ArcGIS Enterprise 공인 SSL 인증서 적용 및 교체 방법

제품 : ArcGIS Enterprise 10.8.x (Windows)

제작일 : 2021 년 06 월 07 일

제작 : 한국에스리 기술지원센터

esri Korea
THE SCIENCE OF WHERE™

개요

본 문서는 ArcGIS Enterprise (ArcGIS Server, Portal for ArcGIS, ArcGIS Data Store)에 사용되는 SSL 인증서 적용 및 교체 방법에 관한 한국에스리 기술문서입니다.

이 문서와 관련된 내용에 대한 문의/건의 등을 원하신다면, 다음의 연락망을 통하여 한국에스리 기술지원센터로 연락 주시기 바랍니다.

- 한국에스리 기술지원센터 (유지관리 고객 대상)
  - 고객지원 홈페이지 : http://www.esrikr.com/self-service/
  - 이메일 : help@esrikr.com
  - 전화 : 080-850-0915 | 운영시간: 평일 오전 9 시 ~ 오후 6 시
- 24 시간 기술지원 리소스 :
  - 한국에스리 기술자료 : http://esrikr.com/article-categories/technical/
  - Esri 기술지원 페이지(영문) : http://support.esri.com
- ArcGIS Pro 도움말 : http://pro.arcgis.com/en/pro-app/help/
- ArcMap 도움말 : http://desktop.arcgis.com/en/arcmap/

목차

웹 서버에서 HTTPS 프로토콜 사용을 위한 SSL 인증서 활성화

HTTPS 프로토콜은 웹 클라이언트 간에 암호화 된 링크를 설정하는데 사용되는 표준 보안 기술로 서버를 식별하고 인증할 뿐만 아니라 전송되는 모든 데이터의 개인 정보 보호 및 무결성을 보장하여 보안 네트워크 통신을 지원합니다.

해당 프로토콜을 사용하여 ArcGIS Web Adaptor 와 Portal for ArcGIS 또는 ArcGIS Server 간의 통신을 암호화 할 수 있습니다. HTTPS 연결을 생성하려면 웹 서버에 서버 인증서가 필요합니다.

인증서는 웹사이트 소유자가 생성해야 하며 디지털로 서명되어야 합니다. 인증서에는 아래 설명된 CA 서명, 도메인 및 자체 서명의 세 가지 유형이 있습니다.

1. CA 서명 인증서

인증 기관 (CA) 서명 인증서는 프로덕션 시스템에 사용해야 하며, 특히 외부 사용자가 ArcGIS Enterprise 포털 배포에 접근할 경우에 사용됩니다. 예를 들어, 포털이 인터넷을 통해 접근할 수 있는 경우 CA 서명 인증서를 사용하면 기관 외부의 클라이언트에 대해 웹사이트 ID 가 확인됩니다.

CA 는 일반적으로 웹사이트의 신뢰성을 보증할 수 있는 제 3 기관으로 웹사이트의 자체 서명된 인증서에 고유한 디지털 서명을 추가하여 웹 사이트의 ID 가 확인되었음을 웹 클라이언트에 보증합니다.

이렇게 보증된 웹 사이트는 웹 브라우저에서 예기치 않은 동작 또는 경고 메시지가 나타나지 않도록 합니다.

2. 도메인 인증서

포털 또는 서버가 방화벽 뒤에 있고, CA 서명 인증서를 사용할 수 없는 경우 도메인 인증서를 사용합니다. 도메인 인증서는 기관의 인증 기관이 서명한 내부 인증서로,

도메인 내의 사용자에게 자체 서명 인증서와 관련된 예기치 않은 동작 또는 경고 메시지가 나타나지 않도록 할 수 있습니다.

그러나, 도메인 인증서는 외부 CA 에서 검증할 수 없으므로 도메인 외부의 사용자는 신뢰할 수 없는 사이트에 대한 브라우저 경고가 표시됩니다.

1) 도메인 인증서 생성 및 HTTPS 활성화

ArcGIS Enterprise 구성 마법사를 완료하려면 기본 배포가 설치되는 머신의 IIS 에 HTTPS 가 활성화되어 있어야 합니다.

HTTPS 가 활성화되어 있지 않으면 구성 마법사를 완료할 수 없으며 다음 오류 메시지가 보고됩니다.

Web Adaptor URL https://mymachine.mydomain.com/server 에 접근할 수 없습니다. 웹 서버에 HTTPS 가 활성화되어 있는지 확인하세요.

2017 년에 Chrome 은 주체 대체 이름 (SAN) 매개변수가 포함된 인증서만 신뢰하도록 하였으며, 이 매개변수는 IIS 관리자 응용프로그램에서 인증서를 생성할 경우에는 구성할 수 없습니다.

IIS 를 사용하는 경우 도메인 인증서를 생성하려면 도메인 인증서 생성을 참고하세요. 이 항목에는 머신에서 적절한 인증서를 생성하여 HTTPS 포트 443 에 바인딩하는 스크립트가 포함되어 있습니다.

3. 자체 서명 인증서

웹사이트 소유자만 서명한 인증서를 자체 서명 인증서라고 합니다. 자체 서명된 인증서는 주로 기관의 내부(LAN) 네트워크 사용자만 사용할 수 있는 웹사이트에서 사용됩니다.

포털을 처음 설정하는 경우 자체 서명 인증서를 사용하여 일부 초기 설정을 수행하면 구성에 성공했는지 빠르게 확인할 수 있습니다.

그러나 자체 서명 인증서를 사용할 경우 다음과 같은 상황이 발생할 수 있습니다.

1) 자체 서명 인증서 사용시 주의 사항

① 웹 브라우저 및 ArcGIS Desktop 에 신뢰할 수 없는 사이트에 대한 경고가 나타납니다. 웹 브라우저에서 자체 서명된 인증서가 발견된 경우 일반적으로 경고가 나타나며 사이트로 이동할지 확인하는 메시지가 나타납니다. 자체 서명된 인증서를 사용하는 한 많은 브라우저에서 경고 아이콘이 나타나거나 주소 표시줄에 빨간색이 나타납니다. 자체 서명된 인증서로 포털을 구성한 경우 이러한 유형의 경고가 표시되는 것을 예상해야 합니다.

② Map Viewer 에서 페더레이션된 서비스를 열거나, 포털에 보안 서비스 항목을 추가하거나, 페더레이션된 서버에서 ArcGIS Server Manager 에 로그인하거나, ArcGIS Maps for Office 에서 포털에 연결할 수 없습니다.

③ 클라이언트 응용프로그램에서 호스팅 서비스를 인쇄하고 포털에 접근할 때 예기치 않은 동작이 발생합니다.

④ ArcGIS Maps for Office 를 실행하는 머신의 **신뢰할 수 있는 루트 인증 기관** 인증서 저장소에 자체 서명된 인증서가 설치되지 않은 경우 ArcGIS Maps for Office 에서 포털에 로그인할 수 없습니다.

주의: 자체 서명된 인증서를 발생하는 문제는 위 목록에 국한되지 않으며 도메인 인증서 또는 CA 서명 인증서를 사용하여 포털을 완전히 테스트하고 배포하는 것이 좋습니다.

2) 웹 사이트에 인증서 바인딩

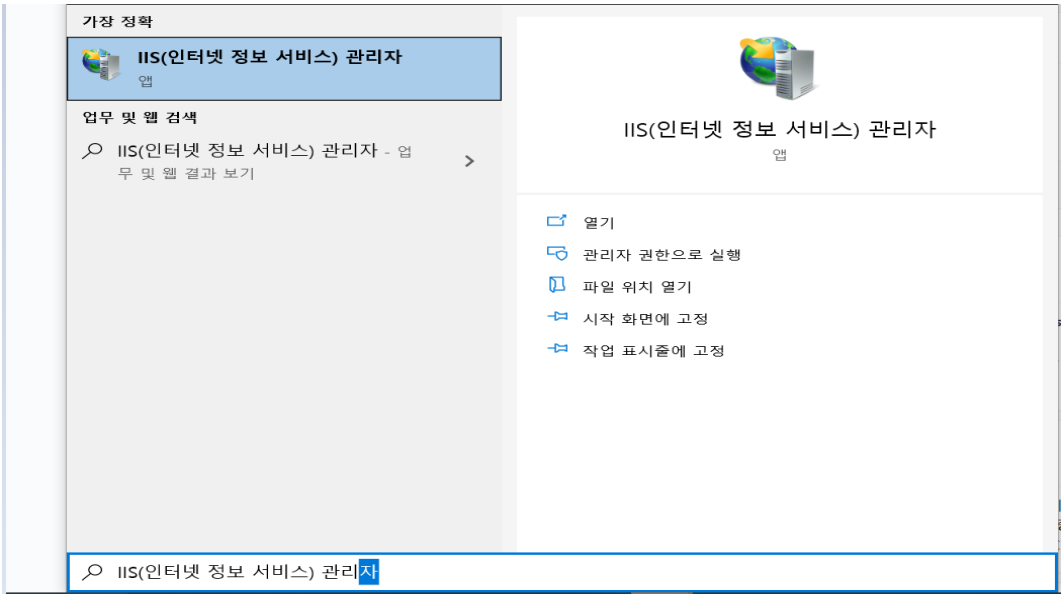
자체 서명된 인증서를 생성한 경우 ArcGIS Web Adaptor 를 호스팅하는 웹사이트에 바인딩해야 합니다. 바인딩은 웹사이트에서 포트 443 을 사용하도록 인증서를 구성하는 프로세스를 의미합니다.

