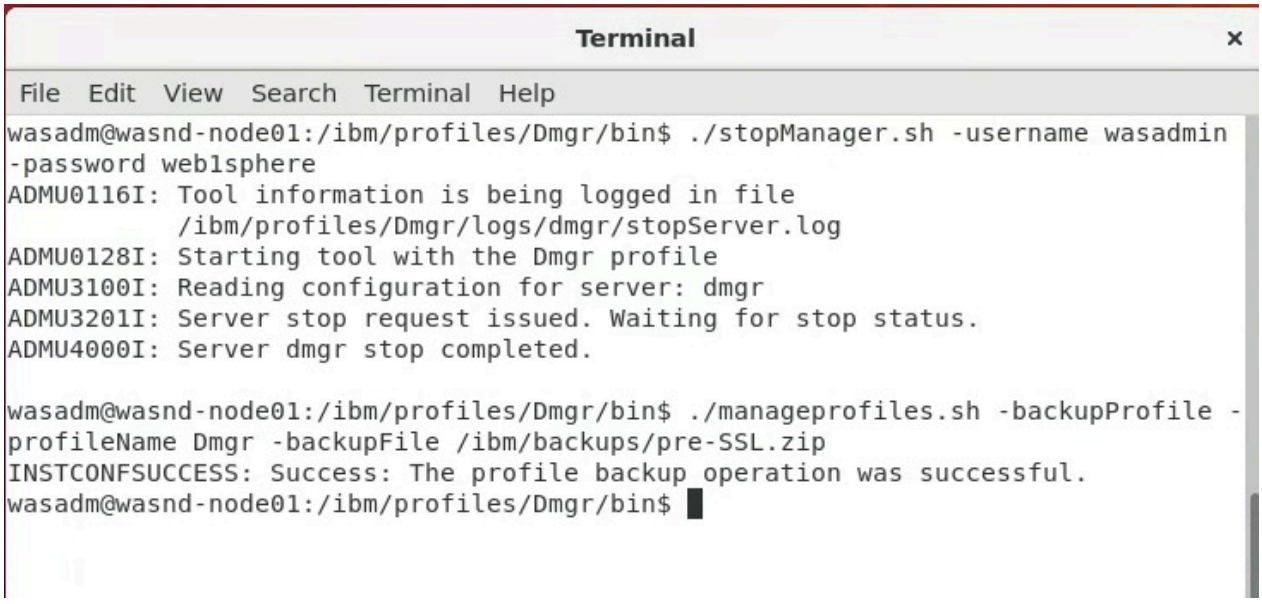
Exercise 14 – Configuring SSL for WebSphere

At the end of this exercise, you should be able to:

- Define the certificate life span of a profile
- Use the administrative console to find and view certificates within the cell
- Configure and run the certificate expiration service
- Propagate the generated plug-in keystore out to the plug-in
- Create a keystore for a web server
- Generate a self-signed key
- Configure IBM HTTP Server to load and use HTTPS

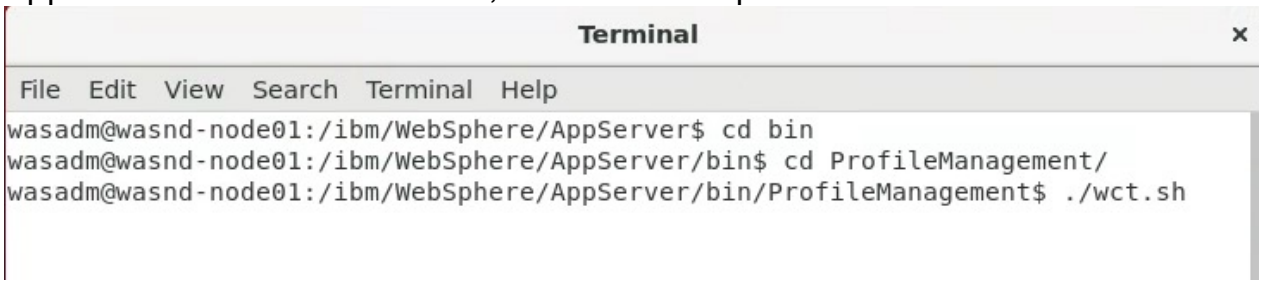
Section 1: Create a backup

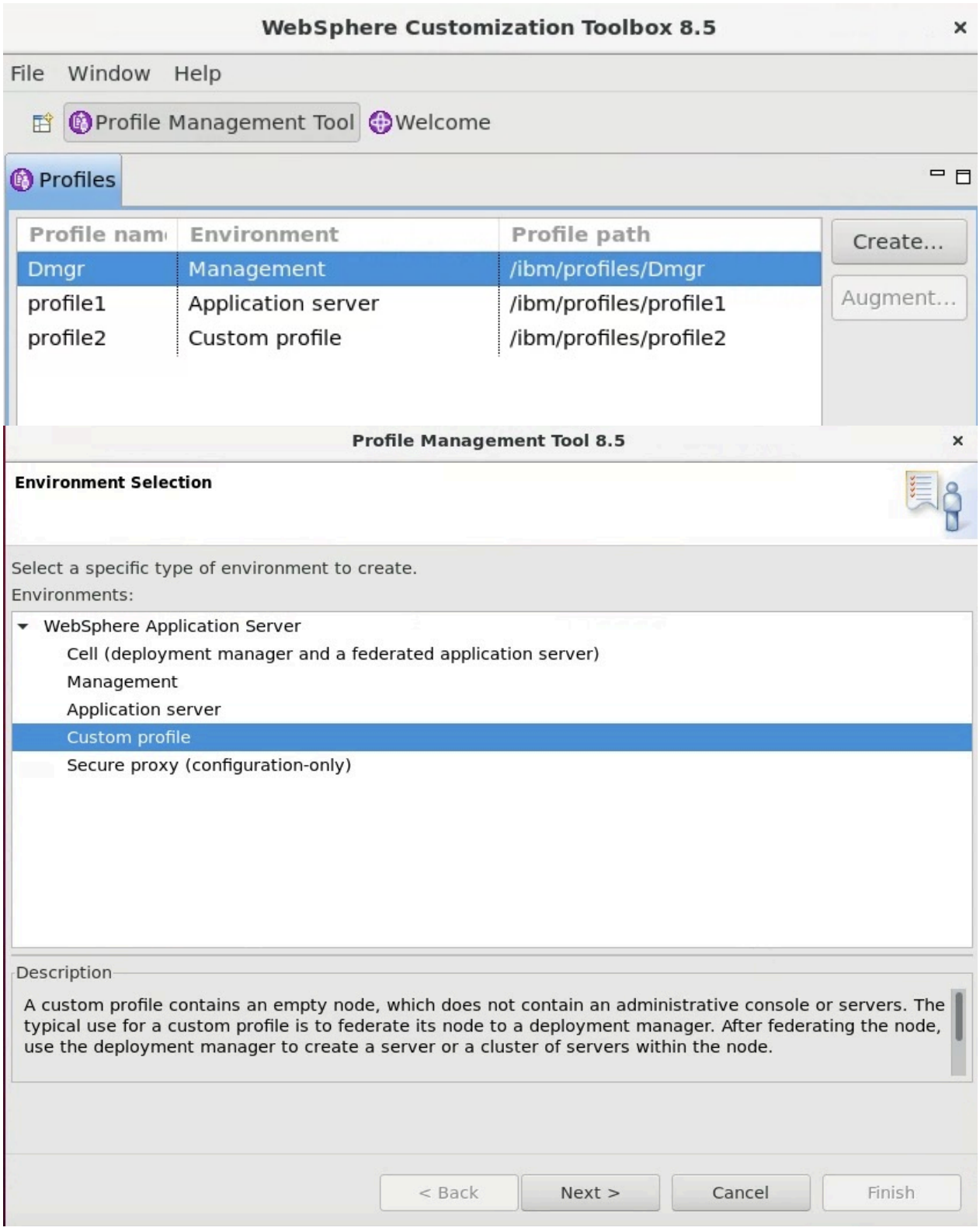
Since this exercise changes the existing environment, which, if done incorrectly, can cause problems for the rest of the exercises, creating a backup is a good idea.

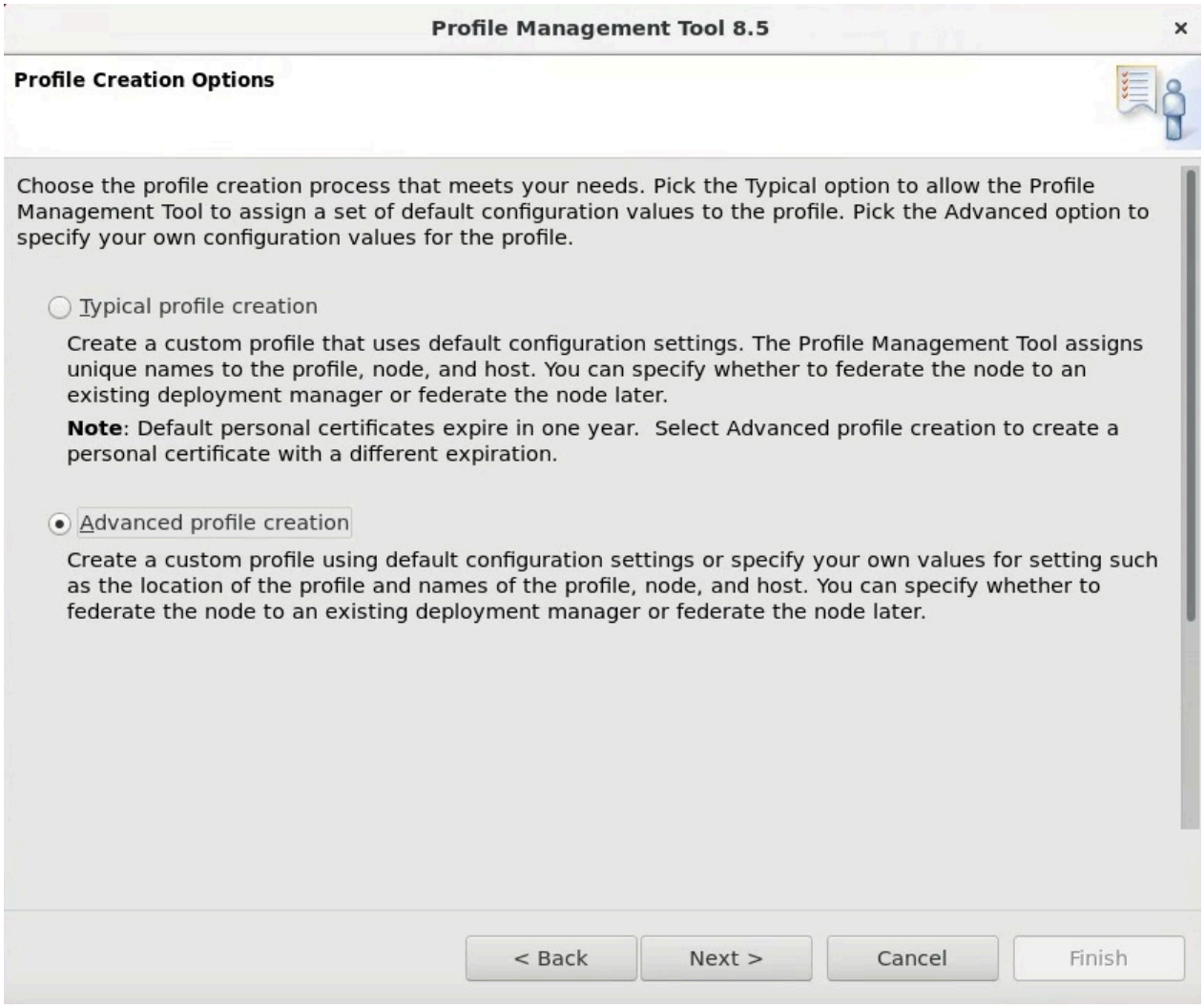


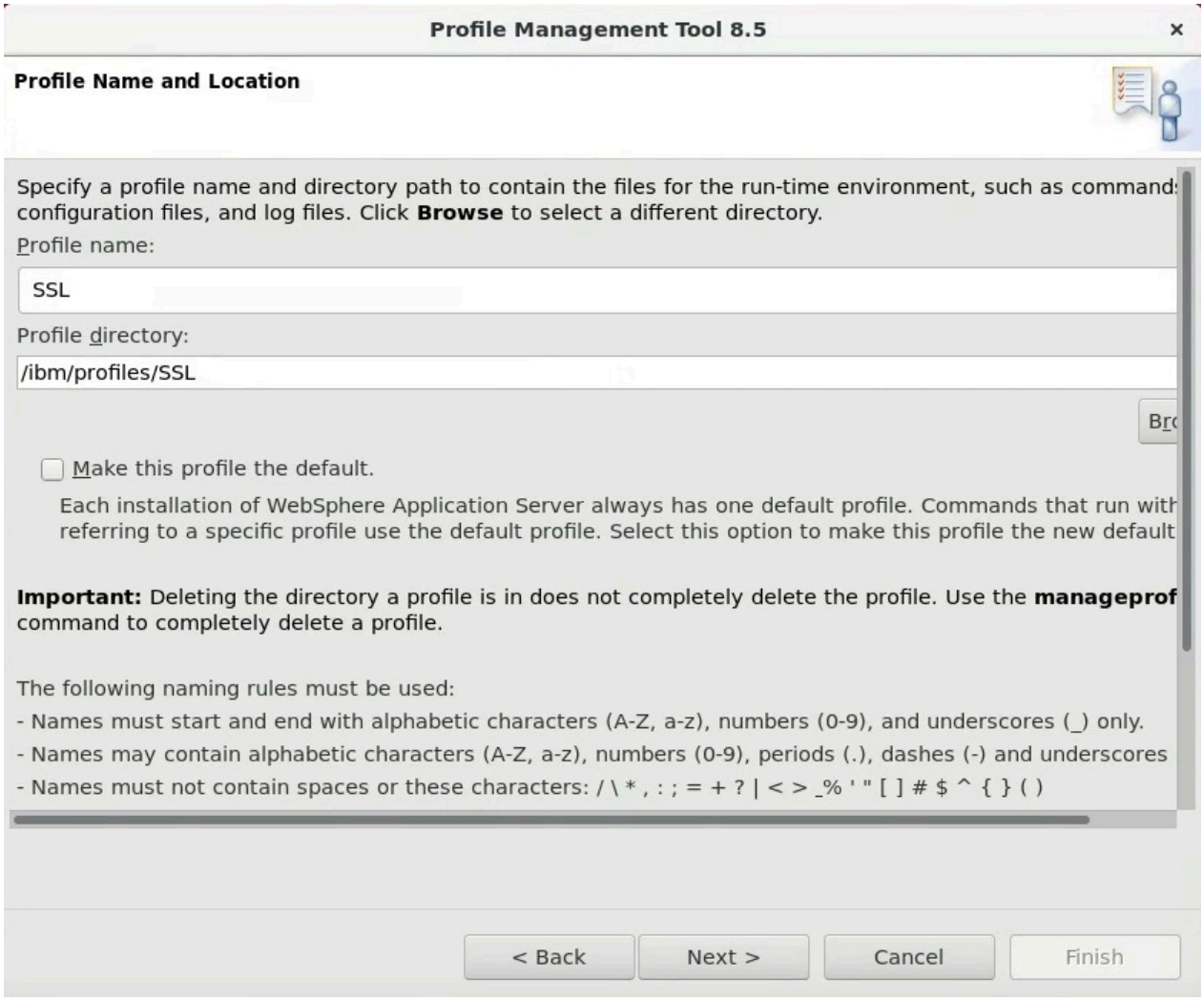
Section 2: Create a profile

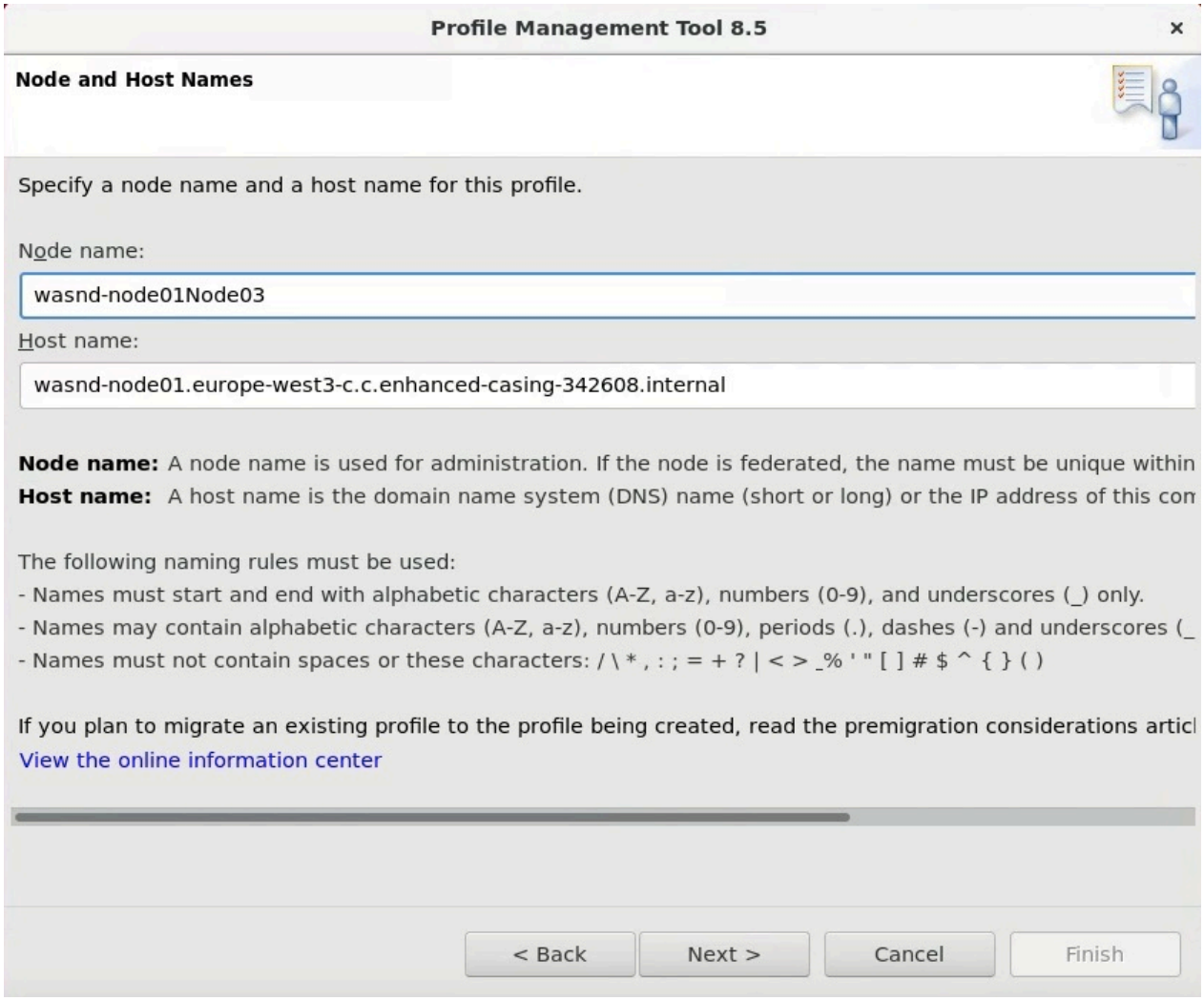
To better understand the various pieces of SSL within the WebSphere Application Server environment, a new custom profile is created.

