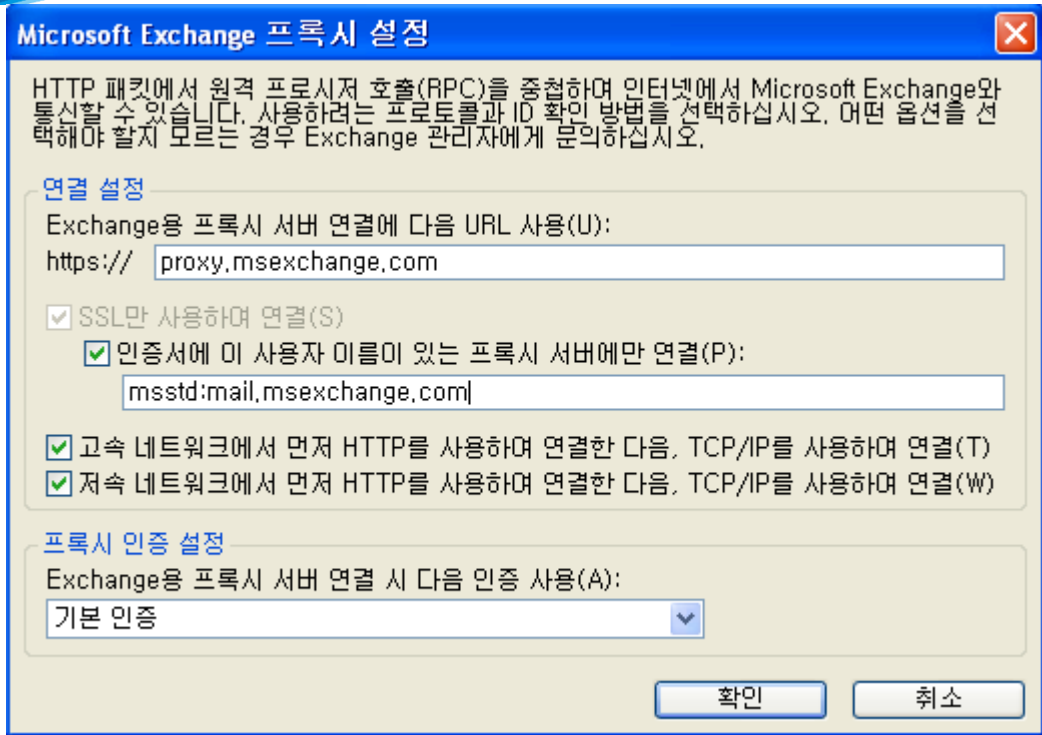
UCERT

www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
 주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.



이제 왜 Outlook 자동프로필 구성시 정상적으로 프로필 구성을 마칠 수 없는지 이해하시겠조?

Outlook 프로필을 자동으로 구성할 경우 인증서 주체이름확인 옵션이 Enable 외며 해당 값은 msstd:proxy.msexchange.com 으로 설정됩니다.

하지만 서버의 인증서의 실제 주체이름은 msstd:mail.msexchange.com 이기 때문에 클라이언트는 잘못된 인증서 주체이름값이 설정되는 것입니다.

기본적으로 Autodiscover 서비스는 Outlook Anywhere 연결주소를 Certificate Principal Name 으로 Outlook 설정합니다

8. 그렇다면 해결방법은?

두 가지 방법이 있습니다

A. 인증서를 생성시 Exchange 프록시(Outlook Anywhere 연결주소) 사용하는 URL 을 인증서의 주체이름으로 하는 인증서를 새로 발급받으시면 됩니다.

아래 명령어처럼 -DomainName 의 첫번째 이름을 Outlook Anywhere 연결주소로 정의할 경우 인증서의 주체이름은 proxy.msexchange.com 으로 정의되어 Autodiscover 서비스에서도 msstd:proxy.msexchange.com 으로 Certificate Principal Name 으로 설정합니다.

