Upload SSL certificate for existing APP Service

Overview

Platform:	Azure
Owner of this SOP:	Fully Managed POD A
Cloud Services:	Azure APP Service

Problem

- When Service request from application team to upload new SSL certificate for an existing application.

Verify the SNOW request for below points:

- Certificate should be attached by the user in SR along with application name, app service
- Certificate should be attached by user in **.pfx** format
- If user hasn’t provided the password for certificate proactively, drop an email to user for the password. This password would be used while importing the certificate in Key Vault.

tester	Reviewer
@ Suresh Potlapalli (Deactivated)	

Process

Raise a Normal Change Request

Please open a Normal change request and get it approved before executing the SSL upload activity.

Please go to page 20 of the below *Change Control document* :

Service Management: As-Is Change Management (ServiceNow)

Please select the respective team assignment group when raising a change request in Service Now create a separate CTASK's for each team to perform the activities.

1. CTASK for Cloud Network - Hub Connectivity - Azure team to upload SSL certificate on APP Gateway
2. CTASK for Cloud Factory - Fully Managed - POD A Team to upload SSL certificate for Azure App service
3. CTASK for Application team to validate the application after the new cert is uploaded.

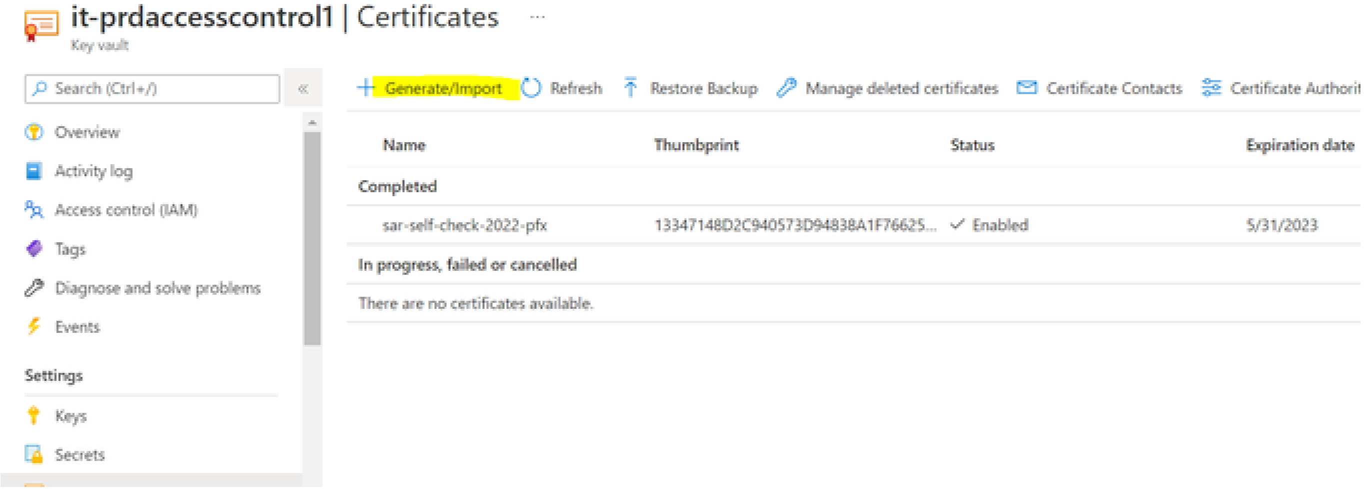
Note

- This process is valid for PaaS Object only. For certs that live inside a VM, the app team should manage themselves. Suggested to create their own change record and create a Ctask for the Cloud Net team to update the App Gateway in support of that change.

Solution

Steps for SSL certificate upload to App service

- Go to Azure portal and open Key vault in the requested subscription.
- Go to **Certificates** under **Settings** and click on **Generate/Import** to import the certificate.

