SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for IBM WebSphere Application Server

gemalto

security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-013523-001, Rev. A

Release Date: June 2016

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as IBM WebSphere Application Server.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

IBM WebSphere Application Server provides the ability to deploy and run applications with flexible, secure, and Java EE-certified runtime environments – from lightweight production environments to large enterprise deployments.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to IBM WebSphere Application Server using SafeNet tokens.

It is assumed that the IBM WebSphere Application Server environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

IBM WebSphere Application Server can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) -** SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **IBM WebSphere Application Server**

Environment

The integration environment that was used in this document is based on the following software versions:

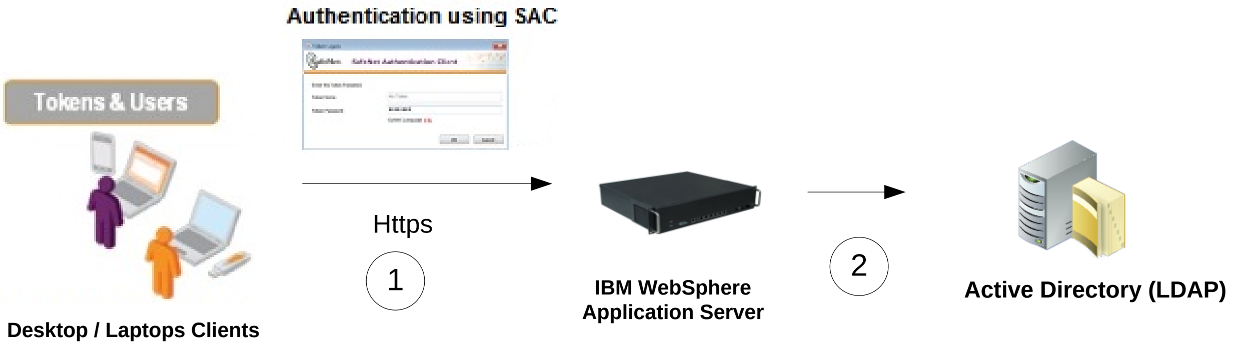
- **SafeNet Authentication Client (SAC)**—Version 10.0
- **IBM WebSphere Application Server**—Version 8.5
- **Windows Server 2008r2 Active Directory and CA server**
- **Windows 7 x32 as Client**

Audience

This document is targeted to system administrators who are familiar with IBM WebSphere Application Server, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

The diagram below illustrates the flow of certificate-based authentication:



1. A user attempts to connect to the IBM WebSphere Application Server using the IBM WebSphere Application Server client application URL. The user inserts the SafeNet token on which his or her certificate resides, and, when prompted, enters the token password.

2. After successful authentication, the user is allowed access to IBM WebSphere Application.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for IBM WebSphere Application Server using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client 10.0 should be installed on all client machines.
- SafeNet Authentication Client should be installed on the certificate authority from where a certificate will be enrolled on the token.
- Active Directory, LDAP server, IBM WebSphere Application Server, and client are up and running and should communicate with each other.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of tokens that can be used as a second authentication factor for users who authenticate to IBM WebSphere Application Server.

SafeNet Authentication Client 10.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110/5105

Smart Cards

- IDPrime MD 830-FIPS
- IDPrime MD 830-ICP
- IDPrime MD 3810
- IDPrime MD 3810 MIFARE 1K

Software Tokens

- SafeNet eToken Virtual

Configuring IBM WebSphere Application Server

Configuring IBM WebSphere Application server requires:

- Configuring an LDAP Repository, page 7
- Adding a CA Root Certificate, page 14
- Setting up the Application to Use the Client Certificate Authentication, page 17

Configuring an LDAP Repository

1. In a web browser, open the following url:

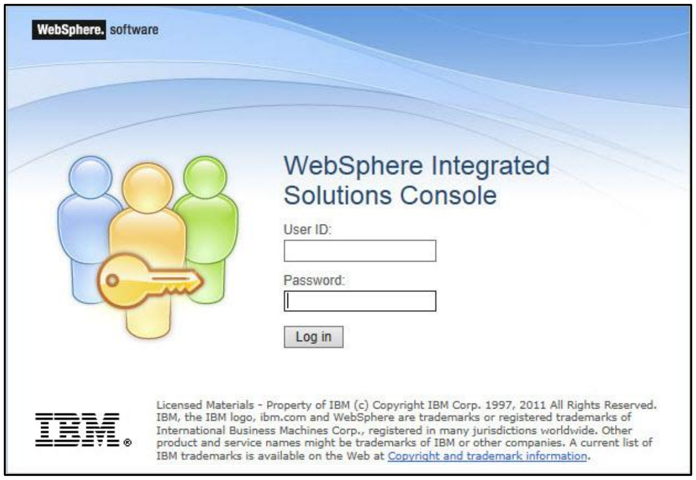
   http://<WebSphere Application Server IP address or name>:<port number>/ibm/console

   Or

   https://< WebSphere Application Server IP address or name>:<port number>/ibm/console

> **NOTE:** The port number will be according to the created installation profile.

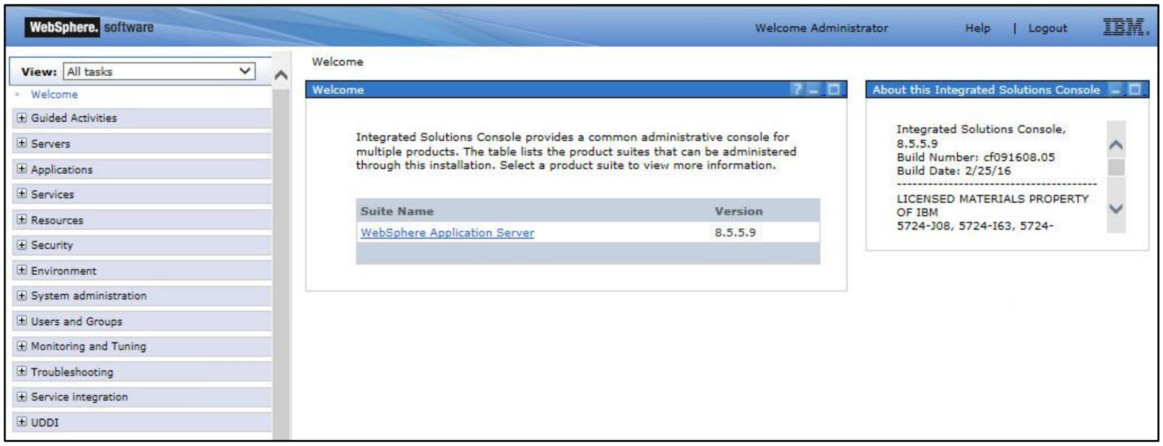
2. On the WebSphere Application Server login window, enter the administrator user ID and password, and then click **Log in**.



Licensed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved. IBM, the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

After successful login, the WebSphere Application Server Administrator console is displayed.



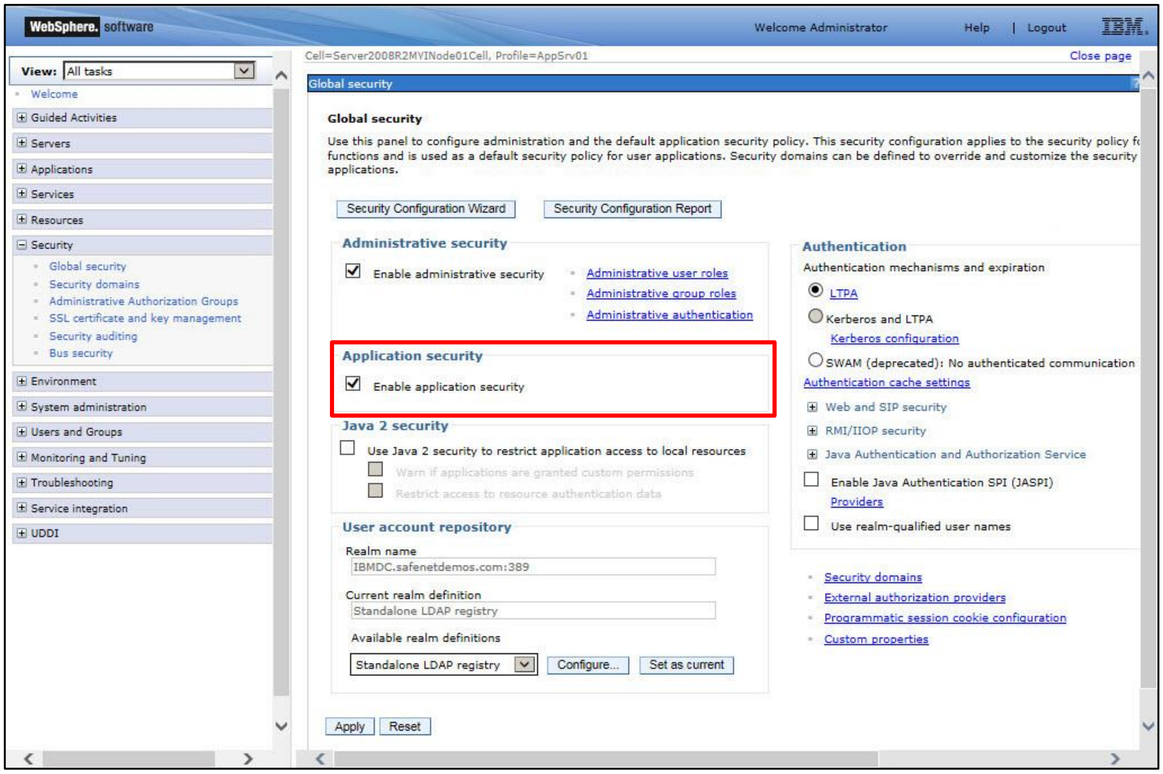
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.9

Integrated Solutions Console, 8.5.5.9
Build Number: cf091608.05
Build Date: 2/25/16
LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

3. On the WebSphere Application Server Administrator console, in the left pane, click **Security** > **Global security**, and then in the center pane, under **Application security**, select **Enable application security**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy fo functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security applications.

Administrative security
☑ Enable administrative security

Application security
☑ Enable application security

Java 2 security
□ Use Java 2 security to restrict application access to local resources
□ Warn if applications are granted custom permissions
□ Restrict access to resource authentication data

User account repository
Realm name: IBMDC.safenetdemos.com:389
Current realm definition: Standalone LDAP registry
Available realm definitions: Standalone LDAP registry

Authentication
Authentication mechanisms and expiration
● LTPA
○ Kerberos and LTPA
○ SWAM (deprecated): No authenticated communication
□ Enable Java Authentication SPI (JASPI)
□ Use realm-qualified user names

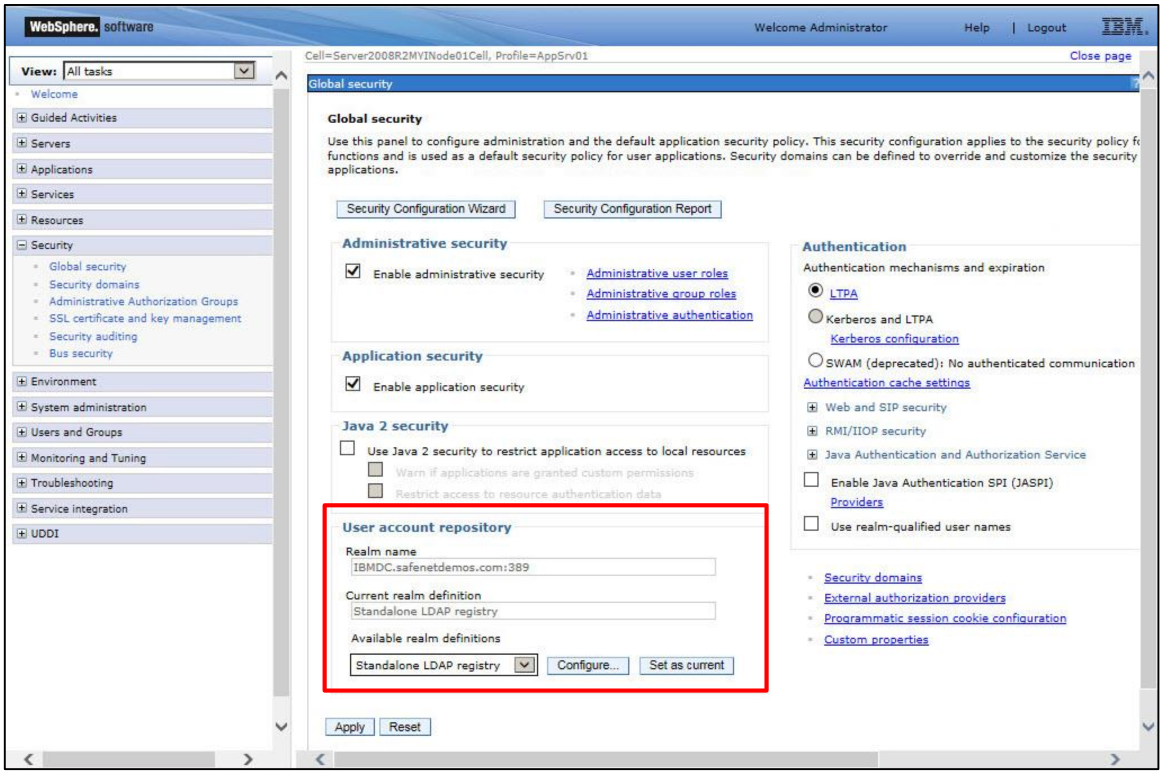
(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

4. Under **User account repository**, perform the following steps:

   a. In the **Available realm definitions** field, select **Standalone LDAP registry**.

   b. **Click Set as current**.

   c. Click **Configure**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy fo functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security applications.