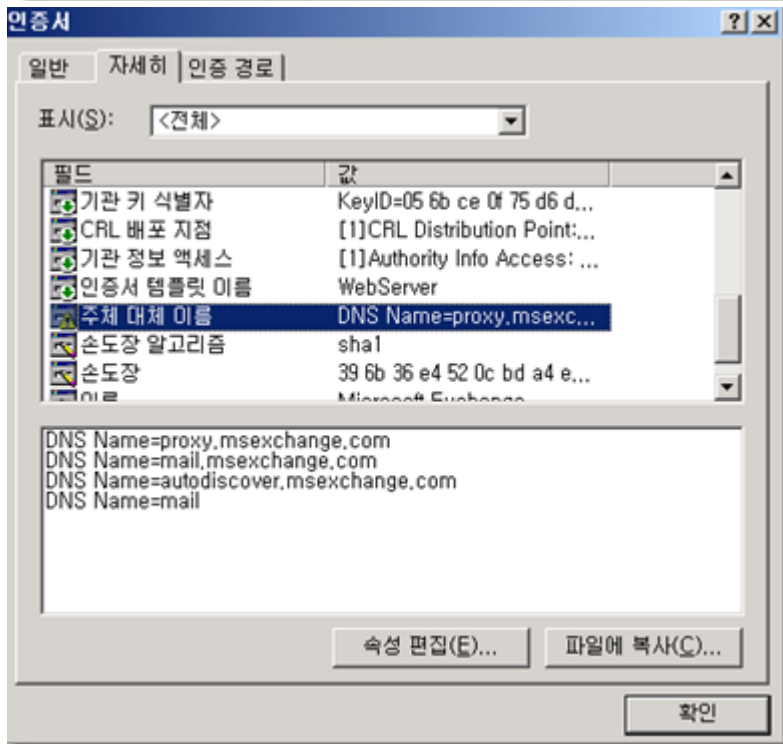
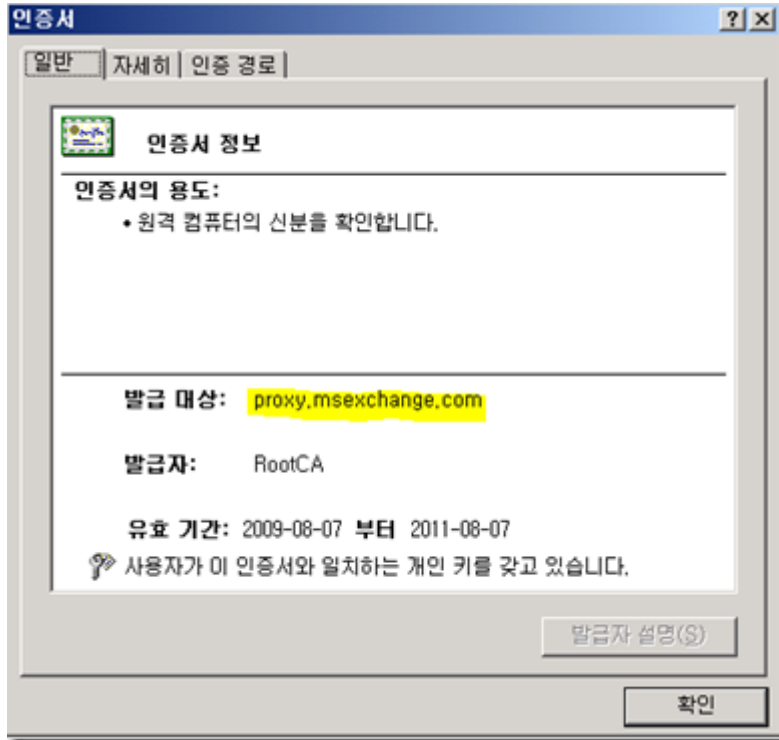
New-ExchangeCertificate -GenerateRequest -DomainName
proxy.msexchange.com,mail.msexchange.com,autodiscover.msexchange.com,mail -Path c:\WCertreq.txt



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

이렇게 하여 발급된 인증서는 아래와 같으며 주체이름이 곧 Outlook Anywhere 연결주소와 동일하게 됩니다. 이때 Outlook 자동프로필에 설정되는 인증서 주체이름값 또한 msstd:proxy.msexchange.com 으로 되겠지요 (왜냐하면 기본적으로 Outlook Anywhere 외부연결주소로 msstd 가 정의되니까요)



위의 작업후에 Autodiscover 를 통해서 자동프로필 구성시 오류가 없을것입니다.