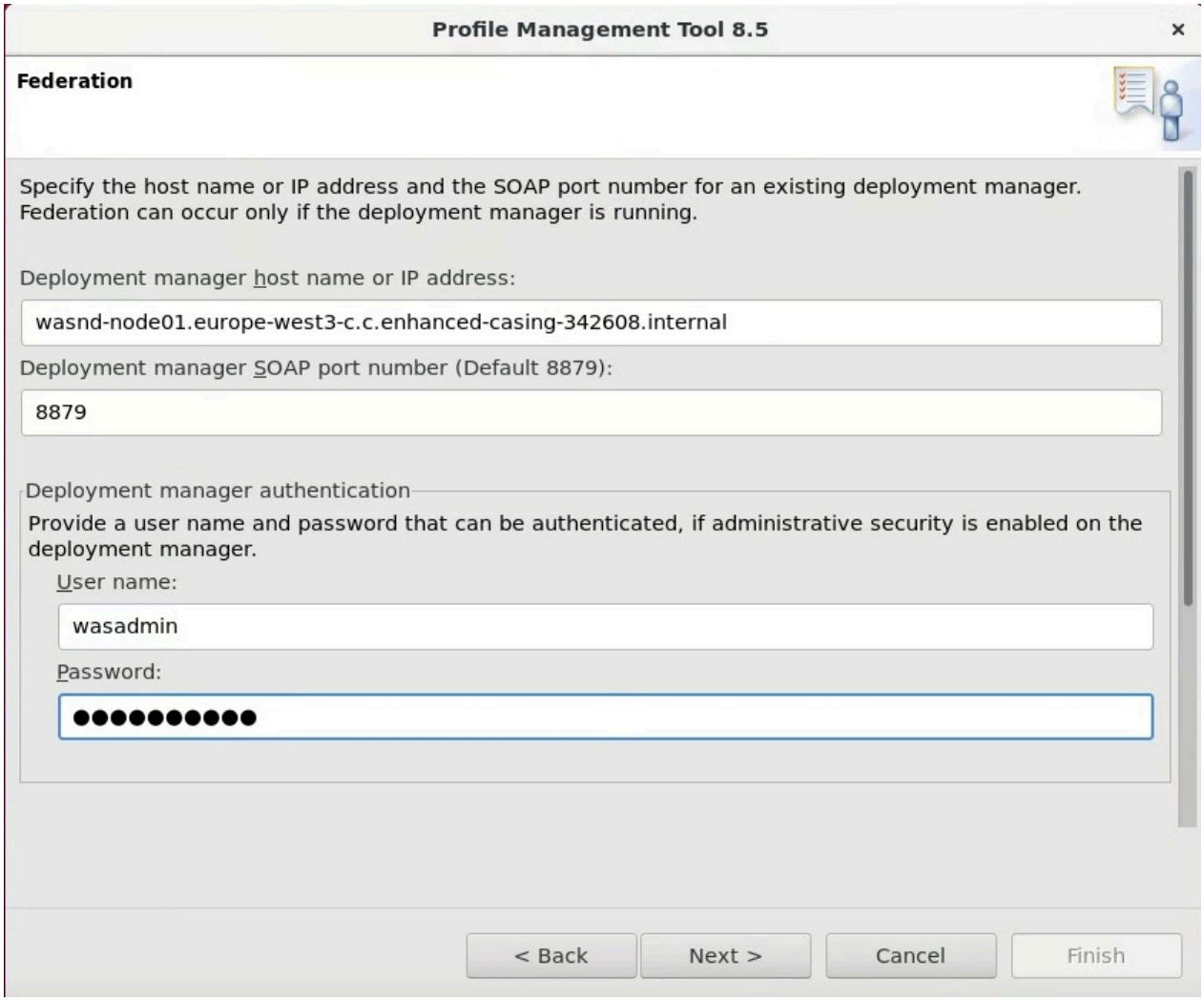



WebSphere Customization Toolbox 8.5
File
Window
Help
Profile Management Tool
Welcome
Profiles
Profile nam
Environment
Profile path
Dmgr
Management
/ibm/profiles/Dmgr
profile1
Application server
/ibm/profiles/profile1
profile2
Custom profile
/ibm/profiles/profile2
Create...
Augment...
Profile Management Tool 8.5
Environment Selection
Select a specific type of environment to create.
Environments:
WebSphere Application Server
Cell (deployment manager and a federated application server)
Management
Application server
Custom profile
Secure proxy (configuration-only)
Description
A custom profile contains an empty node, which does not contain an administrative console or servers. The typical use for a custom profile is to federate its node to a deployment manager. After federating the node, use the deployment manager to create a server or a cluster of servers within the node.
< Back
Next >
Cancel
Finish

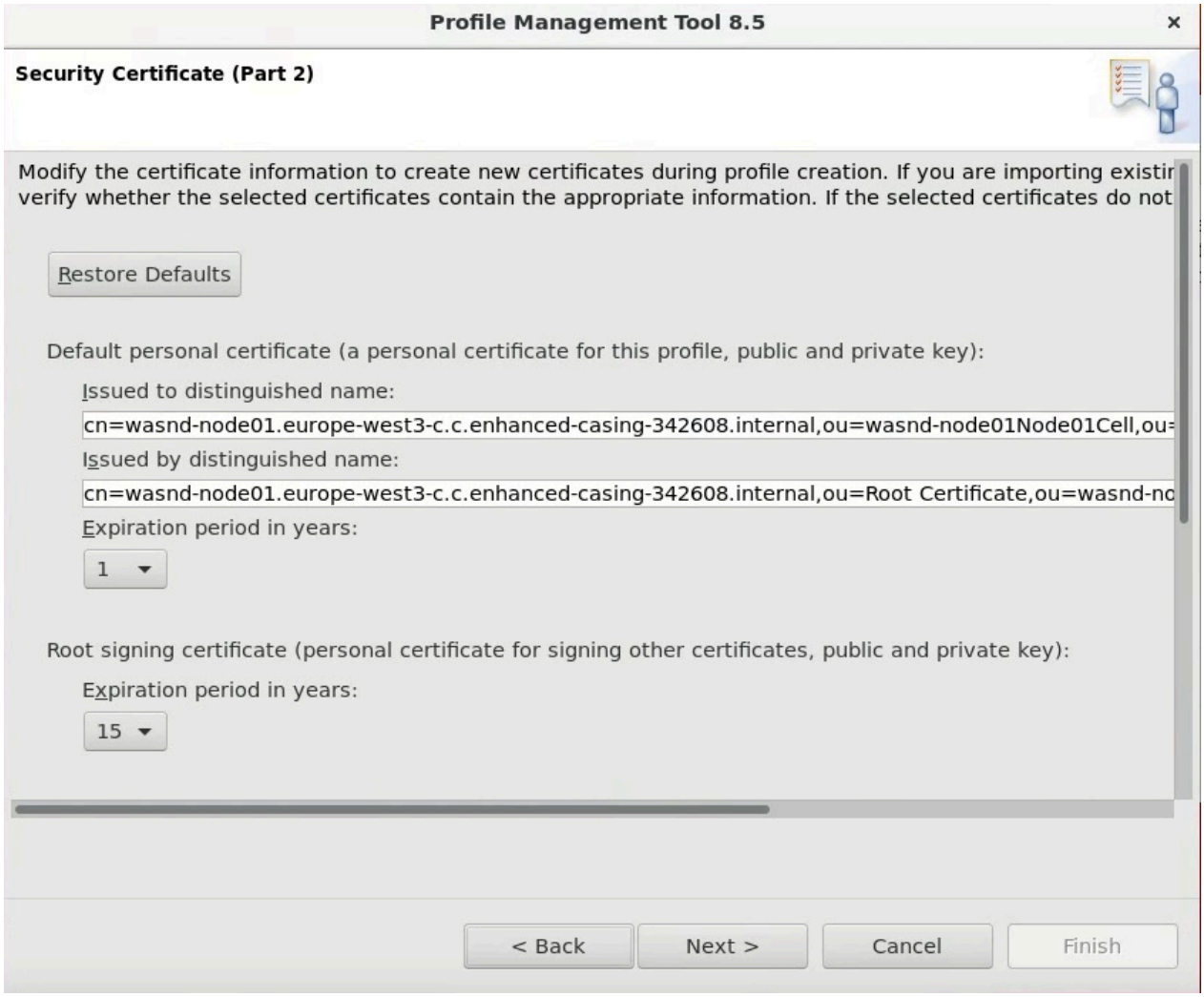

Profile Management Tool 8.5
Profile Creation Options
Choose the profile creation process that meets your needs. Pick the Typical option to allow the Profile Management Tool to assign a set of default configuration values to the profile. Pick the Advanced option to specify your own configuration values for the profile.
Typical profile creation
Create a custom profile that uses default configuration settings. The Profile Management Tool assigns unique names to the profile, node, and host. You can specify whether to federate the node to an existing deployment manager or federate the node later.
Note: Default personal certificates expire in one year. Select Advanced profile creation to create a personal certificate with a different expiration.
Advanced profile creation
Create a custom profile using default configuration settings or specify your own values for setting such as the location of the profile and names of the profile, node, and host. You can specify whether to federate the node to an existing deployment manager or federate the node later.
< Back
Next >
Cancel
Finish

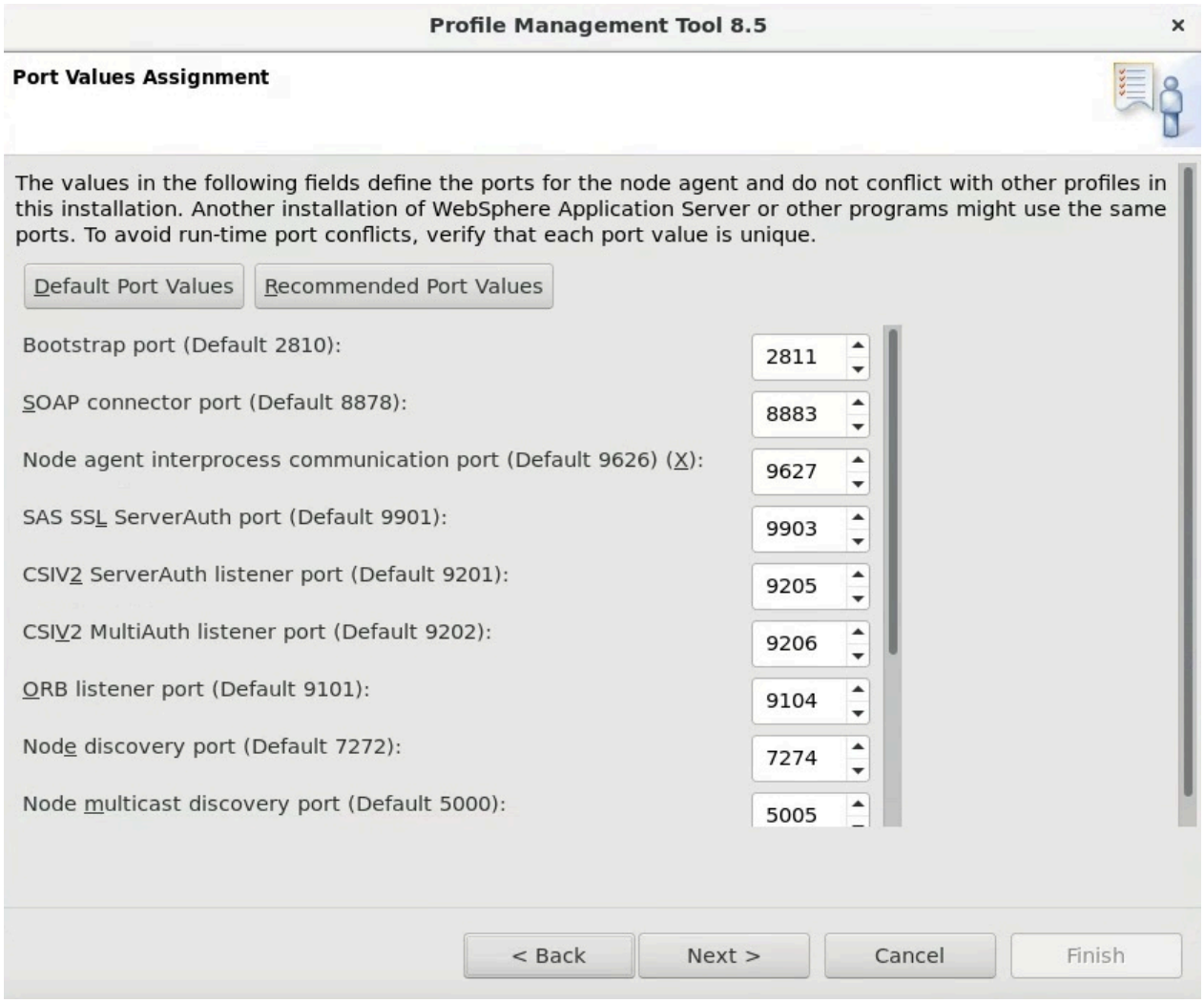

Profile Management Tool 8.5
Profile Name and Location
Specify a profile name and directory path to contain the files for the run-time environment, such as command
configuration files, and log files. Click Browse to select a different directory.
Profile name:
SSL
Profile directory:
/ibm/profiles/SSL
Br
Make this profile the default.
Each installation of WebSphere Application Server always has one default profile. Commands that run with
referring to a specific profile use the default profile. Select this option to make this profile the new default
Important: Deleting the directory a profile is in does not completely delete the profile. Use the manageprof
command to completely delete a profile.
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
< Back
Next >
Cancel
Finish

