

Lietotāja instrukcija
Konfigurācija ar REST

Izmaiņas domēna autentifikācijas konfigurēšanai
Pašapkalpošanās WEB

Horizon 475.versija

Šo dokumentu vai tā daļas neatkarīgi no izmantojamajiem līdzekļiem nedrīkst reproducēt, pārraidīt, pārrakstīt, uzglabāt elektroniskā meklēšanas sistēmā vai tulkot kādā citā valodā bez iepriekš saņemtas Visma Enterprise atļaujas.

© SIA Visma Enterprise, 2016. Visas tiesības aizsargātas

SIA Visma Enterprise
Kronvalda blv. 3/5
Rīgā, LV - 1010

Tālr.: 6711 6211
Fakss.: 6711 6212
E-pasts: visma@visma.lv

Tirdzniecības un Preču zīmes

Visas tekstā izmantotās preču zīmes pieder to īpašniekiem un ir izmantotas tikai kā atsauces.

Saturs

IEVADS	4
SERTIFIKĀTA ĢENERĒŠANA NO HORIZON	4
UZĢENERĒTĀ SERTIFIKĀTA EKSPORTS.....	5
SERTIFIKĀTA IMPORTS WINDOWS SERTIFIKĀTU GLABĀTUVĒ	5
PAŠAPKALPOŠANĀS WEB KONFIGURĒŠANA	10
HORIZON UZSTĀDĪJUMI	11
IESPĒJAMĀS KĻŪDAS	11
IZMAIŅU LAPA	14

Ievads

Jaunajās izstrādēs tiek izmantoti REST lietojumi, piemēram, Darba laika uzskaitē, Laikrakstis, Darbavieta.

Lai nodrošinātu vidi REST lietojumiem no Pašapkalpošanās WEB, nepieciešams veikt šajā dokumentā aprakstītās darbības.

Nepieciešams:

- 1) uzģenerēt sertifikātu pāri un Horizon sertifikātu glabātuvē (keystore) ieimportēt publisko sertifikātu, piešķirt piekļuves tiesības.
- 2) datoram, uz kura atrodas IIS, iekonfigurēt privāto atslēgu.

FTGserverim jābūt nokonfigurētam rest portam.

Nākamajās sadaļās pa šiem aprakstīts risinājums, apraksts veidots izmantojot Windows Server 2012R2 standard edition, citās versijās ir iespējamās atšķirības.

Sertifikāta ģenerēšana no Horizon

Izmantojot Horizon sertifikātu glabātuvē (*Sistēma -> Administrēt -> Sertifikātu glabātuve*), jāģenerē pašparakstīts sertifikāts. To veic, nospiežot pogu **Pievienot** un no piedāvātajām darbībām izvēloties darbību **Ģenerēt pašparakstītu sertifikātu**.

Tiks piedāvāts ievadlogs sertifikāta aprakstīšanai, kā arī paroles norādīšanai. Šeit var ievadīt vērtības, kas norādītas uzņēmuma aprakstā Horizon. Ja tiek norādīta parole, tad tā jāatceras, pretējā gadījumā, nezinot paroli, nebūs iespējams sertifikātu izmantot tālāk.

Pašparakstīts sertifikāts - ievade

Derīgs no: 27.04.2016.

Derīgs līdz: 27.04.2041.

Īpašnieks

Nosaukums (CN): CERT_001_Horizon

Valsts (C):

Apgabals (ST):

Pilsēta (L):

Organizācija (O): Fermeris

Organizācijas nodaļa (OU):

Parole:

Saglabāt Atcelt

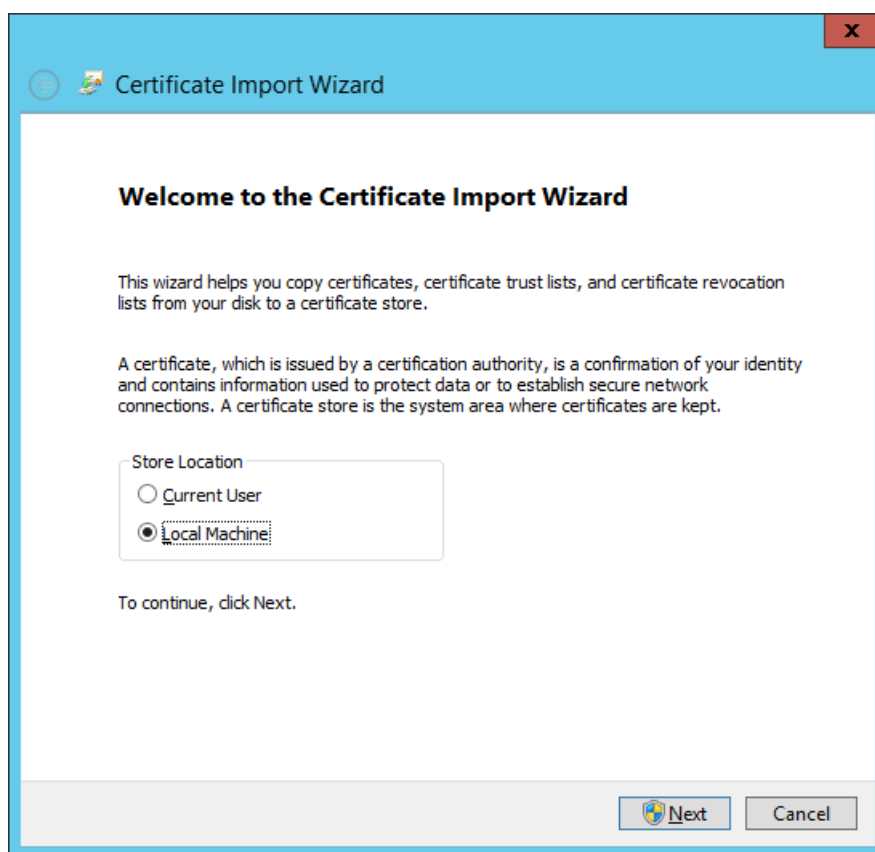
Darbības rezultātā Horizon sertifikātu glabātuvē ir izveidota publiskā atslēga un sertifikātu pāris.

Uzģenerētā sertifikāta eksports

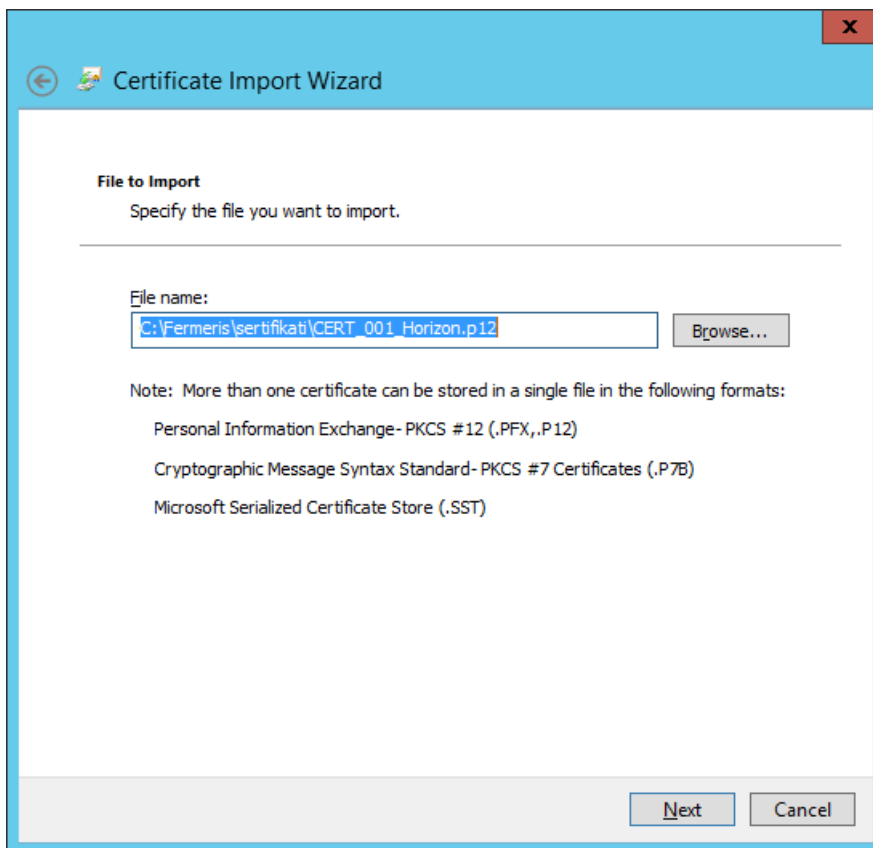
Izveidoto sertifikātu eksportē, izmantojot izvēlnē **Darbības** pieejamo darbību **Eksportēt sertifikāta failu**. Noklusētais eksporta formāts (.p12) ir derīgs importam Windows sertifikātu glabātvē.