B. Exchange Management Shell 을 통해서 Certificate Princinal Name 을 변경하면 Autodiscover 서비스에 의해서 리턴되는 Cert Principal Name 을 변경하실 수 있습니다.

아래에서 확인하시면 기본적으로 EXPR 공급자(HTTPS)에 정의된 CertPrincipalName 은 NULL 이며 이 설정의 경우 Outlook Anywhere 의 외부연결주소의 URL 을 인증서 주체이름으로 설정합니다.

```
[PS] C:\>Get-OutlookProvider EXPR | ft certprincipalname
```

```
CertPrincipalName
-----
```

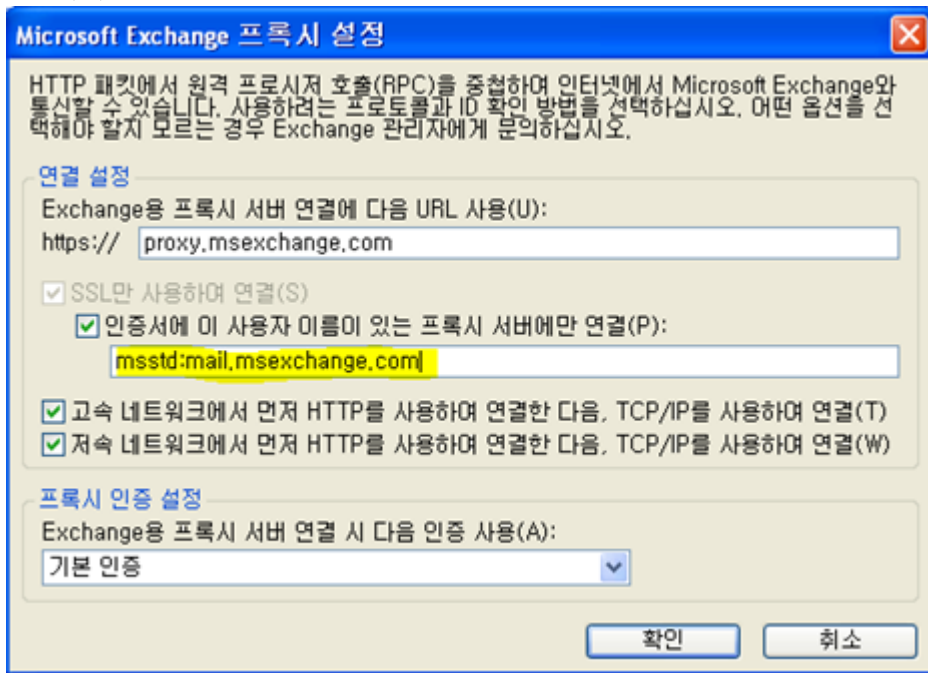
다음처럼 Set 명령어를 통해 CertPrincipalName 을 다른 값으로 지정합니다. 아래처럼 설정할 경우

Autodiscover 서비스에 의해서 반환되는 CertPrincipalName 은 msstd:mail.msexchange.com 입니다. 이는 전자메일구성 테스트를 통하여 확인하실 수 있습니다.

```
[PS] C:\>Set-OutlookProvider EXPR -CertPrincipalName msstd:mail.msexchange.com
[PS] C:\>
```

이렇게 설정한 후에 Outlook 자동프로필 구성을 마치면 Exchange 프록시 구성을 확인하시면 msstd:mail.msexchange.com 으로 입력되며 mail.msexchange.com 은 곧 CAS 서버의 인증서 주체이름이므로 정상적으로 Outlook 을 연결하실 수 있습니다.

이 방♦♦을 사용하시면 서버의 인증서를 새로 발급하지 않으셔도 되는 것이지요.



written by dyjung

www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.