Administrative security

☑ Enable administrative security

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

□ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Realm name: IBMDC.safenetdemos.com:389

Current realm definition: Standalone LDAP registry

Available realm definitions: Standalone LDAP registry

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

○ SWAM (deprecated): No authenticated communication

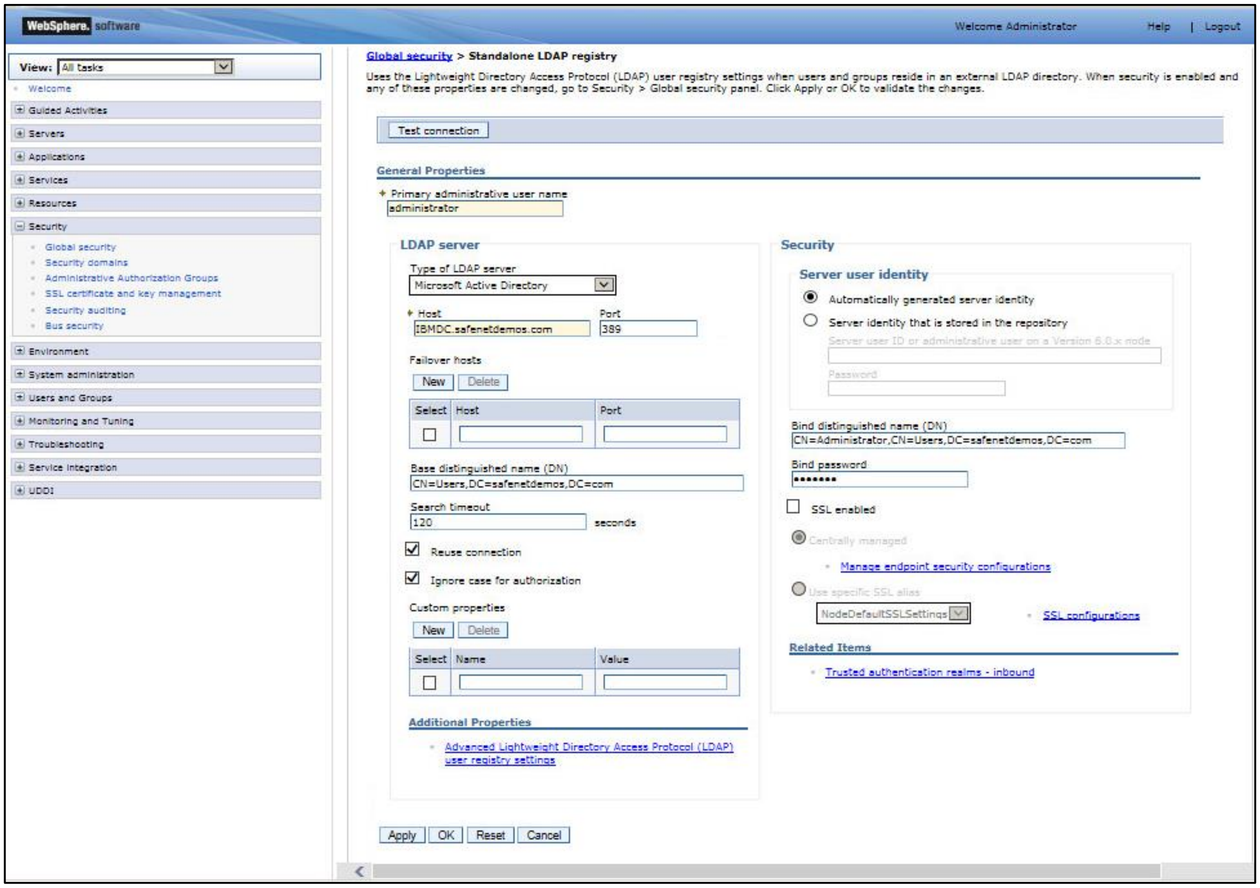
□ Enable Java Authentication SPI (JASPI)

□ Use realm-qualified user names

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

5. Under **General Properties**, complete the following fields, and then click **OK**:

Primary administrative user name	Enter the user name of the primary administrative user. The user is defined with administrative privileges in the user registry.
Type of LDAP server	Select **Microsoft Active Directory**.
Host	Enter the LDAP server host name or IP address.
Base distinguished name (DN)	Enter the base distinguished name of the directory.
Bind distinguished name (DN)	Enter the full distinguished name of the administrator.
Bind password	Enter the administrator password.



Global security > Standalone LDAP registry

Uses the Lightweight Directory Access Protocol (LDAP) user registry settings when users and groups reside in an external LDAP directory. When security is enabled and any of these properties are changed, go to Security > Global security panel. Click Apply or OK to validate the changes.

General Properties

* Primary administrative user name: administrator

LDAP server

Type of LDAP server: Microsoft Active Directory

* Host: IBMDC.safenetdemos.com

Port: 389

Failover hosts

Select	Host	Port
□		

Base distinguished name (DN): CN=Users,DC=safenetdemos,DC=com

Search timeout: 120 seconds

☑ Reuse connection

☑ Ignore case for authorization

Custom properties

Select	Name	Value
□		

Additional Properties

- Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

Security

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Bind distinguished name (DN): CN=Administrator,CN=Users,DC=safenetdemos,DC=com

Bind password: •••••••

□ SSL enabled

● Centrally managed

- Manage endpoint security configurations

○ Use specific SSL alias

NodeDefaultSSLSettings

- SSL configurations

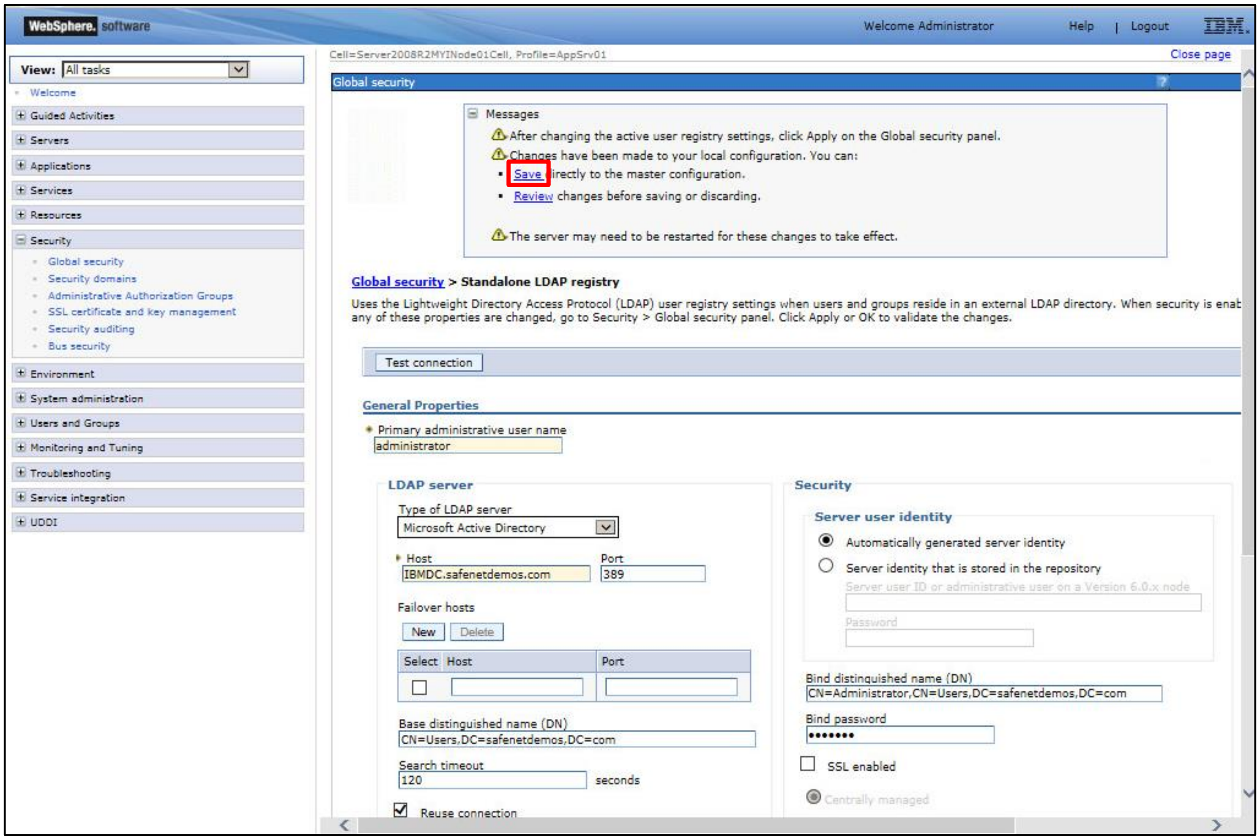
Related Items

- Trusted authentication realms - inbound

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

6. Click **Save**.

NOTE: Click **Test connection** to ensure that the connection with the LDAP server is successfully established.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Global security

Messages

⚠ After changing the active user registry settings, click Apply on the Global security panel.

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Global security > Standalone LDAP registry

Uses the Lightweight Directory Access Protocol (LDAP) user registry settings when users and groups reside in an external LDAP directory. When security is enab any of these properties are changed, go to Security > Global security panel. Click Apply or OK to validate the changes.

General Properties

* Primary administrative user name: administrator

LDAP server

Type of LDAP server: Microsoft Active Directory

* Host: IBMDC.safenetdemos.com Port: 389

Failover hosts

Select	Host	Port
□		

Base distinguished name (DN): CN=Users,DC=safenetdemos,DC=com

Search timeout: 120 seconds

☑ Reuse connection

Security

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Bind distinguished name (DN): CN=Administrator,CN=Users,DC=safenetdemos,DC=com

Bind password: •••••••

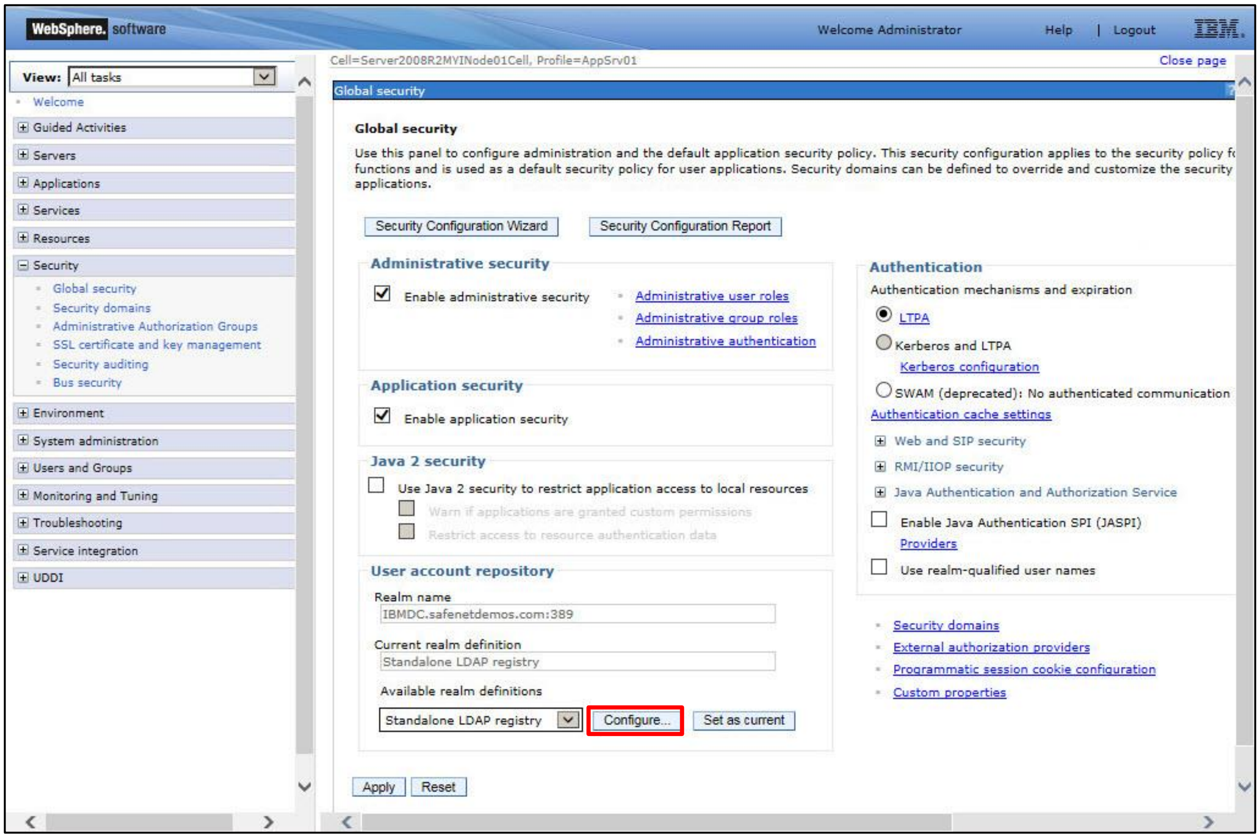
□ SSL enabled

● Centrally managed

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

7. In the left pane, click **Security** > **Global security**, and then in the center pane, under **User account repository**, click **Configure**.

NOTE: Ensure that **Standalone LDAP registry** is selected in the **Available realm definitions** field.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy fo functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security applications.

