Configuring LDAP authentication and SSO for OMNIbus Web GUI and Impact

Non-customer-specific version 3.6

December 12, 2016

Author: Dave Thompson (dthmpson@us.ibm.com)

CONTENTS

Overview

This document describes the process and the steps required to perform the following tasks:

- Setup Active Directory authentication for OMNIbus Web GUI installed under DASH (Dashboard Application Services Hub), including using an SSL connection to Active Directory.
- Setup Active Directory authentication for an Impact Cluster installed on separate hosts than the DASH server, including using an SSL connection to Active Directory.
- Setup SSO (Single Sign-on) between DASH and Impact.
- Add an Impact GUI Console Integration to DASH so that the Impact GUI can be launched from the DASH GUI.

This document assumes that OMNIbus, Web GUI, DASH, and Impact are already installed and functional. This document does not cover any work related to ITNM (IBM Tivoli Network Manager).

Products and versions used for this example

NOI (Netcool Operations Insight) version 1.4

Web GUI 8.1

Omnibus 8.1

Impact 7.1

Microsoft Active Directory is used as the LDAP directory.

LDAP structure for this example

BaseDN: DC=xyz,DC=com

Users: OU=XYZ Users,DC=xyz,DC=com

Groups: OU=Groups,DC=xyz,DC=com

Netcool permissions are based on the Netcool groups:

E.g.:   cn=netcool_admin,OU=Groups,DC=xyz,DC=com

Chapter 1 Configuring Active Directory authentication for Web GUI when the ObjectServer is currently used for authentication

Web GUI user authentication overview

Web GUI users accounts must be configured in two locations: in DASH, so that they can log in to the Web GUI, and in the ObjectServer so that they can use tools that write to the ObjectServer such as the Active Event List. The authentication mechanism for Web GUI users is provided by the Virtual Member Manager (VMM) component.

You can use VMM to access and maintain user data in multiple repositories, and to federate that data into a single virtual repository. The federated repository consists of a single named *realm*, which is a set of independent user repositories. The ObjectServer or an LDAP directory can be defined as a repository. All user names need to be unique across the repositories. All repositories in the realm need to be running when the Web GUI is started under normal conditions.

If Web GUI users are authenticated against an LDAP directory rather than the ObjectServer, the users in the LDAP repository can be synchronized with the ObjectServer so that they can use functions that write to the ObjectServer.

The high-level steps to set up external LDAP authentication are:

1. If Web GUI is already using ObjectServer authentication, you will need to remove the ObjectServer repository from the realm.
2. Contact your LDAP administrator and obtain information about the LDAP directory; details regarding the required information are provided later in this document. You will need this information to add the LDAP repository to the VMM realm.
3. Configure a repository that uses the LDAP directory, and add the LDAP repository to the VMM realm.
4. Assign the ncw_admin role or the ncw_user role to the users and groups that you want to be synchronized to the ObjectServer. If you assign the roles to user groups rather than the individual users, the roles cascade to the users in the groups.
5. Enable synchronization of the LDAP users with the ObjectServer. Users with the specified roles are then synchronized with the ObjectServer so that they can use the Web GUI functions that write to the ObjectServer.

Important! While synchronization is enabled, the ObjectServer cannot be defined as a repository in the VMM realm

1.1 Backup the file repository and security configuration files

You can use these files to restore the previous VMM configuration in case something goes wrong while setting up LDAP authentication.

__1. Backup the VMM configuration file wmconfig.xml. Example location: /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config/wimconfig.xml

If the configuration of Active Directory authentication fails, you can recover the original ObjectServer based authentication configuration for DASH by copying the backup file back to the original location, and then restarting DASH.

__2. Optionally backup the following files:

- /opt /IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/security.xml
- /opt/ /IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/fileRegistry.xml

1.1 Determine if user accounts in Active Directory will be created or modified from the DASH.

If you intend to be able to create or modify user accounts in Active Directory from DASH, there are several considerations:

- You will need an LDAP "bind user" account with read and write access to your Active Directory instance.
- You will need to use a secure connection to Active Directory.
- You will need to change the RDN (Relative Distinguished Name) property for the PersonAccount entity type in your federated repository.
    - This will require some additional steps the first time that you change or save any of your file-based repository users (including the DASH administrative user) after making this change to the PersonAccount entity type settings.

1.2 Verify that you have the required LDAP information from your LDAP administrator

__1. The hostname and port of the primary LDAP server.

The default port is 389, or 636 for a secure connection.

__2. The hostname and port of the backup LDAP server, if you plan to use a backup LDAP server.

__3. The type of LDAP directory.

For example, Microsoft Active Directory.

__4. The version of LDAP that is supported by the LDAP directory.

__5. The username and password of the “bind user”. In this example, we will use CN=Administrator,CN=Users,DC=xyz,DC=com.

- This user connects to the LDAP directory to query the LDAP subtree where your users and groups will exist.
- This user must be a unique user in the VMM realm.
- No spaces are allowed in the user name.
- If you want to be able to add users and groups to LDAP using the DASH GUI, this user needs write permissions on the LDAP subtree where the users and groups will be created.
    - With Microsoft Active Directory, you will also need to use a secure connection to be able to add users from the DASH GUI.

__6. The LDAP base DN (Distinguished Name) where all searches start, and the LDAP subtree(s) where the users and groups will exist.

- In this example, the base DN is: DC=xyz,DC=com.
- In this example, users will exist in: OU=XYZ Users,DC=xyz,DC=com
- In this example, groups will exist in: OU=Groups,DC=xyz,DC=com

__7. Determine whether an SSL connection will be used from DASH to the LDAP directory.

Additional setup steps are required if SSL is used; those steps are covered in this document.

1.3 Verify that the ObjectServer and Active Directory are available

__1. Verify that the LDAP server is up, and that its fully qualified host name can be accessed (pinged at this point) from the DASH server.

__2. Verify that the ObjectServer is up and check that ObjectServer based users can login to the Web GUI.

1.4 Remove the ObjectServer repository from the DASH federated repository

This is required for user synchronization from DASH / LDAP to the ObjectServer to work correctly.

Deletion of default DASH Web GUI users

NOI technical training materials recommend deleting the default Web GUI users and groups from DASH if they were previously created using the OMNIbus Web GUI Configuration Tool prior to converting from ObjectServer to LDAP authentication. The Omnibus 8.1.0 documentation does not address this topic in the case of converting from ObjectServer to LDAP authentication, and only requires deleting the default Web GUI users in the case of converting from a file based repository to LDAP authentication.

The default users and groups are the ncoadmin and ncouser users, and the Netcool_OMNIbus_Admin and Netcool_OMNIbus_User groups. The approach of removing these users and groups from DASH prior to removing the ObjectServer repository was used successfully in the lab environment that was used when creating this document. Note that this document does not address the use case where ITNM is already installed and DASH user accounts and groups for ITNM access have already been created using ObjectServer authentication.

It is also recommended to remove any “custom” file-based repository users that were manually added after the initial DASH and Web GUI installation. However, you must leave users such as smadmin that are required by JazzSM / DASH. Also, if you have added file-based repository users for the purpose of allowing access to Web GUI when Active Directory is not available, you should not delete those users.

Only groups and users that are either in Active Directory or in the local file based repository used by WebSphere will initially be available in DASH and the WebSphere administrative console after Active Directory authentication is configured. Typically, the only user in the file-based repository is the smadmin user.

You will also need to re-apply roles to the users and groups after changing to Active Directory authentication. Unless you are changing the authentication mechanism on a new installation DASH and Web GUI, you should document the existing groups, users, group memberships, and group and user role mappings so that the same settings can be re-applied.

For reference, the roles listed for the default groups in the OMNIbus 8.1 documentation are listed here:

Netcool_OMNIbus_Admin:

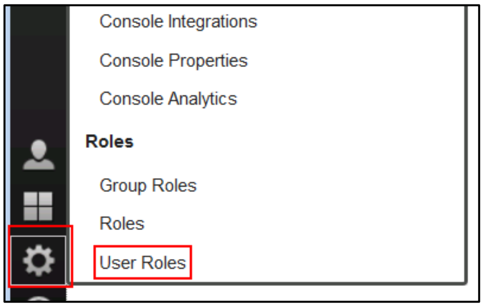
- ncw_admin
- ncw_dashboard_editor
- ncw_gauges_editor

- ncw_user
- netcool_rw

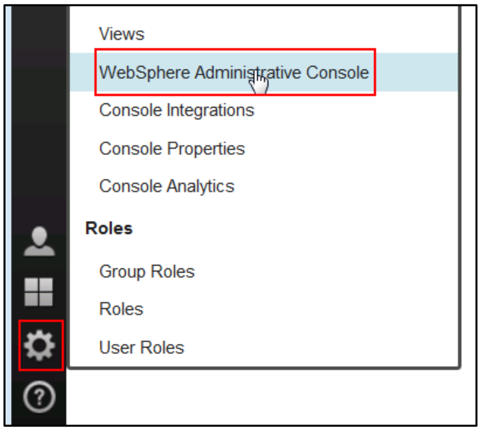
Netcool_OMNIbus_Admin:

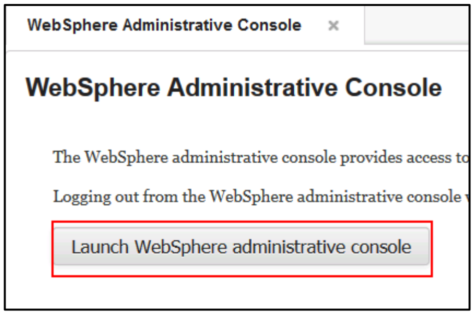
- ncw_user
- netcool_ro

__1. Login to the DASH GUI as the DASH administrative user (typically smadmin), select **User Roles**, and remove any DASH roles from all ObjectServer based users. Note that this does not include the smadmin user; do not modify this user.