Sertifikāta imports Windows sertifikātu glabātvē

Tālāk jāizmanto Windows standarta funkcija sertifikāta importam un jāimportē izveidotais sertifikāts Windows sertifikātu glabātvē uz Web servera. To veic, uzklikšķinot uz eksportētā sertifikāta faila. Windows automātiski atpazīst formātu .p12 un iedarbina importa vedni. Tālāk pa soļiem jāseko importa vednim un jāspiež poga **Next**, lai pārietu uz nākamo soli.



Glabātuve jāizvēlas "Local Machine".



The screenshot shows the 'Certificate Import Wizard' window. The title bar is blue with a back arrow, a help icon, and the text 'Certificate Import Wizard'. The main content area is white. Under the heading 'File to Import', there is a sub-heading 'Specify the file you want to import.' followed by a horizontal line. Below this is a 'File name:' label, a text input field containing the path 'C:\Fermeris\sertifikati\CERT_001_Horizon.p12', and a 'Browse...' button. A 'Note' section follows, stating 'More than one certificate can be stored in a single file in the following formats:' and listing three formats: 'Personal Information Exchange - PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom right, there are 'Next' and 'Cancel' buttons.

File to Import
Specify the file you want to import.

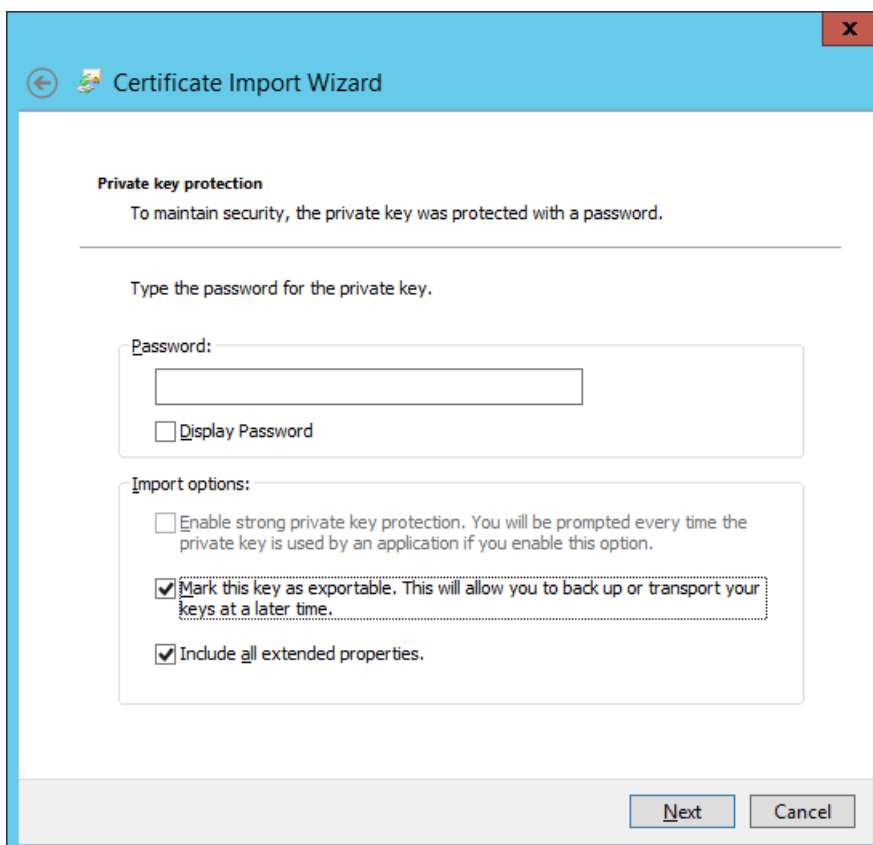
File name:
C:\Fermeris\sertifikati\CERT_001_Horizon.p12 Browse...

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange - PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Next Cancel

Nākamajā solī jānorāda parole, ar kuru ir aizsargāts sertifikāts. Ja sertifikāts nav aizsargāts ar paroli, tad tā nav jānorāda. Obligāti jāatzīmē opcija “Mark this key as exportable”.