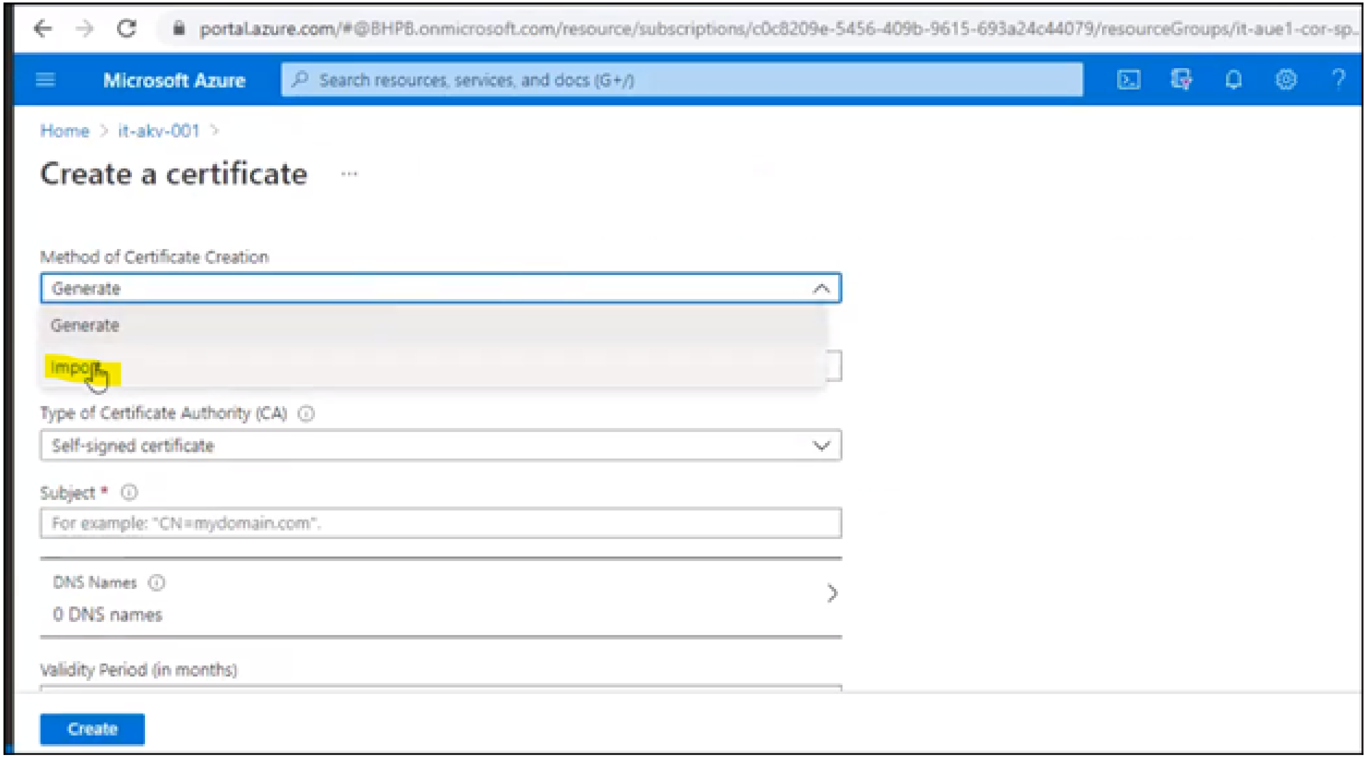


it-prdaccesscontrol1 | Certificates ...

Key vault

Name	Thumbprint	Status	Expiration date
Completed			
sar-self-check-2022-pfx	13347148D2C940573D94838A1F76625...	✓ Enabled	5/31/2023
In progress, failed or cancelled			
There are no certificates available.			

- Select **Import** from the drop-down menu.



portal.azure.com/#@BHPB.onmicrosoft.com/resource/subscriptions/c0c8209e-5456-409b-9615-693a24c44079/resourceGroups/it-aue1-cor-sp...

Create a certificate ...