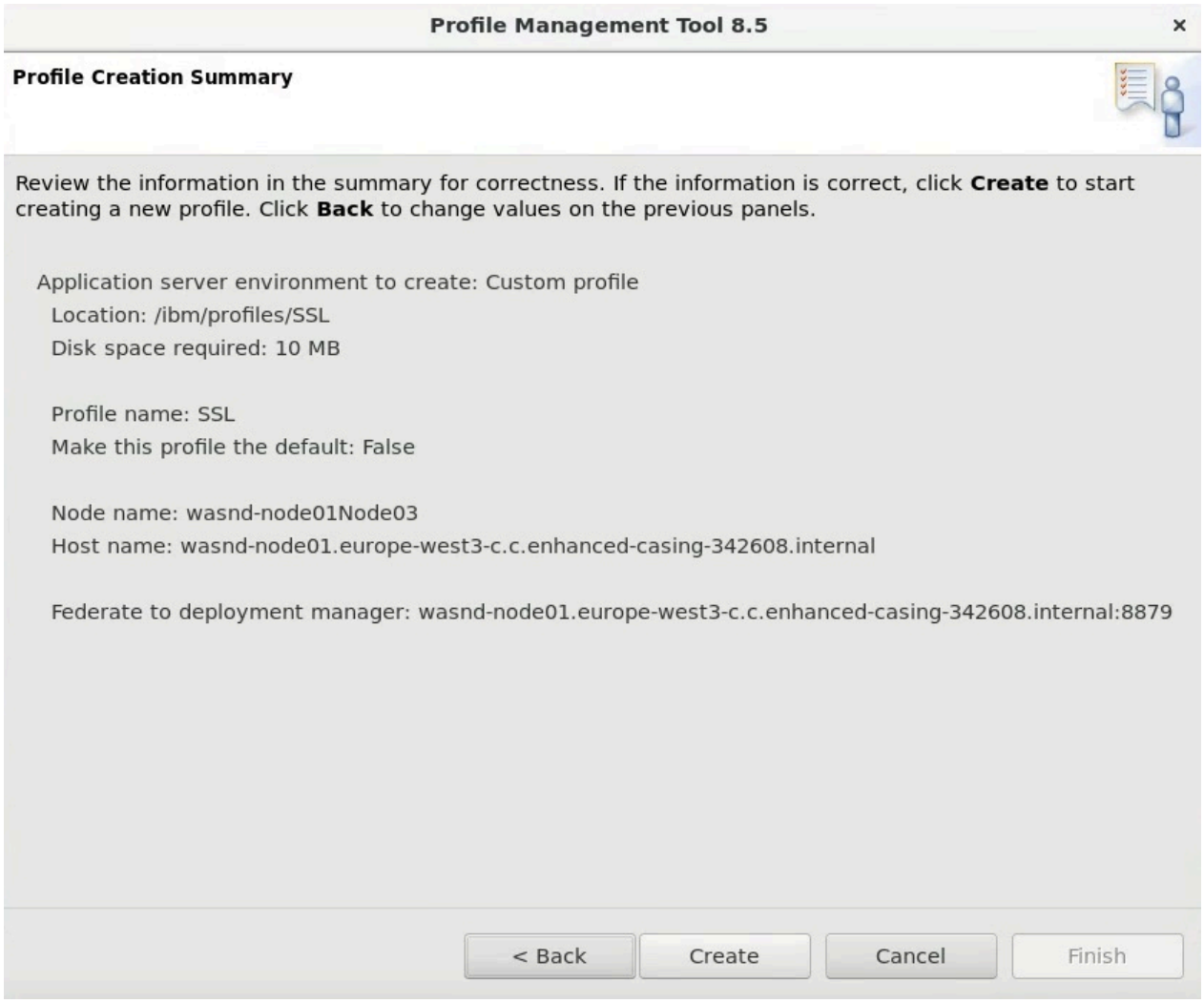

Profile Management Tool 8.5
Node and Host Names
Specify a node name and a host name for this profile.
Node name:
wasnd-node01Node03
Host name:
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Node name: A node name is used for administration. If the node is federated, the name must be unique within
Host name: A host name is the domain name system (DNS) name (short or long) or the IP address of this com
The following naming rules must be used:
- Names must start and end with alphabetic characters (A-Z, a-z), numbers (0-9), and underscores (_) only.
- Names may contain alphabetic characters (A-Z, a-z), numbers (0-9), periods (.), dashes (-) and underscores (_
- Names must not contain spaces or these characters: / \ * , : ; = + ? | < > _% ' " [ ] # $ ^ { } ( )
If you plan to migrate an existing profile to the profile being created, read the premigration considerations artic
View the online information center
< Back
Next >
Cancel
Finish

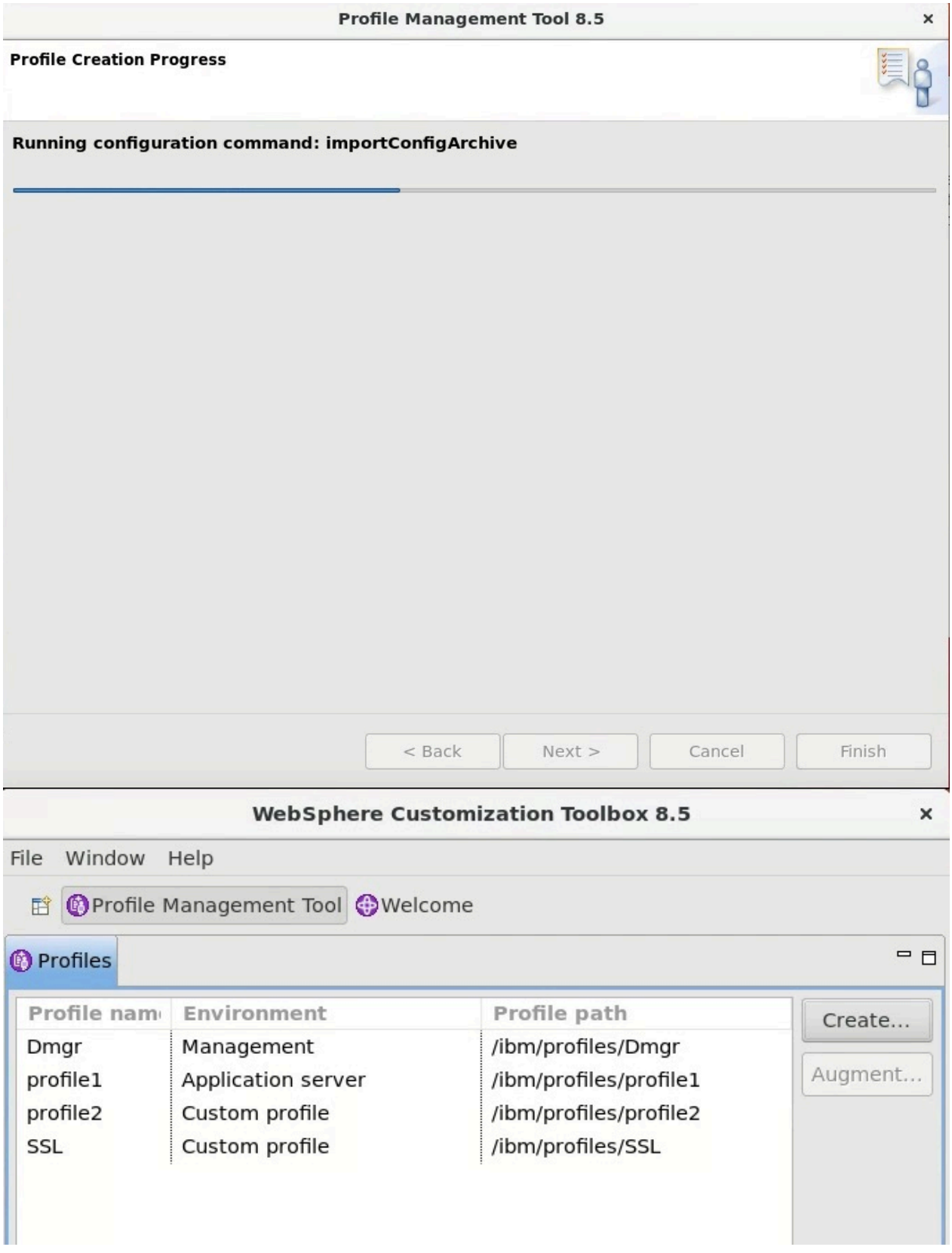

Profile Management Tool 8.5
Federation
Specify the host name or IP address and the SOAP port number for an existing deployment manager.
Federation can occur only if the deployment manager is running.
Deployment manager host name or IP address:
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Deployment manager SOAP port number (Default 8879):
8879
Deployment manager authentication
Provide a user name and password that can be authenticated, if administrative security is enabled on the deployment manager.
User name:
wasadmin
Password:
< Back
Next >
Cancel
Finish

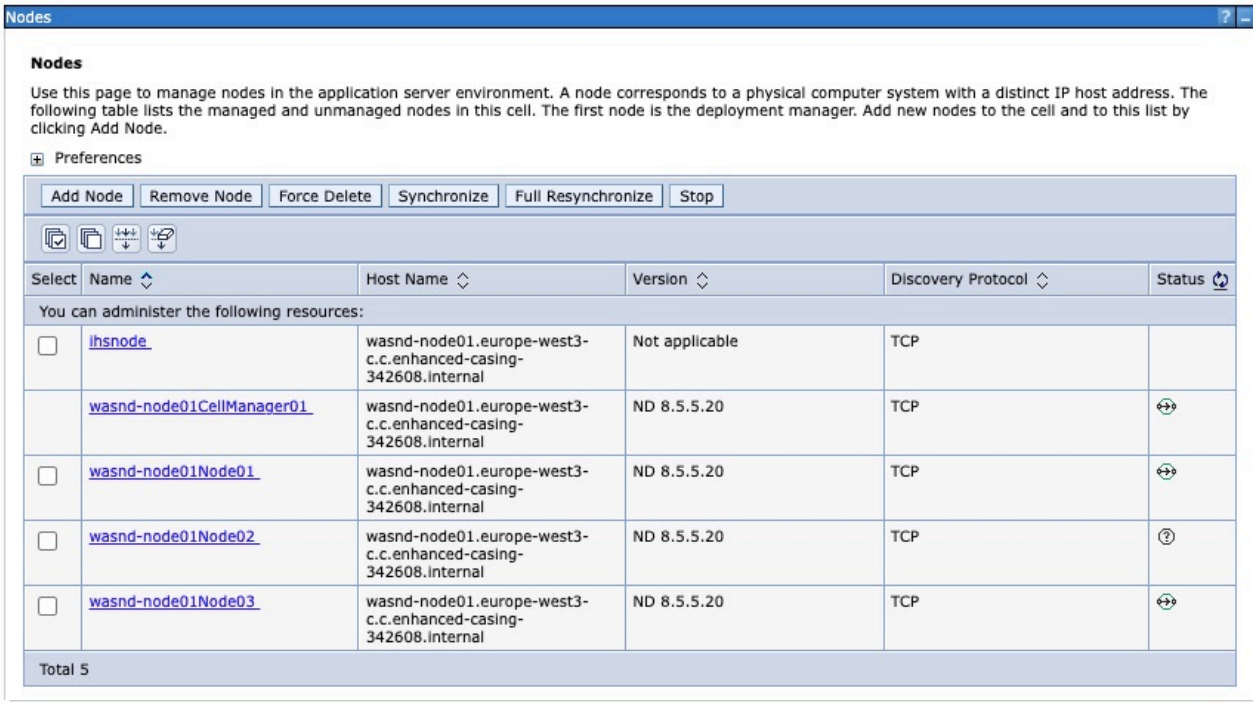

Profile Management Tool 8.5
Security Certificate (Part 1)
Choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, proceed to Part 2 and provide the certificate information. To import existing certificates from keystores, locate the certificates then proceed to Part 2 and verify the certificate information.
Create a new default personal certificate.
Import an existing default personal certificat
Default personal certificate
Path:
Browse...
Password:
Keystore type:
Keystore alias:
Create a new root signing certificate.
Import an existing root signing certificate.
Root signing certificate
< Back
Next >
Cancel
Finish

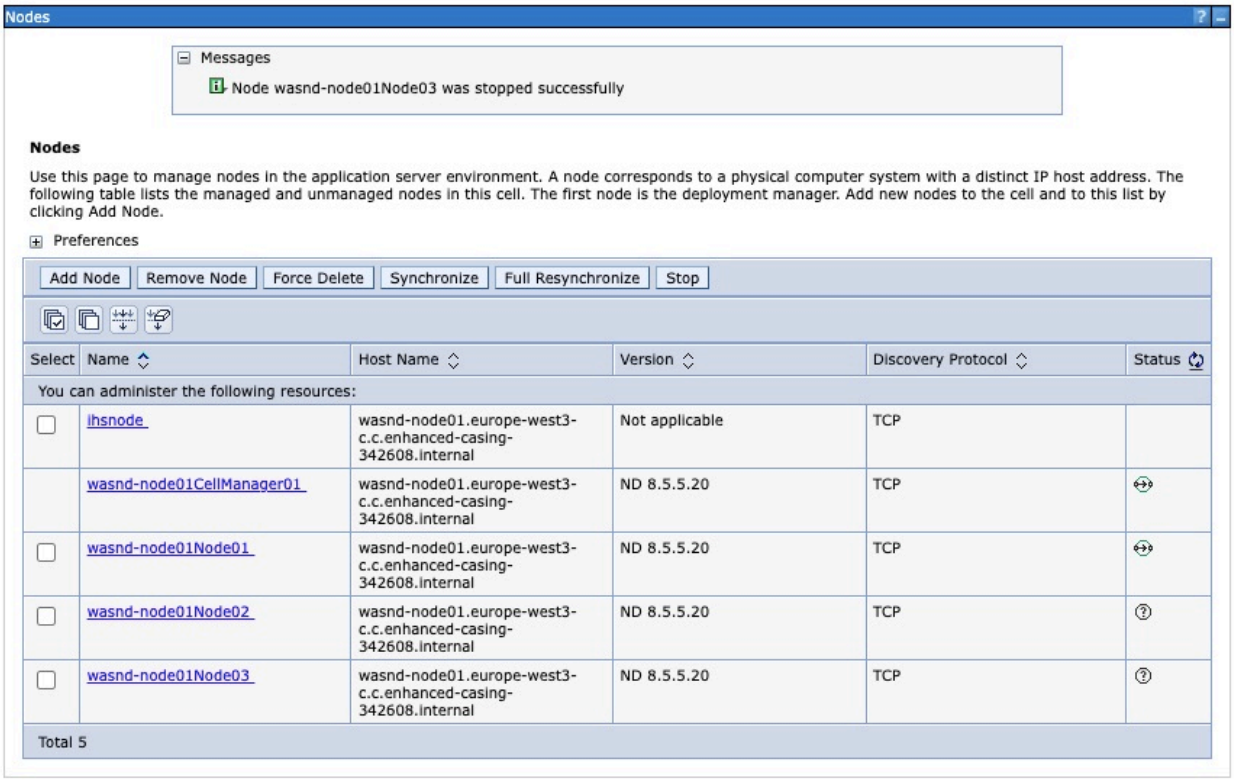

Profile Management Tool 8.5
Security Certificate (Part 2)
Modify the certificate information to create new certificates during profile creation. If you are importing existir
verify whether the selected certificates contain the appropriate information. If the selected certificates do not
Restore Defaults
Default personal certificate (a personal certificate for this profile, public and private key):
Issued to distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=wasnd-node01Node01Cell,ou=
Issued by distinguished name:
cn=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal,ou=Root Certificate,ou=wasnd-nc
Expiration period in years:
1
Root signing certificate (personal certificate for signing other certificates, public and private key):
Expiration period in years:
15
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Port Values Assignment
The values in the following fields define the ports for the node agent and do not conflict with other profiles in this installation. Another installation of WebSphere Application Server or other programs might use the same ports. To avoid run-time port conflicts, verify that each port value is unique.
Default Port Values
Recommended Port Values
Bootstrap port (Default 2810):
2811
SOAP connector port (Default 8878):
8883
Node agent interprocess communication port (Default 9626) (X):
9627
SAS SSL ServerAuth port (Default 9901):
9903
CSIV2 ServerAuth listener port (Default 9201):
9205
CSIV2 MultiAuth listener port (Default 9202):
9206
ORB listener port (Default 9101):
9104
Node discovery port (Default 7272):
7274
Node multicast discovery port (Default 5000):
5005
< Back
Next >
Cancel
Finish


Profile Management Tool 8.5
Profile Creation Summary
Review the information in the summary for correctness. If the information is correct, click Create to start creating a new profile. Click Back to change values on the previous panels.
Application server environment to create: Custom profile
Location: /ibm/profiles/SSL
Disk space required: 10 MB
Profile name: SSL
Make this profile the default: False
Node name: wasnd-node01Node03
Host name: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Federate to deployment manager: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal:8879
< Back
Create
Cancel
Finish

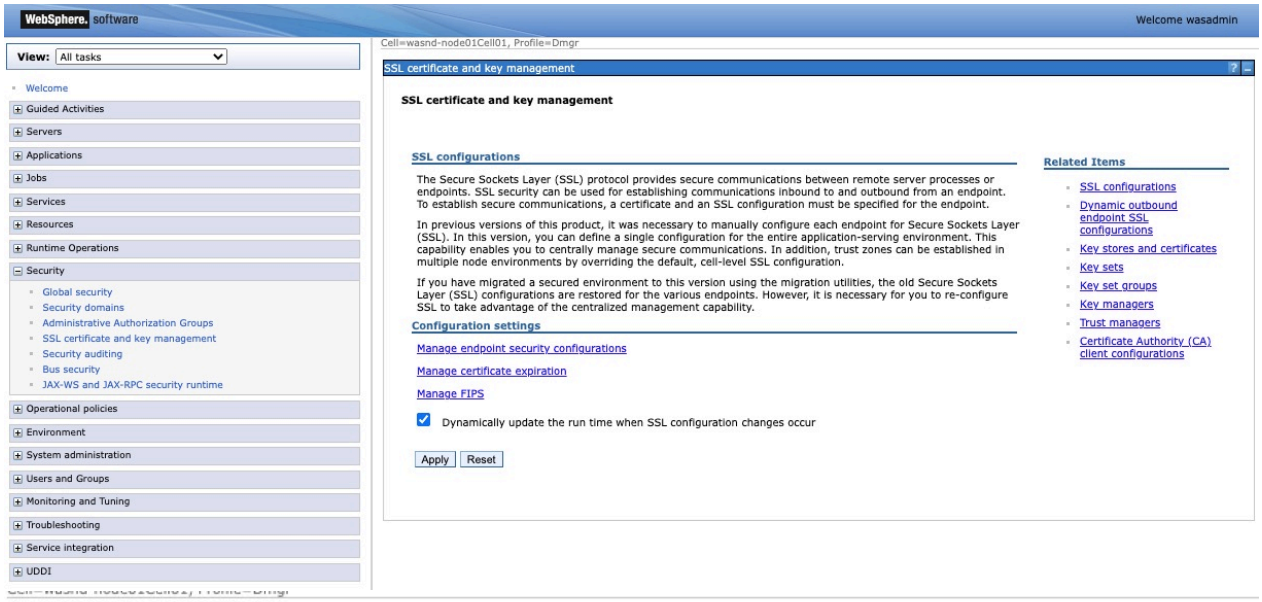

Profile Management Tool 8.5
Profile Creation Progress
Running configuration command: importConfigArchive
< Back
Next >
Cancel
Finish
WebSphere Customization Toolbox 8.5
File
Window
Help
Profile Management Tool
Welcome
Profiles
Profile nam
Environment
Profile path
Dmgr
Management
/ibm/profiles/Dmgr
profile1
Application server
/ibm/profiles/profile1
profile2
Custom profile
/ibm/profiles/profile2
SSL
Custom profile
/ibm/profiles/SSL
Create...
Augment...