Administrative security

☑ Enable administrative security

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Realm name: IBMDC.safenetdemos.com:389

Current realm definition: Standalone LDAP registry

Available realm definitions: Standalone LDAP registry

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

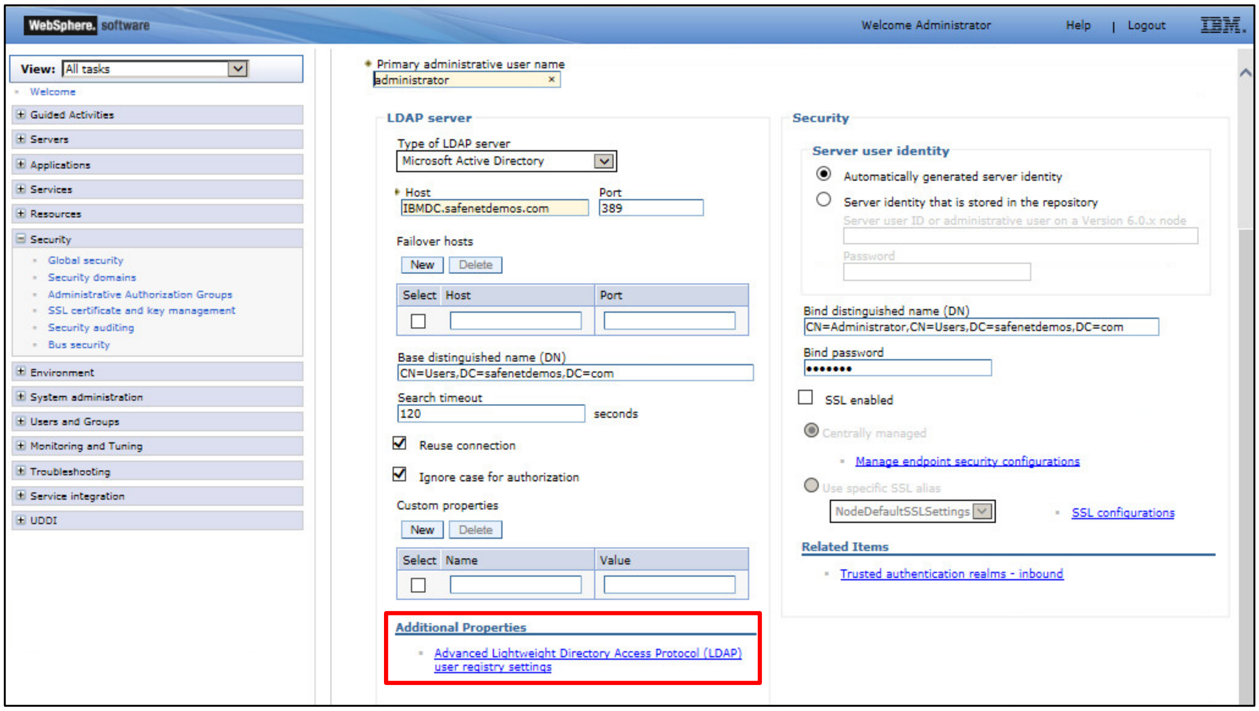
○ SWAM (deprecated): No authenticated communication

☐ Enable Java Authentication SPI (JASPI)

☐ Use realm-qualified user names

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

8. Under **Additional Properties**, click **Advanced Lightweight Directory Access Protocol (LDAP) user registry settings**.



* Primary administrative user name: administrator

LDAP server

Type of LDAP server: Microsoft Active Directory

* Host: IBMDC.safenetdemos.com

Port: 389

Failover hosts

Select	Host	Port
□		

Base distinguished name (DN): CN=Users,DC=safenetdemos,DC=com

Search timeout: 120 seconds

☑ Reuse connection

☑ Ignore case for authorization

Custom properties

Select	Name	Value
□		

Security

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Bind distinguished name (DN): CN=Administrator,CN=Users,DC=safenetdemos,DC=com

Bind password: •••••••

□ SSL enabled

● Centrally managed

○ Use specific SSL alias: NodeDefaultSSLSettings

Related Items

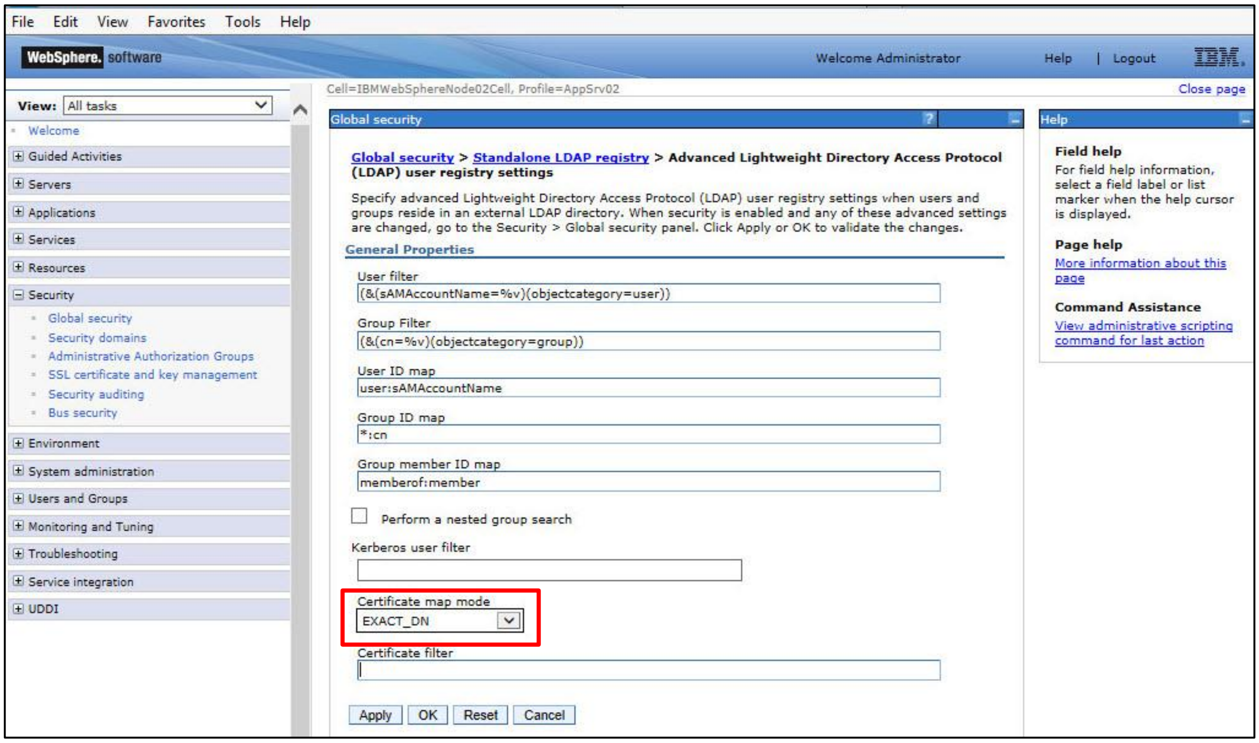
- Trusted authentication realms - inbound

Additional Properties

- Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

9. Under **General Properties**, ensure that in the **Certificate map mode** field, **Exact_DN** is selected.



Cell=IBMWebSphereNode02Cell, Profile=AppSrv02

Global security > Standalone LDAP registry > Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

Specify advanced Lightweight Directory Access Protocol (LDAP) user registry settings when users and groups reside in an external LDAP directory. When security is enabled and any of these advanced settings are changed, go to the Security > Global security panel. Click Apply or OK to validate the changes.

General Properties

User filter: (&(sAMAccountName=%v)(objectcategory=user))

Group Filter: (&(cn=%v)(objectcategory=group))

User ID map: user:sAMAccountName

Group ID map: *:cn

Group member ID map: memberof:member

□ Perform a nested group search

Kerberos user filter:

Certificate map mode: EXACT_DN

Certificate filter:

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Page help

More information about this page

Command Assistance

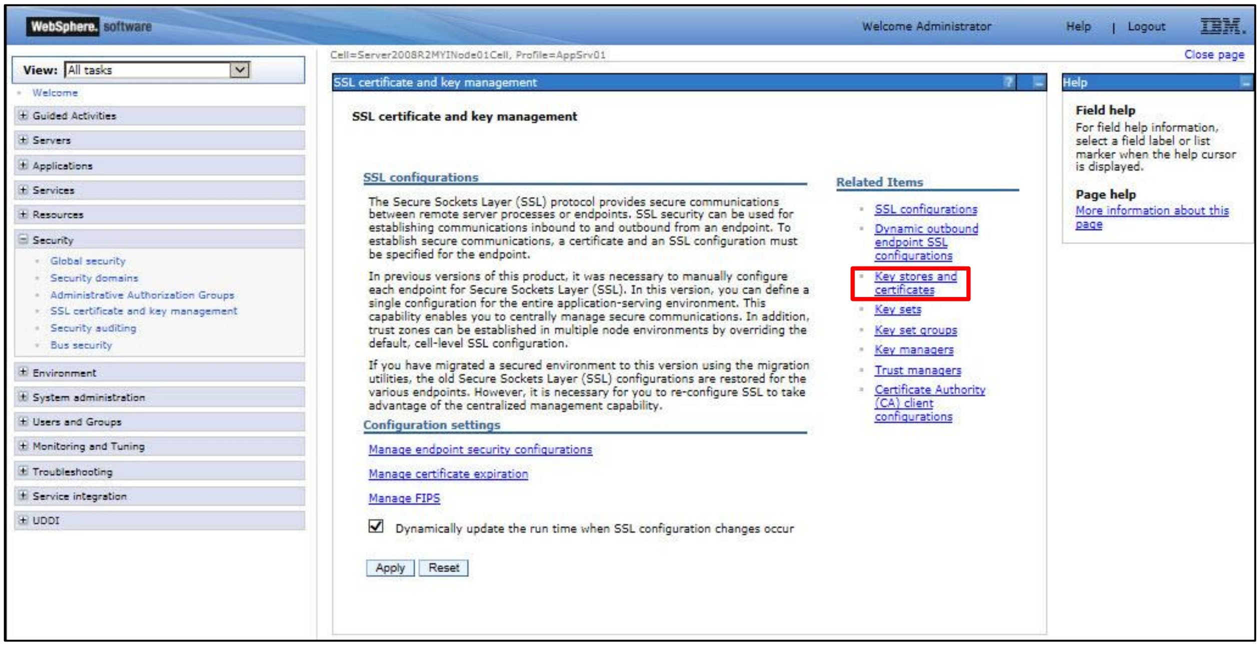
View administrative scripting command for last action

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

Adding a CA Root Certificate

Add a CA root certificate to the default trust store on the IBM WebSphere Application server.

1. On the WebSphere Application Server Administrator console, in the left pane, click **Security** > **SSL certificate and key management**, and then in the center pane, under **Related Items**, click **Key stores and certificates**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

☑ Dynamically update the run time when SSL configuration changes occur

Field help

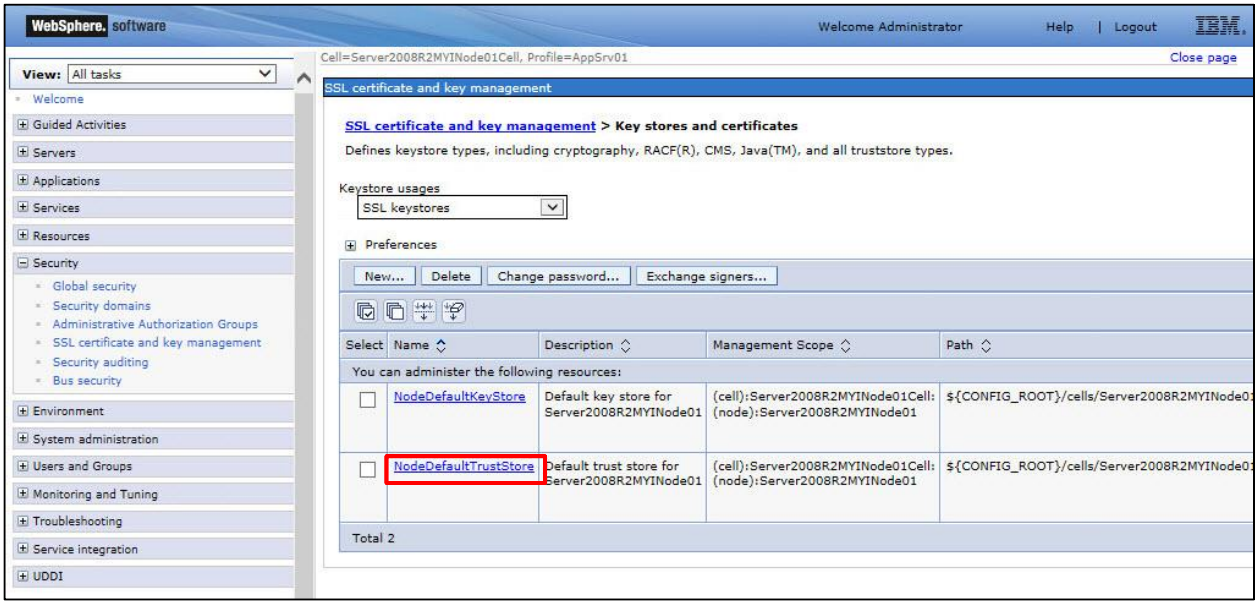
For field help information, select a field label or list marker when the help cursor is displayed.