Method of Certificate Creation: Generate

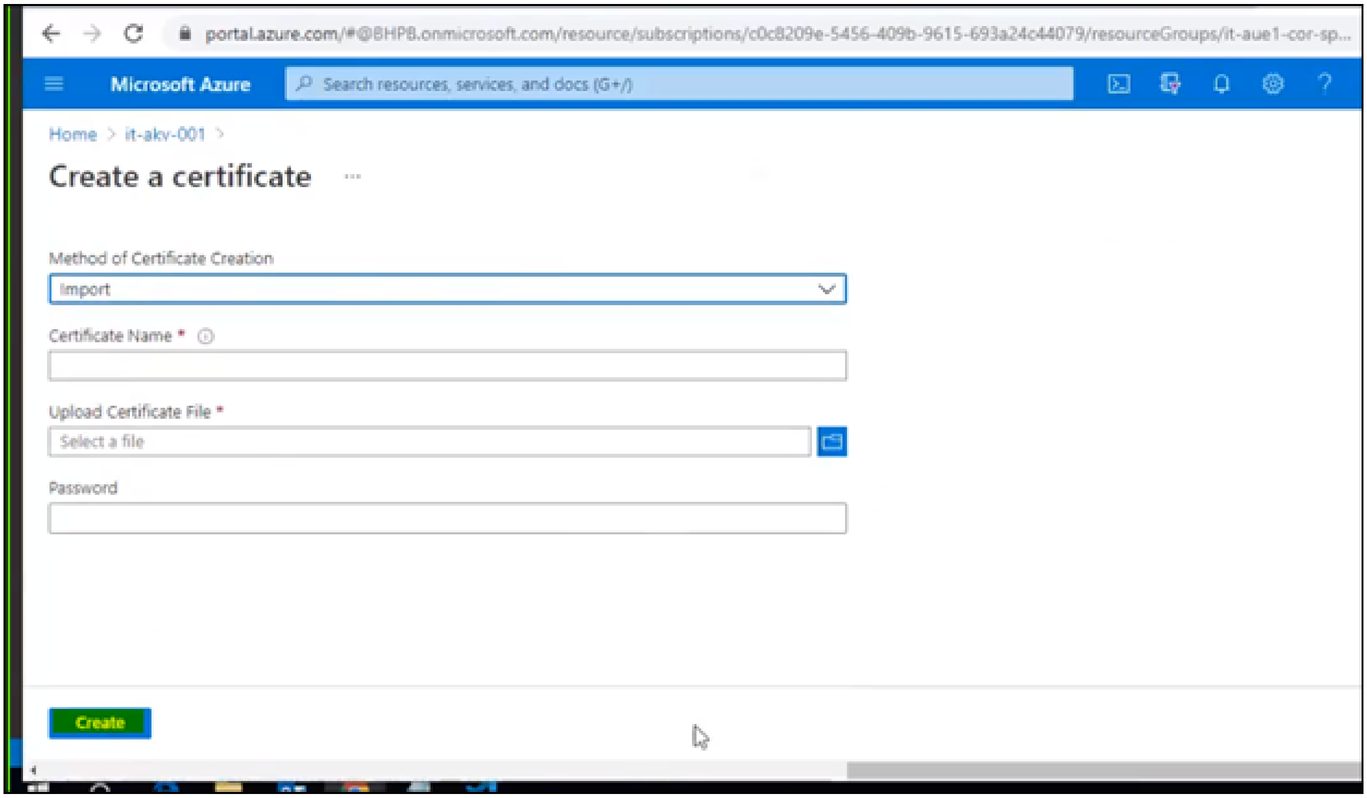
Type of Certificate Authority (CA): Self-signed certificate

Subject *: For example: "CN=mydomain.com".

DNS Names: 0 DNS names

Validity Period (in months)

- Fill in the certificate name
- Browse .pfx file from your local computer and type in the password shared by the user for certificate.
- Then click on **Create** and certificate will be imported in the Key Vault.



portal.azure.com/#@BHPB.onmicrosoft.com/resource/subscriptions/c0c8209e-5456-409b-9615-693a24c44079/resourceGroups/it-aue1-cor-sp...

Create a certificate ...