Section 3: Examine the node certificates

This new node has a couple of certificates that are associated with it. This section of the exercise uses the administrative console to examine them.



SSL certificate and key management

SSL certificate and key management > **Key stores and certificates**

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

Keystore usages

SSL keystores

Preferences

New... Delete Change password... Exchange signers...

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
☐	CMSKeyStore	CMSKeyStore for web server webserver1.	(cell):wasnd-node01Cell01:(node):ihsnode:(server):webserver1	${CONFIG_ROOT}/cells/wasnd-node01Cell01/nodes/ihsnode/servers/webserver1/plugin-key.kdb
☐	CellDefaultKeyStore	Default key store for wasnd-node01Cell01	(cell):wasnd-node01Cell01	${CONFIG_ROOT}/cells/wasnd-node01Cell01/key.p12
☐	CellDefaultTrustStore	Default trust store for wasnd-node01Cell01	(cell):wasnd-node01Cell01	${CONFIG_ROOT}/cells/wasnd-node01Cell01/trust.p12
☐	NodeDefaultKeyStore	Default key store for wasnd-node01Node01	(cell):wasnd-node01Cell01:(node):wasnd-node01Node01	${CONFIG_ROOT}/cells/wasnd-node01Cell01/nodes/wasnd-node01Node01/key.p12
☐	NodeDefaultKeyStore	Default key store for wasnd-node01Node02	(cell):wasnd-node01Cell01:(node):wasnd-node01Node02	${CONFIG_ROOT}/cells/wasnd-node01Cell01/nodes/wasnd-node01Node02/key.p12

Cell=wasnd-node01Cell01, Profile=Dmgr

SSL certificate and key management

SSL certificate and key management > **Key stores and certificates** > **NodeDefaultKeyStore**

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

General Properties

Name
NodeDefaultKeyStore

Description
Default key store for wasnd-node01Node03

Management scope
(cell):wasnd-node01Cell01:(node):wasnd-node01Node03

Path
${CONFIG_ROOT}/cells/wasnd-node01Cell01/nodes/wasnd-node01Node03/key.p12

* Password

Type
PKCS12

Remotely managed
Host list

Read only

Initialize at startup

Enable cryptographic operations on hardware device

Apply OK Reset Cancel

Additional Properties

- Signer certificates
- Personal certificates
- Personal certificate requests
- Custom properties

Cell=wasnd-node01Cell01, Profile=Dmgr

SSL certificate and key management

SSL certificate and key management > **Key stores and certificates** > **NodeDefaultKeyStore** > **Personal certificates**

Manages personal certificates.

Preferences

Create Delete Receive from a certificate authority... Replace... Extract... Import... Export... Revoke... Renew

Select		Alias	Issued To	Issued By	Serial Number	Expiration
You can administer the following resources:						
		default	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=wasnd-node01Node01Cell, OU=wasnd-node01Node03, O=IBM, C=US	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US	15723727026053	Valid from Mar 3, 2022 to Mar 3, 2023.
			CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US	13204361536190	Valid from Mar 2, 2022 to Feb 26, 2037.
Total 2						

Cell=wasnd-node01Cell01, Profile=Dmgr

SSL certificate and key management

SSL certificate and key management > **Key stores and certificates** > **NodeDefaultKeyStore** > **Personal certificates** > **default**

Manages personal certificates.

General Properties

Alias
default

Version
X509 V3

Key size
2048 bits

Serial number
15723727026053

Validity period
Valid from Mar 3, 2022 to Mar 3, 2023.

Issued to
CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=wasnd-node01Node01Cell, OU=wasnd-node01Node03, O=IBM, C=US

Issued by
CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US

Fingerprint (SHA digest)
59:CE:F9:53:E7:6F:7D:5D:9B:AE:47:6B:39:8E:19:76:57:E2:7B:FB

Signature algorithm
SHA256withRSA(1.2.840.113549.1.1.11)

Key Usage

Extended Key Usage
ServerAuth_Id(1.3.6.1.5.5.7.3.1),ClientAuth_Id(1.3.6.1.5.5.7.3.2)

DNS name
wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal

Cell=wasnd-node01Cell01, Profile=Dmgr

SSL certificate and key management

SSL certificate and key management > **Key stores and certificates** > **NodeDefaultKeyStore** > **Signer certificates**

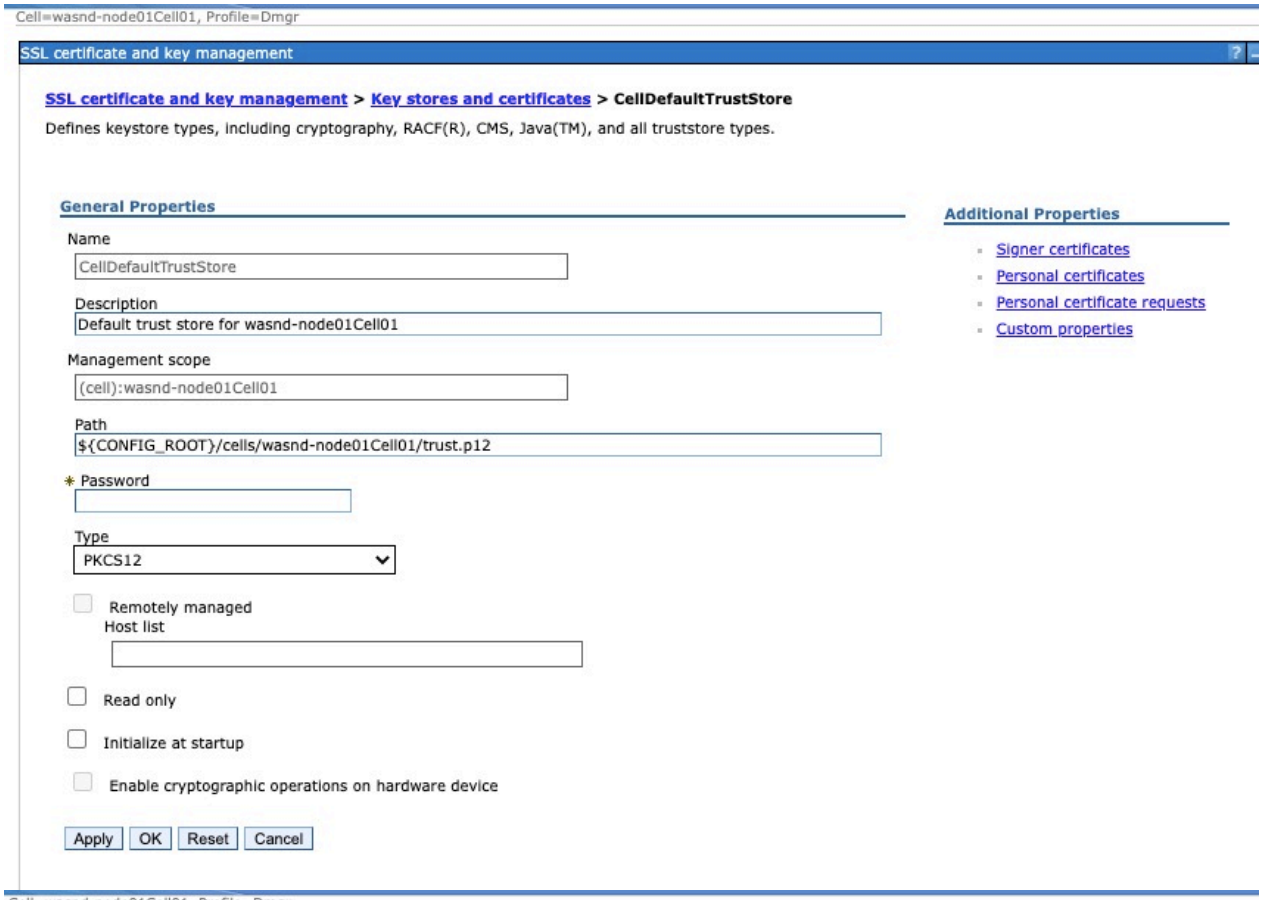
Manages signer certificates in key stores.

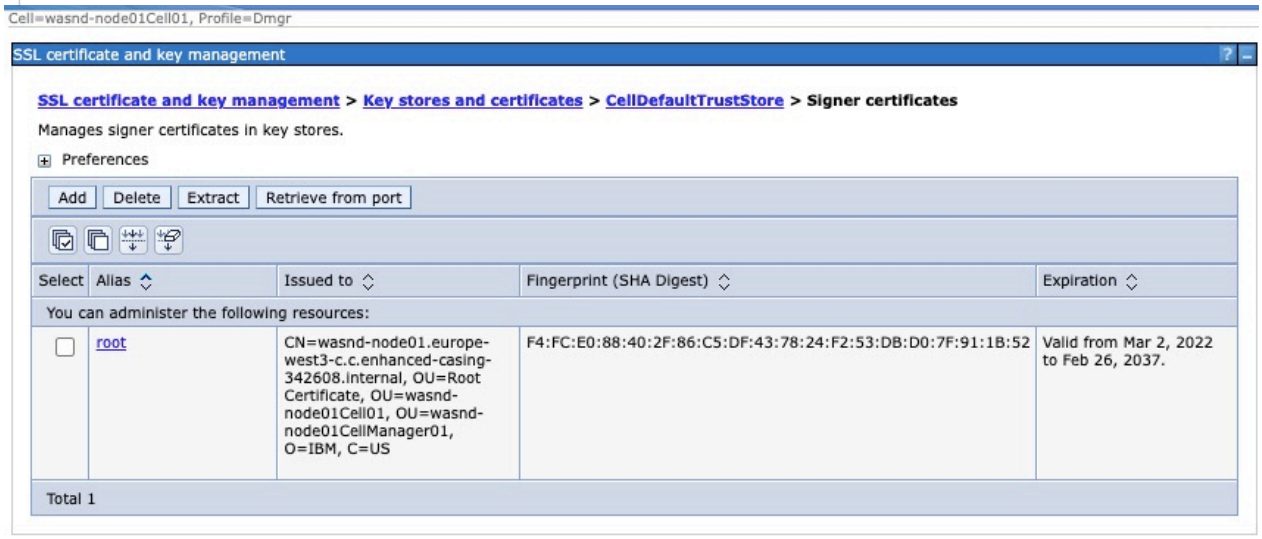
Preferences

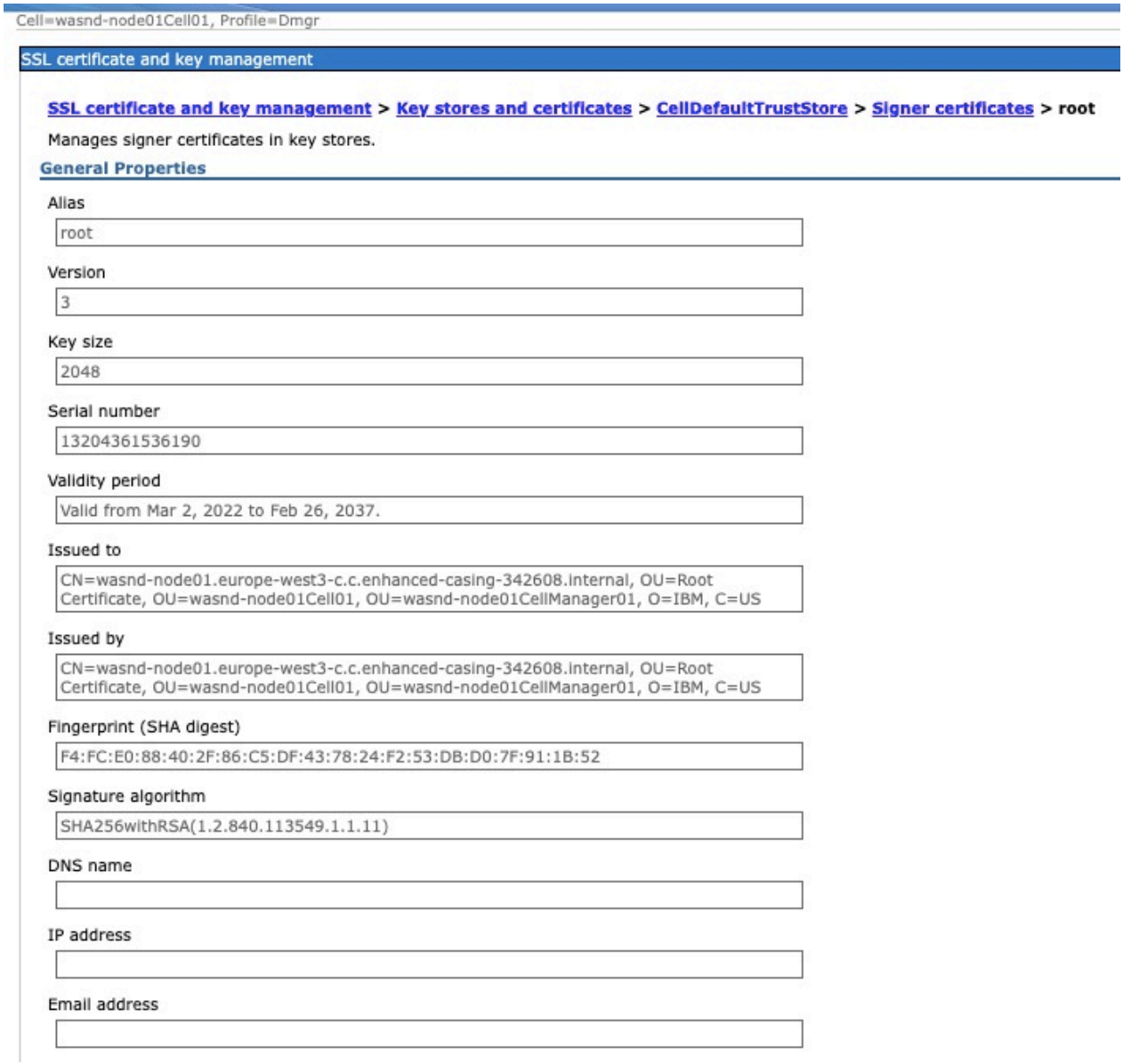
Add | Delete | Extract | Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
None				

Total 0

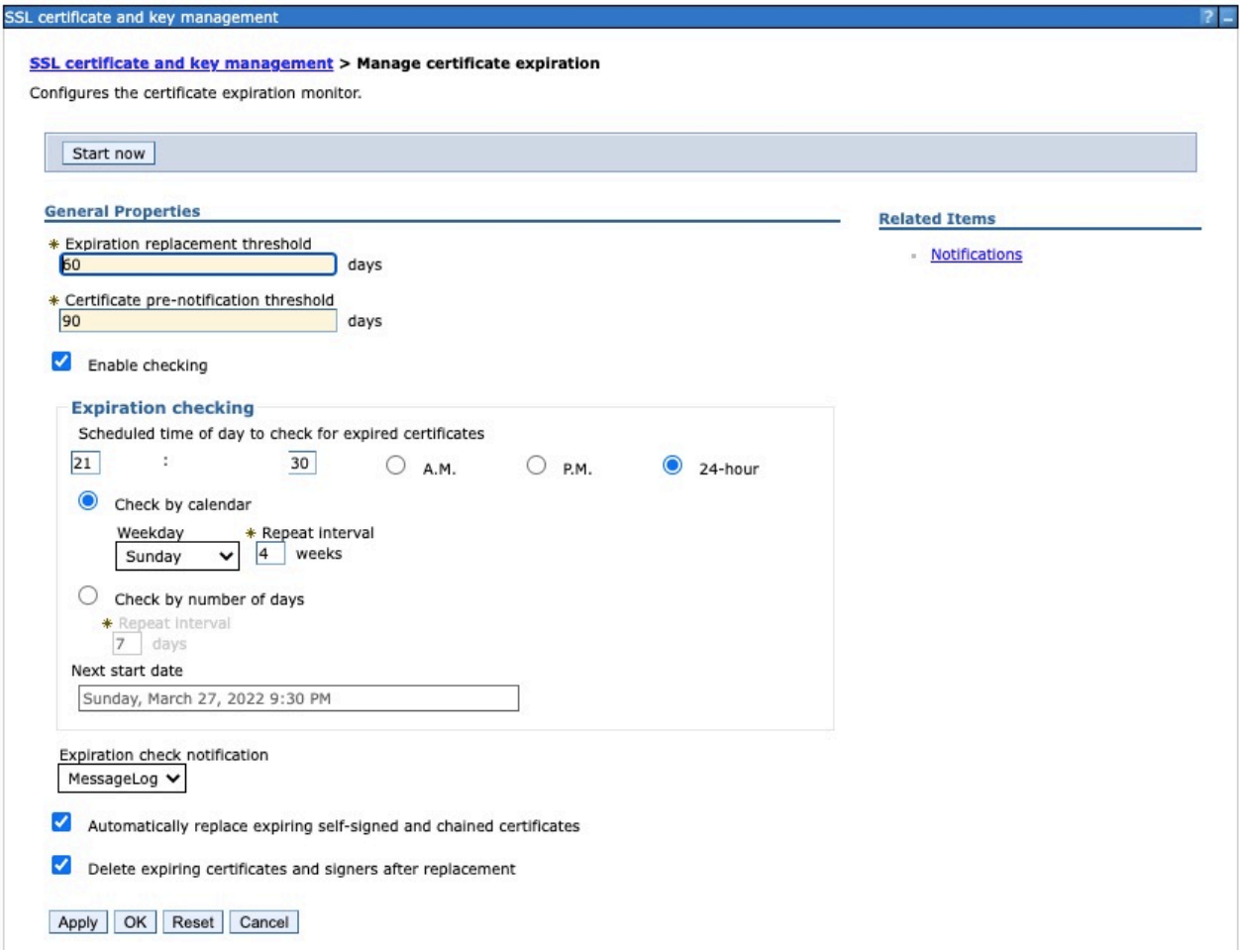

Cell=wasnd-node01Cell01, Profile=Dmgr
SSL certificate and key management
SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore
Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.
General Properties
Name
CellDefaultTrustStore
Description
Default trust store for wasnd-node01Cell01
Management scope
(cell):wasnd-node01Cell01
Path
${CONFIG_ROOT}/cells/wasnd-node01Cell01/trust.p12
* Password
Type
PKCS12
Remotely managed
Host list
Read only
Initialize at startup
Enable cryptographic operations on hardware device
Apply
OK
Reset
Cancel
Additional Properties
Signer certificates
Personal certificates
Personal certificate requests
Custom properties