인증서를 웹 사이트와 바인딩하는 방법은 웹 서버의 버전 및 플랫폼에 달라질 수 있으며 자세한 내용은 시스템 관리자에게 문의하거나 웹 서버 설명서를 참고하여 주시기 바랍니다.

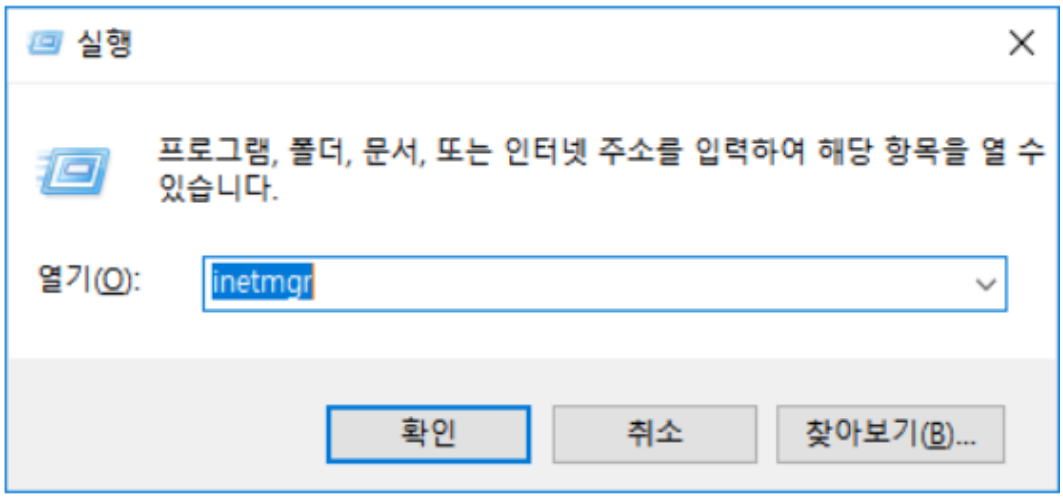
IIS 에서 인증서를 바인딩하는 단계는 아래와 같습니다.