__2. From the DASH GUI, select **Console Settings -> WebSphere Administrative Console**, and then launch the WebSphere administrative console:




WebSphere Administrative Console ×

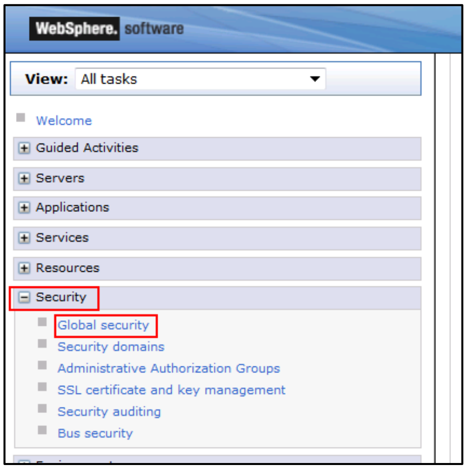
WebSphere Administrative Console

The WebSphere administrative console provides access to

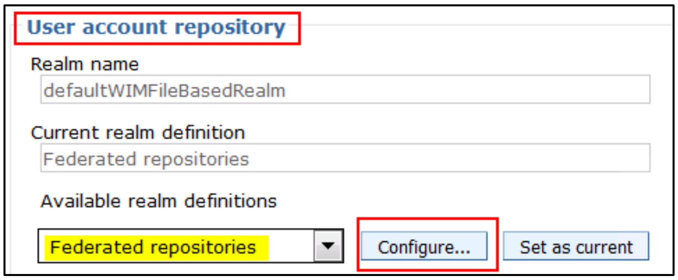
Logging out from the WebSphere administrative console

Launch WebSphere administrative console

__3. Once in the WebSphere Administrative Console, select **Security -> Global Security**:



__4. Under the **User account repository** section, make sure that the **Federated repositories** option is selected under **Available realm definitions**, then click the **Configure…** button.



User account repository

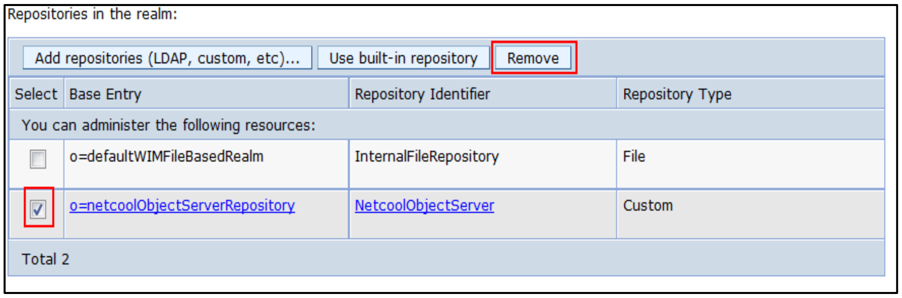
Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

__5. Remove all references to the ObjectServer from the federated repository.

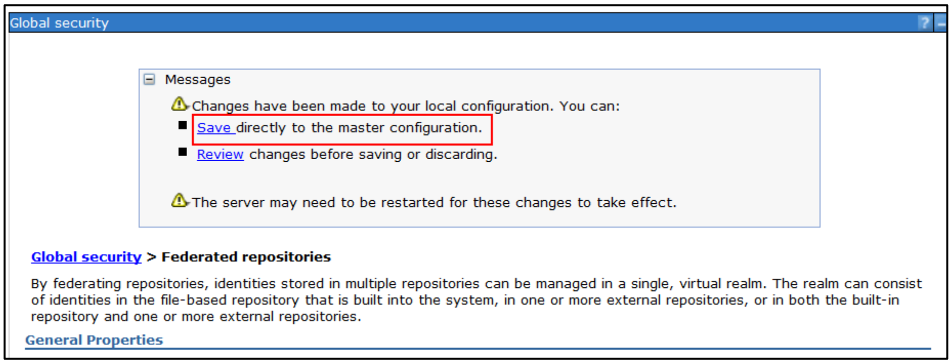
__a. Check the selection box for the ObjectServer repository, then click the **Remove** button:



Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
☑	o=netcoolObjectServerRepository	NetcoolObjectServer	Custom
Total 2			

__b. Click **Save directly to the master configuration**.



Global security

Messages

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

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

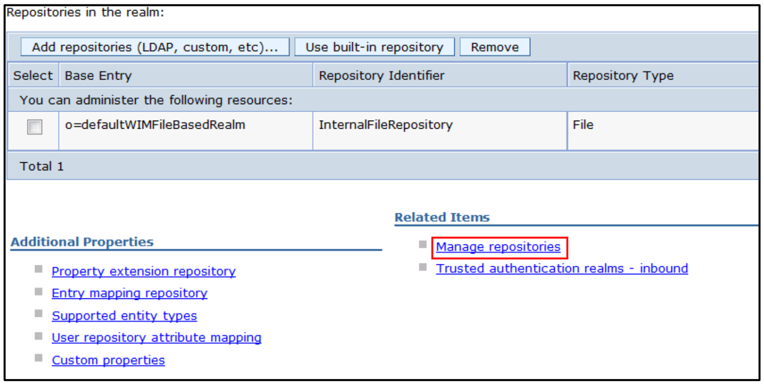
The server may need to be restarted for these changes to take effect.

Global security > **Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

__c. In the **Related Items** section below the **Repositories in the realm** section click **Manage Repositories**:



Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

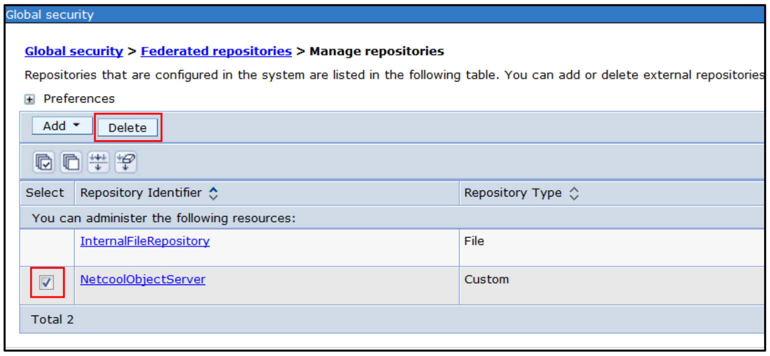
Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types
- User repository attribute mapping
- Custom properties

Related Items

- Manage repositories
- Trusted authentication realms - inbound

__d. Check (select) the selection box for the **NetcoolObjectServer** repository and click the **Delete** button:



Global security

Global security > Federated repositories > **Manage repositories**

Repositories that are configured in the system are listed in the following table. You can add or delete external repositories

Preferences

Select	Repository Identifier	Repository Type
You can administer the following resources:		
	InternalFileRepository	File
☑	NetcoolObjectServer	Custom
Total 2		

__e. Save directly to the master configuration.

__6. Restart DASH

1.5 Add file based repository "emergency" users

This step is optional, and should only be performed if:

- You want to have “emergency use” Web GUI users other than the DASH administrative user available in the situation where Active Directory is not available for authentication.
- You have not already added file based repository users for this purpose during your initial setup of DASH prior to setting up ObjectServer based authentication.

Notes regarding file base repository users:

- These users are intended for emergency access to the Web GUI only.
- These users cannot be added to Active Directory based groups, and so will not be synched into the ObjectServer.
- Since these users cannot be added to Active Directory based groups, OMNIbus related roles will need to be assigned directly to the users.
- These users may have read-only access to the Web GUI, depending on addition steps you take that are outside of the scope of this document.
- The passwords for these users will not be maintained in Active Directory and therefore may not be checked for corporate password rules compliance.

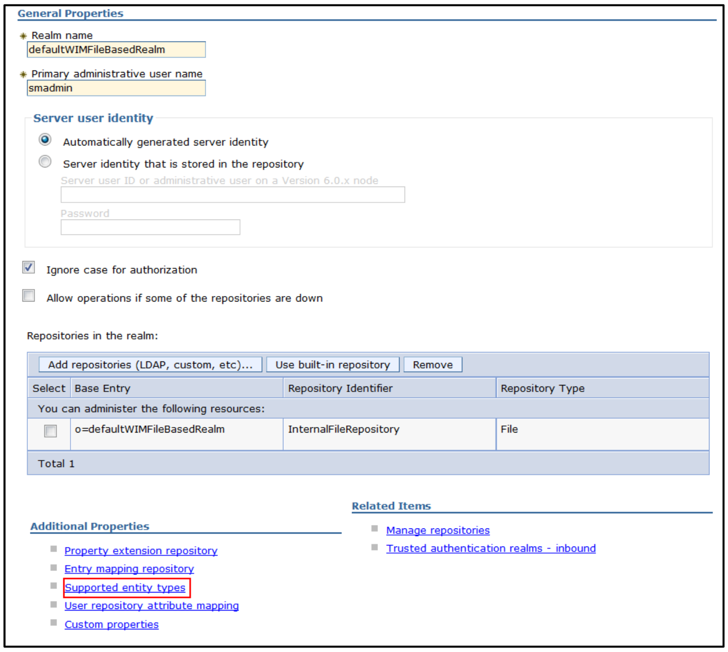
__1. Check that all supported entity types for the file based repository use o=defaultWIMFileBasedRealm for their **Base Entry for the Default Paren**t value.

__a. Login to the DASH GUI as the DASH administrative user, select **Console Settings -> WebSphere Administrative Console**, and then launch the WebSphere administrative console.

__b. Once in the WebSphere Administrative Console, select **Security -> Global Security.**

__c. Under the **User account repository** section, make sure that the **Federated repositories** option is selected under **Available realm definitions**, then click the **Configure…** button.

__d. Near the bottom of the resulting page, click Supported entity types:



General Properties

* Realm name: defaultWIMFileBasedRealm

* Primary administrative user name: smadmin

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

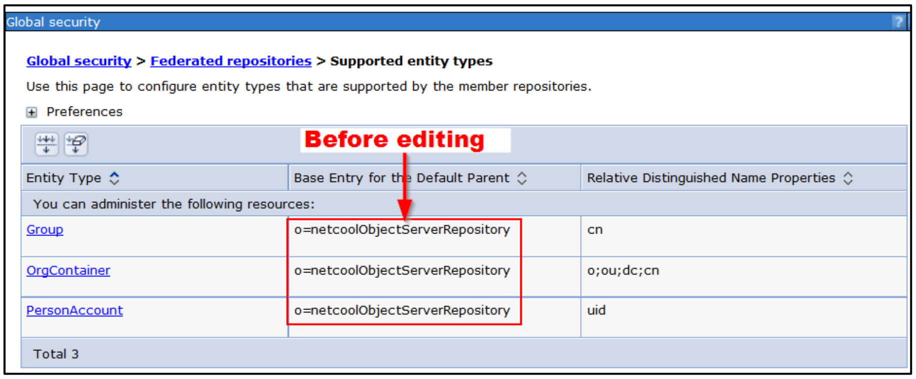
☑ Ignore case for authorization

□ Allow operations if some of the repositories are down

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

__e. If the value of **Base Entry for the Default Parent** for each **Entity Type** is not **o=defaultWIMFileBasedRealm**, edit the **Entity Type** to change the value of **Base Entry for the Default Parent** to **o=defaultWIMFileBasedRealm**. Save your changes directly to the master configuration when prompted to do so.