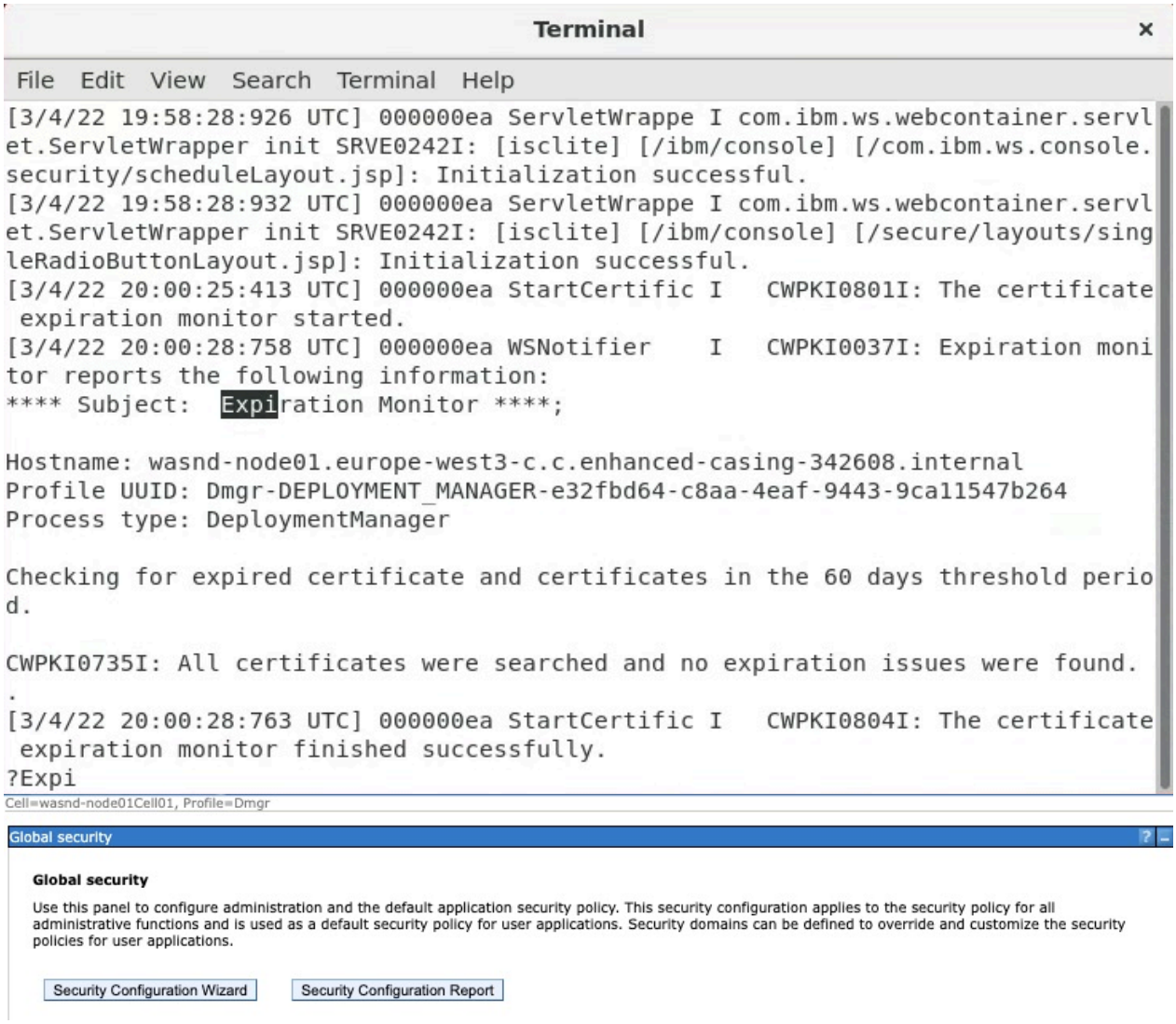

Cell=wasnd-node01Cell01, Profile=Dmgr
SSL certificate and key management
SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates
Manages signer certificates in key stores.
Preferences
Add
Delete
Extract
Retrieve from port
Select
Alias
Issued to
Fingerprint (SHA Digest)
Expiration
You can administer the following resources:
root
CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US
F4:FC:E0:88:40:2F:86:C5:DF:43:78:24:F2:53:DB:D0:7F:91:1B:52
Valid from Mar 2, 2022 to Feb 26, 2037.
Total 1

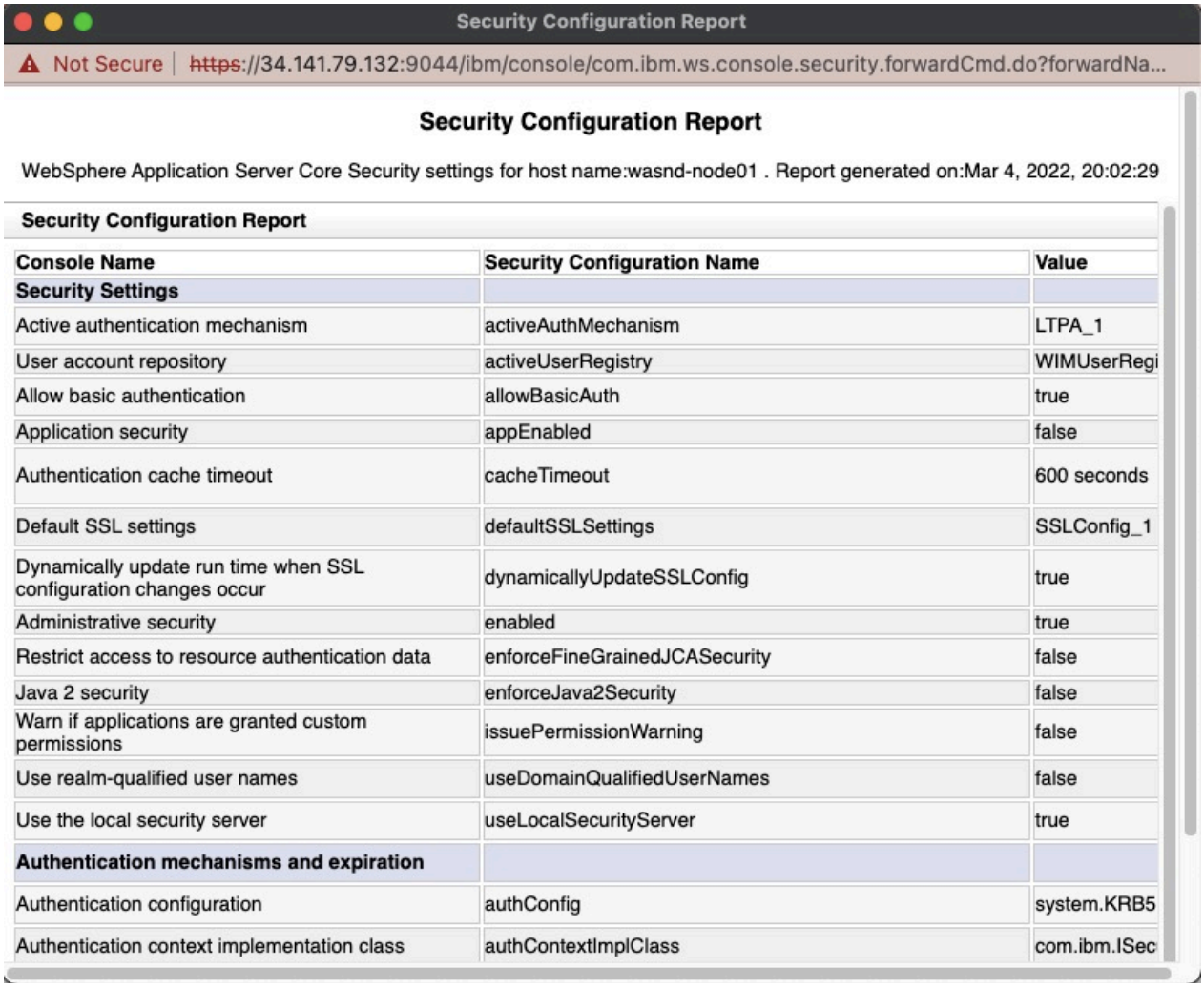


Section 4: Examine certificate expiration and updating

Since the personal certificates have a life span of only one year, administrators must be aware that these certificates expire. Fortunately, WebSphere has a built-in mechanism to automatically renew these certificates when they are about to expire. And, since the signer certificates remain the same, it is not necessary to propagate anything new to the remote nodes or plug-in.


SSL certificate and key management
SSL certificate and key management > Manage certificate expiration
Configures the certificate expiration monitor.
Start now
General Properties
Expiration replacement threshold
60
days
Certificate pre-notification threshold
90
days
Enable checking
Expiration checking
Scheduled time of day to check for expired certificates
21
:
30
A.M.
P.M.
24-hour
Check by calendar
Weekday
Sunday
Repeat interval
4
weeks
Check by number of days
Repeat interval
7
days
Next start date
Sunday, March 27, 2022 9:30 PM
Expiration check notification
MessageLog
Automatically replace expiring self-signed and chained certificates
Delete expiring certificates and signers after replacement
Apply
OK
Reset
Cancel
Related Items
Notifications


Terminal
File Edit View Search Terminal Help
[3/4/22 19:58:28:926 UTC] 000000ea ServletWrappe I com.ibm.ws.webcontainer.servl
et.ServletWrapper init SRVE0242I: [isclite] [/ibm/console] [/com.ibm.ws.console.
security/scheduleLayout.jsp]: Initialization successful.
[3/4/22 19:58:28:932 UTC] 000000ea ServletWrappe I com.ibm.ws.webcontainer.servl
et.ServletWrapper init SRVE0242I: [isclite] [/ibm/console] [/secure/layouts/sing
leRadioButtonLayout.jsp]: Initialization successful.
[3/4/22 20:00:25:413 UTC] 000000ea StartCertific I CWPKI0801I: The certificate
expiration monitor started.
[3/4/22 20:00:28:758 UTC] 000000ea WSNotifier I CWPKI0037I: Expiration moni
tor reports the following information:
**** Subject: Expiration Monitor ****;
Hostname: wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal
Profile UUID: Dmgr-DEPLOYMENT_MANAGER-e32fbd64-c8aa-4eaf-9443-9ca11547b264
Process type: DeploymentManager
Checking for expired certificate and certificates in the 60 days threshold perio
d.
CWPKI0735I: All certificates were searched and no expiration issues were found.
.
[3/4/22 20:00:28:763 UTC] 000000ea StartCertific I CWPKI0804I: The certificate
expiration monitor finished successfully.
?Expi
Cell=wasnd-node01Cell01, Profile=Dmgr
Global security
Global security
Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.
Security Configuration Wizard
Security Configuration Report

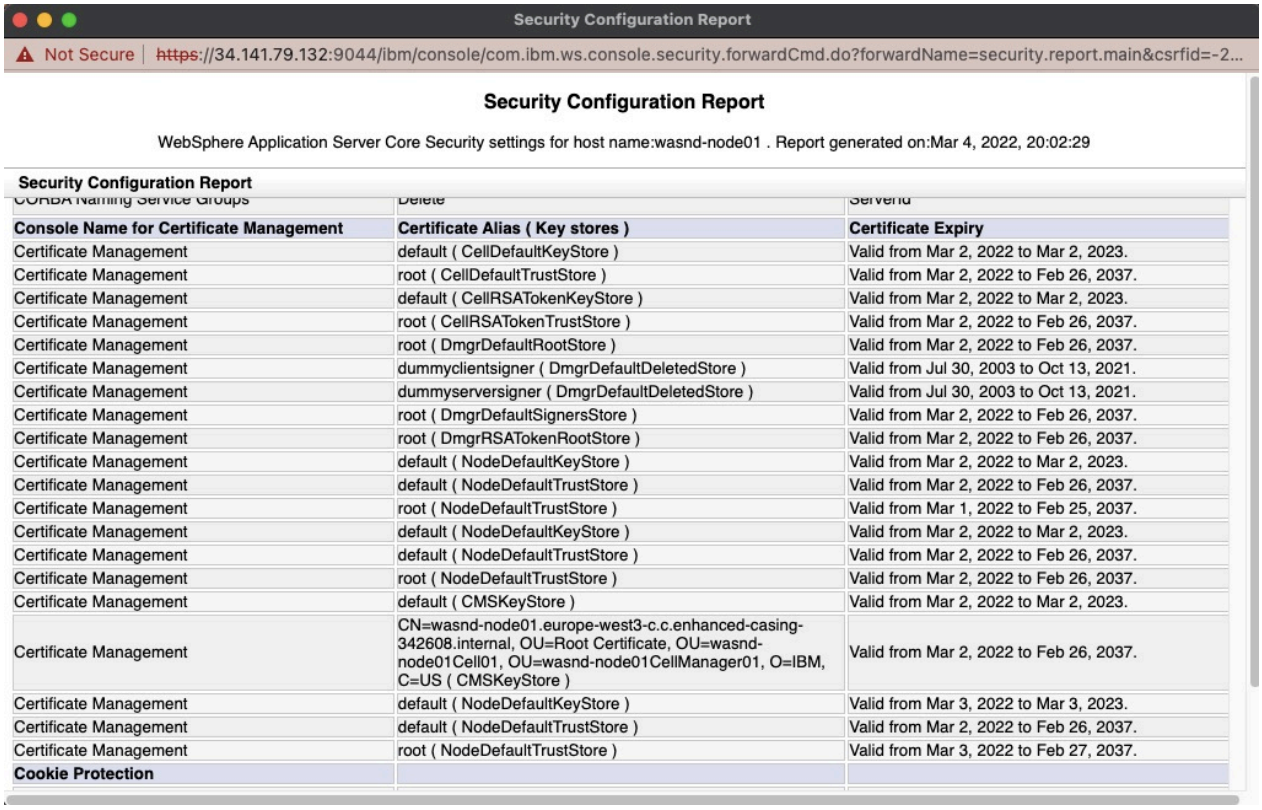


Security Configuration Report

WebSphere Application Server Core Security settings for host name:wasnd-node01 . Report generated on:Mar 4, 2022, 20:02:29

Security Configuration Report

Console Name	Security Configuration Name	Value
Security Settings		
Active authentication mechanism	activeAuthMechanism	LTPA_1
User account repository	activeUserRegistry	WIMUserRegi
Allow basic authentication	allowBasicAuth	true
Application security	appEnabled	false
Authentication cache timeout	cacheTimeout	600 seconds
Default SSL settings	defaultSSLSettings	SSLConfig_1
Dynamically update run time when SSL configuration changes occur	dynamicallyUpdateSSLConfig	true
Administrative security	enabled	true
Restrict access to resource authentication data	enforceFineGrainedJCASecurity	false
Java 2 security	enforceJava2Security	false
Warn if applications are granted custom permissions	issuePermissionWarning	false
Use realm-qualified user names	useDomainQualifiedUserNames	false
Use the local security server	useLocalSecurityServer	true
Authentication mechanisms and expiration		
Authentication configuration	authConfig	system.KRB5
Authentication context implementation class	authContextImplClass	com.ibm.ISec