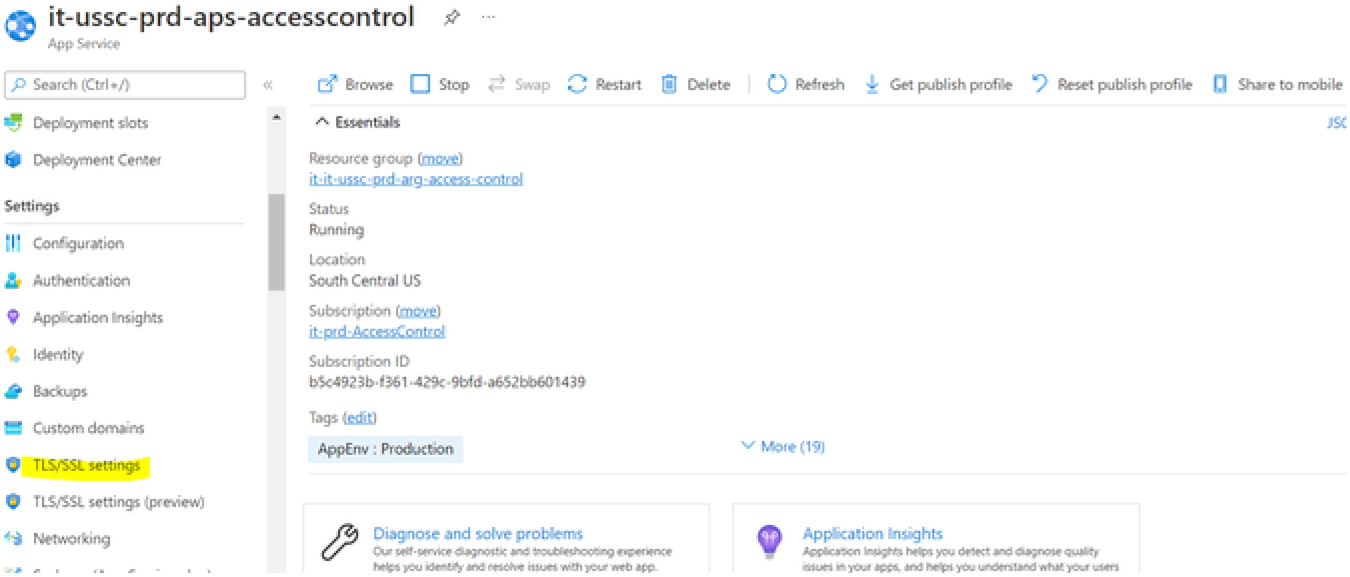
Method of Certificate Creation: Import

Certificate Name *

Upload Certificate File *: Select a file

Password

- Now Go to Azure App Service and go to TLS/SSL settings blade,.



it-ussc-prd-aps-accesscontrol

App Service

Resource group (move)
it-it-ussc-prd-arg-access-control

Status
Running

Location
South Central US

Subscription (move)
it-prd-AccessControl

Subscription ID
b5c4923b-f361-429c-9bfd-a652bb601439

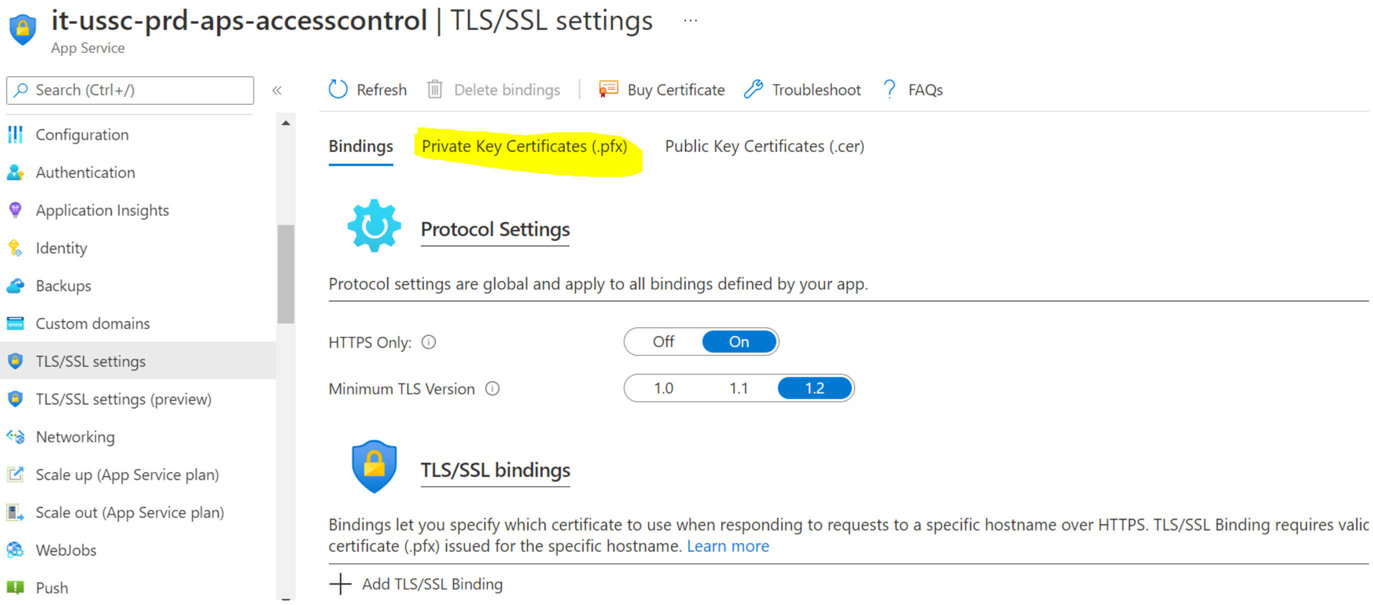
Tags (edit)
AppEnv : Production

More (19)

Diagnose and solve problems
Our self-service diagnostic and troubleshooting experience helps you identify and resolve issues with your web app.