Global security

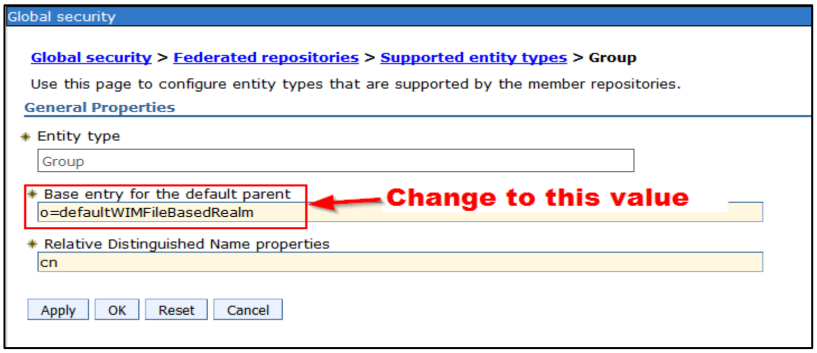
Global security > Federated repositories > **Supported entity types**

Use this page to configure entity types that are supported by the member repositories.

⊞ Preferences

Before editing

Entity Type	Base Entry for the Default Parent	Relative Distinguished Name Properties
You can administer the following resources:		
Group	o=netcoolObjectServerRepository	cn
OrgContainer	o=netcoolObjectServerRepository	o;ou;dc;cn
PersonAccount	o=netcoolObjectServerRepository	uid
Total 3		



Global security

Global security > Federated repositories > Supported entity types > **Group**

Use this page to configure entity types that are supported by the member repositories.

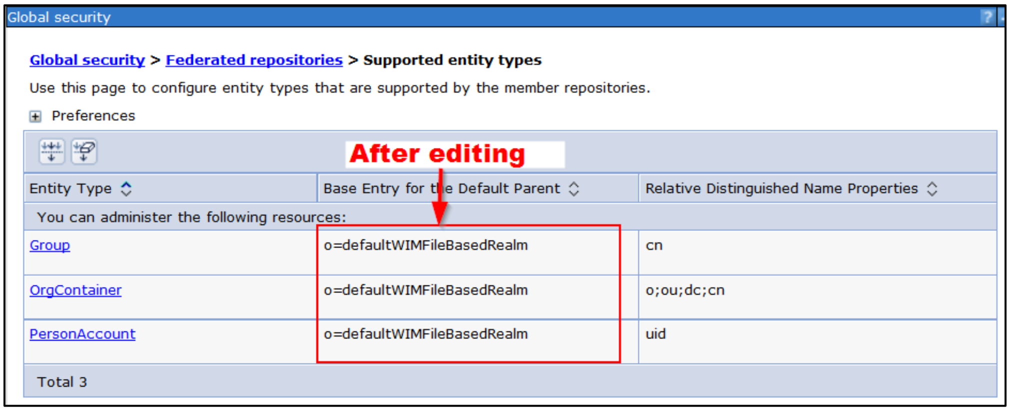
General Properties

* Entity type
Group

* Base entry for the default parent
o=defaultWIMFileBasedRealm

Change to this value

* Relative Distinguished Name properties
cn



Global security

Global security > Federated repositories > **Supported entity types**

Use this page to configure entity types that are supported by the member repositories.

⊞ Preferences

After editing

Entity Type	Base Entry for the Default Parent	Relative Distinguished Name Properties
You can administer the following resources:		
Group	o=defaultWIMFileBasedRealm	cn
OrgContainer	o=defaultWIMFileBasedRealm	o;ou;dc;cn
PersonAccount	o=defaultWIMFileBasedRealm	uid
Total 3		

__f. If you made any changes, log out of the WebSphere Administrative Console and the DASH GUI, and restart DASH so that the changes take effect.

__2. If you restarted DASH, log back into the DASH GUI as the DASH administrative user and launch the WebSphere Administrative Console.

__3. In the WebSphere Administrative Console, navigate to **Users and Groups->Manage Users** and add user accounts for emergency use if Active Directory is not available.

__4. From the DASH GUI, navigate to **Console Settings->Roles->User Roles** and add roles such as **ncw_user** or **ncw_admin** to allow the users the desired access levels to the Web GUI.

1.6 Import the Active Directory server's SSL certificate into DASH

> **Perform this step only if you are using a secure connection to the Active Directory server**
>
> If you do not use a secure connection for your initial install and later change to a secure connection, you can perform this step later when you change to a secure connection.

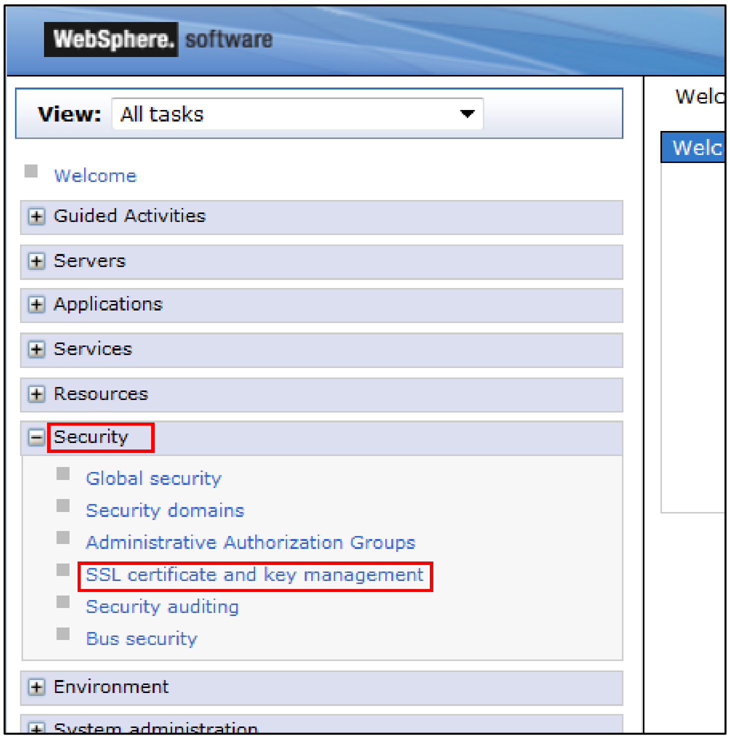
This work must be performed on all DASH servers.

__1. Verify that you can ping the fully qualified hostname of the Active Directory server from the DASH server.

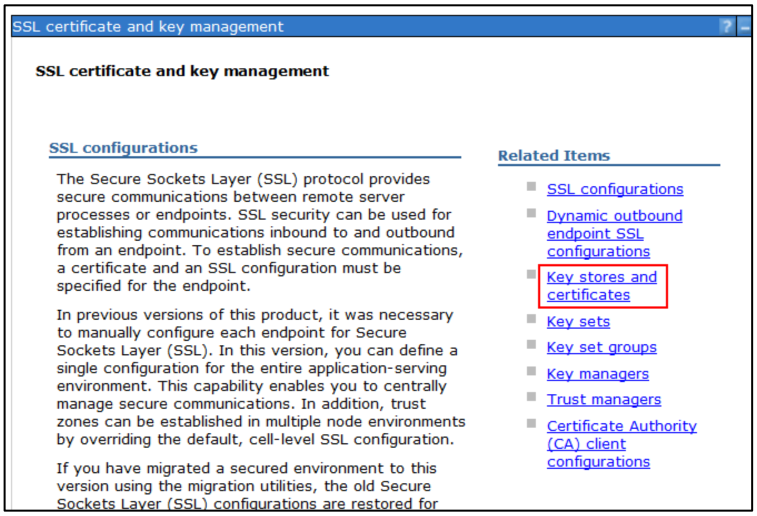
__2. Verify that you have obtained the SSL port used for Active Directory from your Active Directory administrator.

__3. Login to the DASH GUI as the DASH administrative user, select **Console Settings -> WebSphere Administrative Console**, and then launch the WebSphere administrative console.

__4. In the main WebSphere administrative console menu, navigate to **Security -> SSL certificate and key management**.



__5. From the **SSL certificate and key management panel**, click **Key stores and certificates**.


SSL certificate and key management
Related Items
SSL configurations
Dynamic outbound endpoint SSL configurations
Key stores and certificates
Key sets
Key set groups
Key managers
Trust managers
Certificate Authority (CA) client configurations