The screenshot shows the 'Certificate Import Wizard' window at the 'Private key protection' step. The title bar is blue with a back arrow, a help icon, and the text 'Certificate Import Wizard'. The main content area is white. Under the heading 'Private key protection', there is a sub-heading 'To maintain security, the private key was protected with a password.' followed by a horizontal line. Below this is the instruction 'Type the password for the private key.' and a 'Password:' label. There is a text input field for the password and a 'Display Password' checkbox. Below this is an 'Import options:' section with three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (checked), and 'Include all extended properties.' (checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

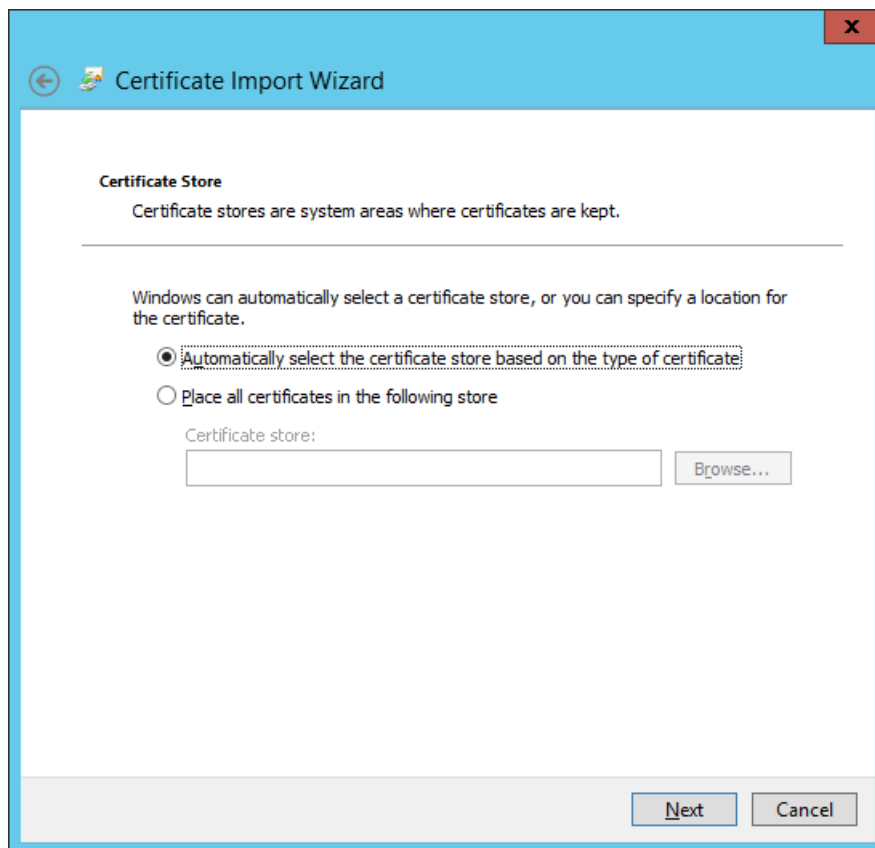
Password:
[Text Input Field] Display Password

Import options:

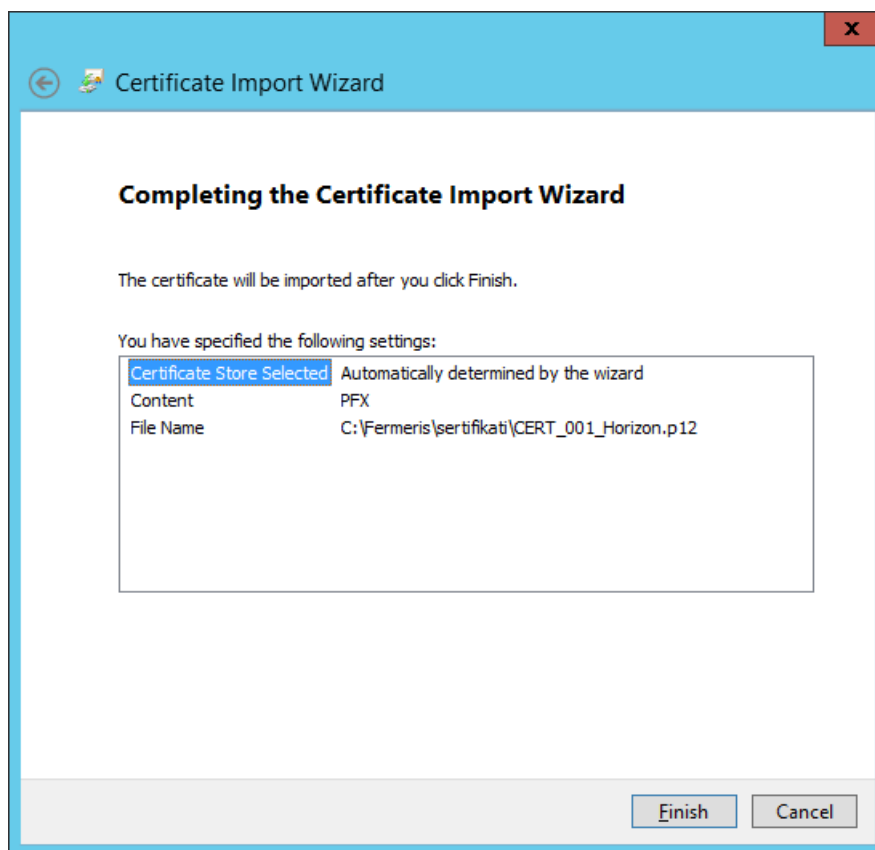
- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Include all extended properties.