Page help

More information about this page

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

2. Click **NodeDefaultTrustStore**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

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

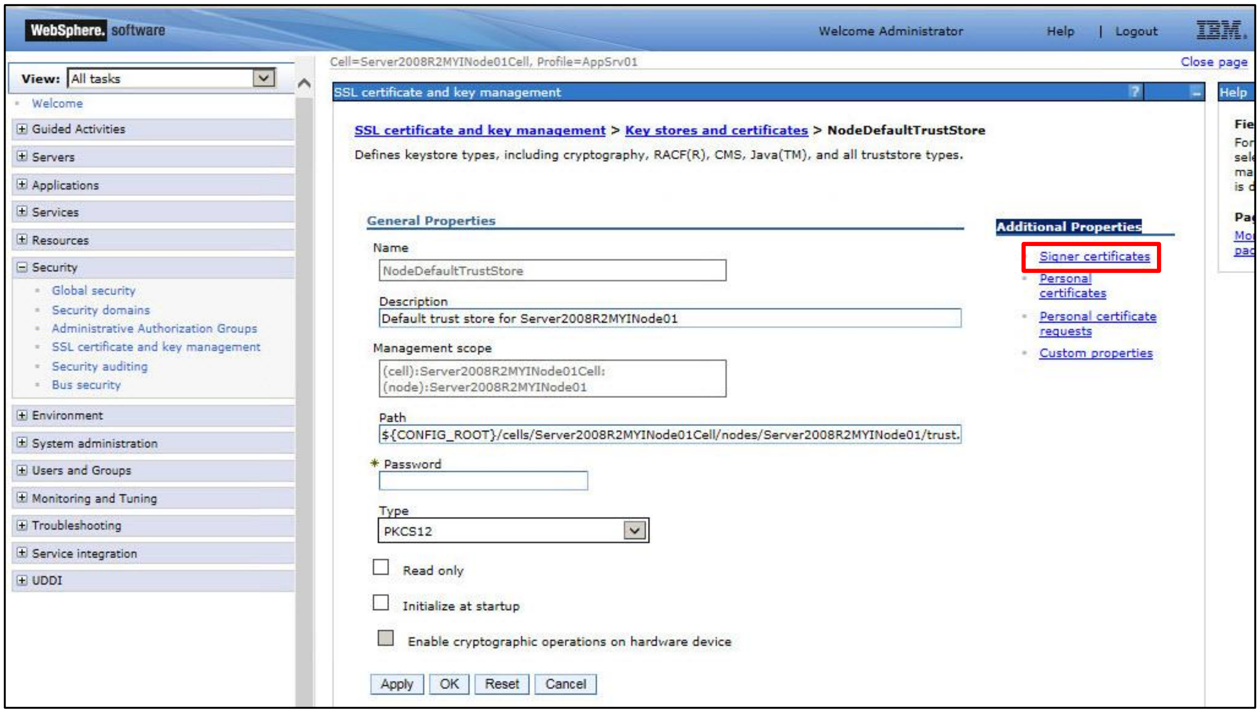
Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

Keystore usages: SSL keystores

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
□	NodeDefaultKeyStore	Default key store for Server2008R2MYINode01	(cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01	${CONFIG_ROOT}/cells/Server2008R2MYINode0
□	NodeDefaultTrustStore	Default trust store for Server2008R2MYINode01	(cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01	${CONFIG_ROOT}/cells/Server2008R2MYINode0
Total 2				

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

3. Under **Additional Properties**, click **Signer certificates**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

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

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

General Properties

Name: NodeDefaultTrustStore

Description: Default trust store for Server2008R2MYINode01

Management scope: (cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01

Path: ${CONFIG_ROOT}/cells/Server2008R2MYINode01Cell/nodes/Server2008R2MYINode01/trust.

* Password

Type: PKCS12

□ Read only

□ Initialize at startup

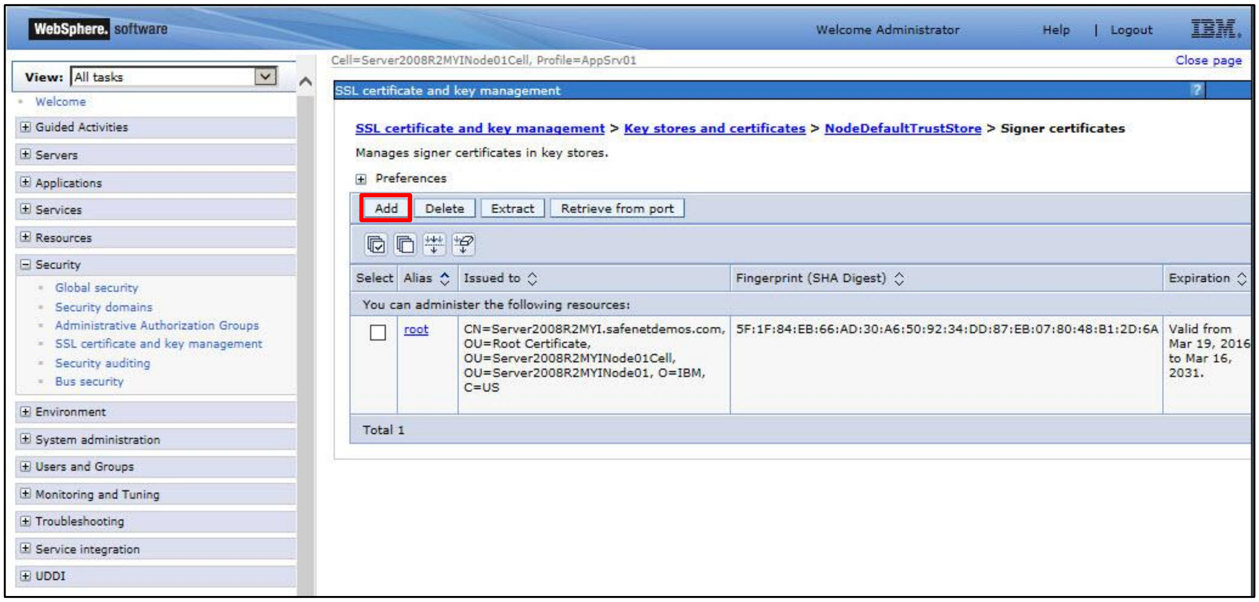
□ Enable cryptographic operations on hardware device

Additional Properties

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

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

4. Click **Add**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates

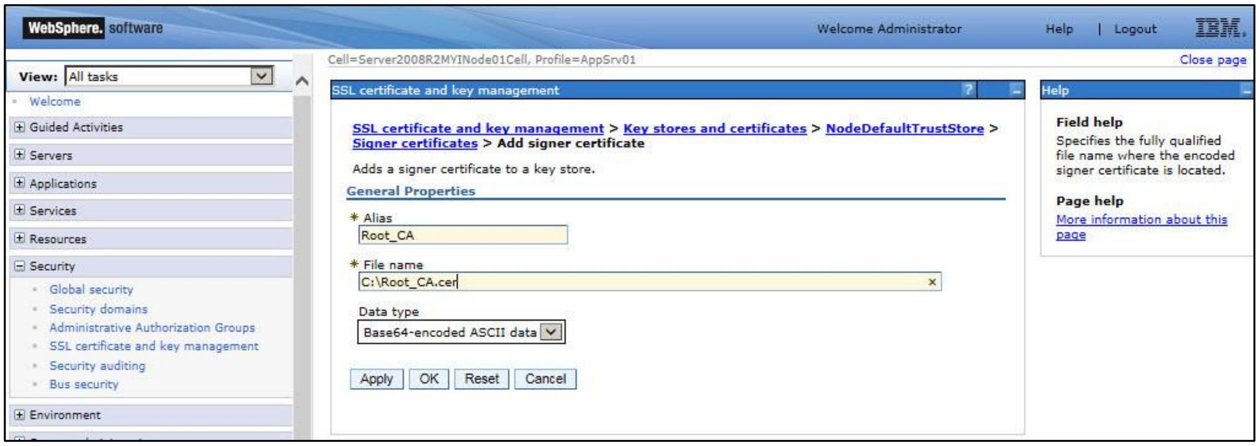
Manages signer certificates in key stores.

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
□	root	CN=Server2008R2MYI.safenetdemos.com, OU=Root Certificate, OU=Server2008R2MYINode01Cell, OU=Server2008R2MYINode01, O=IBM, C=US	5F:1F:84:EB:66:AD:30:A6:50:92:34:DD:87:EB:07:80:48:B1:2D:6A	Valid from Mar 19, 2016 to Mar 16, 2031.
Total 1				

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

5. Under **General Properties**, complete the following fields, and then click **OK**.

Alias	Enter an alias for the signer certificate (for example, **Root_CA**). The alias is used to refer the signer certificate in the key store.
File name	Enter the full path to the signer certificate file.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > **Add signer certificate**

Adds a signer certificate to a key store.

General Properties

* Alias
Root_CA

* File name
C:\Root_CA.cer

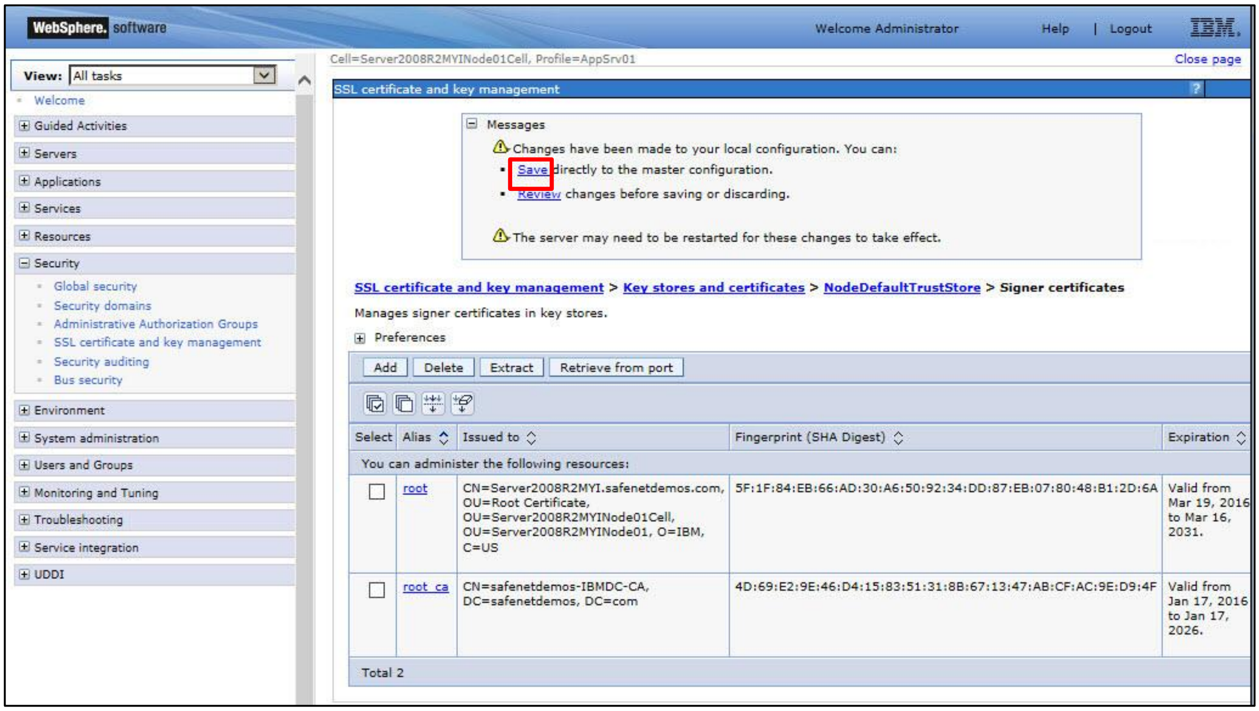
Data type
Base64-encoded ASCII data

Field help
Specifies the fully qualified file name where the encoded signer certificate is located.

Page help
More information about this page

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

6. The CA root certificate is added. Click **Save**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

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

Manages signer certificates in key stores.

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
□	root	CN=Server2008R2MYI.safenetdemos.com, OU=Root Certificate, OU=Server2008R2MYINode01Cell, OU=Server2008R2MYINode01, O=IBM, C=US	5F:1F:84:EB:66:AD:30:A6:50:92:34:DD:87:EB:07:80:48:B1:2D:6A	Valid from Mar 19, 2016 to Mar 16, 2031.
□	root_ca	CN=safenetdemos-IBMDC-CA, DC=safenetdemos, DC=com	4D:69:E2:9E:46:D4:15:83:51:31:8B:67:13:47:AB:CF:AC:9E:D9:4F	Valid from Jan 17, 2016 to Jan 17, 2026.
Total 2				

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

Setting up the Application to Use the Client Certificate Authentication

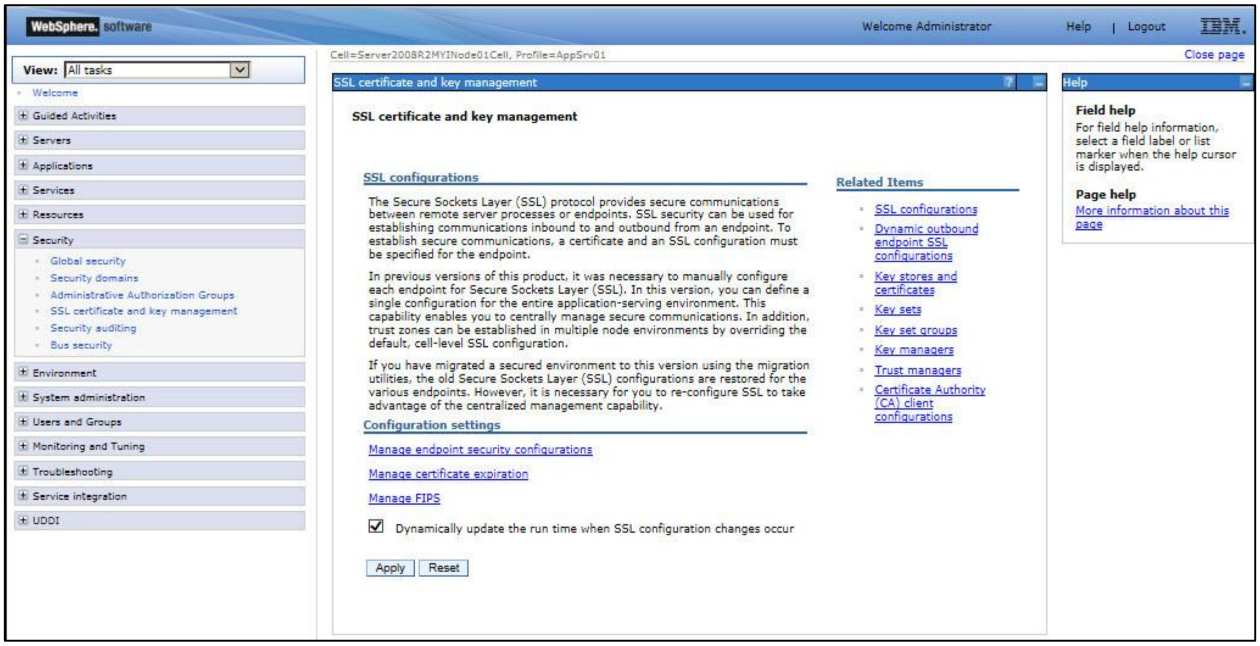
Performing client certificate authentication with the .ear application requires:

- Defining Quality of Protection (QoP) Settings for the SSL Client Authentication, page 17
- Updating the Application to Support the Client Certificate Authentication, page 20
- Installing the Enterprise Application, page 21
- Starting the Enterprise Application, page 24

NOTE: In this solution, the IBM WebSphere **DefaultApplication.ear** application is used.