Application Insights
Application Insights helps you detect and diagnose quality issues in your apps, and helps you understand what your users

- Select private key certificates and then select Import Azure Key Vault certificate



Protocol Settings

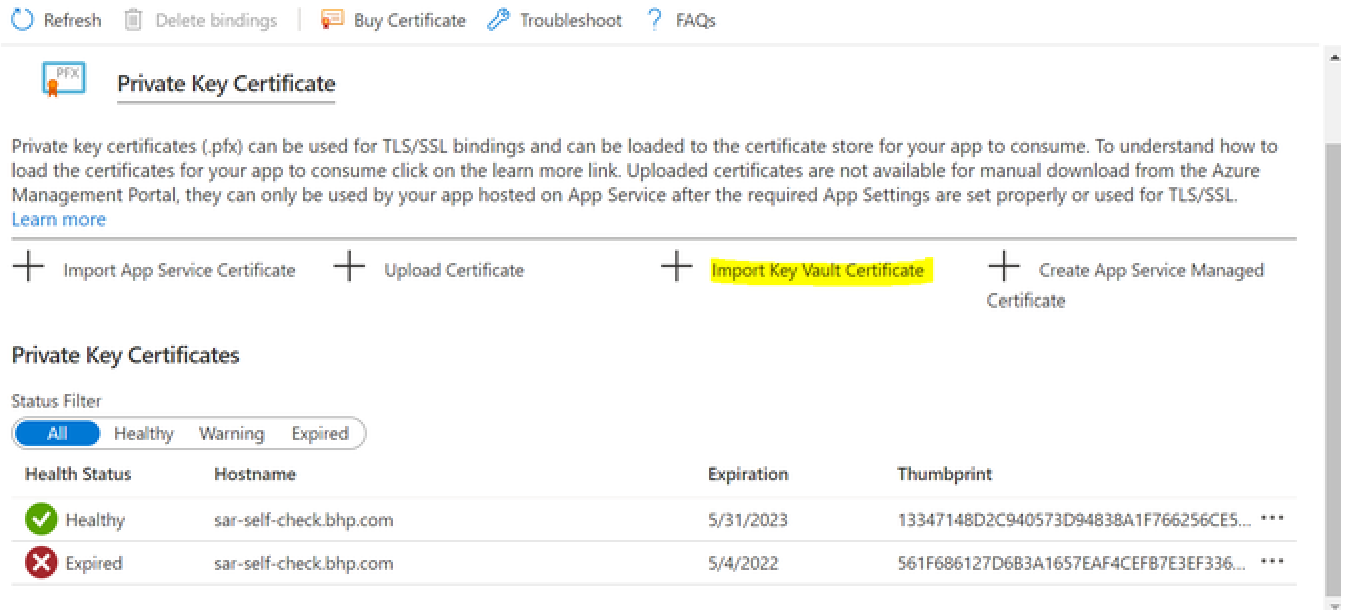
Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only: Off [✓ On]

Minimum TLS Version 1.0 1.1 [✓ 1.2]

TLS/SSL bindings

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valic certificate (.pfx) issued for the specific hostname. Learn more



Private Key Certificate

Private key certificates (.pfx) can be used for TLS/SSL bindings and can be loaded to the certificate store for your app to consume. To understand how to load the certificates for your app to consume click on the learn more link. Uploaded certificates are not available for manual download from the Azure Management Portal, they can only be used by your app hosted on App Service after the required App Settings are set properly or used for TLS/SSL. Learn more