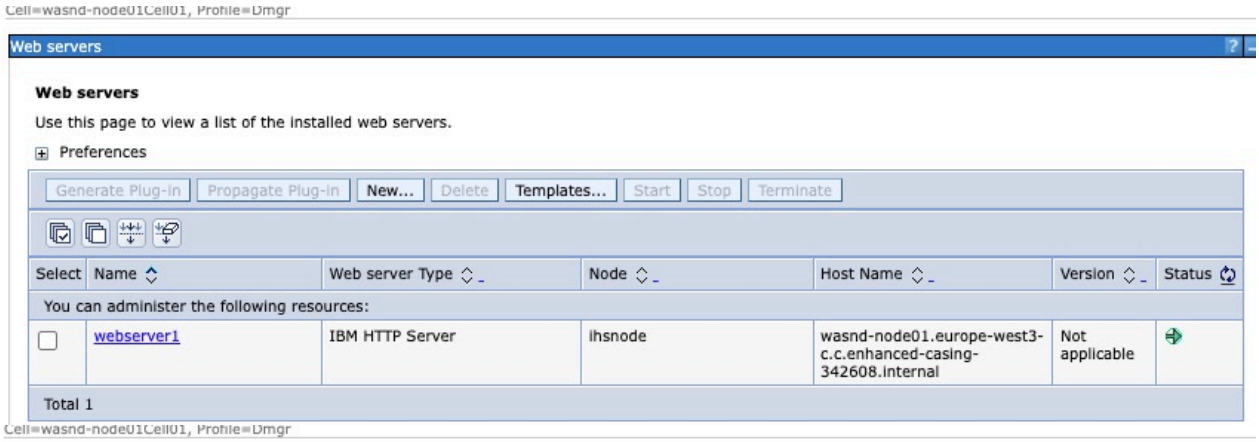
Console Name for Certificate Management	Certificate Alias (Key stores)	Certificate Expiry
Certificate Management	default (CellDefaultKeyStore)	Valid from Mar 2, 2022 to Mar 2, 2023.
Certificate Management	root (CellDefaultTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	default (CellRSATokenKeyStore)	Valid from Mar 2, 2022 to Mar 2, 2023.
Certificate Management	root (CellRSATokenTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	root (DmgrDefaultRootStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	dummyclientsigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 to Oct 13, 2021.
Certificate Management	dummyserversigner (DmgrDefaultDeletedStore)	Valid from Jul 30, 2003 to Oct 13, 2021.
Certificate Management	root (DmgrDefaultSignersStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	root (DmgrRSATokenRootStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	default (NodeDefaultKeyStore)	Valid from Mar 2, 2022 to Mar 2, 2023.
Certificate Management	default (NodeDefaultTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	root (NodeDefaultTrustStore)	Valid from Mar 1, 2022 to Feb 25, 2037.
Certificate Management	default (NodeDefaultKeyStore)	Valid from Mar 2, 2022 to Mar 2, 2023.
Certificate Management	default (NodeDefaultTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	root (NodeDefaultTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	default (CMSKeyStore)	Valid from Mar 2, 2022 to Mar 2, 2023.
Certificate Management	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US (CMSKeyStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	default (NodeDefaultKeyStore)	Valid from Mar 3, 2022 to Mar 3, 2023.
Certificate Management	default (NodeDefaultTrustStore)	Valid from Mar 2, 2022 to Feb 26, 2037.
Certificate Management	root (NodeDefaultTrustStore)	Valid from Mar 3, 2022 to Feb 27, 2037.
Cookie Protection		

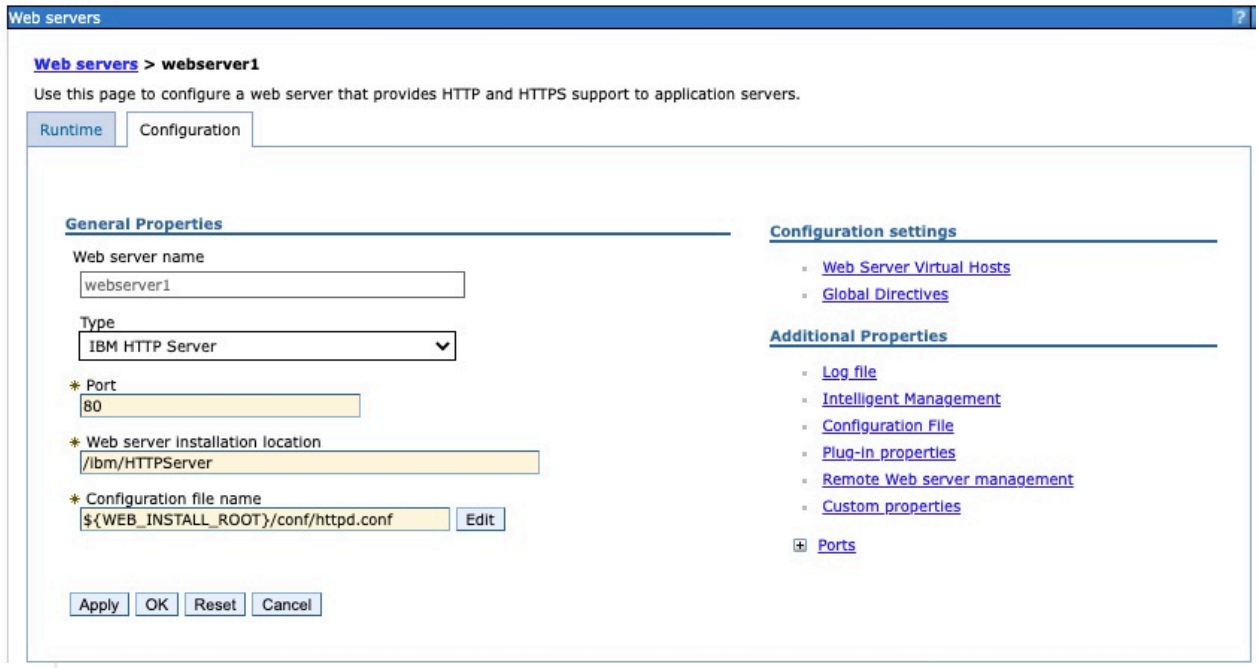
Section 5: Plug-in key ring propagation

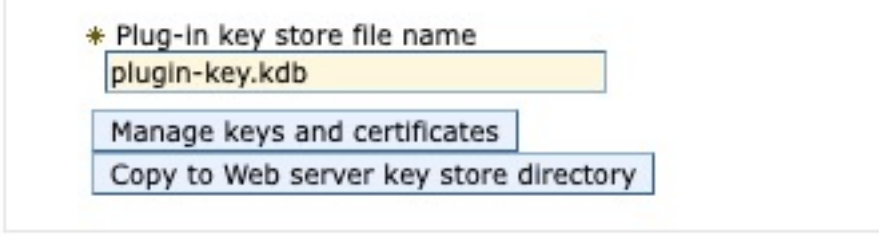
Not only are the processes within cells (deployment managers, node agents, and application servers) required to have certificates and know about other signer certificates, so are the web server plug-ins. To secure the communication between the web server plug-ins and the application servers, the plug-ins and application servers must be able to negotiate an SSL session. They must have personal certificates (by default the application servers use the node personal certificate) and have access to the other signer certificates.

WebSphere is able to make sure that all of the required certificates are available to the web server plug-in by creating the plug-in keystores from within WebSphere. By doing so, WebSphere can make sure that not only does the plug-in have a valid personal certificate, but it also has the necessary cell root signer certificate. At the same time, WebSphere can ensure that the plug-in signer certificate is also available in the cell truststore.

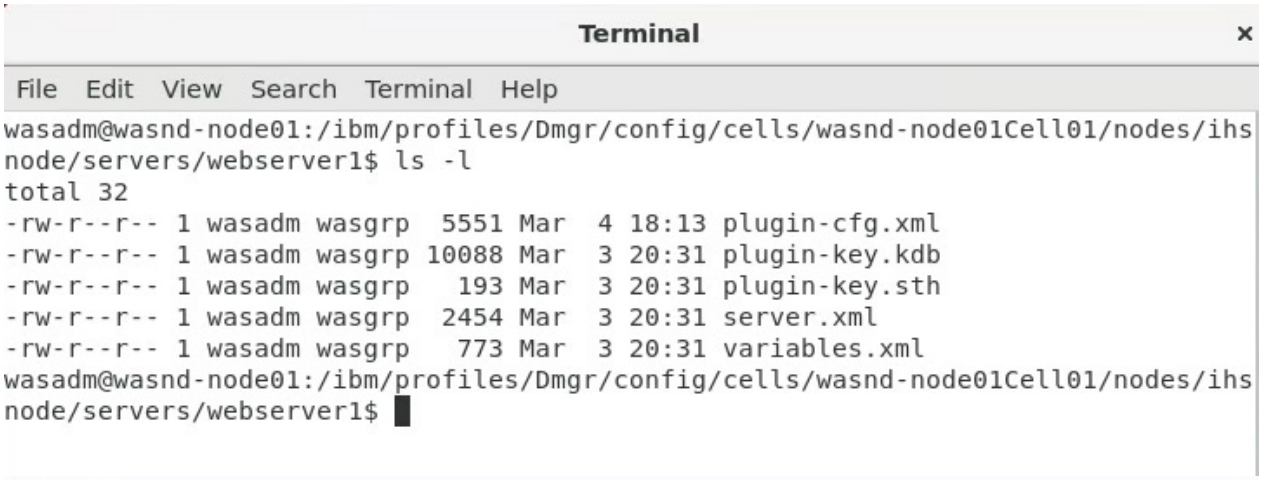
The real problem with this approach is that after WebSphere generates the plug-in keystore, it still must be propagated to the host that is running the web server. The propagation process of plug-in keystores is similar to the propagation of the plugin-cfg.xml file. It is usually done manually, but in some cases can be configured to be done automatically (usually not desirable).

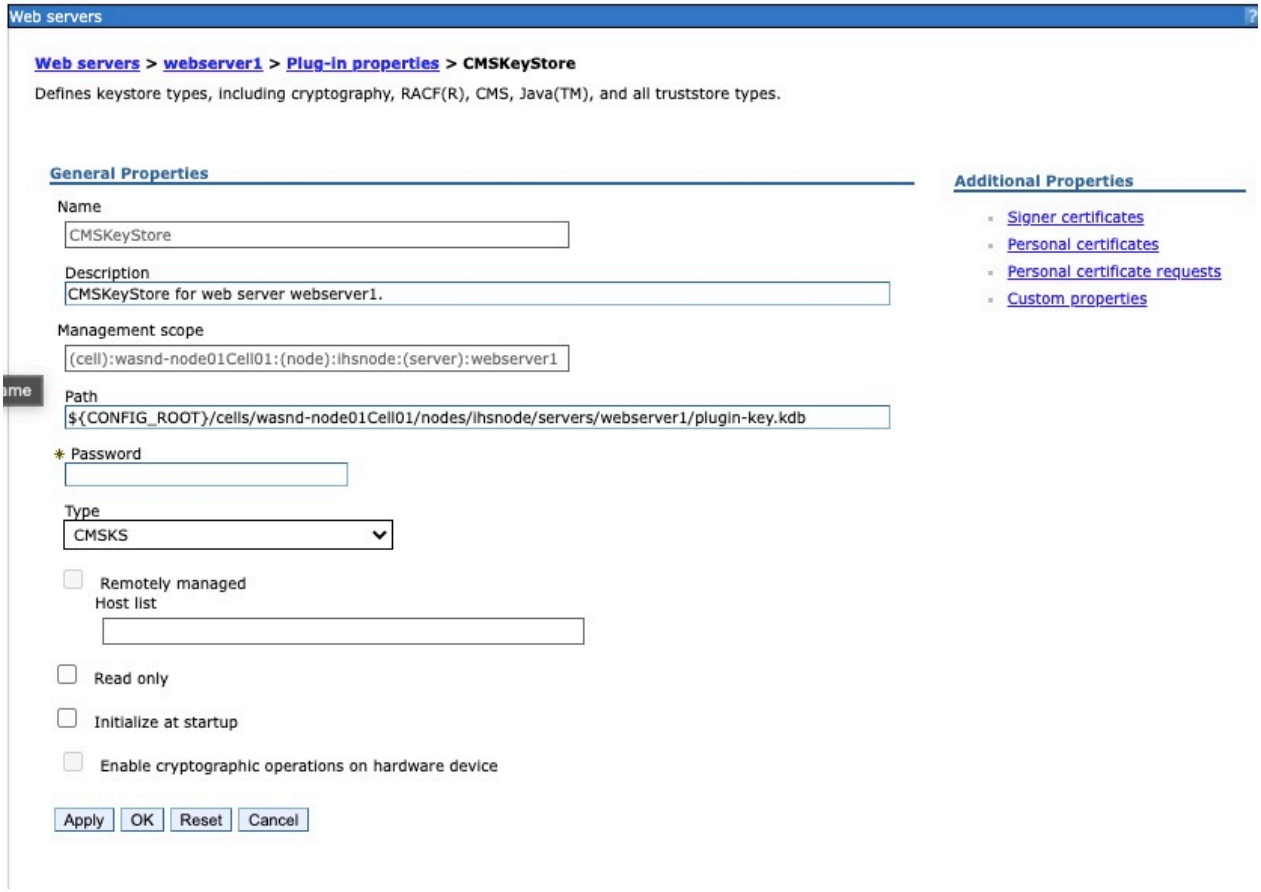






/opt/IBM/WebSphere/AppServer/profiles/Dmgr/config/cells/*<cell-name>*/nodes/*<node-name>*/servers/webserver1/nodes/ihsnode/servers/*<web-server>*


Terminal
File Edit View Search Terminal Help
wasadm@wasnd-node01:/ibm/profiles/Dmgr/config/cells/wasnd-node01Cell01/nodes/ihs
node/servers/webserver1$ ls -l
total 32
-rw-r--r-- 1 wasadm wasgrp 5551 Mar 4 18:13 plugin-cfg.xml
-rw-r--r-- 1 wasadm wasgrp 10088 Mar 3 20:31 plugin-key.kdb
-rw-r--r-- 1 wasadm wasgrp   193 Mar 3 20:31 plugin-key.sth
-rw-r--r-- 1 wasadm wasgrp 2454 Mar 3 20:31 server.xml
-rw-r--r-- 1 wasadm wasgrp   773 Mar 3 20:31 variables.xml
wasadm@wasnd-node01:/ibm/profiles/Dmgr/config/cells/wasnd-node01Cell01/nodes/ihs
node/servers/webserver1$


Web servers
Web servers > webserver1 > Plug-in properties > CMSKeyStore
Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.
General Properties
Name
CMSKeyStore
Description
CMSKeyStore for web server webserver1.
Management scope
(cell):wasnd-node01Cell01:(node):ihsnode:(server):webserver1
Path
${CONFIG_ROOT}/cells/wasnd-node01Cell01/nodes/ihsnode/servers/webserver1/plugin-key.kdb
* Password
Type
CMSKS
Remotely managed
Host list
Read only
Initialize at startup
Enable cryptographic operations on hardware device
Apply
OK
Reset
Cancel
Additional Properties
Signer certificates
Personal certificates
Personal certificate requests
Custom properties

Web servers

Web servers > **webserver1** > **Plug-in properties** > **CMSKeyStore** > **Signer certificates**

Manages signer certificates in key stores.

Preferences

Add | Delete | Extract | Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
☐	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US	CN=wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal, OU=Root Certificate, OU=wasnd-node01Cell01, OU=wasnd-node01CellManager01, O=IBM, C=US	F4:FC:E0:88:40:2F:86:C5:DF:43:78:24:F2:53:DB:D0:7F:91:1B:52	Valid from Mar 2, 2022 to Feb 26, 2037.

Total 1

Web servers

Messages

- PLGC0064I: The plug-in keyring file is propagated from /ibm/profiles/Dmgr/config/cells/wasnd-node01Cell01/nodes/ihsnode/servers/webserver1/plugin-key.kdb to /ibm/WebSphere/Plugins/config/webserver1/plugin-key.kdb on the Web server computer.
- PLGC0069I: The propagation of the plug-in keyring is complete for the Web server. wasnd-node01Cell01.ihsnode.webserver1.
- PLGC0066I: The plug-in stash file is propagated from /ibm/profiles/Dmgr/config/cells/wasnd-node01Cell01/nodes/ihsnode/servers/webserver1/plugin-key.sth to /ibm/WebSphere/Plugins/config/webserver1/plugin-key.sth on the Web server computer.
- PLGC0071I: The propagation of the plug-in stash file is complete for the Web server. wasnd-node01Cell01.ihsnode.webserver1.

Web servers > **webserver1** > **Plug-in properties**

Use this page to configure a web server plug-in. The plug-in passes HTTP requests from a web server to WebSphere(R) application servers.