Next Cancel

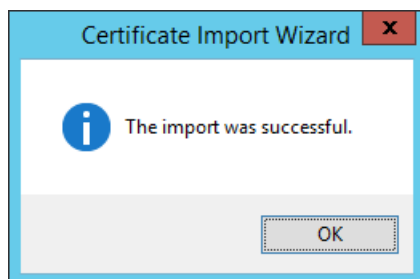
Sertifikāta faila novietošanai atstāj opciju "Automatically select the certificate store based on the type of certificate".



Nākamais solis ir fināla solis, kurā redzami norādītie uzstādījumi. Lai pabeigtu importu, jānospiež **Finish**.

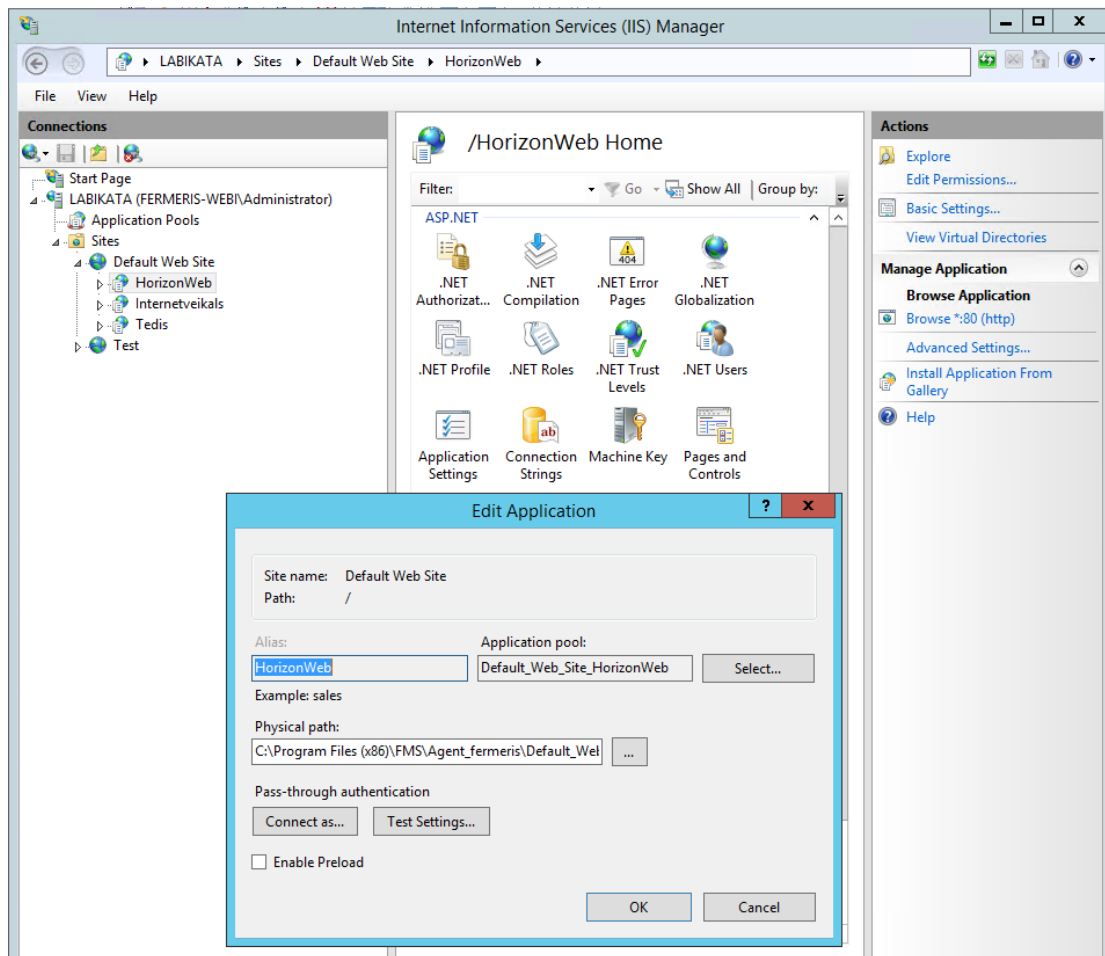


Par veiksmīgu sertifikāta importu liecina paziņojums:

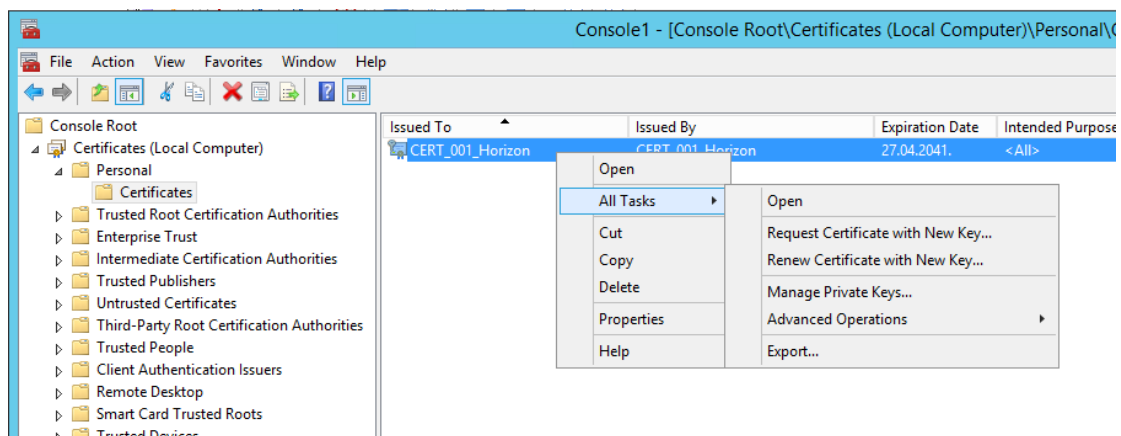


Šī procesa rezultātā ir pabeigts sertifikāta imports.

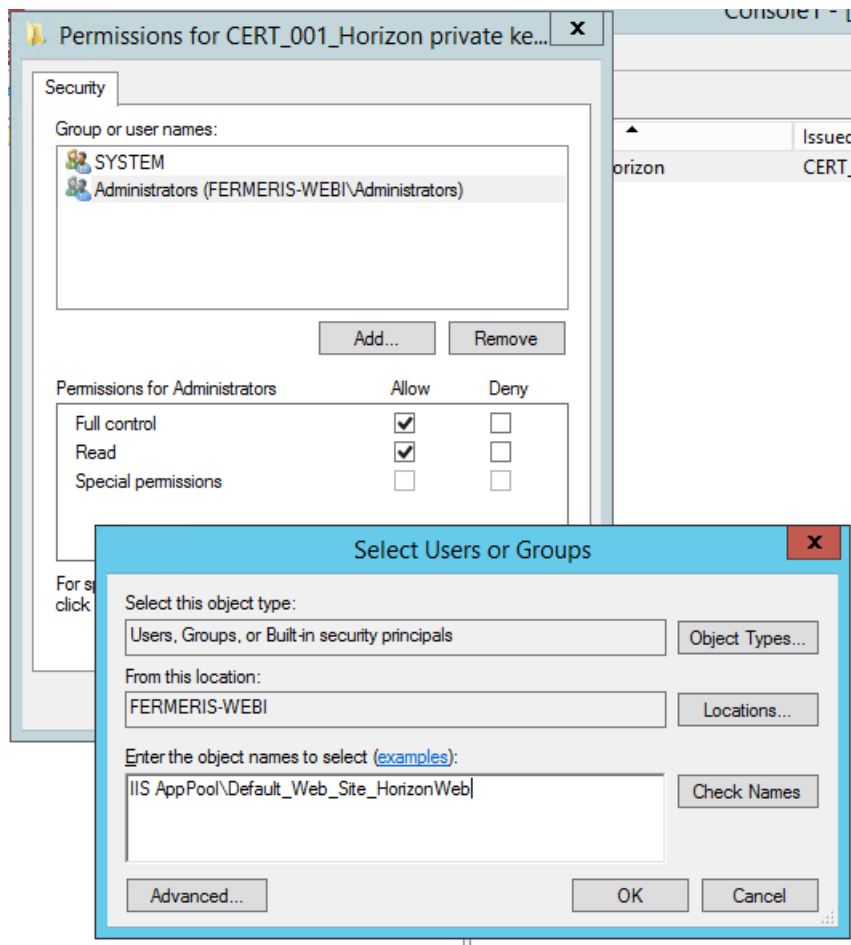
Horizon Web "Application Pool" jāpiešķir tiesības piekļūt Sertifikāta privātai atslēgai. Vispirms jānoskaidro "Application Pool" nosaukums. Lai to izdarītu, jāatver "IIS manager" un nostājas uz Horizon web aplikācijas jānospiež "Basic settings".