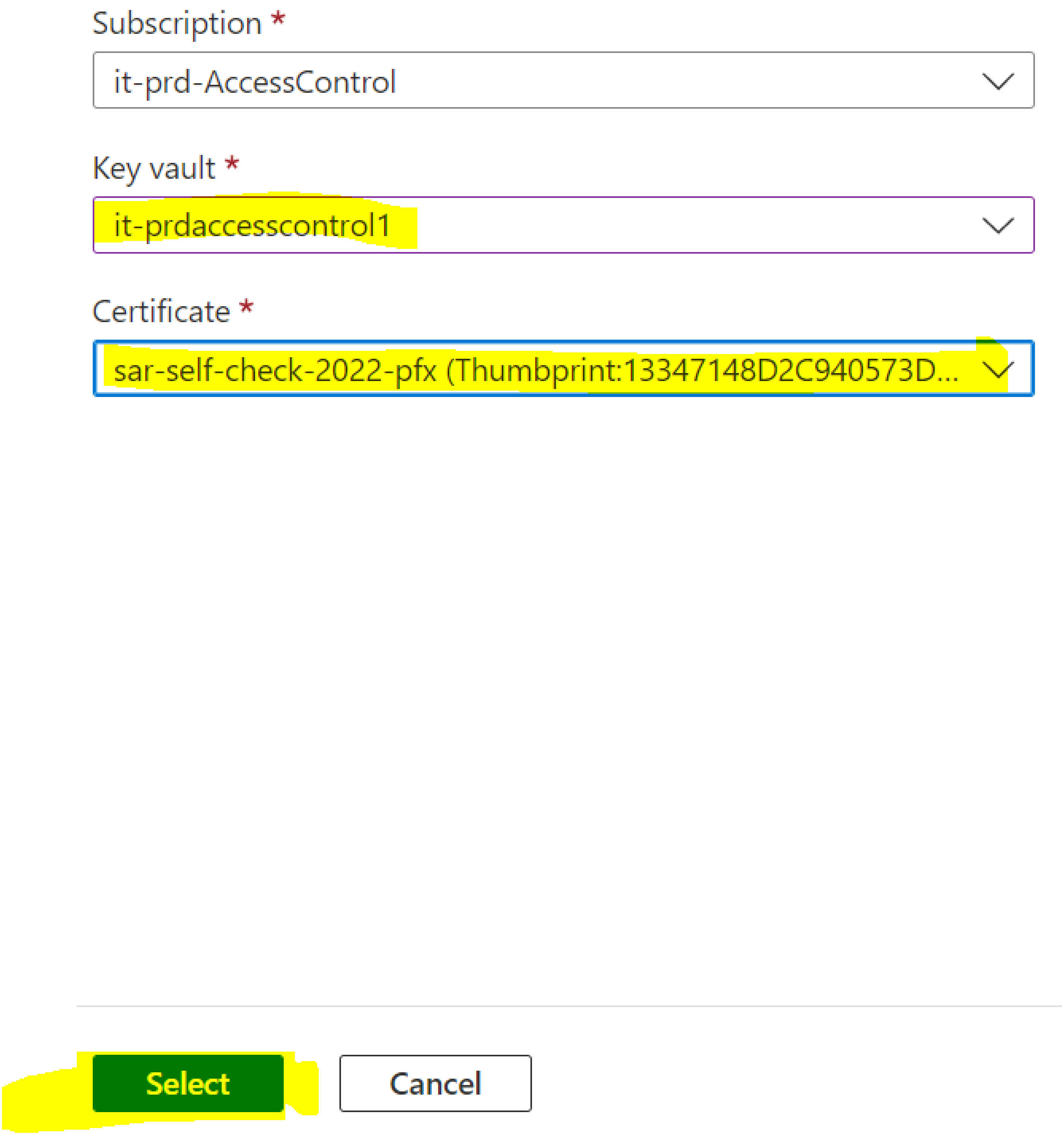
Import App Service Certificate
Upload Certificate
Import Key Vault Certificate
Create App Service Managed Certificate

Private Key Certificates

Status Filter [✓ All] Healthy Warning Expired

Health Status	Hostname	Expiration	Thumbprint
✓ Healthy	sar-self-check.bhp.com	5/31/2023	13347148D2C940573D94838A1F766256CE5... •••
✗ Expired	sar-self-check.bhp.com	5/4/2022	561F686127D6B3A1657EAF4CEFB7E3EF336... •••

- Now select the Key vault and new certificate uploaded to the key vault and click on select.