SSL certificate and key management

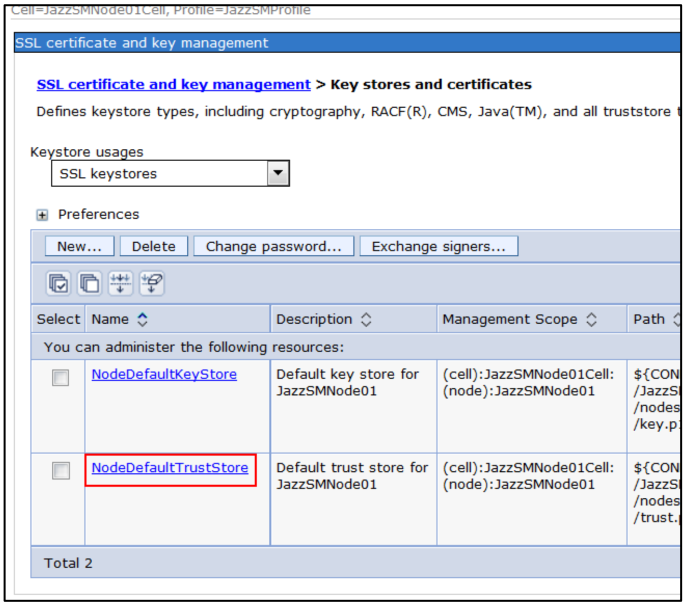
SSL configurations

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

__6. From the **Key stores and certificates** panel, click **NodeDefaultTrustStore**.



Cell=JazzSMNode01Cell, Profile=JazzSMProfile

SSL certificate and key management

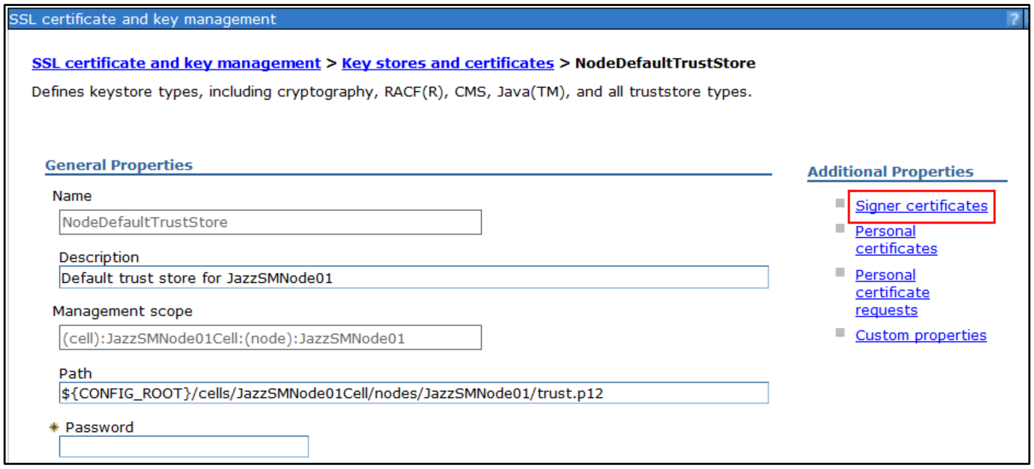
SSL certificate and key management > Key stores and certificates

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

Keystore usages: SSL keystores

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
□	NodeDefaultKeyStore	Default key store for JazzSMNode01	(cell):JazzSMNode01Cell:(node):JazzSMNode01	${CON /JazzS /nodes /key.p
□	NodeDefaultTrustStore	Default trust store for JazzSMNode01	(cell):JazzSMNode01Cell:(node):JazzSMNode01	${CON /JazzS /nodes /trust.
Total 2				

__7. From the **NodeDefaultTrustStore** panel, click **Signer Certificates**.



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 JazzSMNode01

Management scope: (cell):JazzSMNode01Cell:(node):JazzSMNode01

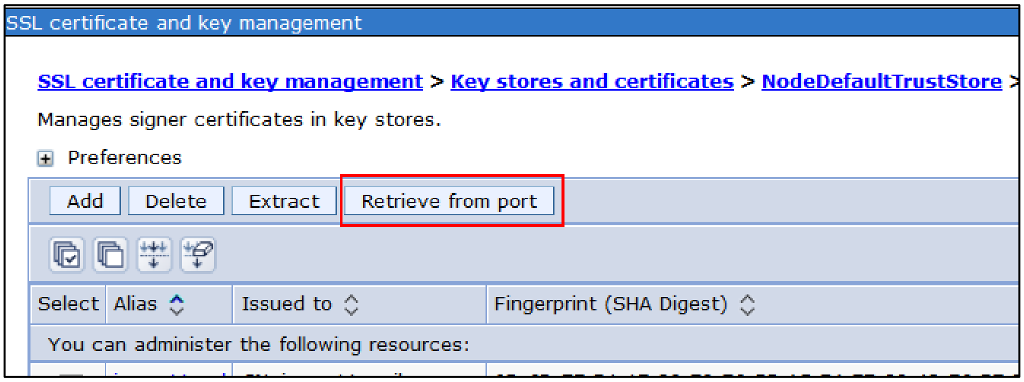
Path: ${CONFIG_ROOT}/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12

* Password

Additional Properties

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

__8. From the **Signer certificates** panel, click the **Retrieve from port** button.



SSL certificate and key management

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

Manages signer certificates in key stores.

Select	Alias	Issued to	Fingerprint (SHA Digest)
You can administer the following resources:			

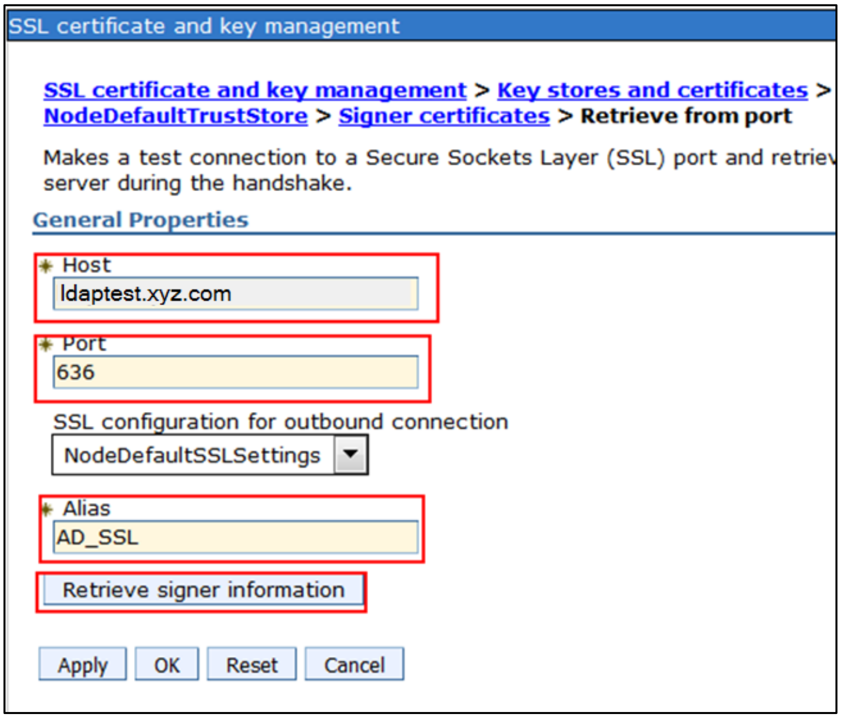
__9. In the **Retrieve from port** panel, fill in the following data fields:

__a. Host: Enter the fully qualified hostname of the Active Directory server

__b. Port: Enter the SSL port that Active Directory is listening on. The default is 636, but you should use the SSL port provided by your Active Directory administrator.

__c. Alias: A string to reference this signer certificate in the DASH key store This can be a string of your choice, such as **AD_SSL**.

__d. Leave the **SSL configuration for outbound connection** value set to **NodeDefaultSSLSettings**.



SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Retrieve from port

Makes a test connection to a Secure Sockets Layer (SSL) port and retriev server during the handshake.

General Properties

* Host: ldaptest.xyz.com

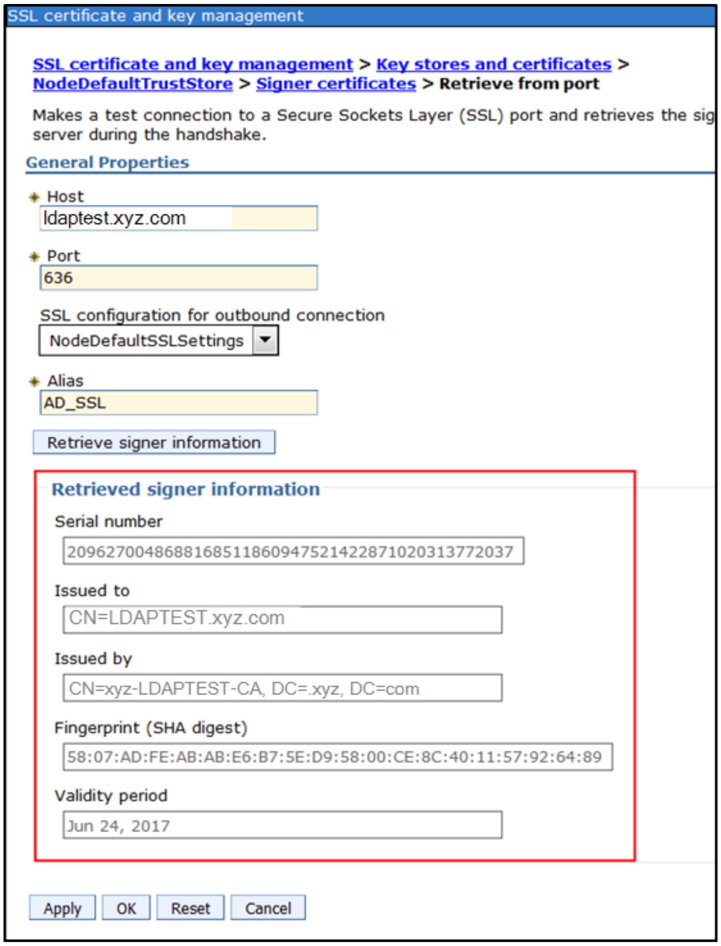
* Port: 636

SSL configuration for outbound connection: NodeDefaultSSLSettings

* Alias: AD_SSL

__10. Click the **Retrieve signer information** button.

You should see the retrieved signer information:



SSL certificate and key management

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

Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the sig server during the handshake.

General Properties

* Host: ldaptest.xyz.com

* Port: 636

SSL configuration for outbound connection: NodeDefaultSSLSettings

* Alias: AD_SSL

Retrieved signer information

Serial number: 2096270048688168511860947521422871020313772037

Issued to: CN=LDAPTEST.xyz.com

Issued by: CN=xyz-LDAPTEST-CA, DC=.xyz, DC=com

Fingerprint (SHA digest): 58:07:AD:FE:AB:AB:E6:B7:5E:D9:58:00:CE:8C:40:11:57:92:64:89

Validity period: Jun 24, 2017

Important! You must successfully retrieve the signer information before continuing

Correct any issues and retrieve the signer information before continuing.

__11. Click **OK**.

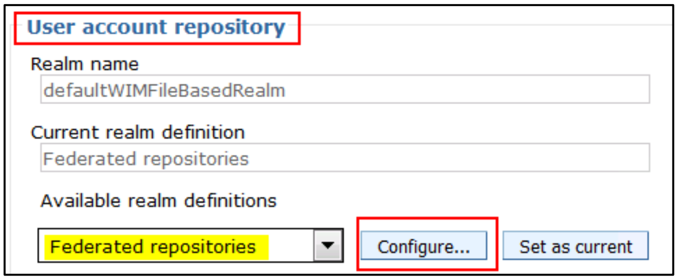
__12. Save directly to the master configuration.