① IIS (인터넷 정보 서비스) 관리자 실행

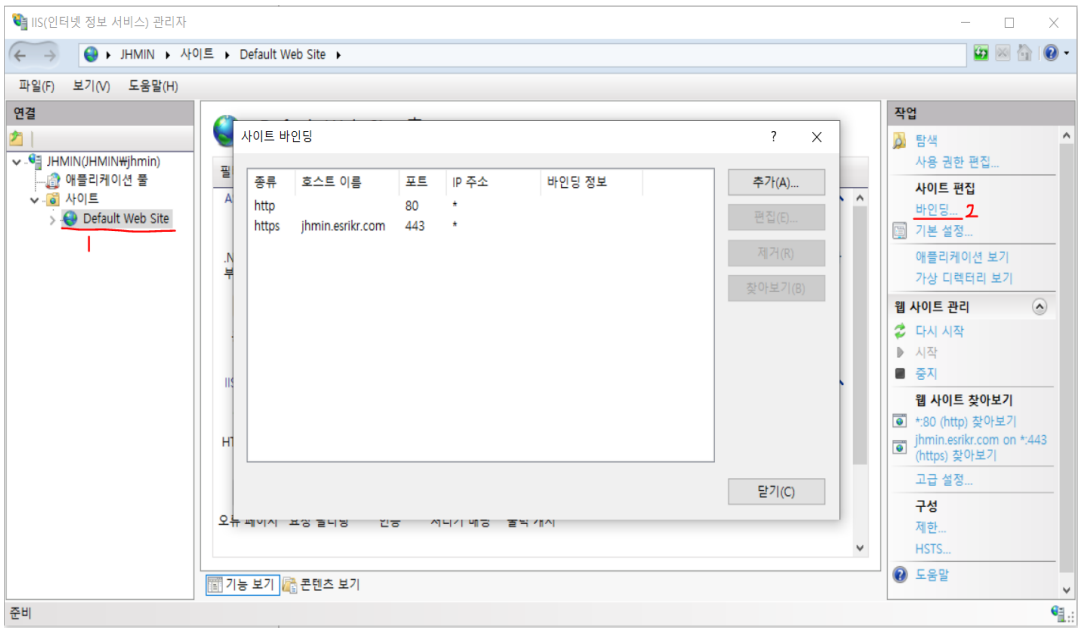
Windows 검색창에 IIS 또는 인터넷 정보 서비스 검색 후 실행



Windows 키 + R > inetmgr 입력 후 실행

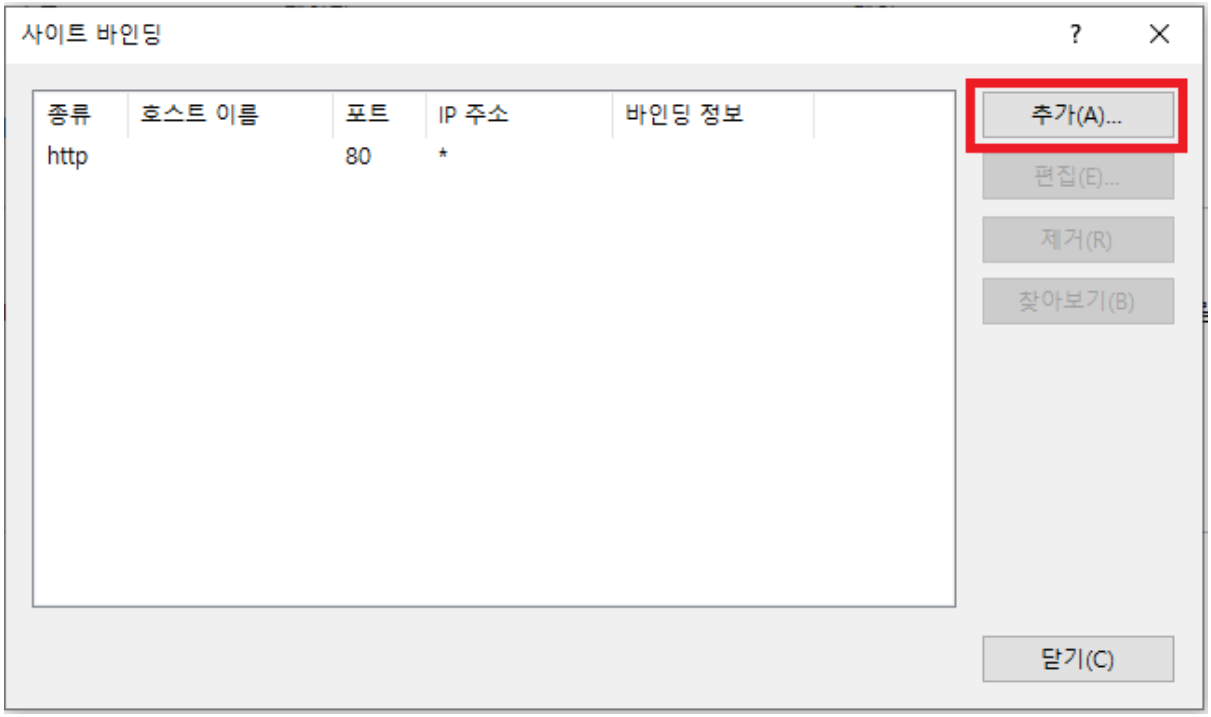


② IIS 관리자 창에서 Default Web site 를 클릭 후 오른쪽 작업창의 바인딩을 클릭

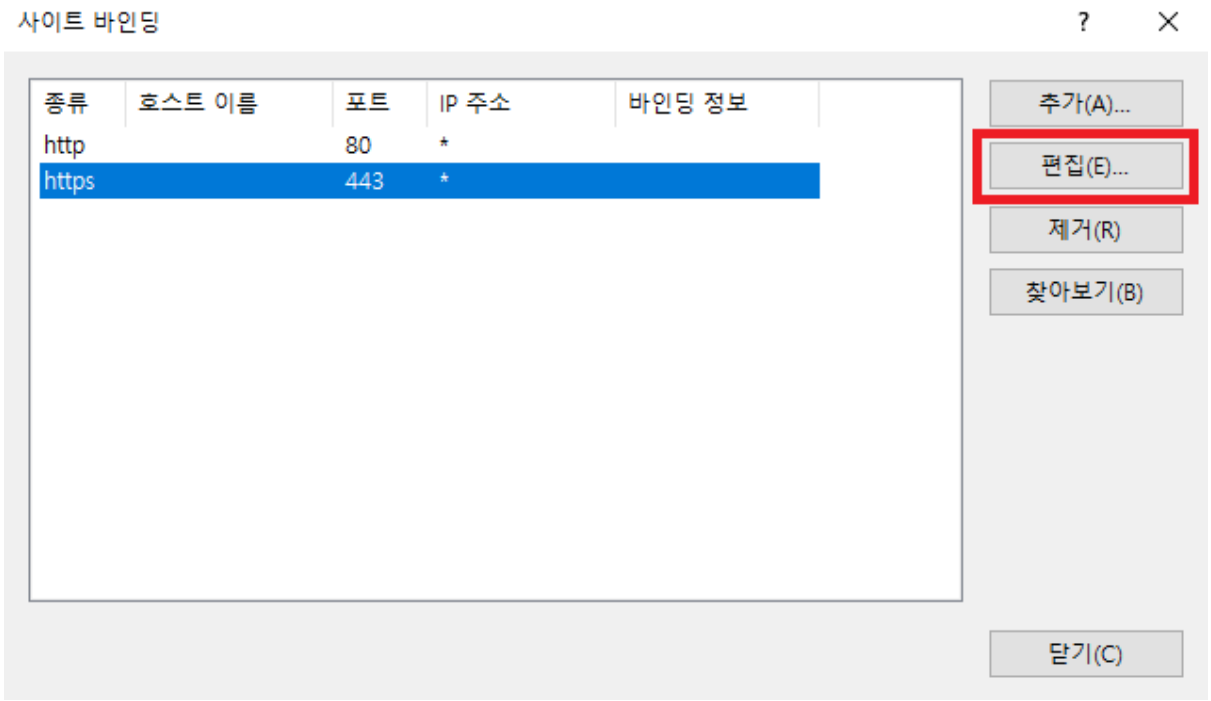


③ 사이트 바인딩 창에서 포트 443 의 목록 생성 및 편집

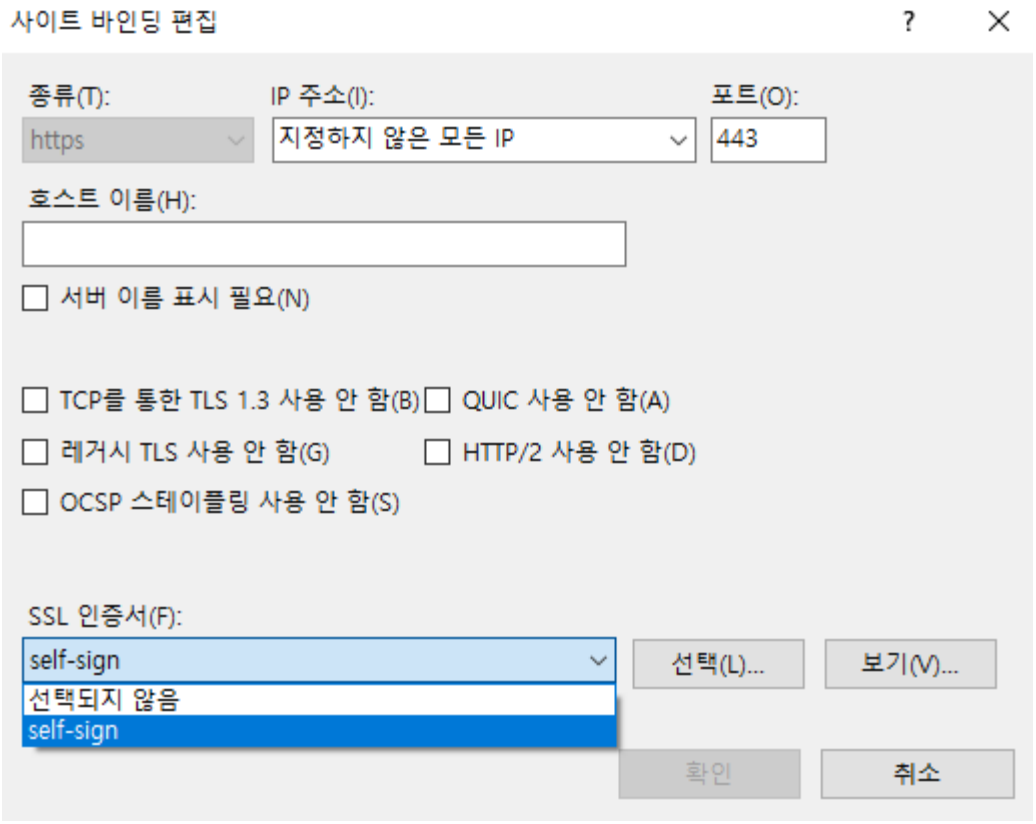
바인딩 목록에서 포트 443 항목이 없다면 **추가**를 클릭하여 항목을 생성하고. 유형 드롭다운 목록에서 https 를 선택합니다.

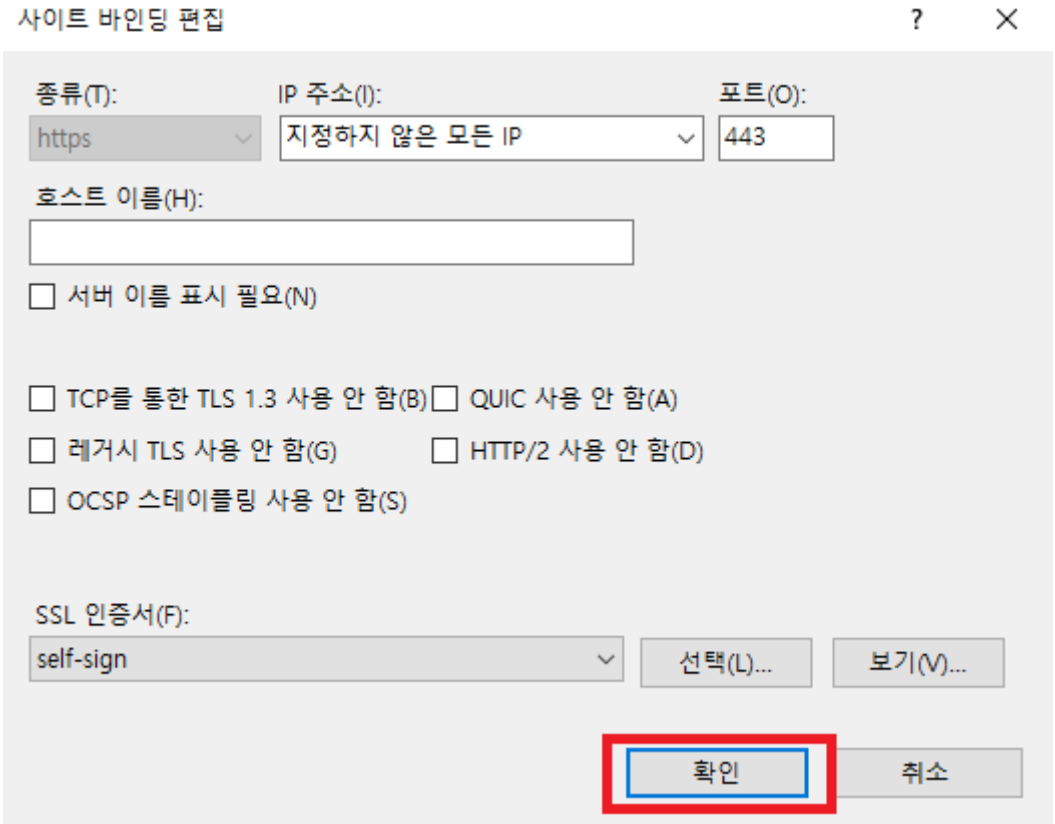


바인딩 목록에서 포트 443 항목을 찾은 경우, **편집**을 클릭합니다.



SSL 인증서 항목을 자체 서명 인증서로 변경한 후, **확인**을 클릭합니다.