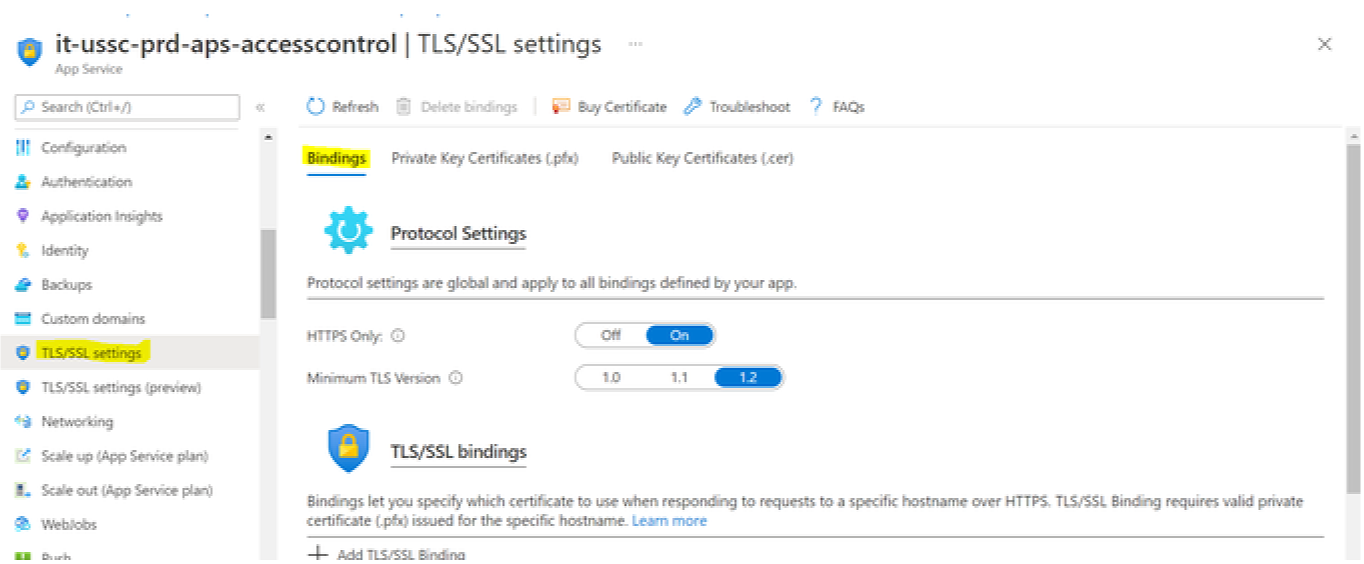


Subscription *
it-prd-AccessControl

Key vault *
it-prdaccesscontrol1

Certificate *
sar-self-check-2022-pfx (Thumbprint:13347148D2C940573D...

- The recently uploaded certificate should be displayed on the list.
- Go to bindings blade from TLS/SSL settings



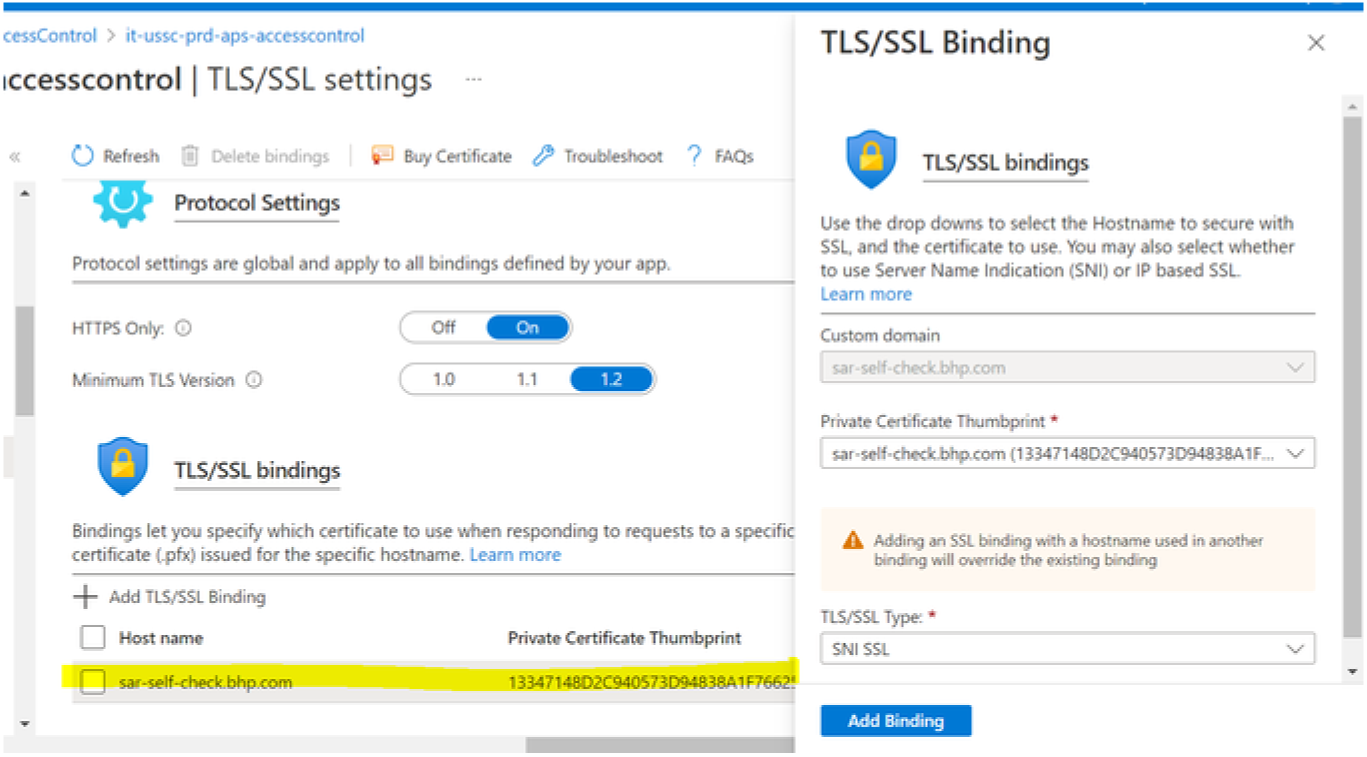
Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only: Off [✓ On]

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname. Learn more

- Select the binding



Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only: Off [✓ On]

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

Bindings let you specify which certificate to use when responding to requests to a specific certificate (.pfx) issued for the specific hostname. Learn more

Host name	Private Certificate Thumbprint
sar-self-check.bhp.com	13347148D2C940573D94838A1F7662!