1.7 Adding the LDAP repository to DASH

__1. Login to the DASH GUI as the DASH administrative user, select **Console Settings -> WebSphere Administrative Console**, and then launch the WebSphere administrative console.

__2. Navigate to **Security -> Global Security**.

__3. Under the **User account repository** section, select the **Federated repositories** option under **Available realm definitions**, then click the **Configure…** button.



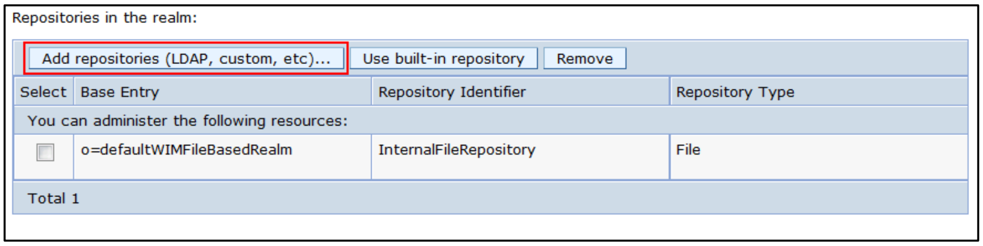
User account repository

Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

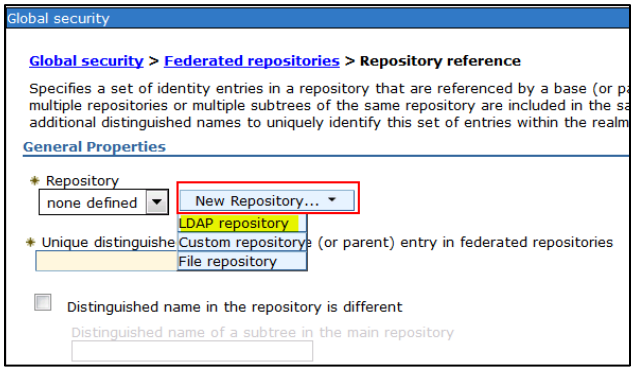
__4. Click the **Add repositories** button:



Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

__5. Click **New Repository** and select **LDAP repository**.



Global security

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or p
multiple repositories or multiple subtrees of the same repository are included in the sa
additional distinguished names to uniquely identify this set of entries within the realm

General Properties

Repository: none defined

Unique distinguishe (or parent) entry in federated repositories

□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository

__6. Fill in or select the following fields:

__a. Repository identifier: Provide a unique identifier for this repository in the WebSphere cell. This can be a string of your choice. Use a name that is meaningful to you.

__b. Directory Type: Select the type of LDAP directory you are using. For this example, we are using **Microsoft Windows Active Directory**.

__c. Primary host name: The resolvable hostname of the primary LDAP server that you obtained from your LDAP administrator. Technically this can be an IP address, but it is recommended to use the fully qualified host name.

__d. Port: The LDAP port number that you obtained from your LDAP administrator.

> ⚠ **Important! This port number is different for secure and non-secure communications**

__i. If you are using non-secure communications, enter the non-SSL port number that your Active Directory administrator gave you. The default non-secure port is 389.

__ii. If you are using secure communications, enter the SSL port number that your Active Directory administrator gave you. The default SSL port is 636.

__e. You can add a hostname and port for a failover LDAP server if your LDAP administrator provided this information. Otherwise leave the failover server information blank.

__f. Bind distinguished name: This is the “bind user” that you obtained from your LDAP administrator.

__g. Bind password: The password for the bind user, obtained from your LDAP administrator.

__h. Federated repository properties for login: leave the value as **uid** for this example.

- This is the name of the property from the account in federated repository that will be used to login to the application server. Technically this is a semi-colon delimited list, so more values can be added.
- All login properties are searched during login. If multiple entries or no entries are found, an exception is thrown. For example, if you specify the login properties as **uid;mail** and the login ID as Bob, the search filter searches for **uid=Bob** or **mail=Bob**. When the search returns a single entry, then authentication can proceed. Otherwise, an exception is thrown.
- Supported configurations: If you define multiple login properties, the first login property is programmatically mapped to the federated repositories principalName property. For example, if you set uid;mail as the login properties, the LDAP attribute uid value is mapped to the federated repositories principalName property. If you define multiple login properties, after login, the first login property is returned as the value of the principalName property.

__i. LDAP attribute for Kerberos principal name: Leave the value blank for this example.

This specifies the LDAP attribute for Kerberos principal name. This field can be modified when Kerberos is configured and Kerberos is one of the active or preferred authentication mechanisms

__j. Certificate mapping: Leave the value as **EXACT_DN** for this example.

This determines whether to use exact distinguished name or a certificate filter to map X.509 certificates to into an LDAP directory.

__k. Certificate filter: Leave the value blank for this example.

- This is the certificate filter that will be used if the selection for certificate mapping is **CERTIFICATE_FILTER**.
- The filter is used to map attributes in the client certificate to entries in the LDAP repository
- The syntax or structure of this filter is: *LDAP attribute=${Client certificate attribute}*
- An example of a simple certificate filter is: `uid=${SubjectCN}`.

__l. Require SSL communications: Leave this box unchecked unless you are going to use SSL for communications with the LDAP server.

Important! You must have already added the SSL certificate for Active Directory to DASH if you select “Requires SSL communications”

Be sure that you have first completed the **Add file based repository “emergency” users**

This step is optional, and should only be performed if:

You want to have “emergency use” Web GUI users other than the DASH administrative user available in the situation where Active Directory is not available for authentication.

You have not already added file based repository users for this purpose during your initial setup of DASH prior to setting up ObjectServer based authentication.

Notes regarding file base repository users:

These users are intended for emergency access to the Web GUI only.

These users cannot be added to Active Directory based groups, and so will not be synched into the ObjectServer.

Since these users cannot be added to Active Directory based groups, OMNIbus related roles will need to be assigned directly to the users.

These users may have read-only access to the Web GUI, depending on addition steps you take that are outside of the scope of this document.

The passwords for these users will not be maintained in Active Directory and therefore may not be checked for corporate password rules compliance.

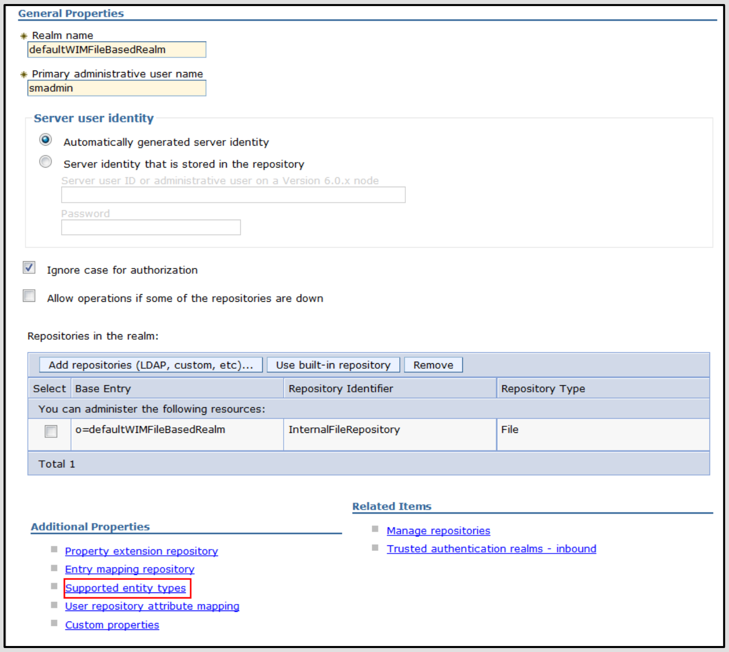
Check that all supported entity types for the file based repository use o=defaultWIMFileBasedRealm for their **Base Entry for the Default Parent** value.

Login to the DASH GUI as the DASH administrative user, select **Console Settings -> WebSphere Administrative Console**, and then launch the WebSphere administrative console.

Once in the WebSphere Administrative Console, select **Security -> Global Security.**

Under the **User account repository** section, make sure that the **Federated repositories** option is selected under **Available realm definitions**, then click the **Configure…** button.

Near the bottom of the resulting page, click Supported entity types:



General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
smadmin

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

☑ Ignore case for authorization

☐ Allow operations if some of the repositories are down

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types
- User repository attribute mapping
- Custom properties

Related Items

- Manage repositories
- Trusted authentication realms - inbound

If the value of **Base Entry for the Default Parent** for each **Entity Type** is not __i. If you are using SSL communications:

(1) Check the **Require SSL communications** check box.

(2) Select the **Centrally managed** radio button.

> **An SSL connection is required if you want to be able to create new Active Directory users from the DASH GUI**
>
> You cannot create new users or change user passwords from the WebSphere administrative console unless you are using a secure connection.
>
> Note that a bind user with read-write privileges in Active Directory is also required if you want to add or modify users or groups in Active Directory from the WebSphere administrative console.

▪

__b. Support referrals to other LDAP servers. Leave the value as **ignore** for this example.

- “ignore” means that this LDAP repository will not follow referrals to another LDAP server.
- “follow” means that this LDAP repository will follow referrals.