사이트 바인딩 편집
종류(T):
https
IP 주소(I):
지정하지 않은 모든 IP
포트(O):
443
호스트 이름(H):
서버 이름 표시 필요(N)
TCP를 통한 TLS 1.3 사용 안 함(B)
QUIC 사용 안 함(A)
레거시 TLS 사용 안 함(G)
HTTP/2 사용 안 함(D)
OCSP 스테이플링 사용 안 함(S)
SSL 인증서(F):
self-sign
선택되지 않음
self-sign
선택(L)...
보기(V)...
확인
취소


사이트 바인딩 편집
종류(T):
https
IP 주소(I):
지정하지 않은 모든 IP
포트(O):
443
호스트 이름(H):
서버 이름 표시 필요(N)
TCP를 통한 TLS 1.3 사용 안 함(B)
QUIC 사용 안 함(A)
레거시 TLS 사용 안 함(G)
HTTP/2 사용 안 함(D)
OCSP 스테이플링 사용 안 함(S)
SSL 인증서(F):
self-sign
선택(L)...
보기(V)...
확인
취소

ArcGIS Server SSL 인증서 적용

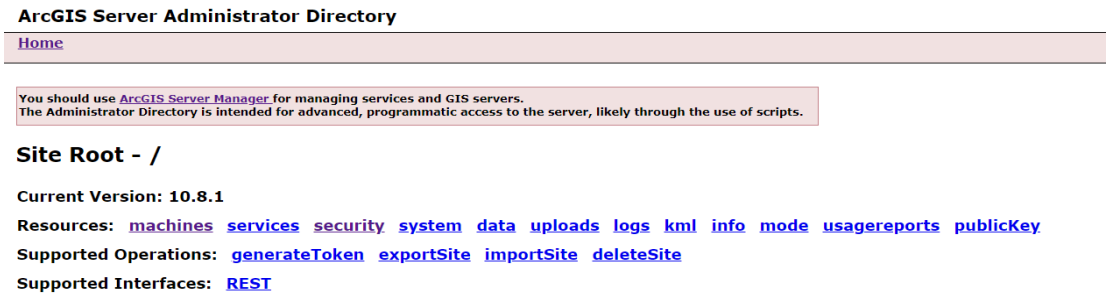
상업용 또는 내부 CA (인증 기관)에서 발급한 인증서가 이미 있는 경우, ArcGIS Server 에서 이 인증서를 이용하여 웹 사이트에 적용할 수 있습니다.

인증서를 ArcGIS Server 로 가져오려면 인증서와 관련 개인 키가 .p12 또는 .pfx 확장자를 가진 파일로 표시되는 PKCS #12 형식으로 저장되어 있어야 합니다.

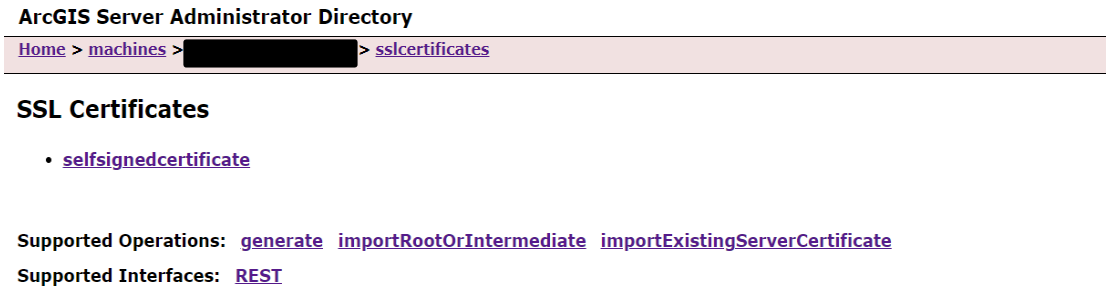
1. ArcGIS Server 로 인증서 가져오기

1) ArcGIS Server Administrator Directory 로 로그인

예. https://gisserver.domain.com:6443/arcgis/admin

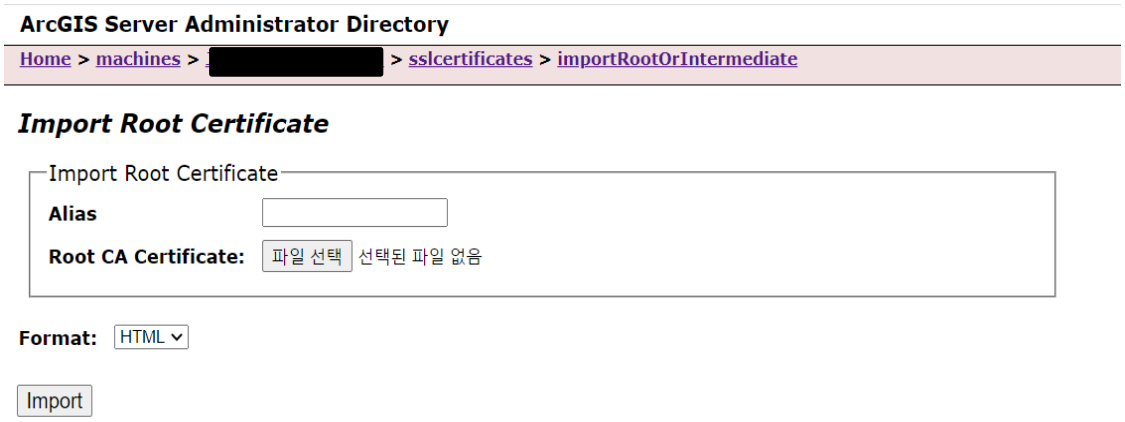


2) Machine > [Machine 이름] > sslcertificates 로 이동



3) importRootOrIntermediate 를 클릭

ArcGIS Server 에 적용하기 위해 가져오는 인증서는 CA 에서 발급한 것이므로 먼저 CA 의 루트 또는 중간 인증서를 가져와야 합니다.



4) importExistingServerCertificate 를 클릭

인증서 암호 (Certificate password) 필드에 인증서의 암호를 입력합니다.

별칭 (Alias) 필드에 인증서를 쉽게 식별할 수 있도록 고유 이름을 지정합니다.

인증서 파일 (Certificate File) 필드에서 파일 선택을 클릭하여 .p12 또는 .pfx 파일을 선택합니다.

5) Submit 클릭

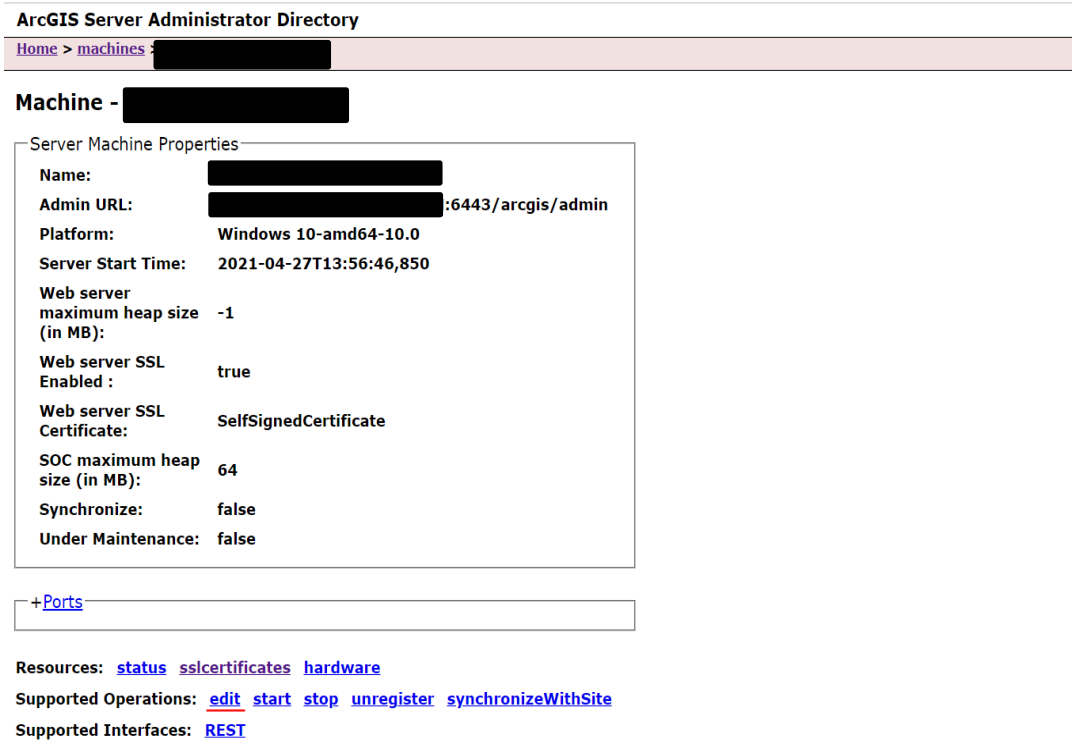
Submit 버튼을 클릭하여 가져오기 한 인증서를 ArcGIS Server 에 저장합니다.