Defining Quality of Protection (QoP) Settings for the SSL Client Authentication

1. On the WebSphere Application Server Administrator console, in the left pane click **Security** > **SSL certificate and key management**, and then, in the center pane, under **Related Items**, click **SSL configurations**.



The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

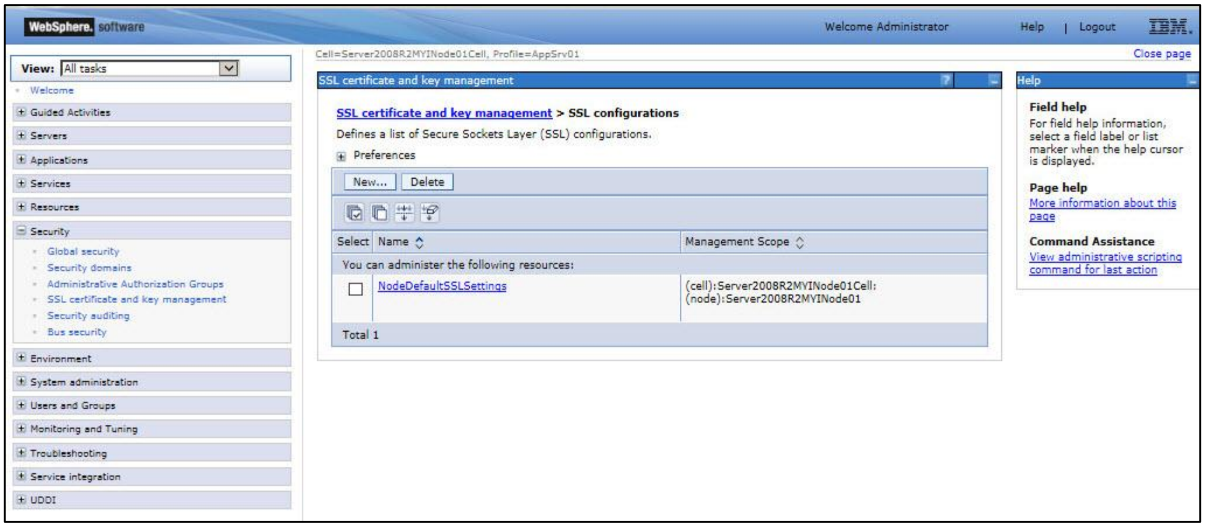
If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

☑ Dynamically update the run time when SSL configuration changes occur

For field help information, select a field label or list marker when the help cursor is displayed.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

2. Click **NodeDefaultSSLSettings**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

SSL certificate and key management > SSL configurations

Defines a list of Secure Sockets Layer (SSL) configurations.

Select	Name	Management Scope
You can administer the following resources:		
□	NodeDefaultSSLSettings	(cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01
Total 1		

Help

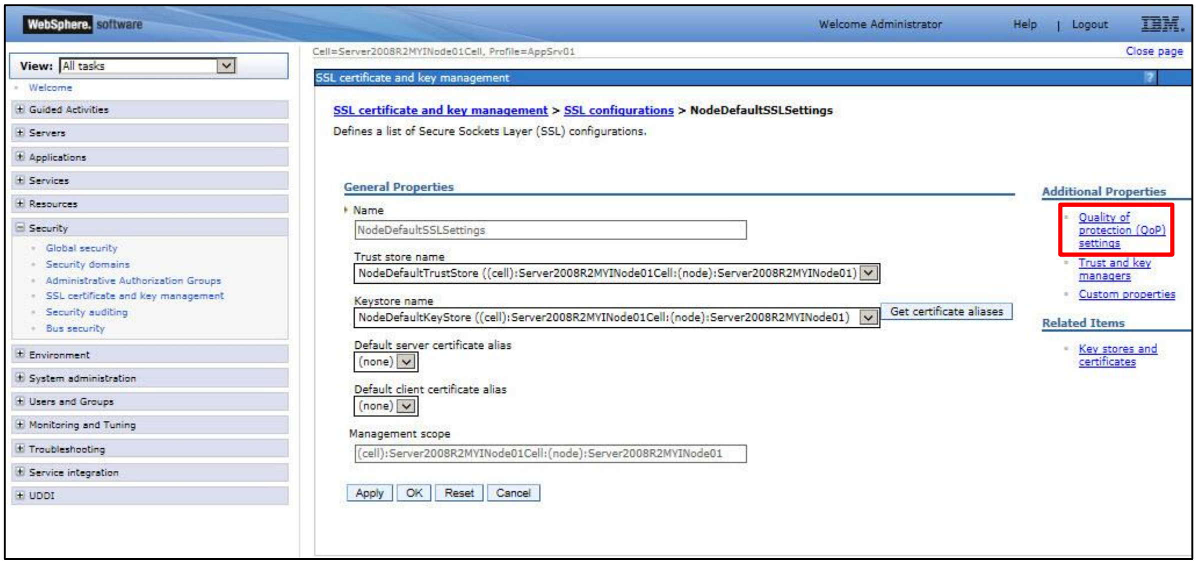
Field help
For field help information, select a field label or list marker when the help cursor is displayed.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

3. Under Additional Properties, click **Quality of protection (QoP) settings** to define Quality of protection (QoP) settings for SSL.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

Name: NodeDefaultSSLSettings

Trust store name: NodeDefaultTrustStore ((cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01)

Keystore name: NodeDefaultKeyStore ((cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01)

Default server certificate alias: (none)

Default client certificate alias: (none)

Management scope: (cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01

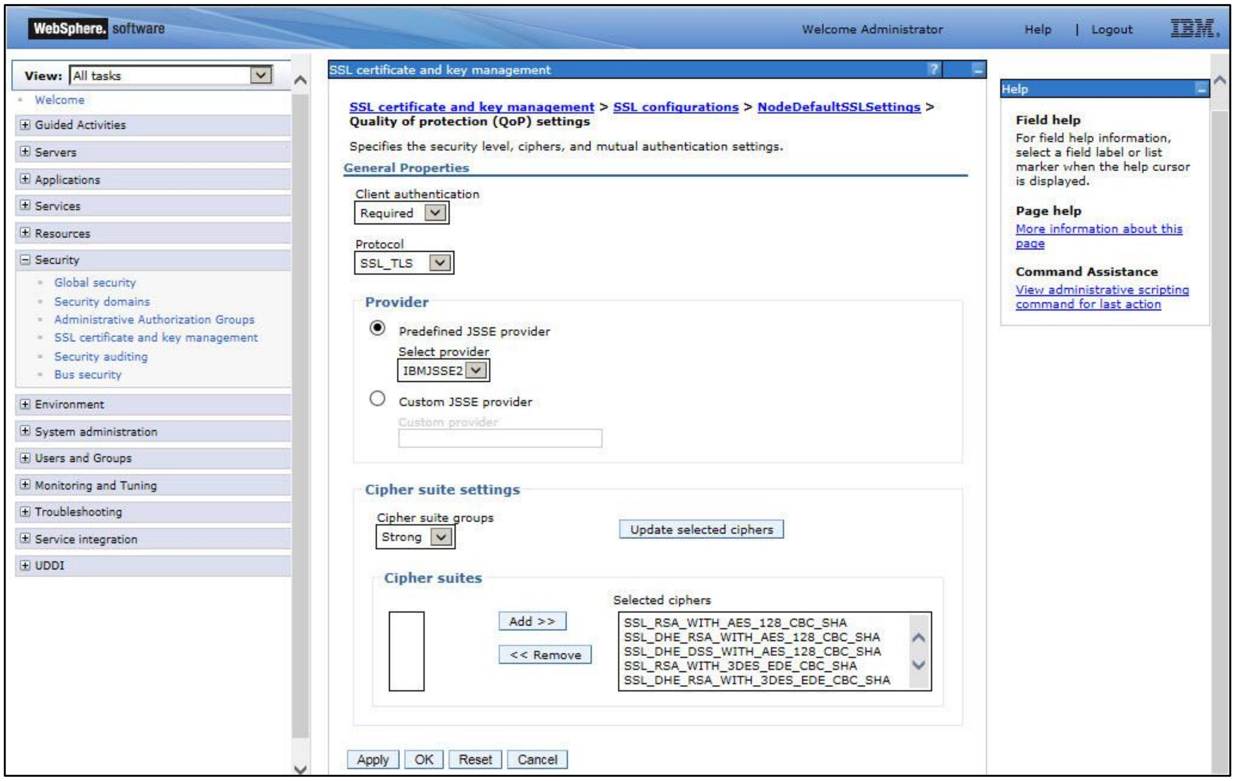
Additional Properties
- Quality of protection (QoP) settings
- Trust and key managers
- Custom properties

Related Items
- Key stores and certificates

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

4. Under **General Properties**, complete the following fields, and then click **OK**.

Client authentication	Select **Required**.
Protocol	Select **SSL_TLS**.



SSL certificate and key management

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings >
Quality of protection (QoP) settings

Specifies the security level, ciphers, and mutual authentication settings.

General Properties

Client authentication: Required

Protocol: SSL_TLS

Provider

● Predefined JSSE provider

Select provider: IBMJSSE2

○ Custom JSSE provider

Custom provider

Cipher suite settings

Cipher suite groups: Strong

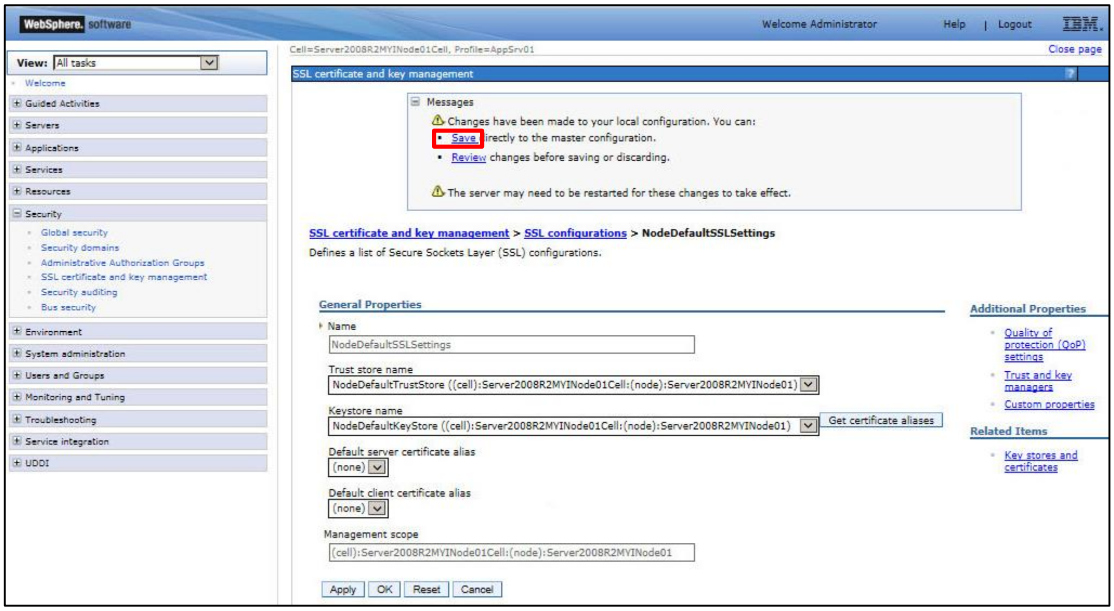
Cipher suites

Selected ciphers:

SSL_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

5. Click **Save**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

SSL certificate and key management

Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

Name: NodeDefaultSSLSettings

Trust store name: NodeDefaultTrustStore ((cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01)

Keystore name: NodeDefaultKeyStore ((cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01)

Default server certificate alias: (none)

Default client certificate alias: (none)

Management scope: (cell):Server2008R2MYINode01Cell:(node):Server2008R2MYINode01

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

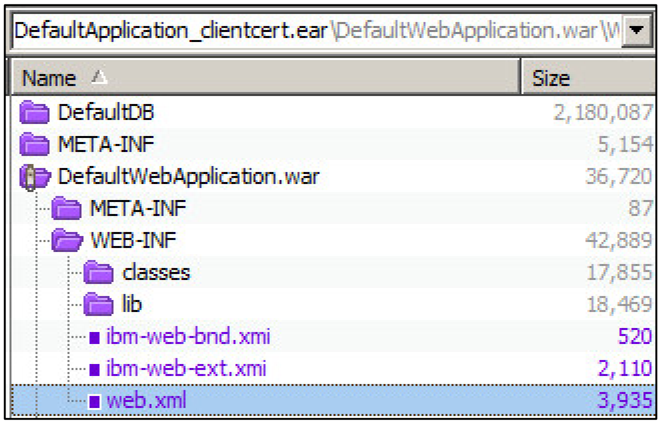
Updating the Application to Support the Client Certificate Authentication

NOTE: It is assumed that **Defaultapplication.ear** is exported and edited.