Runtime | Configuration

Plug-in properties

☐ Ignore DNS failures during Web server startup

* Refresh configuration interval
60 seconds

Repository copy of Web server plug-in files:

* Plug-in configuration file name
plugin-cfg.xml View

☑ Automatically generate the plug-in configuration file

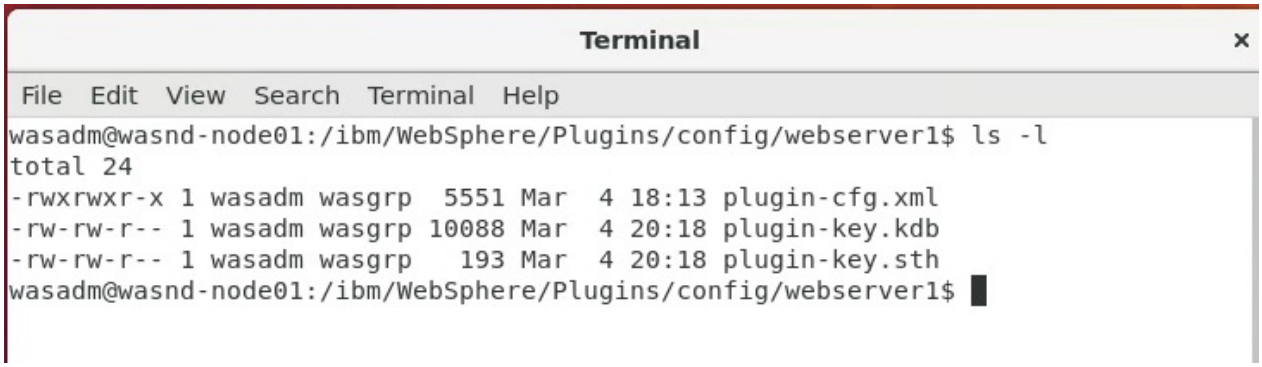
☑ Automatically propagate plug-in configuration file

* Plug-in key store file name
plugin-key.kdb

Manage keys and certificates
Copy to Web server key store directory

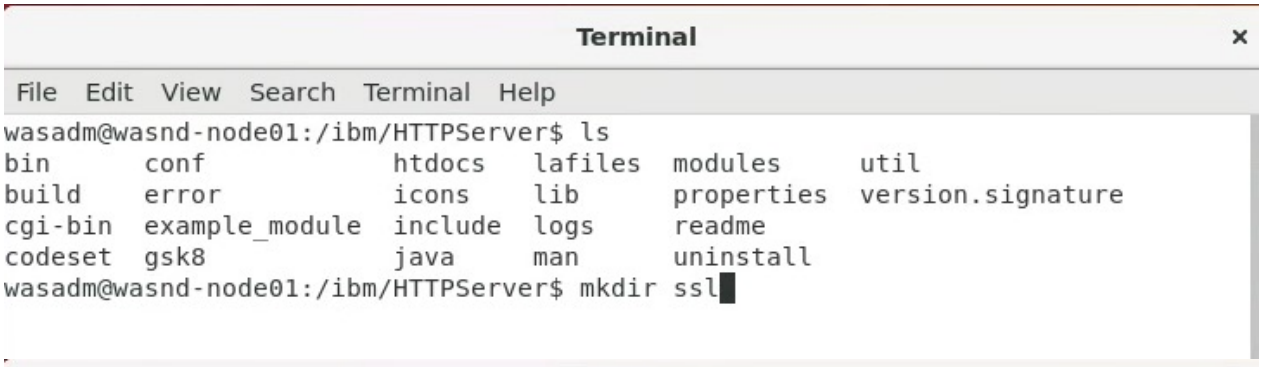
Additional Properties

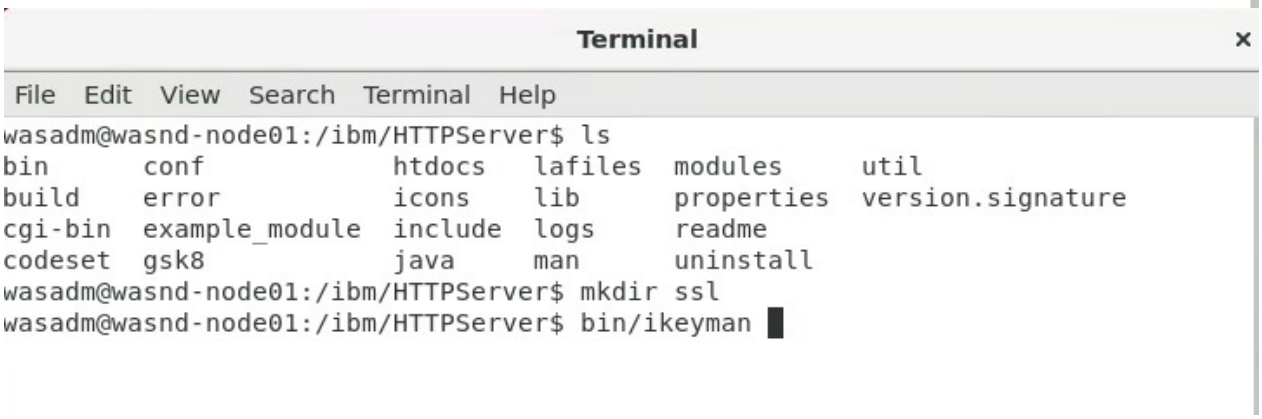
- Request and Response
- Caching
- Request Routing
- Custom Properties

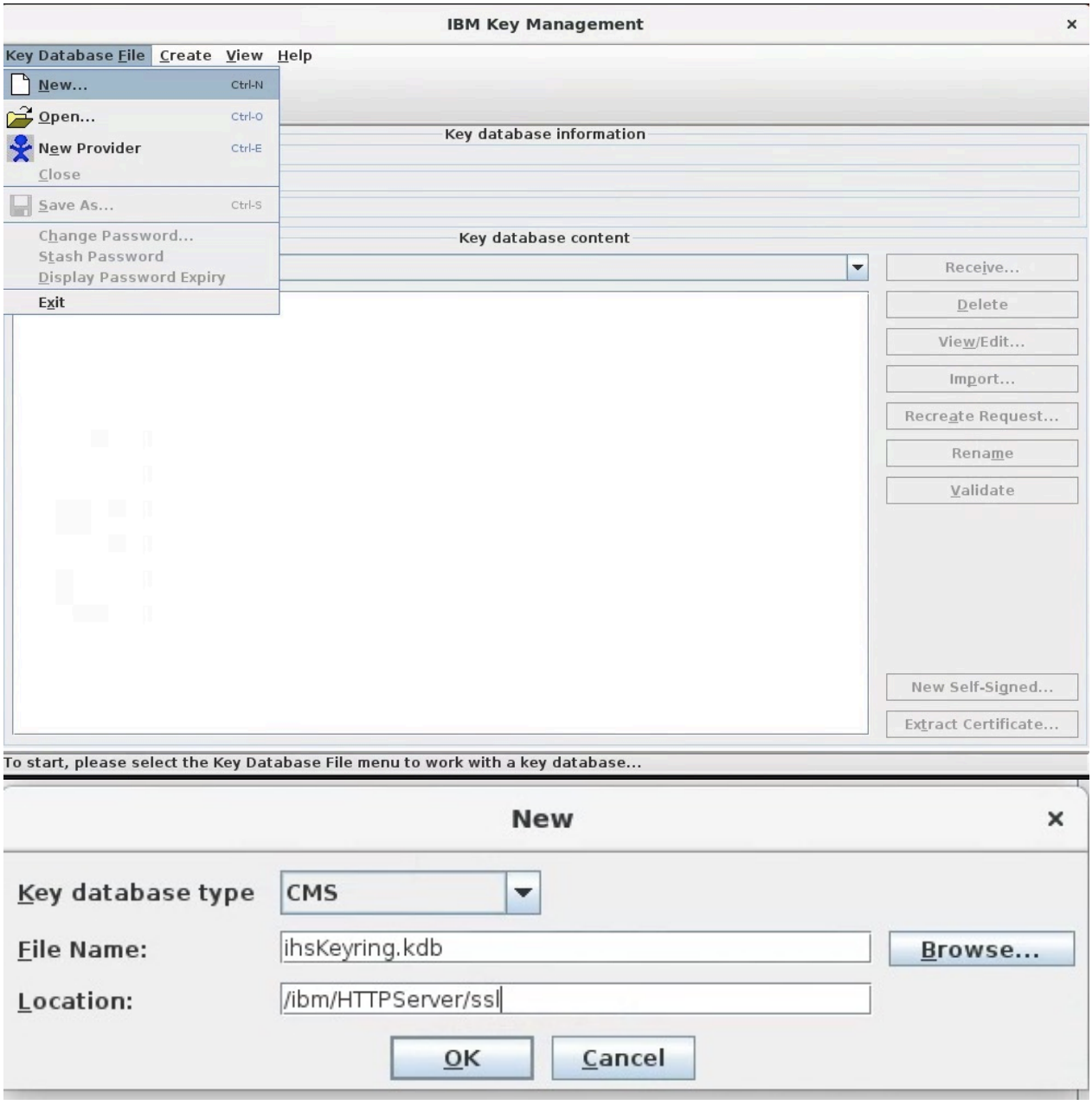


Section 6: Configuring SSL for IBM HTTP Server (optional)

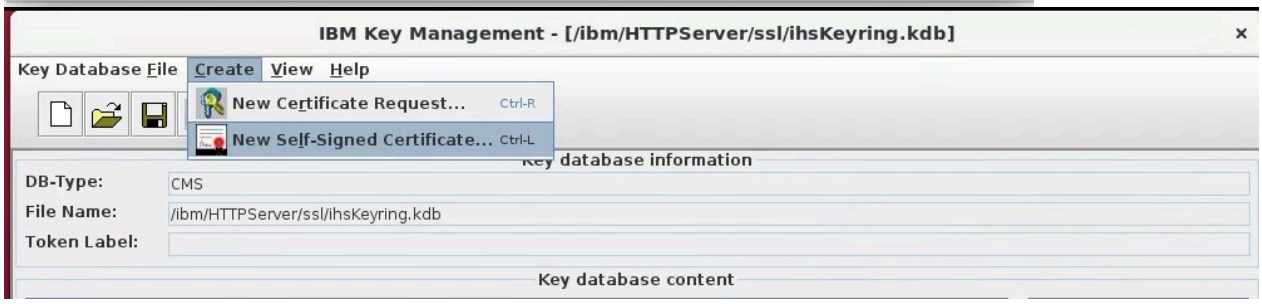
This part of the exercise examines the process of creating a certificate and a key ring for the web server. The steps are used to configure SSL on the connection between the client browser and the web server.

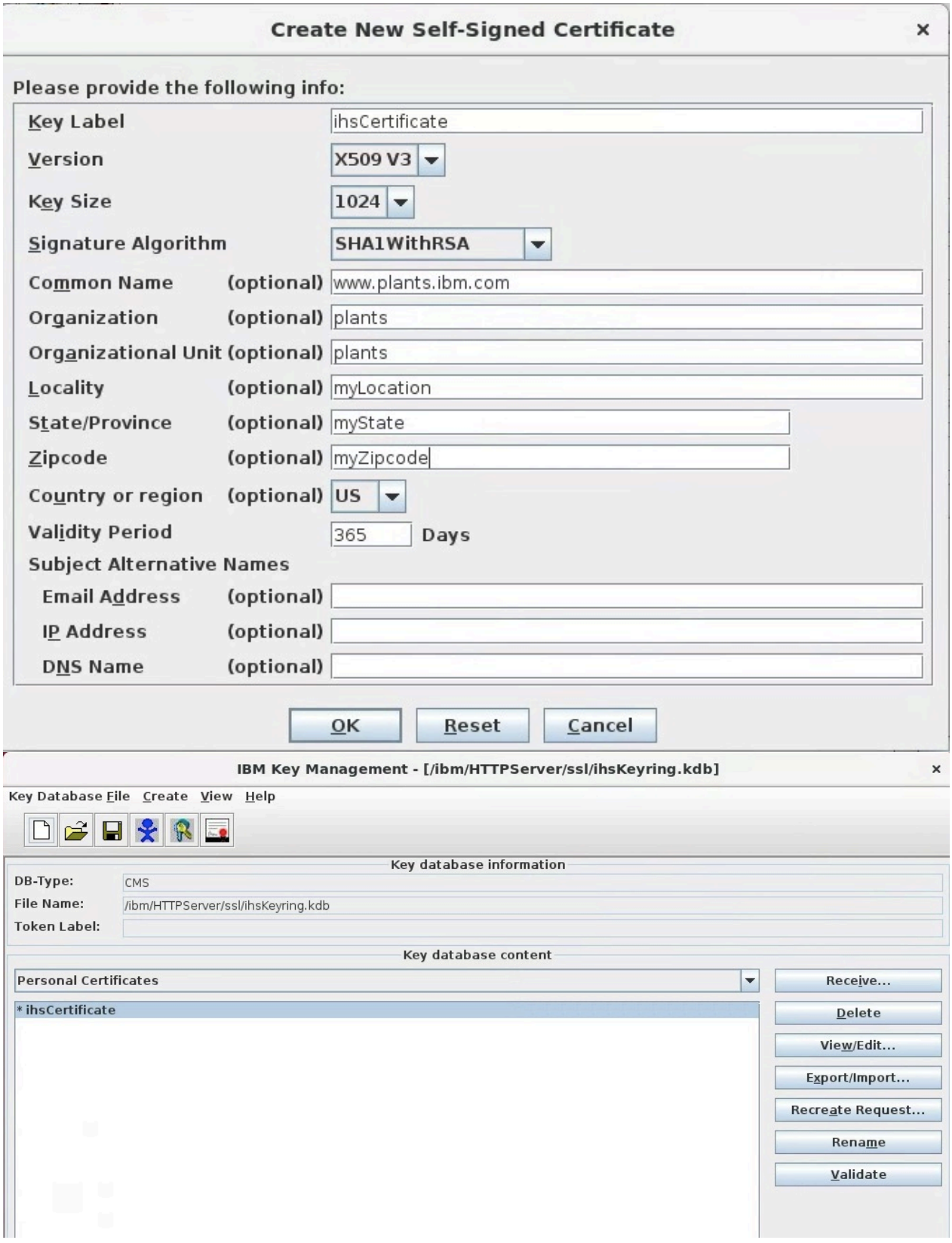


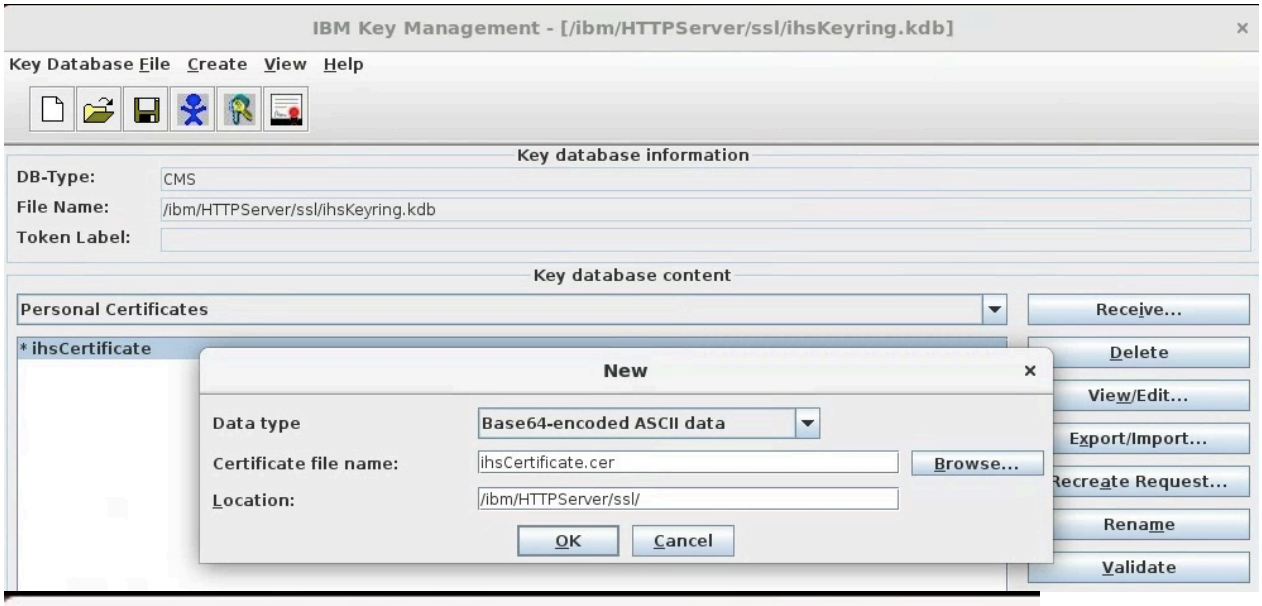



IBM Key Management
Key Database File
Create
View
Help
New... Ctrl-N
Open... Ctrl-O
New Provider Ctrl-E
Close
Save As... Ctrl-S
Change Password...
Stash Password
Display Password Expiry
Exit
Key database information
Key database content
Receive...
Delete
View/Edit...
Import...
Recreate Request...
Rename
Validate
New Self-Signed...
Extract Certificate...
To start, please select the Key Database File menu to work with a key database...
New
Key database type
CMS
File Name:
ihsKeyring.kdb
Browse...
Location:
/ibm/HTTPServer/ssl
OK
Cancel


Password Prompt
Password:
Confirm Password:
Expiration time
60
Days
Stash password to a file
OK
Reset
Cancel


IBM Key Management - [/ibm/HTTPServer/ssl/ihsKeyring.kdb]
Key Database File
Create
View
Help
New Certificate Request... Ctrl-R
New Self-Signed Certificate... Ctrl-L
Key database information
DB-Type:
CMS
File Name:
/ibm/HTTPServer/ssl/ihsKeyring.kdb
Token Label:
Key database content


Create New Self-Signed Certificate
Please provide the following info:
Key Label
ihsCertificate
Version
X509 V3
Key Size
1024
Signature Algorithm
SHA1WithRSA
Common Name (optional)
www.plants.ibm.com
Organization (optional)
plants
Organizational Unit (optional)
plants
Locality (optional)
myLocation
State/Province (optional)
myState
Zipcode (optional)
myZipcode
Country or region (optional)
US
Validity Period
365
Days
Subject Alternative Names
Email Address (optional)
IP Address (optional)
DNS Name (optional)
OK
Reset
Cancel
IBM Key Management - [/ibm/HTTPServer/ssl/ihsKeyring.kdb]
Key Database File
Create
View
Help
Key database information
DB-Type:
CMS
File Name:
/ibm/HTTPServer/ssl/ihsKeyring.kdb
Token Label:
Key database content
Personal Certificates
* ihsCertificate
Receive...
Delete
View/Edit...
Export/Import...
Recreate Request...
Rename
Validate


IBM Key Management - [/ibm/HTTPServer/ssl/ihsKeyring.kdb]
Key Database File Create View Help
Key database information
DB-Type: CMS
File Name: /ibm/HTTPServer/ssl/ihsKeyring.kdb
Token Label:
Key database content
Personal Certificates
* ihsCertificate
Receive...
Delete
View/Edit...
Export/Import...
Recreate Request...
Rename
Validate
New
Data type
Base64-encoded ASCII data
Certificate file name:
ihsCertificate.cer
Browse...
Location:
/ibm/HTTPServer/ssl/
OK
Cancel


IBM Key Manager
Key Database File
Create
View
Help
New... Ctrl-N
Open... Ctrl-O
New Provider Ctrl-E
Close
Save As... Ctrl-S
Change Password...
Stash Password
Display Password Expiry
Exit
hsKeyring.kdb

Terminal

File Edit View Search Terminal Help

```
wasadm@wasnd-node01:/ibm/HTTPServer/ssl$ ls -l
total 20
-rw-r--r-- 1 wasadm wasgrp 1008 Mar  4 20:29 ihsCertificate.cer
-rw-r--r-- 1 wasadm wasgrp 5088 Mar  4 20:27 ihsKeyring.kdb
-rw-r--r-- 1 wasadm wasgrp   80 Mar  4 20:27 ihsKeyring.rdb
-rw-r--r-- 1 wasadm wasgrp  193 Mar  4 20:25 ihsKeyring.sth
wasadm@wasnd-node01:/ibm/HTTPServer/ssl$
```