2. 인증서를 사용하도록 ArcGIS Server 구성하기

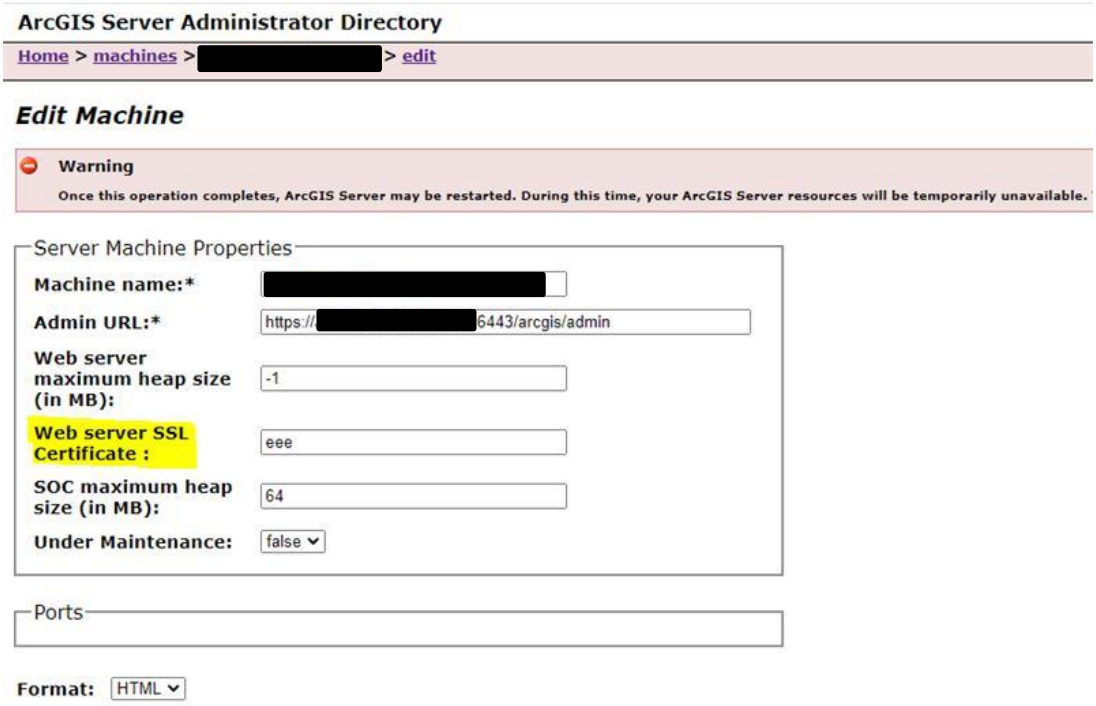
1) ArcGIS Server Administrator Directory 로 로그인

예. https://gisserver.domain.com:6443/arcgis/admin

2) Machine > [Machine 이름] > edit 을 클릭



3) 웹 서버 SSL 인증서 필드에 사용할 인증서 이름을 입력



4) Save Edits 클릭

Save Edits 클릭 후 1~10 분 정도의 시간이 소요될 수 있으며, 이 시간 동안 ArcGIS Server 사이트가 자동으로 다시 시작됩니다.

☞ ArcGIS Server 에서 작업하신 내용이 있다면 인증서 교체 전 저장하여 주시기 바랍니다.

5) SSL 인증서 적용 여부 확인

재시작 된 ArcGIS Server Administrator Directory 에 접근하여 정상적으로 내용이 보여지는지 확인합니다. 만약, 내용 확인이 되지 않는다면 인증서를 변경하여 주시기 바랍니다.

3. GIS Server 로컬 장비에서 배포 구성하기

멀티 머신으로 구성된 ArcGIS Server 의 경우, 위의 1 번 “ArcGIS Server 로 인증서 가져오기”를 각각의 서버 머신에 반복하여 진행해 주셔야 합니다. 모든 인증서를 가져온 후에는 ArcGIS Server 가 설치된 머신을 재시작하여 주시기 바랍니다.

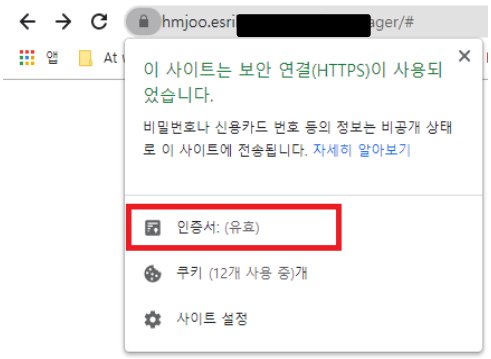
CA 인증기관의 루트 인증서를 운영 체제의 인증서 저장소로 가져오는 방법은 아래와 같습니다.