1. Open the **web.xml** file that is located at the following path:

   <path where the .ear directory is exported>/DefaultWebApplication.war/WEB-INF/web.xml

   NOTE: The **web.xml** file is located in the directory where the **Defaultapplication.ear** file is exported.

   DefaultApplication_clientcert.ear\DefaultWebApplication.war\W

Name	Size
DefaultDB	2,180,087
META-INF	5,154
DefaultWebApplication.war	36,720
META-INF	87
WEB-INF	42,889
classes	17,855
lib	18,469
ibm-web-bnd.xmi	520
ibm-web-ext.xmi	2,110
web.xml	3,935

   (The screen image above is from IBM®. Trademarks are the property of their respective owners.)

2. Edit the **web.xml** file.

3. In the **web.xml** file, add or replace the **<login-config>** tag with the following content to add the client certificate authentication method.

   <login-config>

   <auth-method>CLIENT-CERT</auth-method>

   <login-config>

4. Locate the **<transport-guarantee>** tag and replace it with the following content to change the transport guarantee setting to **CONFIDENTIAL**.

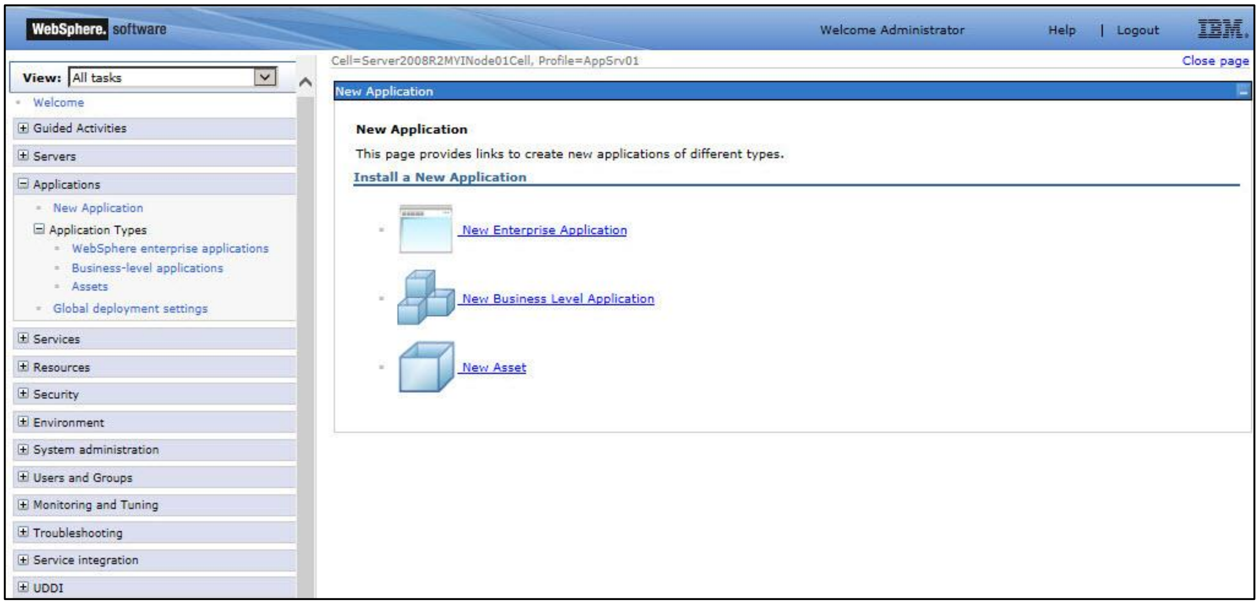
   <transport-guarantee>CONFIDENTIAL</transport-guarantee>

5. Save and close the **web.xml** file.

Installing the Enterprise Application

Install the Enterprise application after the **web.xml** is edited.

1. Log in to the WebSphere Application Server Administrator console.
2. On the WebSphere Application Server Administrator console, in the left pane, click **Applications** > **New Application**, and then in the right pane, click **New Enterprise Application**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

New Application

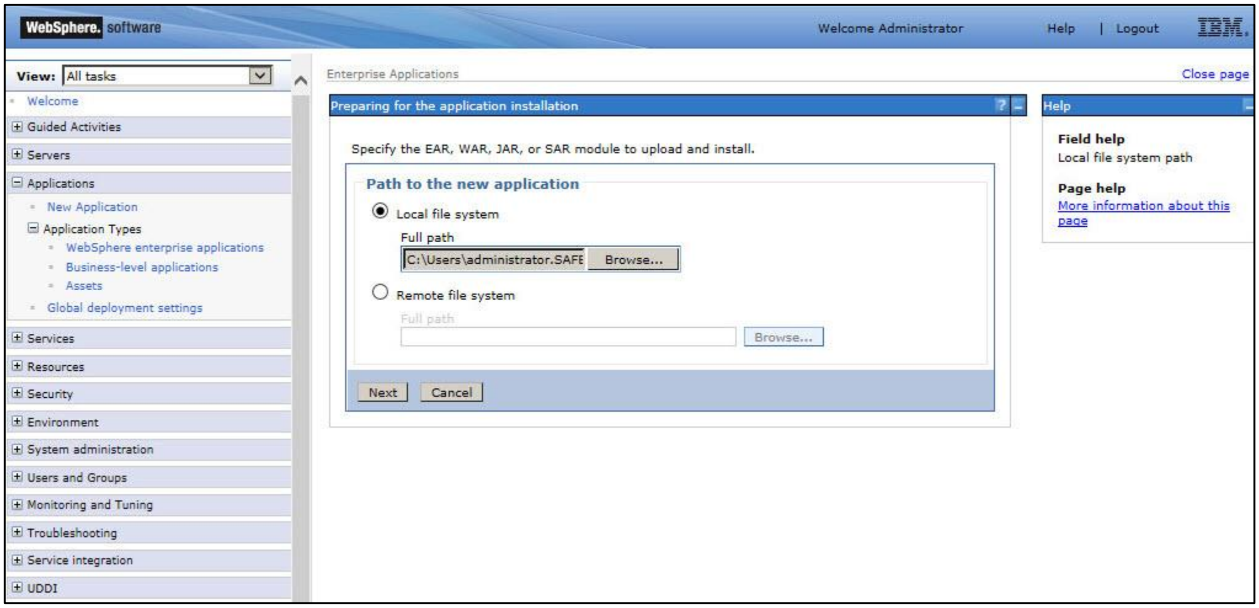
New Application

This page provides links to create new applications of different types.

Install a New Application

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

3. Under **Path to the new application**, select **Local file system**, click **Browse** to select a path to the enterprise application file, and then click **Next**.



Preparing for the application installation

Specify the EAR, WAR, JAR, or SAR module to upload and install.

Path to the new application

● Local file system

Full path: C:\Users\administrator.SAFE

○ Remote file system

Full path:

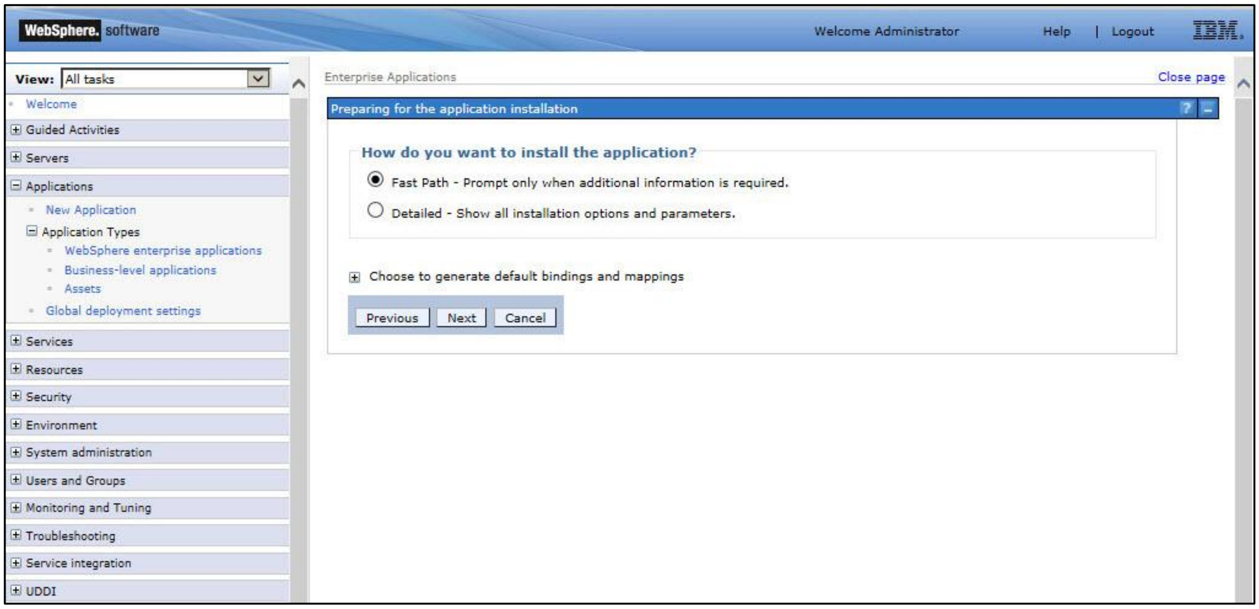
Help

Field help
Local file system path

Page help
More information about this page

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

4. Under **How do you want to install the application?**, select **Fast Path**, and then click **Next.**



Preparing for the application installation

How do you want to install the application?

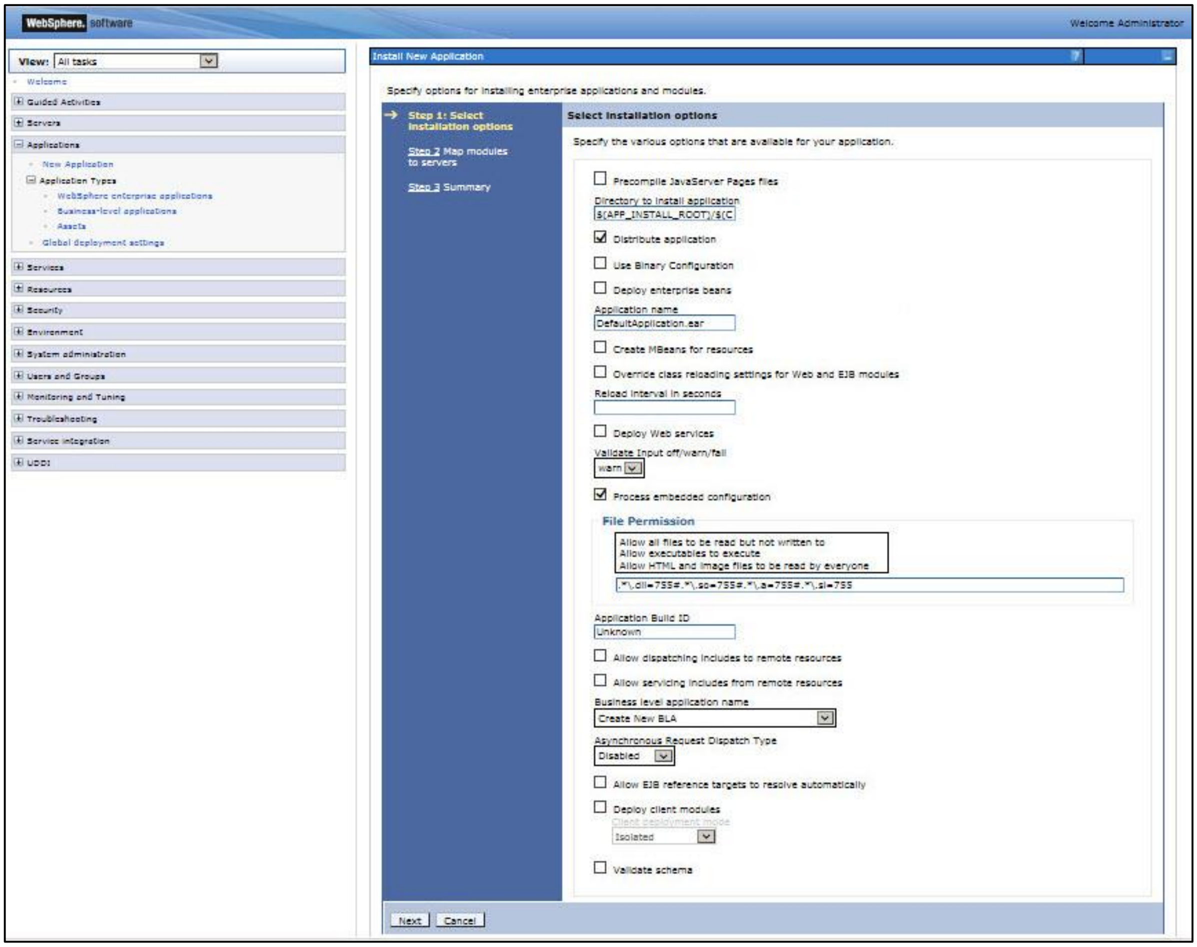
● Fast Path - Prompt only when additional information is required.