Šajā piemērā "Application Pool" nosaukums ir Default_Web_Site_HorizonWeb. Tālāk ir jāatver sertifikātu "MMC Snap-in" jāizvēlas "Computer account". Uz ieimportētā sertifikāta jāizvēlas "Manage Private Keys".



Jāpievieno iepriekš noskaidrotais "Application Pool" nosaukums papildināts ar "IIS AppPool" – mūsu gadījumā "IIS AppPool\ Default_Web_Site_HorizonWeb".



Pašapkalpošanās WEB konfigurēšana

Pēc tam Pašapkalpošanās WEB konfigurācijas failā web.config jānorāda, kuru sertifikātu jāpaņem no Windows sertifikātu glabātuves, lai lietotājs varētu veikt sekmīgu autorizāciju HorizonWEB, izmantojot domēna autorizācijas iespēju.

To norāda, web.config failā pievienojot vai labojot atribūtu FTGRestCertificateName un norādot kā value vērtību to, kas tika ierakstīta laukā Nosaukums (CN), sertifikātu ģenerējot.

```

web.config - Notepad
File Edit Format View Help
<appSettings>
  <!-- FTG servera vārds -->
  <add key="FTGHost" value="Fermeris-wei"/>
  <!-- FTG servera ports -->
  <add key="FTGPort" value="4674"/>
  <!-- FTG REST servera atrašanās vieta -->
  <add key="FTGUr1" value="http://Fermeris-wei:7378/rest/">
  <!-- Sertifikāta nosaukums windows autentifikācijai. Ja windows autentifikācija netiek izmantota, var atstāt tukšu -->
  <add key="FTGRestCertificateName" value="CERT_001_Horizon"/>

```

Horizon uzstādījumi

Sistēma -> Administrēt -> Web drošības uzstādījumi.

Jābūt uzstādītai Horizon identitātes pārsūtīšanai – “lietotāja vārds”.

Web drošības uzstādījumi

Pieslēgums Autentifikācijas metodes Auditpierausti

Weblietotāja autentifikācija (Basic)

lietotāja vārds personas kods e-pasts

SAML identitātes pārsūtīšana

lietotāja vārds personas kods

Bankas SAML autentifikācija pēc personas koda

HorizonPOS autentifikācija

Horizon identitātes pārsūtīšana

lietotāja vārds personas kods e-pasts

Labi Atcelt

Iespējamās kļūdas

Lai pārbaudītu vai konfigurācija veikta pareizi jāatver kāds no apgabaliem, kur izmantoti REST lietojumi.

Ja tiek saņemts kļūdas paziņojums, pēc tā var identificēt iespējamo iemeslu.

Vispirms jāatver kļūdu reģistrs:

<http://localhost/HorizonWeb/elmah>

Error Log for HorizonWeb on FERMERIS-WEBI

RSS FEED RSS DIGEST DOWNLOAD LOG HELP ABOUT

Errors 1 to 7 of total 7 (page 1 of 1). Start with [10](#), [15](#), [20](#), [25](#), [30](#), [50](#) or [100](#) errors per page.