1) ArcGIS Server 에 로그인

2) ArcGIS Server 에서 사용되는 인증서 로컬로 복사하기

브라우저의 자물쇠 아이콘 클릭 > 인증서 클릭

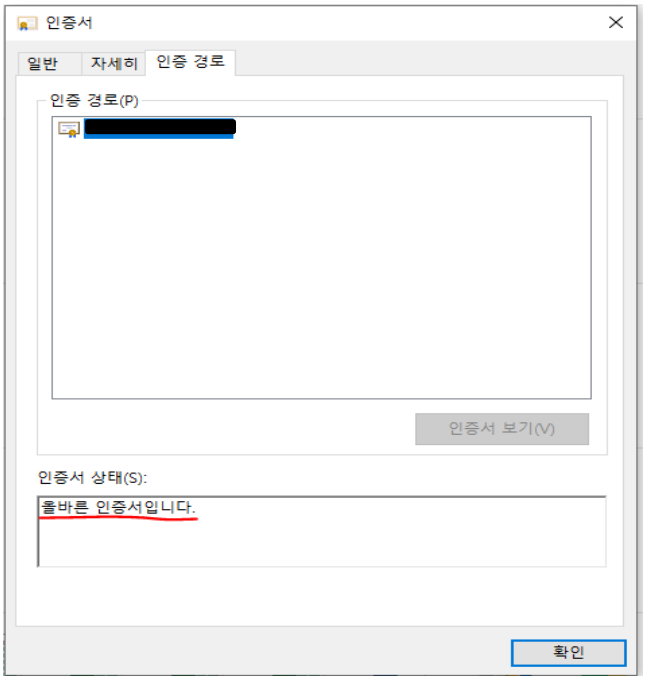
Microsoft Edge



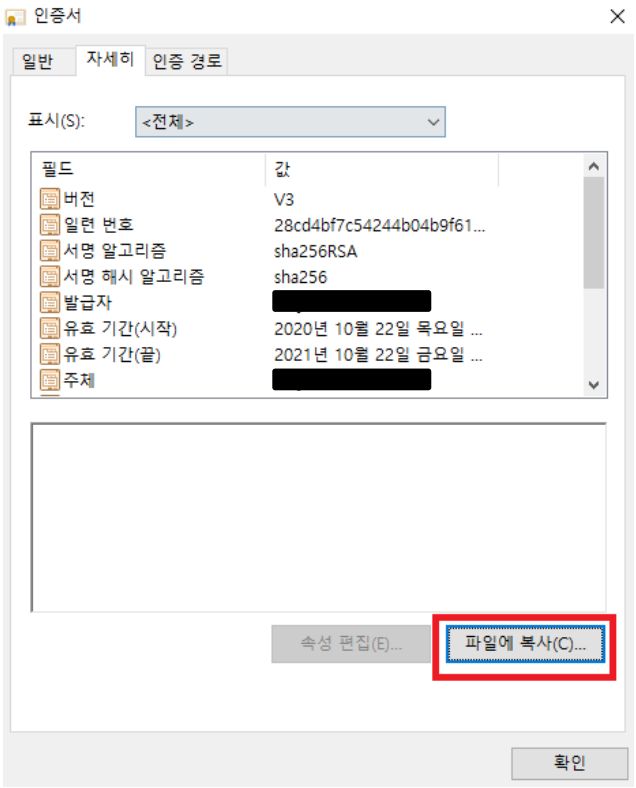
Chrome

3) 인증서 창의 인증 경로 > 인증서 상태 확인하기

인증서 상태가 “올바른 인증서입니다”라고 나왔다면 하위의 11 번으로 이동

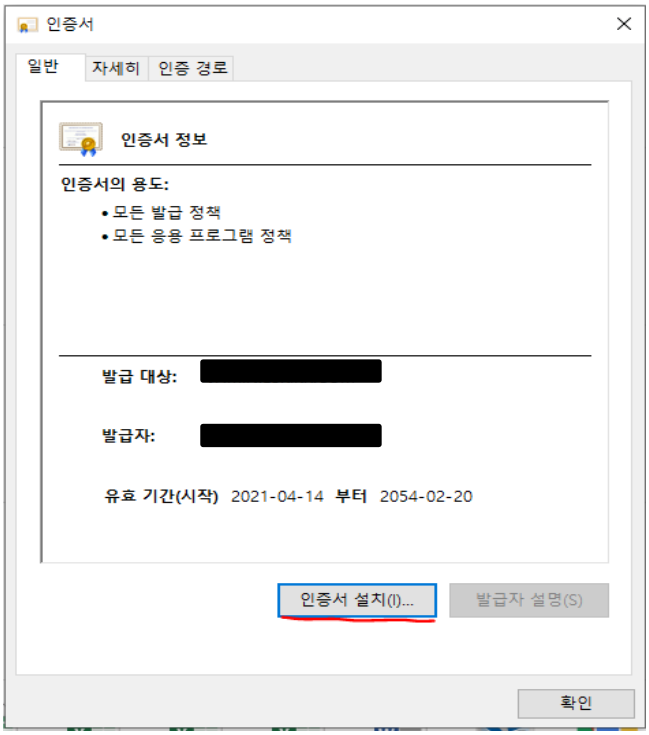


4) 인증서 창의 자세히 > 파일에 복사 클릭하기



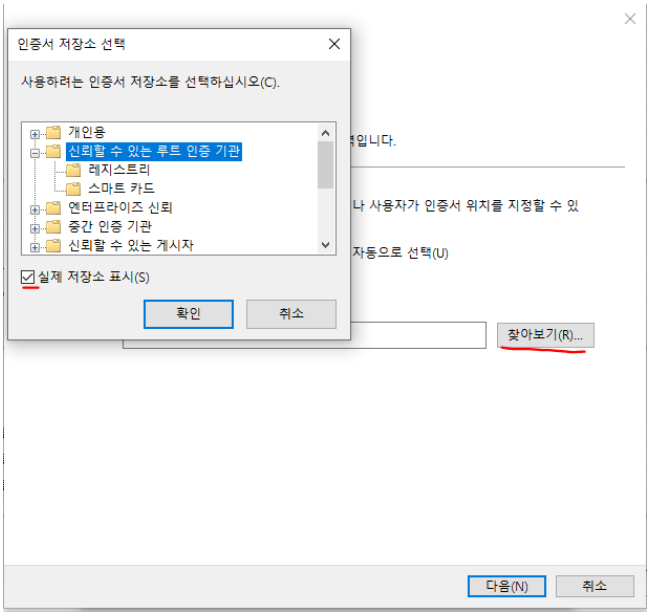
5) 인증서 내보내기 마법사를 통해 로컬 경로에 CA 루트 인증서 파일 저장하기

6) 인증서를 더블 클릭하여 인증서 설치 버튼 클릭하기



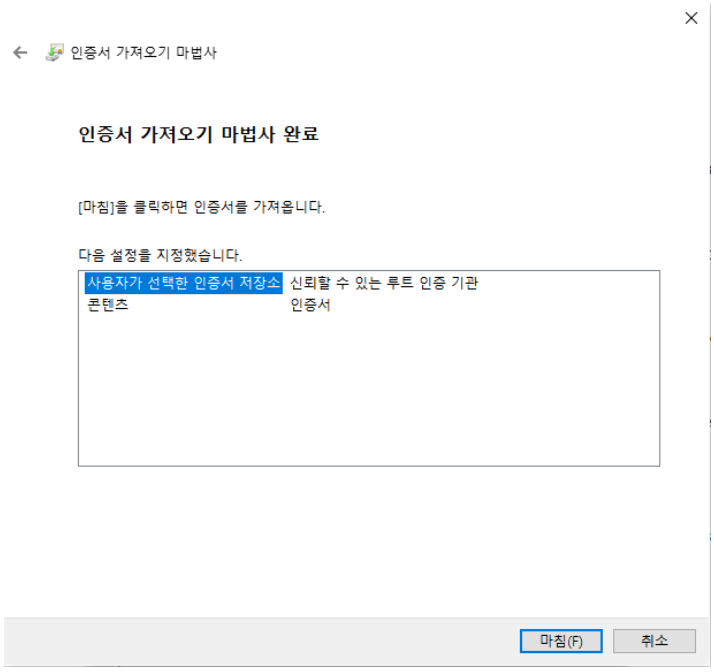
7) 인증서 가져오기 마법사 화면에서 다음을 클릭

8) 인증서 저장소에서 모든 인증서를 다음 저장소에 저장을 클릭한 후, 찾아보기 버튼을 클릭 > 실제 저장소 표시 체크박스 체크



9) 신뢰할 수 있는 루트 인증 기관을 선택한 후 확인 클릭

10) 마침 클릭



11) GIS 서버에 대해 전 단계들을 반복합니다.

Portal for ArcGIS CA 서명 인증서 적용

Portal for ArcGIS 는 암호화해야 하는 정보를 전송하는 경우가 많습니다. 따라서 포털에서는 항상 HTTPS 가 활성화됩니다. 기업(내부) 또는 상용 CA(인증 기관)가 서명한 인증서를 사용하는 것이 좋습니다.

포털 초기 설치 시, 기본적으로 자체 서명된 인증서가 제공 및 적용됩니다. 자체 서명된 인증서를 사용하는 경우 클라이언트는 서버의 ID 를 확인할 수 없어 CA 서명 인증서로 대체하면 배포 보안이 크게 향상됩니다.

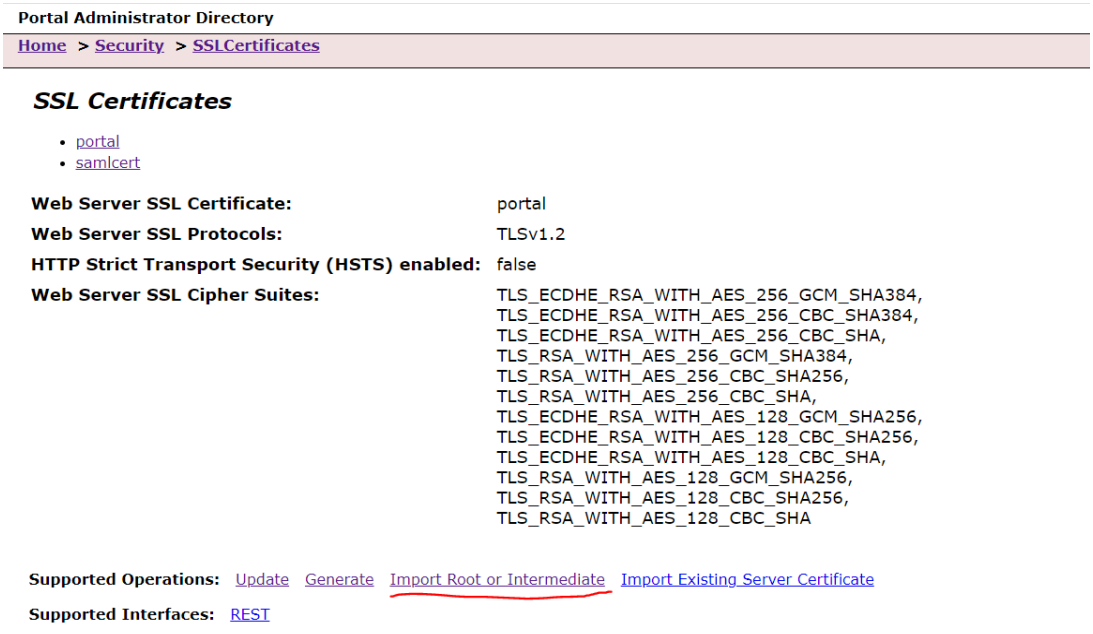
1. 루트 CA 인증서 가져오기

1) ArcGIS Portal Directory 에 내 기관의 관리자로 로그인합니다.

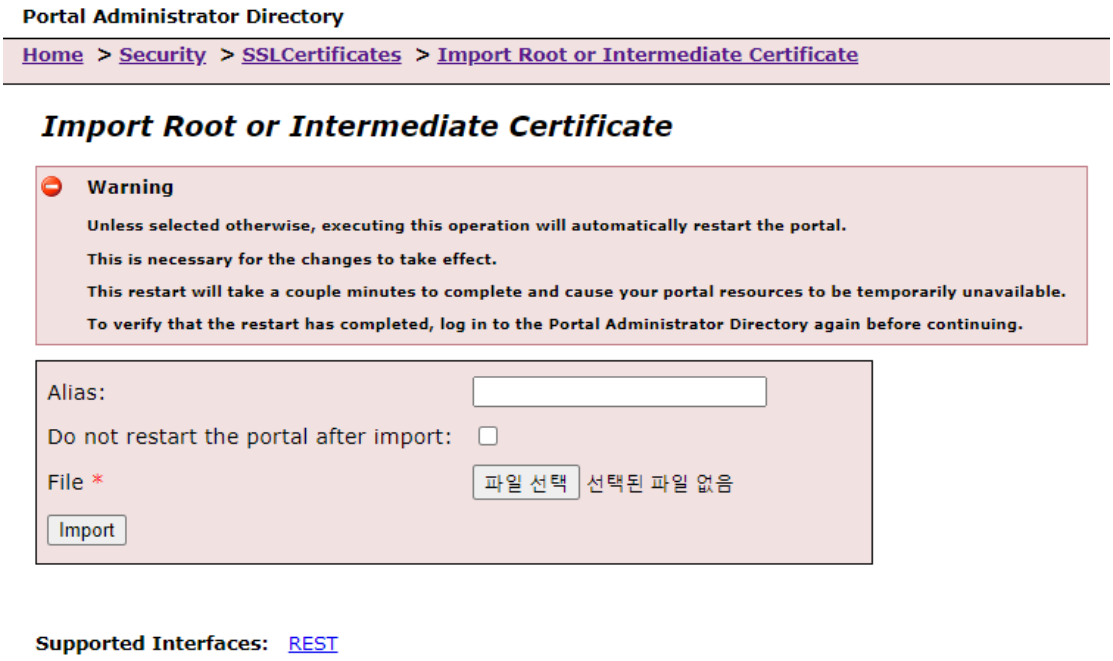
   예. https://webadaptorhost.domain.com/webadaptorname/portaladmin

2) Security > SSLCertificates > Import Root or Intermediate 클릭

   고가용성 포털의 경우, 각 포털 머신에 대해 아래의 단계를 반복합니다.