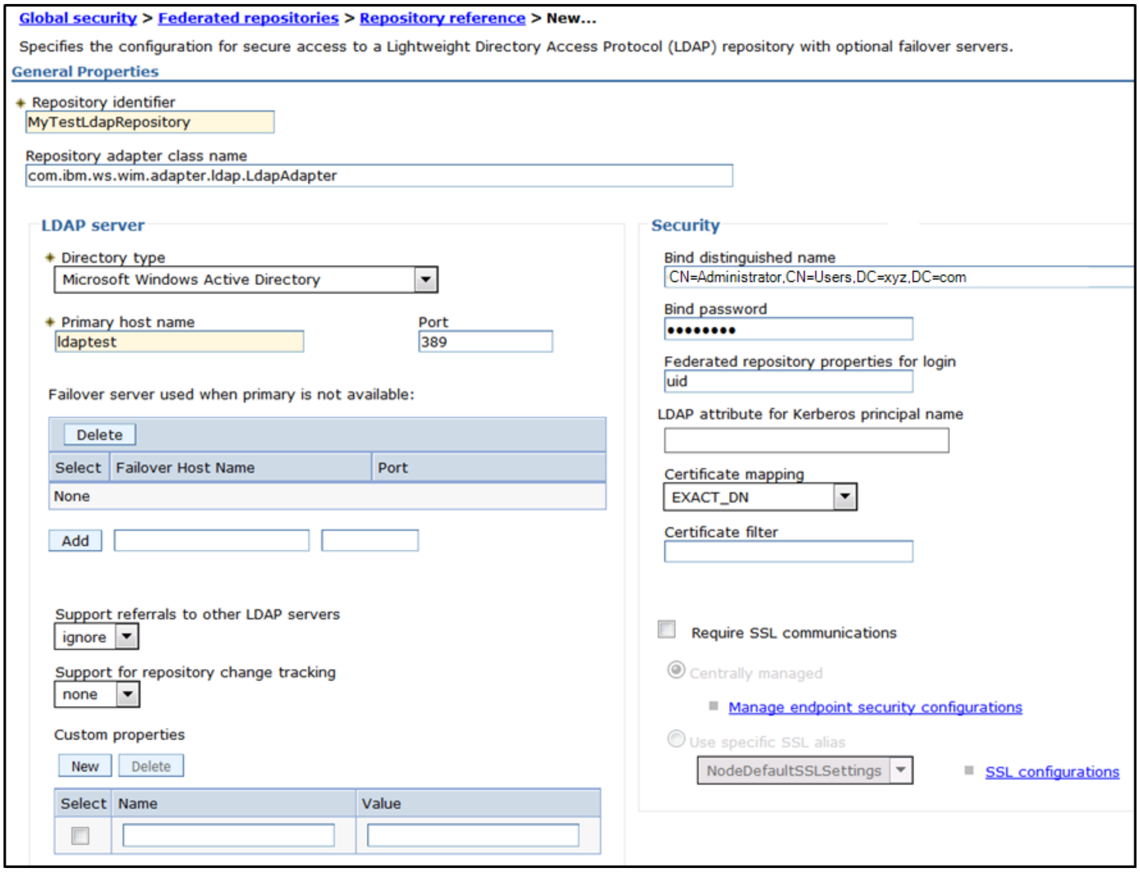
__c. Support for repository change tracking: Leave the value as **none** for this example.

- This specifies the type of support for repository change tracking. The profile manager refers to this value before passing on the request to the corresponding adapter.
  - “none” specifies that there is no change tracking support for this repository.
  - “native” specifies that the repository's native change tracking mechanism is used by virtual member manager to return changed entities.

__d. Custom properties: No custom properties are required for this example.

- Custom properties specify arbitrary name-value pairs of data. The name is a property key and the value is a string value that can be used to set internal system configuration properties.
- Defining a new property enables you to configure settings beyond those that are available in the administrative console.

__e. An example screen capture of a new LDAP Repository reference panel is shown here:



Global security > Federated repositories > Repository reference > New...

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

* Repository identifier: MyTestLdapRepository

Repository adapter class name: com.ibm.ws.wim.adapter.ldap.LdapAdapter

LDAP server

* Directory type: Microsoft Windows Active Directory

* Primary host name: ldaptest

Port: 389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers: ignore

Support for repository change tracking: none

Custom properties

Select	Name	Value
□		

Security

Bind distinguished name: CN=Administrator,CN=Users,DC=xyz,DC=com

Bind password: ••••••••

Federated repository properties for login: uid

LDAP attribute for Kerberos principal name:

Certificate mapping: EXACT_DN

Certificate filter:

□ Require SSL communications

● Centrally managed

Manage endpoint security configurations

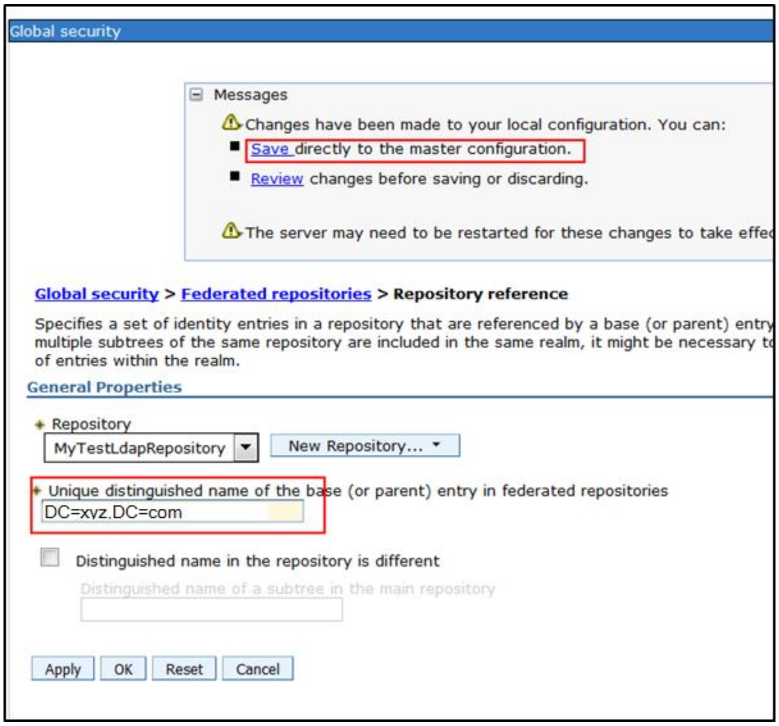
○ Use specific SSL alias: NodeDefaultSSLSettings

SSL configurations

__f. Click **OK**.

__11. In the next panel, enter the distinguished name that will be used as the base entry for this repository in the federated repository, then click **OK**.

- Typically, this will be the base DN that your searches for users and groups start from in the base repository; in this example DC=xyz,DC=com.
- If you want the base DN in the federated repository to be different than the base DN you search from in the LDAP repository, then check the **Distinguished name in the repository is different** check box, and provide the LDAP base DN you are using in the LDAP repository in the **Distinguished name of a subtree in the main repository** field.



Global security

⊟ 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 effec

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry multiple subtrees of the same repository are included in the same realm, it might be necessary t of entries within the realm.

General Properties

* Repository: MyTestLdapRepository ▼ New Repository... ▼

* Unique distinguished name of the base (or parent) entry in federated repositories: DC=xyz,DC=com

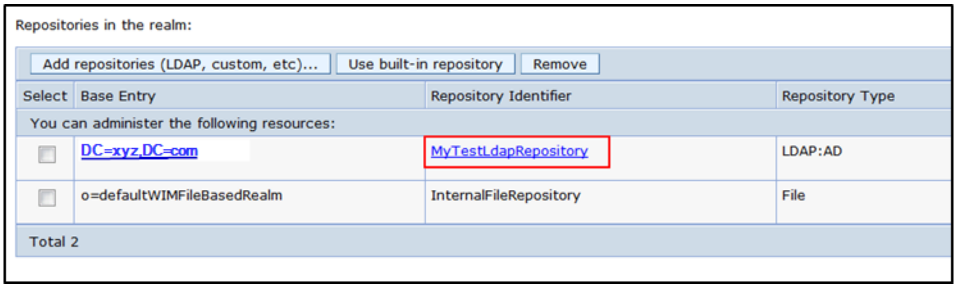
□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository

__12. Save directly to the master configuration.

__13. Define the LDAP subtrees and mappings for user and group information that will be visible from DASH (visible from the WebSphere administrative console).

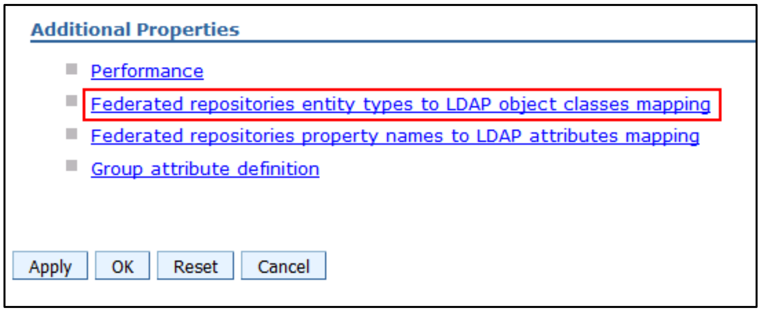
__a. Click the **Repository Identifier** for your LDAP repository in the **Repositories in the realm** table to return to the General Properties panel for that repository.



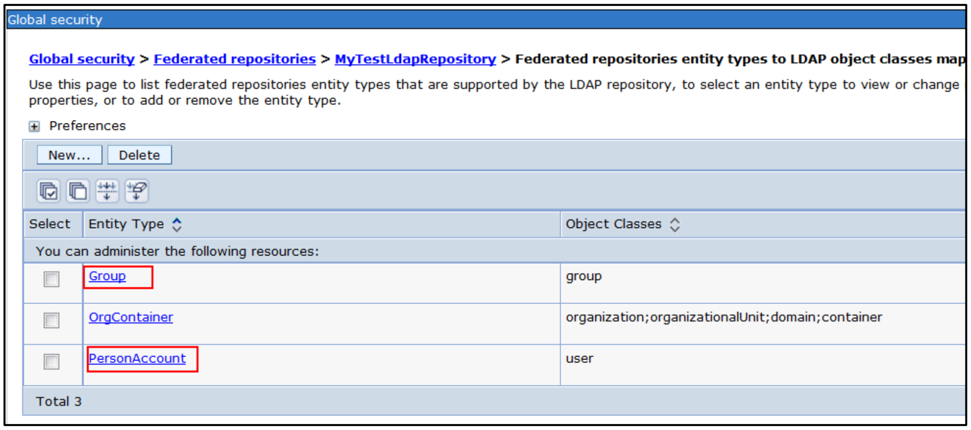
Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	DC=xyz,DC=com	MyTestLdapRepository	LDAP:AD
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 2			

__b. Under **Additional Properties** at the bottom of the **General Properties** panel, click **Federated repositories entity types to LDAP object classes mapping**:


Additional Properties
Performance
Federated repositories entity types to LDAP object classes mapping
Federated repositories property names to LDAP attributes mapping
Group attribute definition
Apply
OK
Reset
Cancel

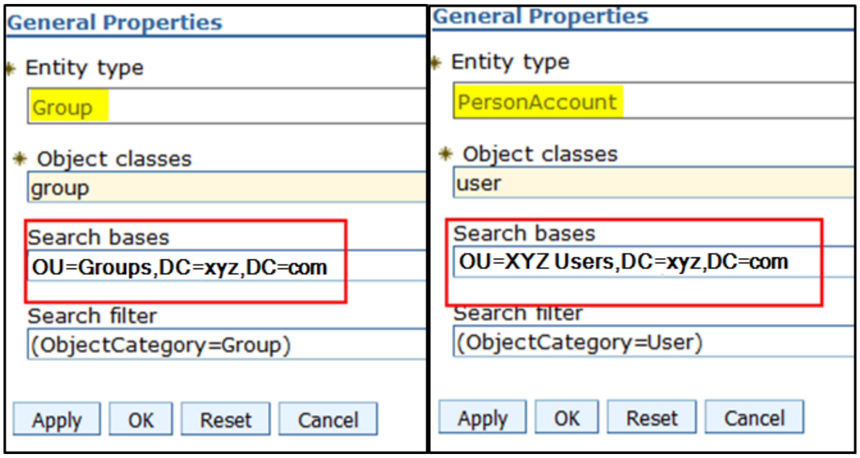
__c. Edit the **Search bases** field of the **Group** and **PersonAccount** entity types as shown:



Global security > Federated repositories > MyTestLdapRepository > Federated repositories entity types to LDAP object classes map

Use this page to list federated repositories entity types that are supported by the LDAP repository, to select an entity type to view or change properties, or to add or remove the entity type.