Terminal

File Edit View Search Terminal Help

```
wasadm@wasnd-node01:/ibm/HTTPServer/ssl$ sudo vi /etc/hosts
```

Terminal

File Edit View Search Terminal Help

```
127.0.0.1 localhost
127.0.0.1 www.plants.ibm.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
169.254.169.254 metadata.google.internal metadata
~
```

Terminal

File Edit View Search Terminal Help

```
wasadm@wasnd-node01:/ibm/HTTPServer/ssl$ sudo vi /etc/hosts
wasadm@wasnd-node01:/ibm/HTTPServer/ssl$ ping www.plants.ibm.com
PING www.plants.ibm.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.035 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.034 ms
```

Terminal

File Edit View Search Terminal Help

```
wasadm@wasnd-node01:/ibm/HTTPServer/conf$ vi httpd.conf
```

Terminal

File Edit View Search Terminal Help

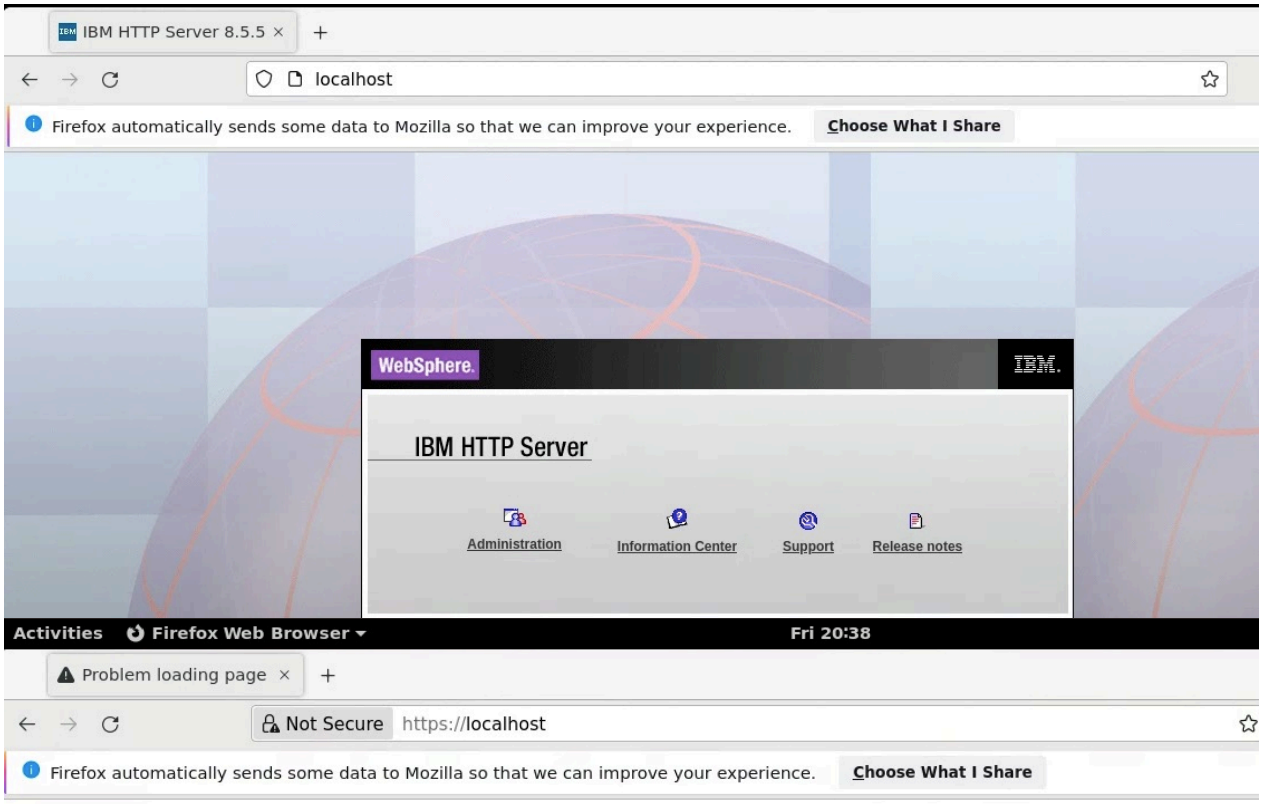
```
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

# Example SSL configuration which supports SSLv3 and TLSv1
# To enable this support:
#   1) Create a key database with ikeyman
#   2) Update the KeyFile directive below to point to that key database
#   3) Uncomment the directives up through the end of the example
#
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
<VirtualHost www.plants.ibm.com:443>
  SSLEnable
</VirtualHost>
KeyFile /ibm/HTTPServer/ssl/ihsKeyring.kdb
SSLDisable
# End of example SSL configuration
```

Section 7: Testing the SSL connection

Terminal

File Edit View Search Terminal Help

```
wasadm@wasnd-node01:/ibm/HTTPServer$ cd bin
wasadm@wasnd-node01:/ibm/HTTPServer/bin$ sudo ./apachectl restart
wasadm@wasnd-node01:/ibm/HTTPServer/bin$
```



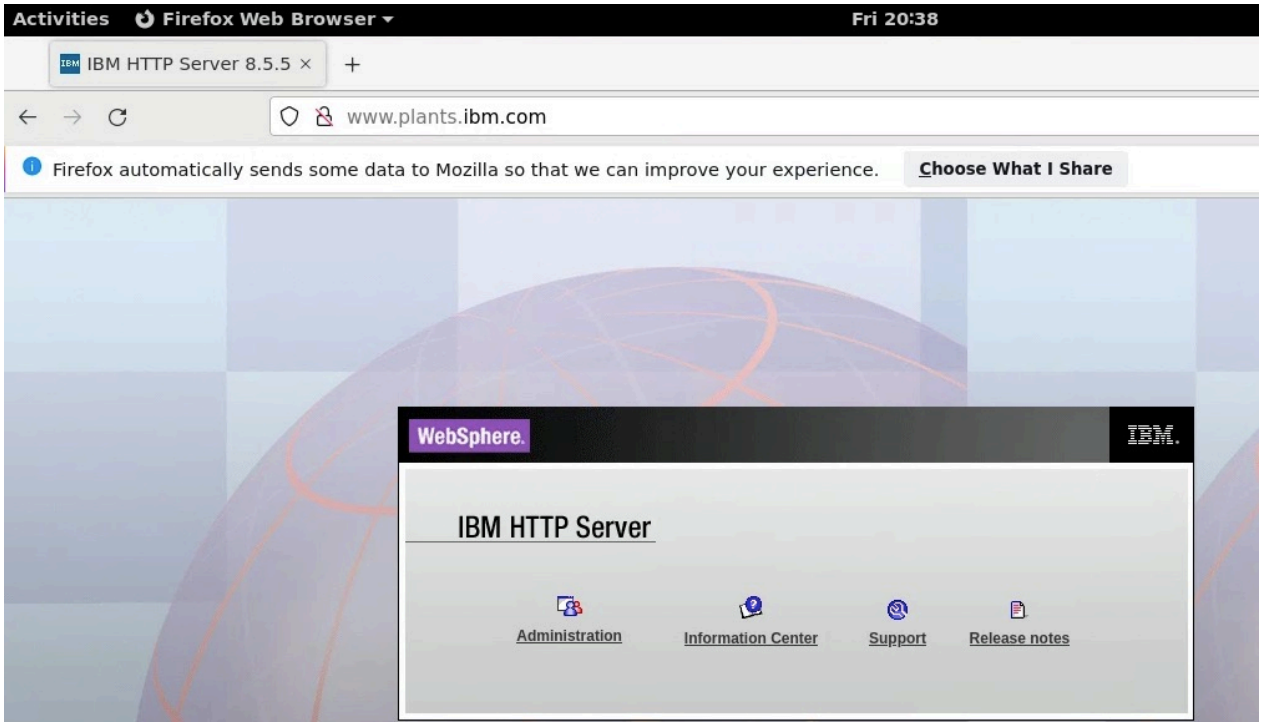
Secure Connection Failed

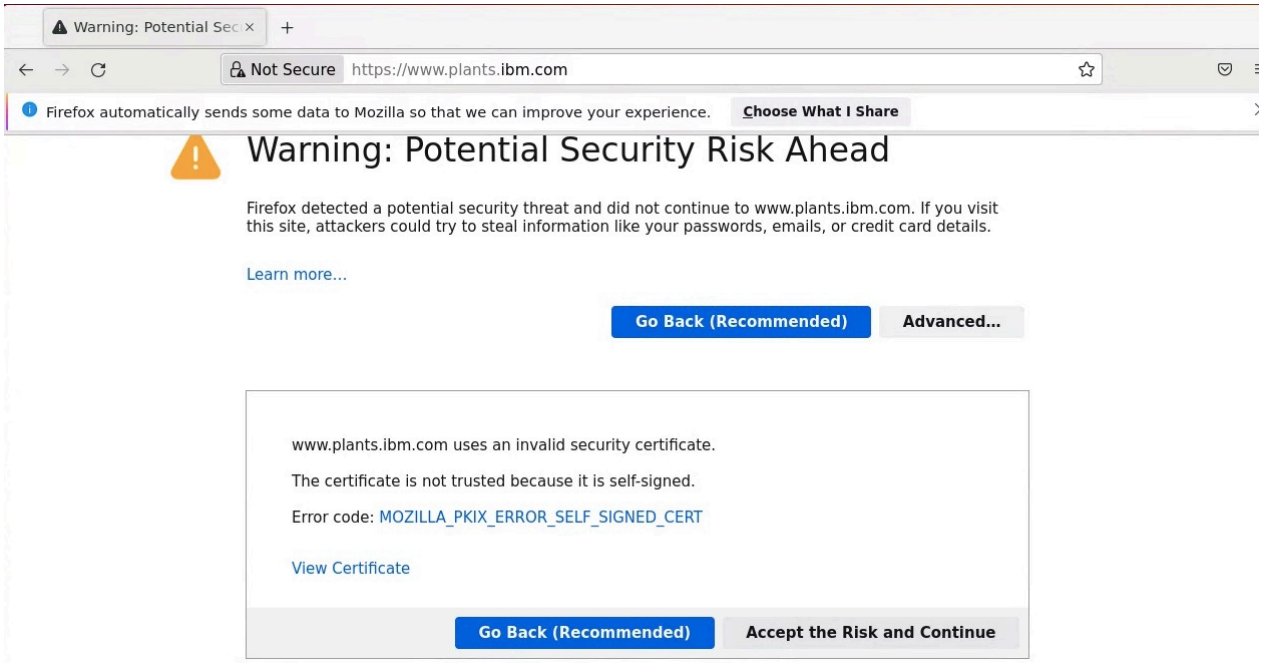
An error occurred during a connection to localhost. PR_CONNECT_RESET_ERROR

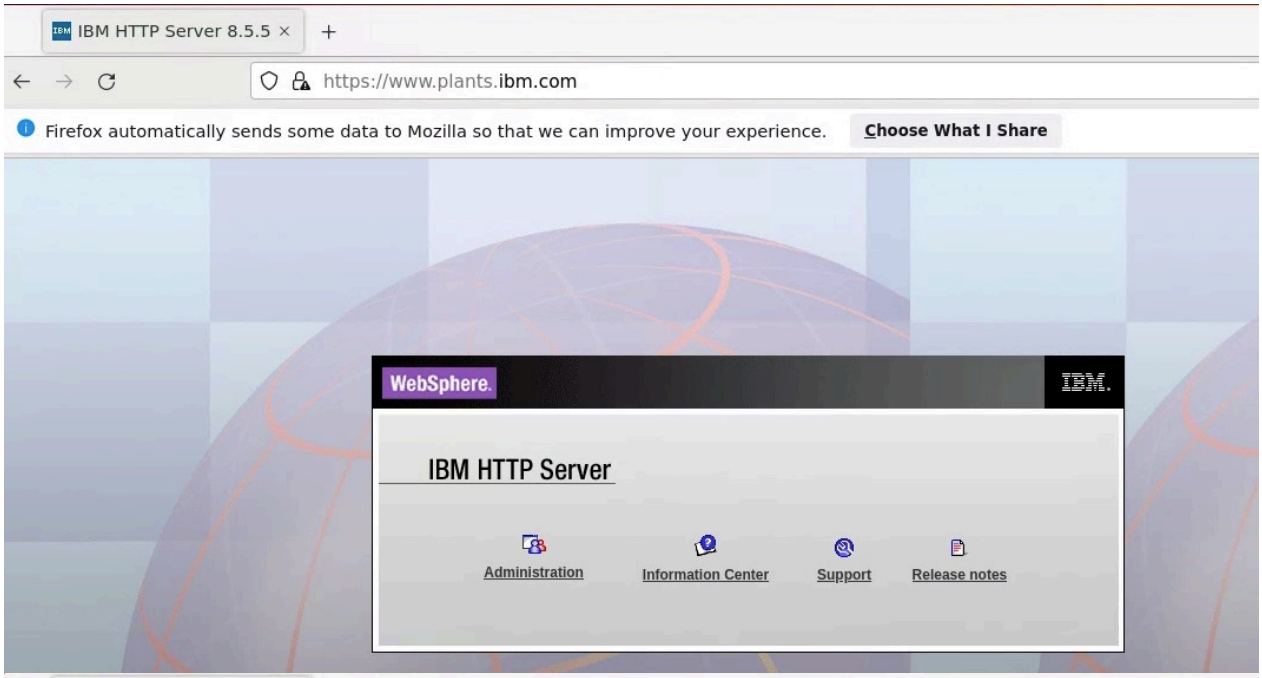
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

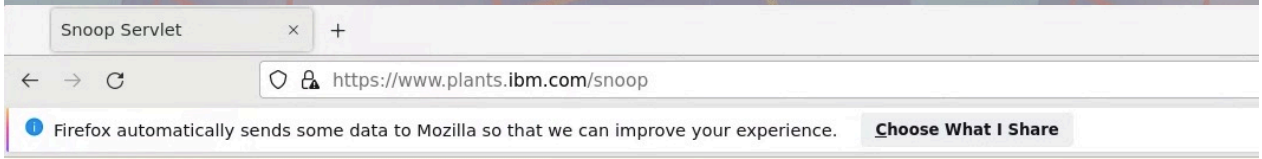
Learn more...

Try Again


Activities
Firefox Web Browser
Fri 20:38
IBM HTTP Server 8.5.5
www.plants.ibm.com
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
WebSphere.
IBM.
IBM HTTP Server
Administration
Information Center
Support
Release notes


Warning: Potential Sec
Not Secure
https://www.plants.ibm.com
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to www.plants.ibm.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
www.plants.ibm.com uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue





Snoop Servlet - Request/Client Information

Requested URL:

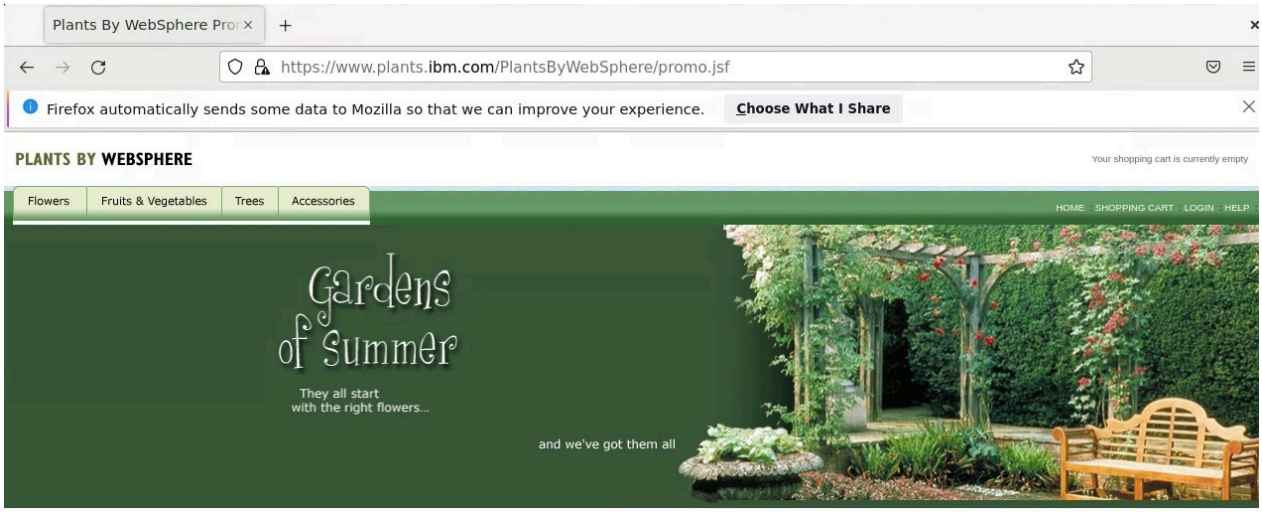
https://www.plants.ibm.com/snoop

Servlet Name:

Snoop Servlet

Request Information:

Request method	GET
Request URI	/snoop
Request protocol	HTTP/1.1
Servlet path	/snoop


Plants By WebSphere Pro
https://www.plants.ibm.com/PlantsByWebSphere/promo.jsf
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
PLANTS BY WEBSPHERE
Your shopping cart is currently empty
Flowers
Fruits & Vegetables
Trees
Accessories
HOME · SHOPPING CART · LOGIN · HELP
Gardens of Summer
They all start with the right flowers...
and we've got them all