3) 파일 선택을 클릭하여 CA 가 제공한 루트 인증서 불러오기



CA 가 추가 중간 인증서를 발급한 경우 동일하게 가져오기를 클릭합니다. CA 서명 인증서는 가져오기를 하지 않습니다.

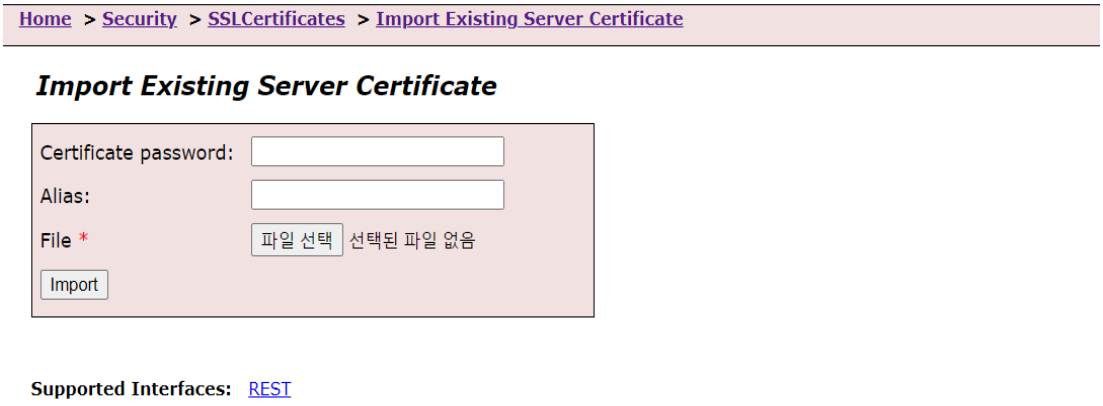
4) Import 클릭하기

Import 클릭 후 1~10 분 정도의 시간이 소요될 수 있으며, 이 시간 동안 Portal for ArcGIS 서비스가 자동으로 다시 시작됩니다.

2. 기존 CA 서명 인증서 가져오기

포털에 CA 서명 인증서를 가져오려면 인증서와 관련 개인 키를 PKCS#12 형식으로 저장해야 하며, 이는 .p12 또는 .pfx 확장자를 가진 파일로 나타납니다.

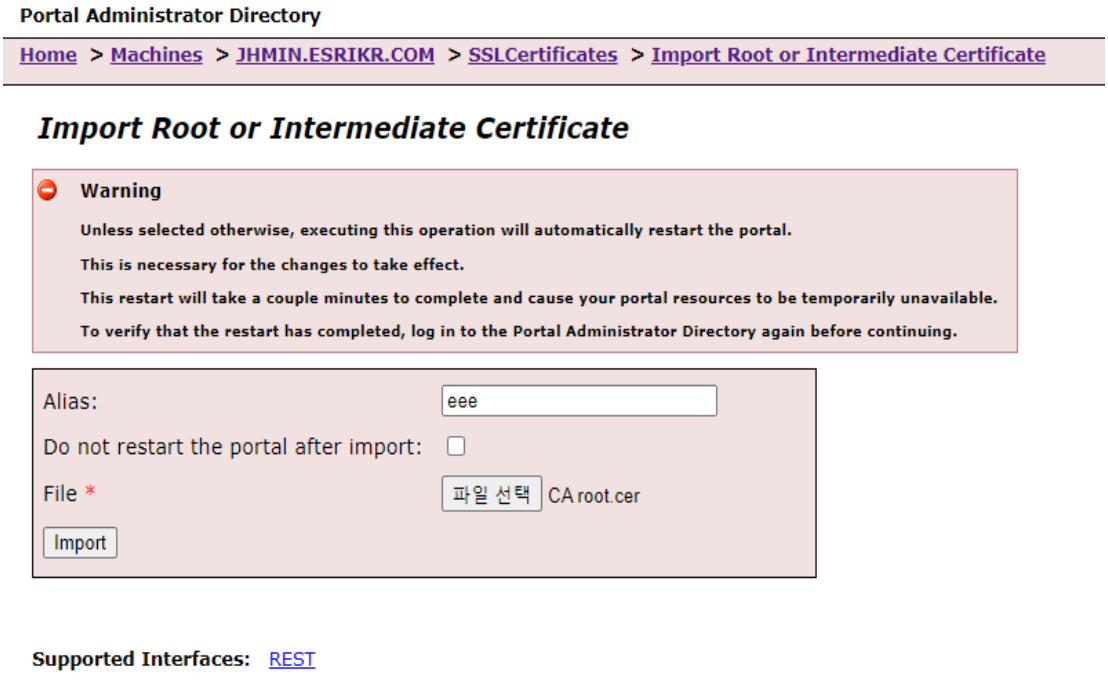
1) Security > SSLCertificates > Import Existing Server Certificates 클릭



인증서 암호 (Certificate password) 필드에 인증서의 암호를 입력합니다.

별칭 (Alias) 필드에 인증서를 쉽게 식별할 수 있도록 고유 이름 (예. rootcert)을 지정합니다.

인증서 파일 (Certificate File) 필드에서 파일 선택을 클릭하여 .p12 또는 .pfx 파일을 선택합니다.