Host	Code	Type	Error	User
FERMERIS-WEBI	0	InvalidOperation	Certificate System.Security.Cryptography.X509Certificates.X500DistinguishedName needs to either support SHA256 signing, or have an exportable private key! Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	ENoSuchFtgConnection	Sistēmas kļūda! Kļūda ir nodota risināšanai programmatūras izstrādātājam. Lai turpinātu darbu ar sistēmu, lūdzam veikt atkārtotu pieslēgšanos sistēmai pēc 3 minūtēm. Atvainojamies par sagādātajām neērtībām! Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	Socket	No connection could be made because the target machine actively refused it 10.11.57.24:7378 Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	Rest	Lietotājs nav atrasts vai neatbilst parole! Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	Rest	Lietotājs nav atrasts vai neatbilst parole! Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	Cryptographic	Keyset does not exist Details...	FERMERIS-WEBI\Administrator
FERMERIS-WEBI	0	Connect	No connection could be made because the target machine actively refused it 10.11.57.24:4674 Details...	

Powered by FI MAH, version 1.2.14318.2000. Copyright (c) 2004-11.. Atif Aziz. All rights reserved. Licensed under [Apache License, Version 2.0](#). Server date is

Kļūdu iemesli:

InvalidOperation	Certificate System.Security.Cryptography.X509Certificates.X500DistinguishedName needs to either support SHA256 signing, or have an exportable private key! Details...
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Pie sertifikāta importa nav norādīta opcija “Mark this key as exportable”.

Rest	Lietotājs nav atrasts vai neatbilst parole! Details...
-------------	------------------------------------------------------------------------

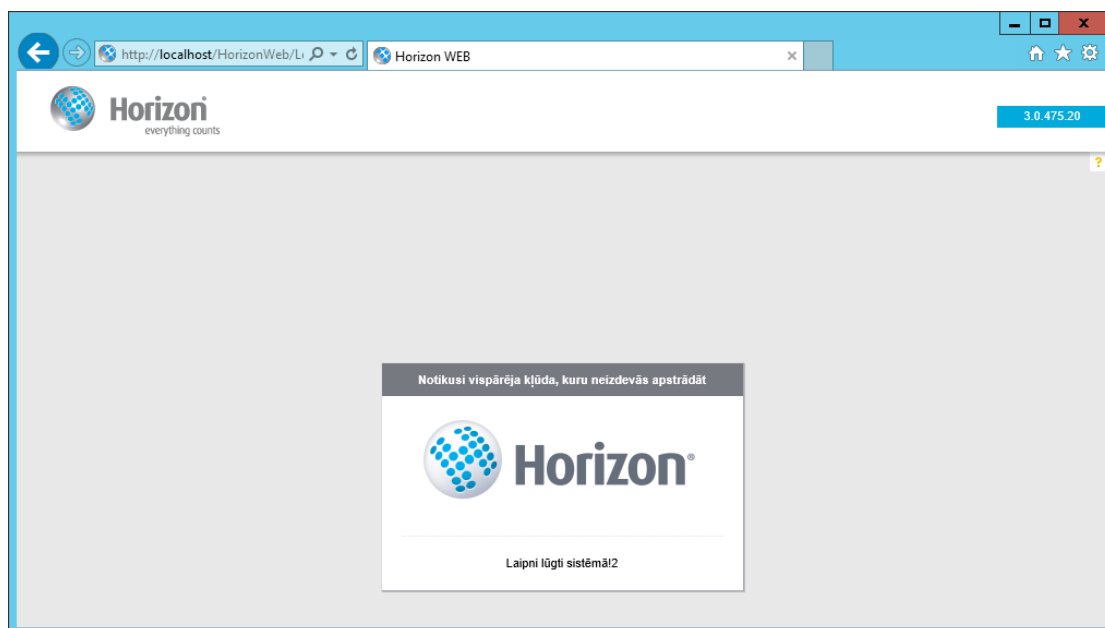
Nav uzstādīts Horizon identitātes pārsūtīšanai – “lietotāja vārds”

Cryptographic	Keyset does not exist Details...
----------------------	--------------------------------------------------

Horizon Web “Application Pool” nav piešķirtas tiesības piekļūt Sertifikāta privātai atslēgai.

DependencyResolution	A delegate registered to create instances of 'FTGRestClient.IFtgRestConnection' returned null. Details...
-----------------------------	---------------------------------------------------------------------------------------------------------------------------

Web.config failā nav norādīts rest servera interfeiss



Web.config failā norādīta nekorekta rest servera adrese, jābūt formātā `http://servera vārds:ports/rest/`

Izmaiņu lapa

Datums	Ver. Nr.	Izmaiņu apraksts	Autors
30.11.2014.	1.0	Izveidots jauns apraksts	A.Ozoliņa
02.05.2016	2.0	Veikti papildinājumi	I.Freimane