Select	Entity Type	Object Classes
You can administer the following resources:		
□	Group	group
□	OrgContainer	organization;organizationalUnit;domain;container
□	PersonAccount	user
Total 3		



* Entity type: Group
* Object classes: group
Search bases: OU=Groups,DC=xyz,DC=com
Search filter: (ObjectCategory=Group)

* Entity type: PersonAccount
* Object classes: user
Search bases: OU=XYZ Users,DC=xyz,DC=com
Search filter: (ObjectCategory=User)

__d. After completing and saving your edits, save directly to the master configuration.

__14. Configure where DASH will create new users and groups in the LDAP repository.

⚠ **Important! Only perform this step if you plan to create or change users and / or groups in Active Directory from DASH**

The changes made in this step will require additional configuration work the first time any of the file-based repository users are changed or saved, particularly the smadmin DASH administrative user.

To avoid losing access to the DASH administrative settings, please read the notes at the start of this section carefully prior to proceeding.

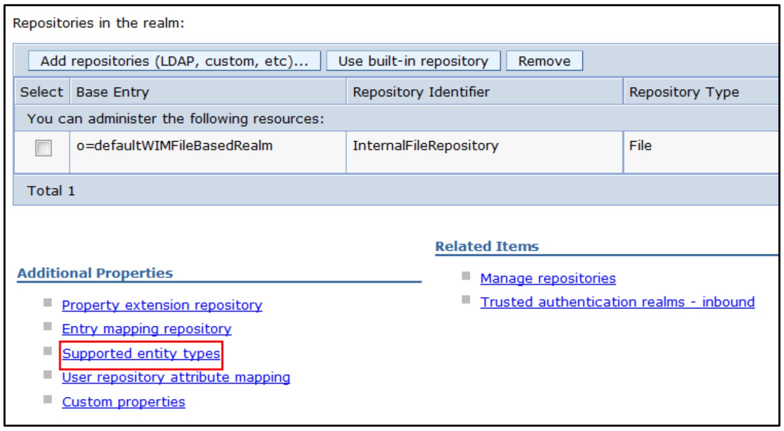
ℹ **New users can only be created if the “bind user” has write privileges in the LDAP directory and an SSL connection is used**

New groups can be created without an SSL connection if the “bind user” has write privileges in the LDAP directory.

This step changes the RDN property for the PersonAccount entity type in your federated repository from **uid** to **cn** to avoid Active Directory errors when adding or changing user accounts from DASH. After making this change, the first time you save any of the file-based repository accounts, their naming conventions will be changed in the file-base repository. For example, **uid=smadmin,o=defaultWIMFileBasedRealm** will be changed to **cn=smadmin,o=defaultWIMFileBasedRealm**. This has the following consequences:

- The user will lose any DASH roles that have been applied.
    - You will need to log into DASH as a user with the iscadmins role and re-apply the roles.
- In the case of the DASH administrative user (smadmin by default), you will need to have another user with the iscadmins role available to restore the iscadmins role to the DASH administrative user.
    - It is suggested that you apply the iscadmins role to at least one Active Directory based user prior to performing this step to avoid losing access to the iscadmins role.
- Also in the case of the DASH administrative user, that user will not be able to log on to WebSphere (including the WebSphere Administrative Console) until DASH has been restarted.
    - This also means that DASH will not stop cleanly using the **stopServer.sh server1** command during the first re-start. The process will need to be killed, then started normally once all related processes (the java processes for DASH and TCR/Cognos Reporting if installed) have stopped.

__a. In the **Additional Properties** section below the **Repositories in the realm** section click on **Supported entity types**:



Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

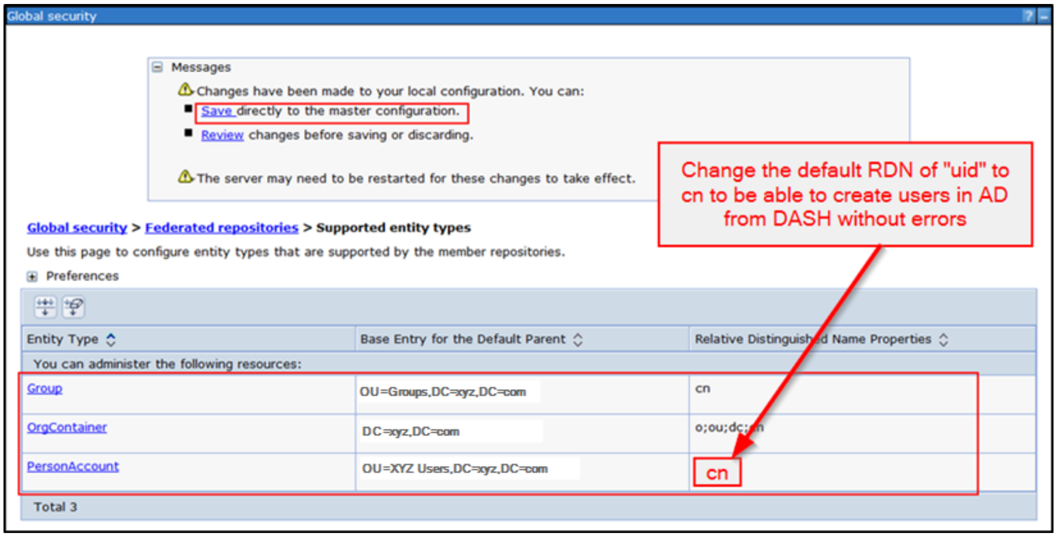
Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types
- User repository attribute mapping
- Custom properties

Related Items

- Manage repositories
- Trusted authentication realms - inbound

__b. Edit the **Group**, **OrgContainer**, and **PersonAccount** entries as shown:



Global security

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.

Global security > Federated repositories > Supported entity types

Use this page to configure entity types that are supported by the member repositories.

⊞ Preferences

Entity Type	Base Entry for the Default Parent	Relative Distinguished Name Properties
You can administer the following resources:		
Group	OU=Groups,DC=xyz,DC=com	cn
OrgContainer	DC=xyz,DC=com	o;ou;dc;cn
PersonAccount	OU=XYZ Users,DC=xyz,DC=com	cn
Total 3		

Change the default RDN of "uid" to cn to be able to create users in AD from DASH without errors

Note that although changing the RDN (Relative Distinguished Name) for PersonAccount from uid to cn will avoid “illegal name” errors when attempting to create new users from DASH, you will also need to use an SSL connection from DASH to Active Directory to be able to create new users or to change user passwords from the DASH GUI.

__c. Save directly to the master configuration.

__15. Optionally perform the work in the next section, **Setup DASH to allow file repository users to log in when Active Directory is down** now to avoid needing to perform an additional re-start of DASH as part of that work.

__16. Re-start DASH.

__17. After DASH restarts:

__a. Login to DASH as smadmin, and launch the WebSphere administrative console.

__b. Check that you can see the users and groups from Active Directory under **Users and Groups -> Manage Users** and **Users and Groups -> Manage Groups**.

1.8 Setup DASH to allow file repository users to log in when Active Directory is down

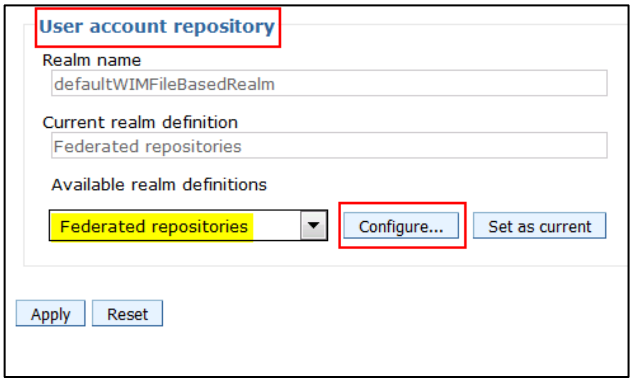
Note that this step could be done when adding the LDAP repository to DASH to avoid another re-start of DASH.

By default, smadmin will be the only file repository based user in DASH. The smadmin user will be able to login and administer DASH if the ObjectServer is not available, but will not have privileges in the ObjectServer to use the Web GUI by default. If you have set up additional file-based repository users to have access to the Web GUI, then you will be able to use those users to at least view events in the Web GUI.

__1. Logon to DASH as smadmin and launch the WebSphere administrative console.

__2. Navigate to **Security -> Global Security**.

__3. Under **User account repository**, verify that **Federated repositories** is selected and click the **Configure** button.