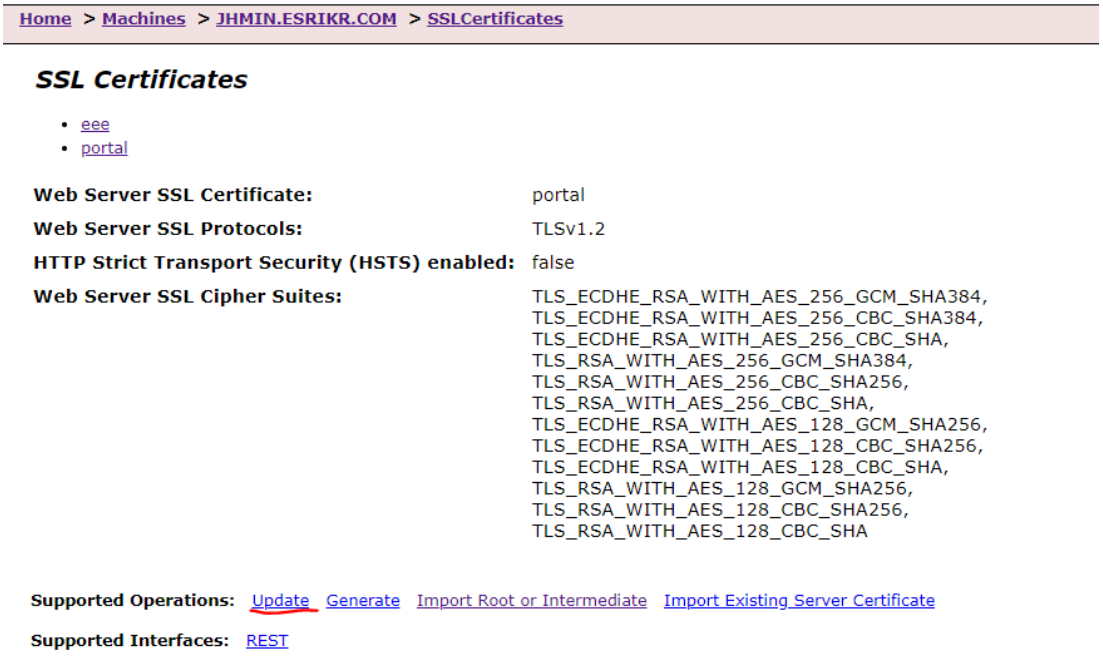


2) Import 클릭하기

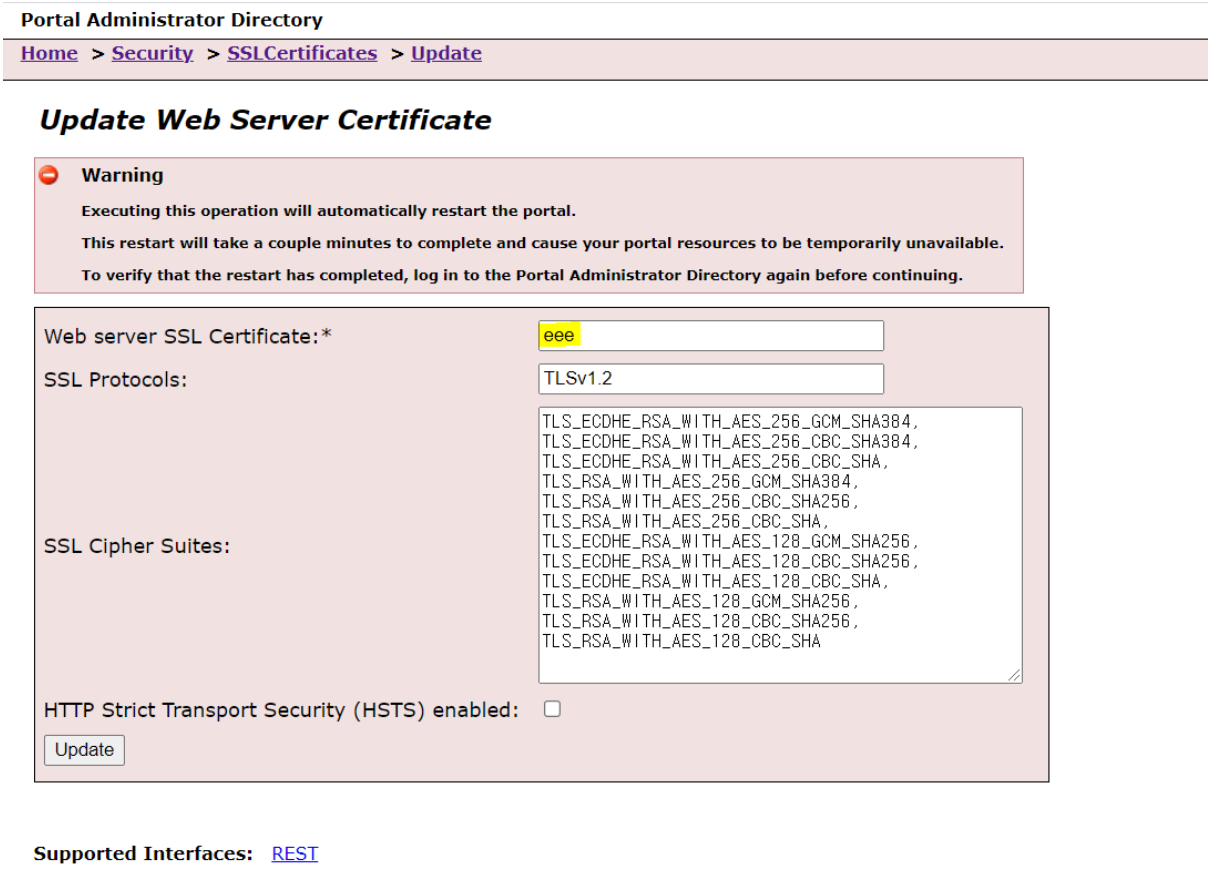
Import 클릭 후 1~10 분 정도의 시간이 소요될 수 있으며, 이 시간 동안 Portal for ArcGIS 서비스가 자동으로 다시 시작됩니다.

3. CA 서명 인증서를 사용하도록 Portal for ArcGIS 구성

1) Security > SSLCertificates > Update 클릭



2) 웹 서버 SSL 인증서 필드에 기존 CA 서명 인증서의 별칭을 입력



3) Update 를 클릭

Update 클릭 후 1~10 분 정도의 시간이 소요될 수 있으며, 이 시간 동안 Portal for ArcGIS 서비스가 자동으로 다시 시작됩니다.

4. HTTPS 를 사용하여 포털에 접근할 수 있는지 확인

1) HTTPS 프로토콜을 사용하여 포털에 접근할 수 있는지 다음의 URL 로 접근

https://portalhost.domain.com:7443/arcgis/home

ArcGIS Data Store 인증서 적용

1. 자체 서명된 인증서 사용

데이터 저장소를 생성할 때 데이터 저장소 구성 마법사는 자체 서명된 SSL 인증서를 사용하여 ArcGIS Data Store 에 접근합니다. 마찬가지로, 호스팅 서버가 데이터 저장소와 통신하거나 데이터 저장소 내의 개별 머신끼리 통신할 때도 자체 서명된 SSL 인증서가 사용됩니다.

2. CA 서명된 인증서 사용

일부 기관의 경우 CA (인증 기관)에서 검증하고 서명한 SSL 인증서나 기관 도메인용으로 생성된 인증서를 통해 모든 상호 작용의 보안이 유지되어야 합니다. 머신에 데이터 저장소를 구성하기 전에 updatesslcertificate 유틸리티를 사용하여 자체 서명된 인증서를 CA 서명 인증서나 도메인 인증서로 바꿀 수 있습니다.

3. 커맨드 유틸리티를 이용하여 SSL 인증서 적용/교체하기

모든 커맨드 유틸리티는 ArcGIS Data Store 머신에서 실행되어야 합니다.
유틸리티는 <ArcGIS Data Store 설치 경로>\datastore\tools 에서 찾을 수 있습니다.

☞ ArcGIS Data Store 유틸리티를 사용하려면 로그인 시 Windows 관리자 그룹의 구성원이어야 하고, 관리자 권한으로 실행 옵션을 사용하여 명령 프롬프트를 열어야합니다.

1) 인증 기관의 SSL 인증서를 받거나 도메인 인증서를 생성

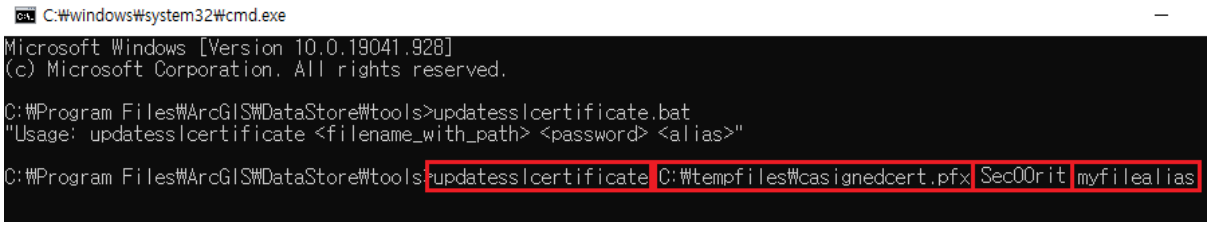
2) PKCS12 형식의 파일 (.pfx 또는 .p12 확장자) 을 생성한 후, 파일의 비밀번호와 별칭 설정

3) updatesslcertificate 유틸리티를 실행하여 ArcGIS Data Store 머신의 자체 서명된 SSL 을 변경

① 관리자 권한을 이용하여 cmd 실행

② <ArcGIS Data Store 설치 경로>\datastore\tools 이동

③ updatesslcertificate <인증서 이름이 포함된 경로> <인증서 비밀번호> <인증서 별칭> 입력



4) ArcGIS Data Store 머신이 여러 대인 경우 각 머신별로 인증서를 업데이트합니다.

5) 데이터 저장소 구성 마법사에 접근할 수 있는지 확인
브라우저에서 데이터 저장소 구성 마법사의 URL (https://<fully qualified data store machine name>:2443/arcgis/datastore) 을 입력합니다.

보안 경고 없이 마법사가 열리면 SSL 인증서가 정상적으로 업데이트 된 것입니다.

본 기술문서는 Esri 에서 제공하는 공식 기술문서를 기반하여 작성되었으며 자세한 내용은 아래의 원문 링크를 통해 확인하실 수 있습니다.

원문 링크

웹 서버에서 HTTPS 활성화—Portal for ArcGIS | ArcGIS Enterprise 문서

Configure ArcGIS Server with an existing CA-signed certificate—ArcGIS Server | Documentation for ArcGIS Enterprise

포털로 인증서 가져오기—Portal for ArcGIS | ArcGIS Enterprise 문서

ArcGIS Data Store SSL 인증서 바꾸기—Portal for ArcGIS | ArcGIS Enterprise 문서

관련 링크

도메인 인증서 생성—Portal for ArcGIS | ArcGIS Enterprise 문서

포털 REST API 디렉터리 정보—Portal for ArcGIS | ArcGIS Enterprise 문서