Use the drop downs to select the Hostname to secure with SSL, and the certificate to use. You may also select whether to use Server Name Indication (SNI) or IP based SSL. Learn more

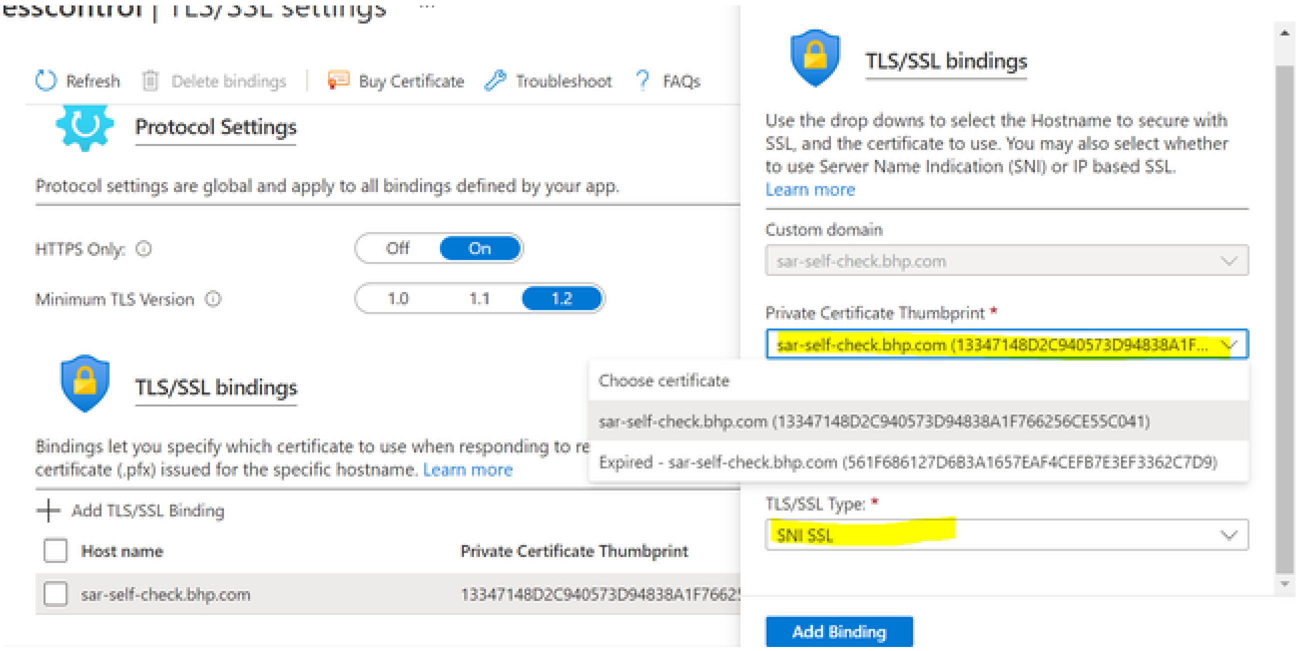
Custom domain: sar-self-check.bhp.com

Private Certificate Thumbprint *: sar-self-check.bhp.com (13347148D2C940573D94838A1F...

Adding an SSL binding with a hostname used in another binding will override the existing binding

TLS/SSL Type: *: SNI SSL

- Select the new uploaded certificate thumbprint and make sure TLS/SSL type is SNI SSL.
-



esscontrol | TLS/SSL settings ...

Protocol Settings

Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only: Off [✓ On]

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

TLS/SSL bindings

Bindings let you specify which certificate to use when responding to re certificate (.pfx) issued for the specific hostname. Learn more

□ Host name	Private Certificate Thumbprint
□ sar-self-check.bhp.com	13347148D2C940573D94838A1F7662!

TLS/SSL bindings

Use the drop downs to select the Hostname to secure with SSL, and the certificate to use. You may also select whether to use Server Name Indication (SNI) or IP based SSL. Learn more

Custom domain: sar-self-check.bhp.com

Private Certificate Thumbprint *: sar-self-check.bhp.com (13347148D2C940573D94838A1F...

Choose certificate
sar-self-check.bhp.com (13347148D2C940573D94838A1F766256CE55C041)
Expired - sar-self-check.bhp.com (561F686127D6B3A1657EAF4CEFB7E3EF3362C7D9)

TLS/SSL Type: *: SNI SSL

- After make the changes inform to Application team to validate the application functionality.