○ Detailed - Show all installation options and parameters.

⊞ Choose to generate default bindings and mappings

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

5. Under **Select installation options**, click **next**.



Install New Application

Specify options for installing enterprise applications and modules.

Select installation options

Specify the various options that are available for your application.

□ Precompile JavaServer Pages files

Directory to install application: $(APP_INSTALL_ROOT)/$(C

☑ Distribute application

□ Use Binary Configuration

□ Deploy enterprise beans

Application name: DefaultApplication.ear

□ Create MBeans for resources

□ Override class reloading settings for Web and EJB modules

Reload interval in seconds:

□ Deploy Web services

Validate Input off/warn/fail: warn

☑ Process embedded configuration

File Permission

Allow all files to be read but not written to
Allow executables to execute
Allow HTML and image files to be read by everyone

.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755

Application Build ID: Unknown

□ Allow dispatching includes to remote resources

□ Allow servicing includes from remote resources

Business level application name: Create New BLA

Asynchronous Request Dispatch Type: Disabled

□ Allow EJB reference targets to resolve automatically

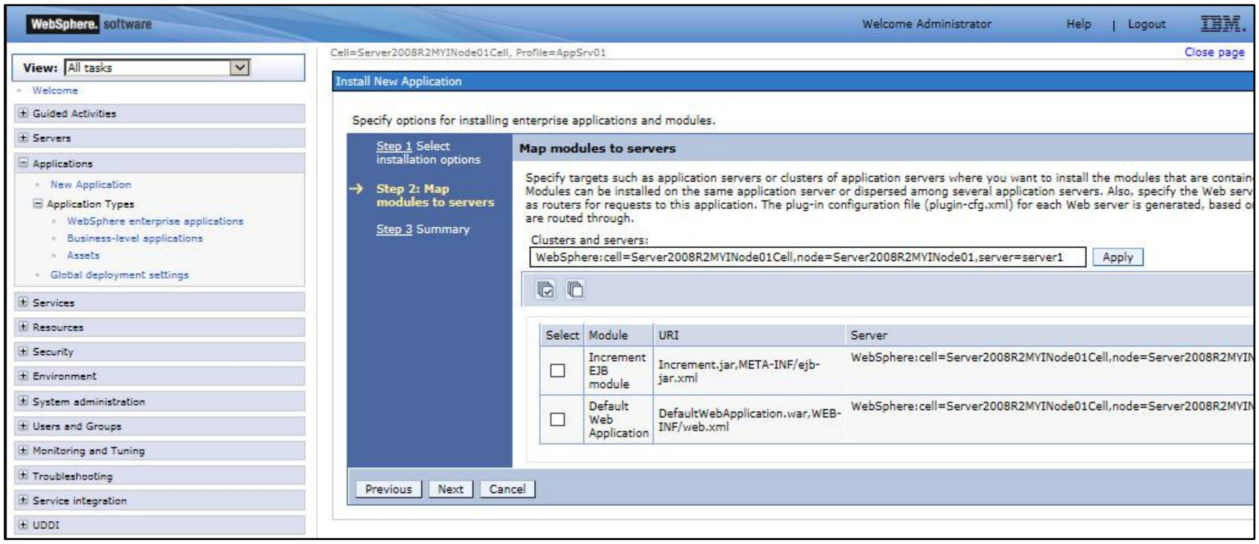
□ Deploy client modules

Client deployment mode: Isolated

□ Validate schema

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

6. Under **Map modules to servers**, click **Next**.



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Install New Application

Specify options for installing enterprise applications and modules.

Step 1 Select installation options

→ Step 2: Map modules to servers

Step 3 Summary

Map modules to servers

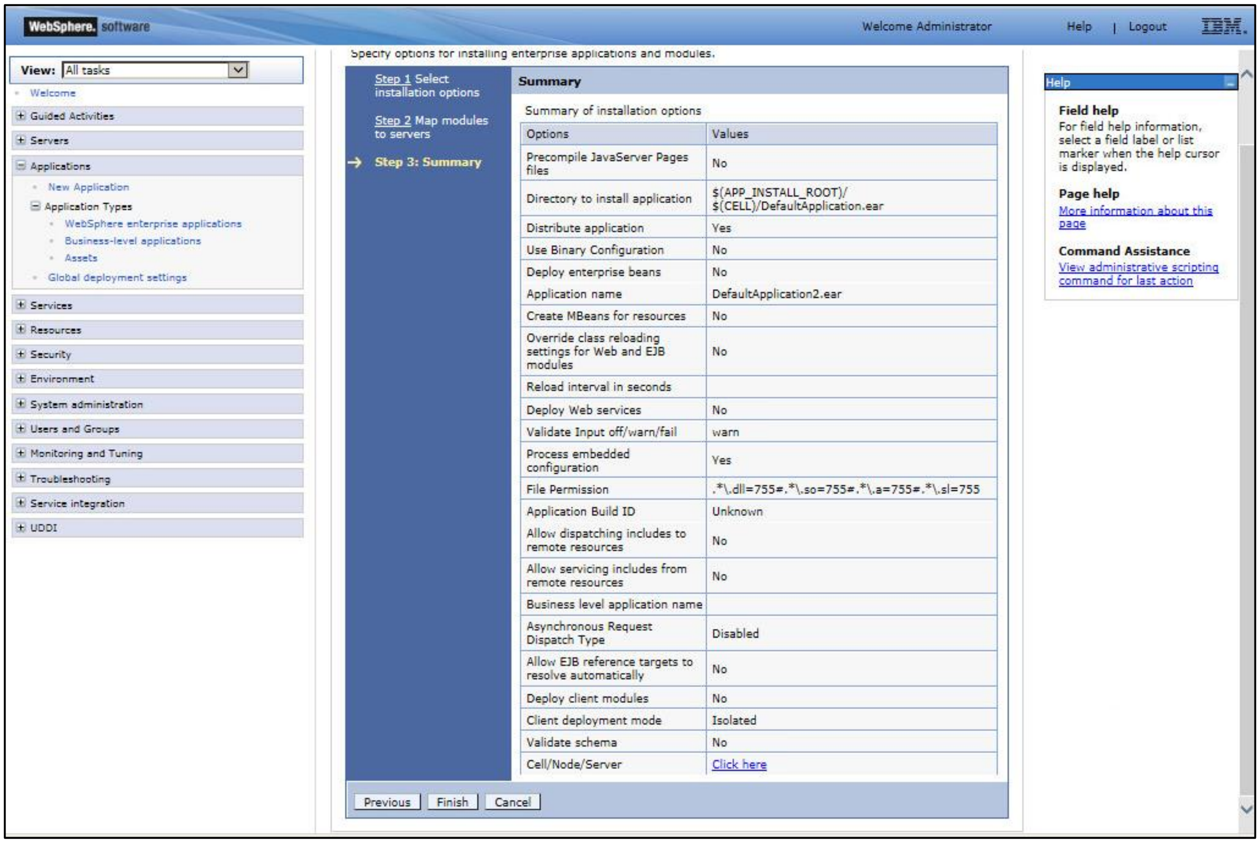
Specify targets such as application servers or clusters of application servers where you want to install the modules that are contain
Modules can be installed on the same application server or dispersed among several application servers. Also, specify the Web serv
as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based o
are routed through.

Clusters and servers:
WebSphere:cell=Server2008R2MYINode01Cell,node=Server2008R2MYINode01,server=server1

Select	Module	URI	Server
□	Increment EJB module	Increment.jar,META-INF/ejb-jar.xml	WebSphere:cell=Server2008R2MYINode01Cell,node=Server2008R2MYIN
□	Default Web Application	DefaultWebApplication.war,WEB-INF/web.xml	WebSphere:cell=Server2008R2MYINode01Cell,node=Server2008R2MYIN

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

7. Under **Summary**, click **Finish**.



Specify options for installing enterprise applications and modules.

Step 1 Select installation options

Step 2 Map modules to servers

→ Step 3: Summary

Summary

Summary of installation options

Options	Values
Precompile JavaServer Pages files	No
Directory to install application	$(APP_INSTALL_ROOT)/ $(CELL)/DefaultApplication.ear
Distribute application	Yes
Use Binary Configuration	No
Deploy enterprise beans	No
Application name	DefaultApplication2.ear
Create MBeans for resources	No
Override class reloading settings for Web and EJB modules	No
Reload interval in seconds	
Deploy Web services	No
Validate Input off/warn/fail	warn
Process embedded configuration	Yes
File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755
Application Build ID	Unknown
Allow dispatching includes to remote resources	No
Allow servicing includes from remote resources	No
Business level application name	
Asynchronous Request Dispatch Type	Disabled
Allow EJB reference targets to resolve automatically	No
Deploy client modules	No
Client deployment mode	Isolated
Validate schema	No
Cell/Node/Server	Click here

Help

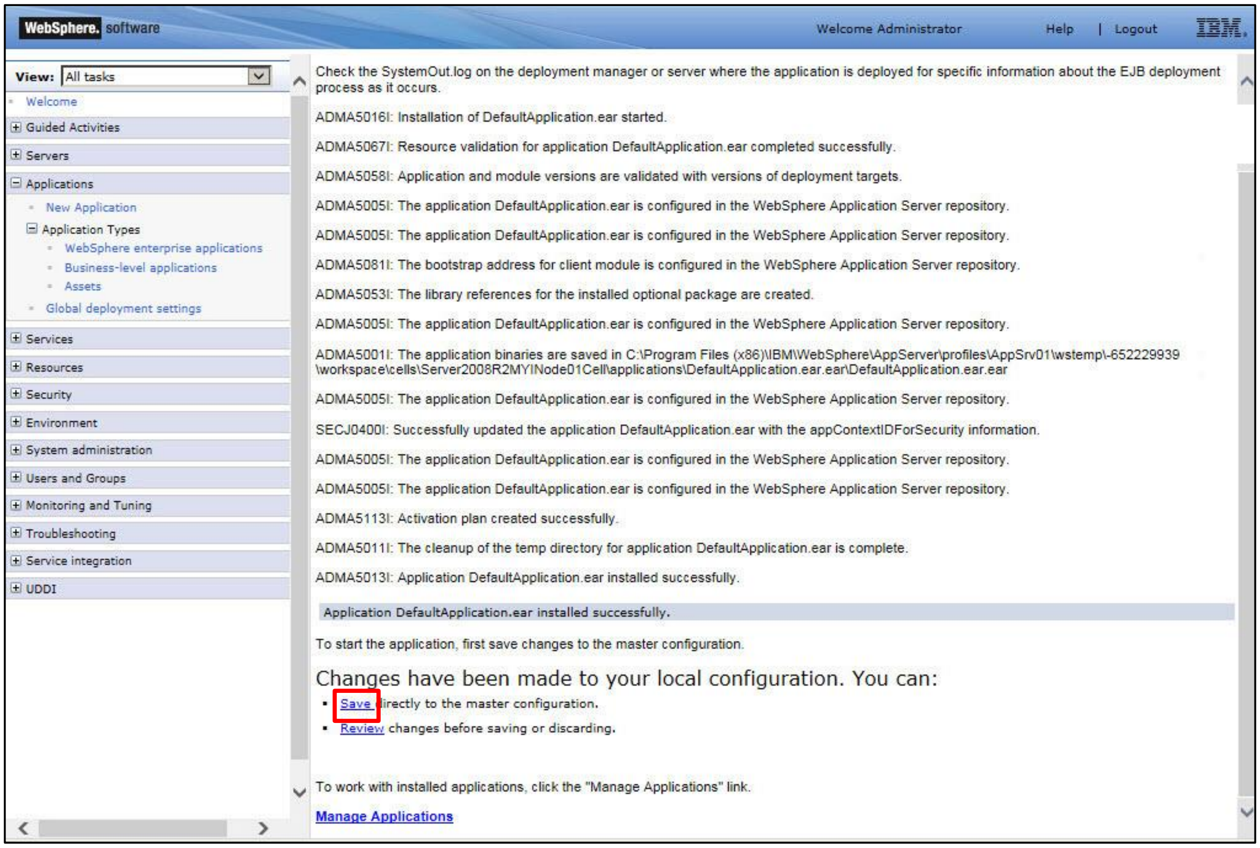
Field help
For field help information, select a field label or list marker when the help cursor is displayed.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

8. After successful installation, click **Save**



```
Check the SystemOut.log on the deployment manager or server where the application is deployed for specific information about the EJB deployment
process as it occurs.

ADMA5016I: Installation of DefaultApplication.ear started.

ADMA5067I: Resource validation for application DefaultApplication.ear completed successfully.

ADMA5058I: Application and module versions are validated with versions of deployment targets.

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

ADMA5081I: The bootstrap address for client module is configured in the WebSphere Application Server repository.

ADMA5053I: The library references for the installed optional package are created.

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

ADMA5001I: The application binaries are saved in C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01\wstemp\-652229939
\workspace\cells\Server2008R2MYINode01Cell\applications\DefaultApplication.ear.ear\DefaultApplication.ear.ear

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

SECJ0400I: Successfully updated the application DefaultApplication.ear with the appContextIDForSecurity information.

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

ADMA5005I: The application DefaultApplication.ear is configured in the WebSphere Application Server repository.

ADMA5113I: Activation plan created successfully.

ADMA5011I: The cleanup of the temp directory for application DefaultApplication.ear is complete.

ADMA5013I: Application DefaultApplication.ear installed successfully.
```

Application DefaultApplication.ear installed successfully.

To start the application, first save changes to the master configuration.

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

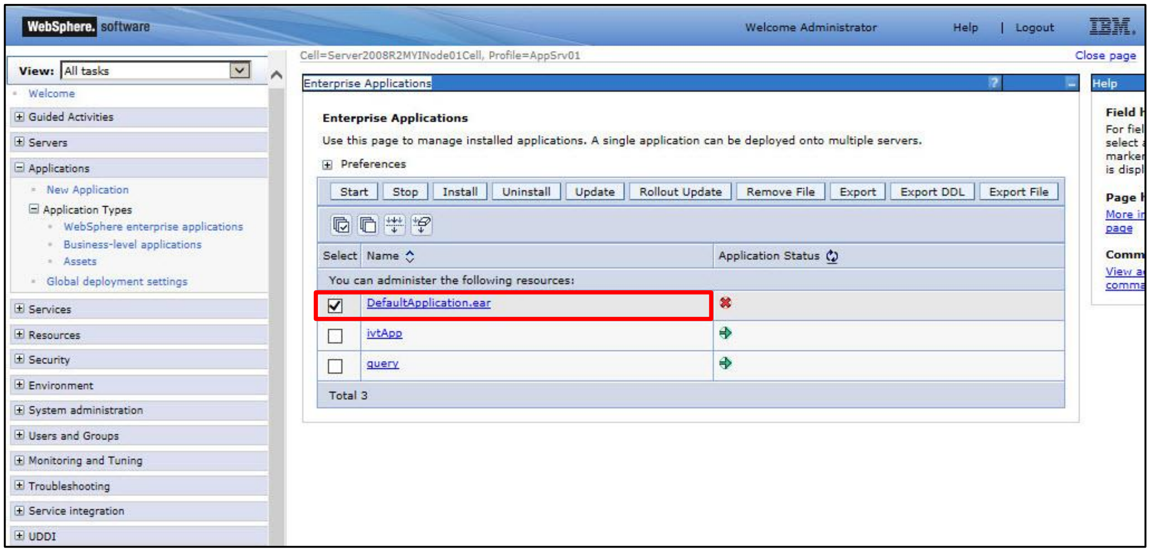
To work with installed applications, click the "Manage Applications" link.

Manage Applications

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

Starting the Enterprise Application

1. On the WebSphere Application Server Administrator console, in the left pane, click **Applications** > **Application Types** > **WebSphere enterprise applications**, and then in the center pane, select the installed application (for example, **DefaultApplication.ear**).



Cell=Server2008R2MYINode01Cell, Profile=AppSrv01

Enterprise Applications

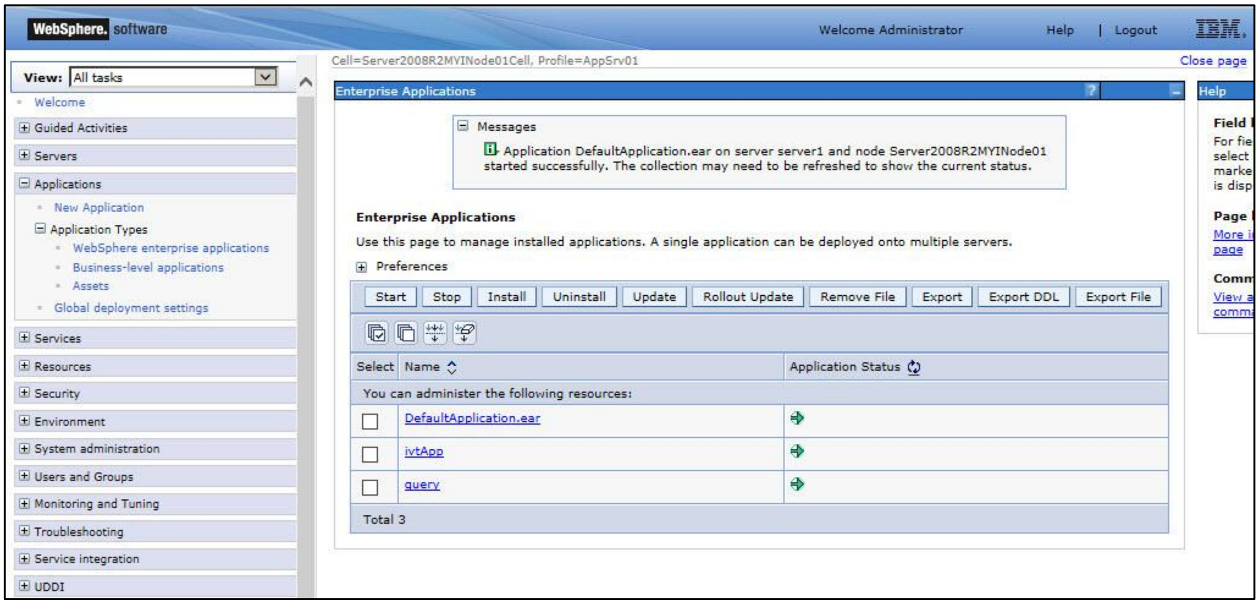
Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
☑	DefaultApplication.ear	✖
□	ivtApp	➔
□	query	➔
Total 3		

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

2. Click **Start**. The application is started successfully and the application status is changed to ➔.



Messages

Application DefaultApplication.ear on server server1 and node Server2008R2MYINode01 started successfully. The collection may need to be refreshed to show the current status.

Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
□	DefaultApplication.ear	➔
□	ivtApp	➔
□	query	➔
Total 3		

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)

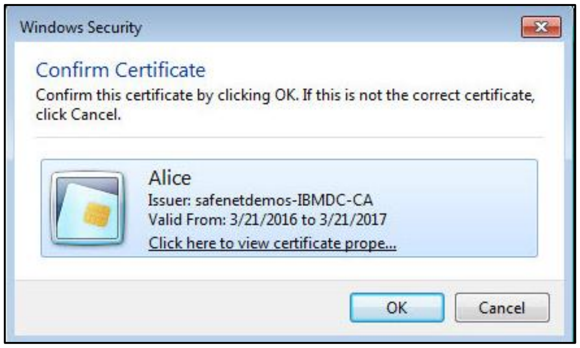
Running the Solution

Before running the solution, ensure that a Smart card user certificate must be present on the SafeNet USB token.

1. Insert the SafeNet USB token into the client machine.
2. In a web browser, open the following url:

   https:// <Server IP or Name>:<SSL Port>/<Application>

   Where, <**Server IP or Name>** is the IP address or name of the IBM WebSphere Application server, **<SSL Port>** is the SSL port number based on the created installation profile, and **<Application>** is the application path (for example, **/snoop)** in **Default App.Ear**.
3. You will be redirected to the **Confirm Certificate** window. Click **OK**.

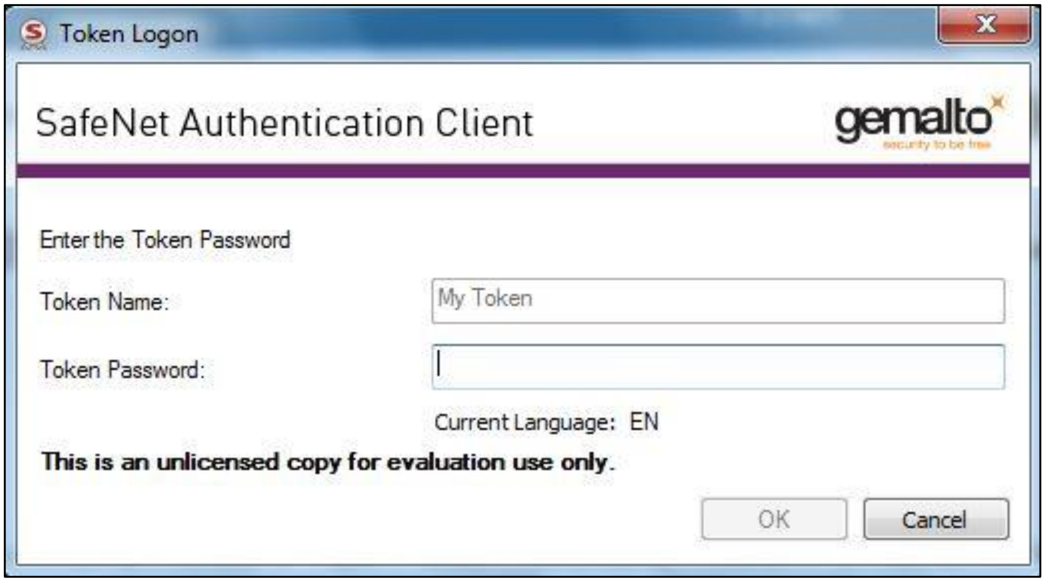


Confirm Certificate

Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

Alice
Issuer: safenetdemos-IBMDC-CA
Valid From: 3/21/2016 to 3/21/2017
Click here to view certificate prope...

4. On the **SafeNet Authentication Client** login window, enter the token password, and then click **OK**.



Enter the Token Password

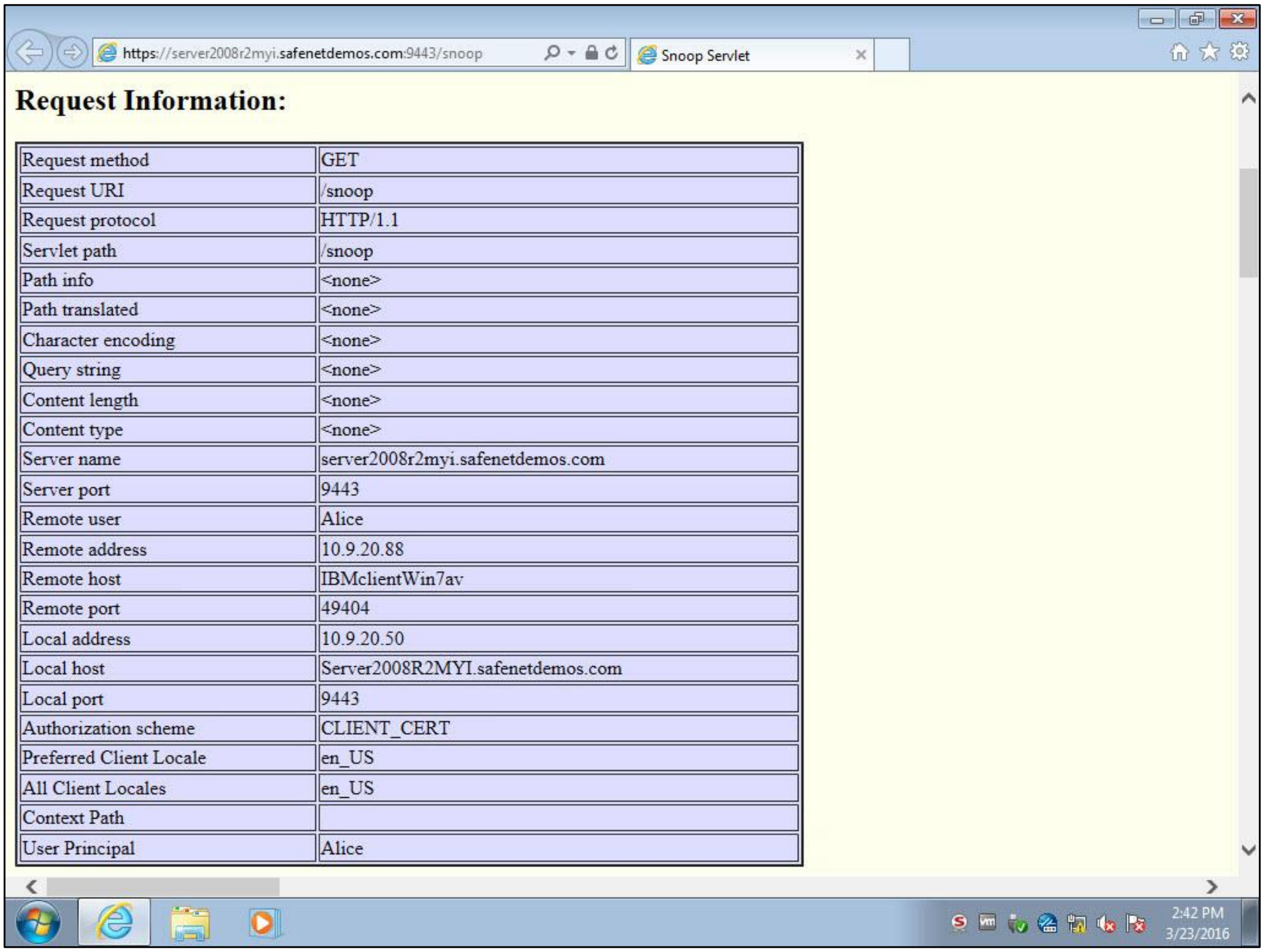
Token Name: My Token

Token Password:

Current Language: EN

This is an unlicensed copy for evaluation use only.

After successful authentication, the requested information is displayed.



Request Information:

Request method	GET
Request URI	/snoop
Request protocol	HTTP/1.1
Servlet path	/snoop
Path info	<none>
Path translated	<none>
Character encoding	<none>
Query string	<none>
Content length	<none>
Content type	<none>
Server name	server2008r2myi.safenetdemos.com
Server port	9443
Remote user	Alice
Remote address	10.9.20.88
Remote host	IBMclientWin7av
Remote port	49404
Local address	10.9.20.50
Local host	Server2008R2MYI.safenetdemos.com
Local port	9443
Authorization scheme	CLIENT_CERT
Preferred Client Locale	en_US
All Client Locales	en_US
Context Path	
User Principal	Alice

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	