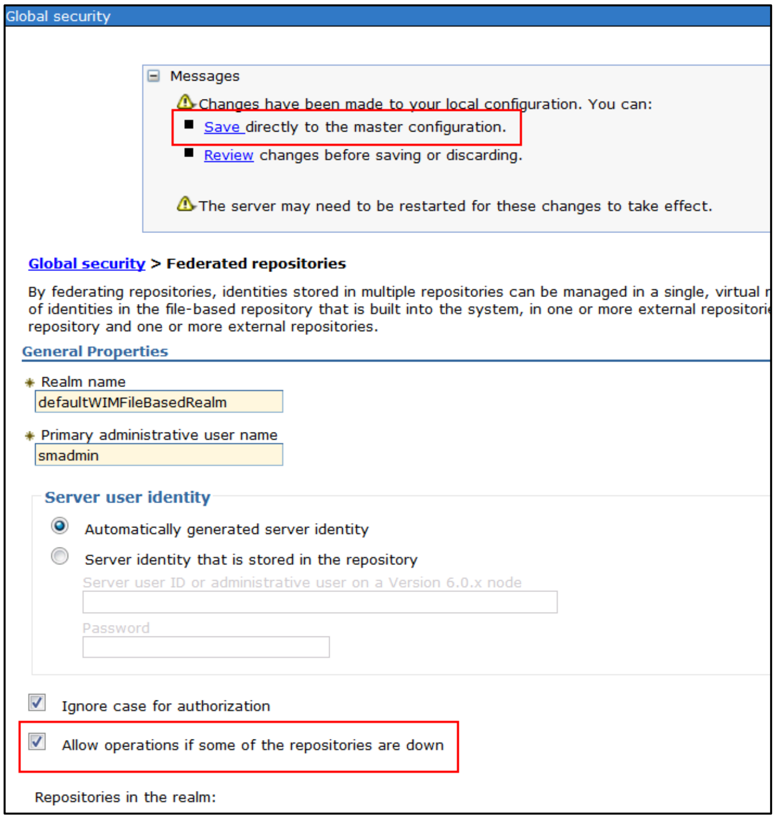
User account repository

Realm name
defaultWIMFileBasedRealm

Current realm definition
Federated repositories

Available realm definitions
Federated repositories

__4. Check the box for **Allow operations if some of the repositories are down**, click **OK** and save directly to the master configuration.



Global security

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.

Global security > **Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual r of identities in the file-based repository that is built into the system, in one or more external repositori repository and one or more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
smadmin

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

☑ Ignore case for authorization

☑ Allow operations if some of the repositories are down

Repositories in the realm:

__5. Restart DASH so that the changes take effect.

1.9 Setting up user synchronization from the LDAP repository to the Object sever

This work is performed on the DASH / Web GUI server.

This functionality allows certain users created in the LDAP repository to be synchronized into the ObjectServer automatically. This is useful since it allows those users to be able to perform tasks against the ObjectServer such as using AEL (Active Event List) context menu tools.

__1. Verify that there are no references to ObjectServer repositories in the DASH/JazzSM wimconfig.xml file.

Example file location:

/opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config/wimconfig.xml

__2. Give the **ncw_admi**n or **ncw_user** role to users that are to be synchronized from LDAP into the ObjectServer.

This can be done from the DASH GUI using the **Roles** or **Group Roles** menus. If you assign the roles to user groups rather than to individual users, the roles cascade to the users in the groups.

Netcool specific groups from Active Directory (such as netcool_admin, NOC_Supervisor and netcool_users) will not yet have the ncw_admin or ncw_user roles assigned.

The exact group names will vary depending on the groups you use or create in your Active Directory instance

__a. From the DASH **Group Roles** menu, assign the **ncw_admin** and / or **ncw_user** roles to those groups based on the roles that were assigned to them prior to changing the authentication mechanism.

Note that if other ncw_* roles were assigned to those groups prior to changing the authentication mechanism, you should re-assign those roles as well, although they are not required for user synchronization from LDAP to the ObjectServer.

__3. Edit the Web GUI server.int file to allow synchronization.

The file is located at <WEBGUI_HOME>/etc/server.init.

__a. Set the property **users.credentials.sync** to **true**.

__b. Verify the value of the **users.credentials.sync.groupname** property.

- The default value is **vmmusers**

- This is the group that synced users will be added to in the ObjectServer.

__4. You can change the synchronization interval by editing the <WEBGUI_HOME>/etc/datasources/ncwDataSourceDefinitions.xml file and editing the **<config maxAge=”time_in_seconds”/>** node, but this is not recommended.

- The default value is 3600 seconds (1 hour).
- The recommended approach to force synchronization of users is to run the webtop_osresync WAAPI routine on the DASH server.
  - WAAPI must be configured for this utility to execute successfully, and the current user set up for WAAPI may not yet be accessible due to the ongoing authentication changes.
  - If you need to specify a different user, edit waapi.init in <WEBGUI_HOME>/waapi/etc/, and set a web GUI administrative user and password in the fields **waapi.user** and **waapi.password**.

__5. Re-start DASH.

1.10 Setup OMNIbus permissions for the synchronized users

__1. Run the webtop_osresync routine on the DASH server to synchronize users, if there are users in LDAP with ncw_admin or ncw_user roles that are not yet in the ObjectServer.

__2. On the aggregation layer ObjectServer, start the nco_config utility.

__3. Logon to the aggregation layer ObjectServer from the nco_config utility.

__4. Verify that the LDAP users that should have been synced based on their roles appear in the ObjectServer and are in the vmmusers group.

Note that the groups that were assigned the ncw_admin or ncw_user roles will also be synced into the ObjectServer.

__5. Assign roles to the vmmusers group:

- AlertsUser
- CatalogUser
- ChannelUser
- ISQL
- ISQLWrite

__6. Logon to DASH as one of the synchronized users in the OMNIbus vmmusers group, open AEL, and verify that event context menu functionality such as acknowledging an event works correctly.

Chapter 2 Configuring Active Directory authentication and SSO for Impact when the ObjectServer is currently used for authentication

Overview

Impact cannot use multiple repositories of more than one type simultaneously. For example, a combination of filed based and LDAP based repositories is not supported. Impact does support multiple repositories of the same type, for example multiple LDAP repositories.

You must disable OMNIbus ObjectServer authentication for Impact prior to enabling LDAP authentication. If you attempt to enable LDAP authentication on an Impact instance where OMNIbus ObjectServer authentication is currently enabled, the script that enables LDAP authentication will fail and you will then need to attempt to recover by using one of the following approaches:

- Reverting to file based authentication by disabling LDAP authentication using the disable option of the confAuth4LDAP script. This is the only officially supported option.
- Manually editing the underlying WebSphere Liberty Profile configuration files. While editing these files is the supported for WebSphere Liberty, it is not directly supported for Impact authentication setup and you will likely require assistance from IBM Support and Impact development if an error occurs.
    - See the appendices for an example of the error that can occur when attempting to convert directly from ObjectServer to LDAP authentication, and for an example of a potential recovery procedure.

You must disable the ObjectServer repository using the disable option of the confAuth4OMNIbus script. This will also create a new file based repository with a new Impact administrator account in that new file based repository. Next you can enable the LDAP repository using the enable option of the confAuth4LDAP script. This will replace the file based repository with the LDAP repository.

Changes made in LDAP may not appear until the authentication cache is cleared

When using the LDAP repository, changes made in LDAP may not appear until the authentication cache is cleared, which can take up to 10 minutes. Disabling or customizing the authentication cache is not recommended since it can cause performance issues.

2.1 Before starting

__1. Verify that the Active Directory server is up, and that its fully qualified host name can be pinged from the Impact server.

__2. Verify that the ObjectServer is up and that the Impact administrative user (typically impactadmin) can logon to Impact.

__3. Verify that the impactadmin user (or the account that you use for this purpose) has been created in Active Directory, and that you know that user's password in Active Directory.

__4. You will need the Active Directory information that your LDAP admin provided for setting up Active Directory authentication for Web GUI / DASH earlier in this document.

__5. If you plan to use an SSL connection to active directory, you will need your Active Directory administrator to export the SSL certificate from the Active Directory server and make it available to you.

2.2 Multiple server installation considerations

Unless otherwise noted, the following steps must be performed on all Impact servers and Impact GUI servers in your installation.

2.3 Backup Impact security configuration files

Reverting to file based authentication by using the disable option of the confAuth4OMNIbus and confAuth4LDAP script will be covered in upcoming sections of this document. There is not an externally documented recovery procedure for the situation where changing the authentication mechanisms fails and then the documented approach of using the disable option to revert to file based authentication also fails. In the unlikely event that this happens, Impact development recommends using the following process:

The procedure is to contact IBM support and then Impact development can investigate what has happened. There is a backup folder where the security scripts store backup copies of most of the files that are changed. However, this is not a plain and simple procedure where everything is stored in the backup folder; some files like the keystore/truststore aren't. There are commands to work with these files to restore the previous configuration, but they are not documented because a person with internal Impact and WebSphere Liberty knowledge is needed to diagnose what went wrong and what state the system is in prior to carrying out the recovery steps. Impact development wrote the scripts for Impact authentication and the current expertise with the scripts and the changes they make resides with the Impact development team.

To be sure that as much as possible of the original Impact authentication configuration is captured in case it is needed later, backup the following files.

__1. <IMPACT_HOME>/wlp/usr/servers/<SERVER-NAME>/server.xml.

__2. <IMPACT_HOME>/wlp/usr/servers/ImpactUI/server.xml.

__3. <IMPACT_HOME>/wlp/usr/shared/config/features.xml.

__4. <IMPACT_HOME>/wlp/usr/shared/config/omnibusRegistry.xml.

__5. <IMPACT_HOME>/wlp/usr/shared/config/ldapRegistry.xml.

__6. <IMPACT_HOME>/install/security/impactdap.properties.

__7. <IMPACT_HOME>/install/security/impactncos.properties.

2.4 Disable ObjectServer authentication

This work is performed on all Impact servers and Impact GUI servers. If the Impact server and Impact GUI server are installed on the same host, performing this work once on that host will disable ObjectServer authentication for both the Impact server and Impact GUI server.

__1. Edit the <IMPACT_HOME>/install/security/impactncos.properties file.

__a. Enter the hostname of your primary ObjectServer as the value for the **NCOSPrimaryHost** property.

__b. Enter the port for that ObjectServer as the value for the **NCOSPrimaryPort** property.

__c. If your OMNIbus configuration includes a backup ObjectServer, enter the hostname and port of the backup server as the values for the properties **NCOSSecondaryHost** and **NCOSSecondaryPort**.

__d. Verify that the user listed as the value of the **username** property exists in the ObjectServer and has read access to the security DB (the ObjectServer DB).

In the lab environment used when creating this environment, the value of the **username** property was **root**, meaning the ObjectServer root user account (not the Linux OS root user account).

__e. Save the file.

__2. From a terminal window, change directory to <IMPACT_HOME>/install/security.

__3. Execute the confAuth4OMNIbus.sh script with the **disable** argument:

```
./confAuth4OMNIbus.sh disable <username> <userpassword>
<currentpassword>
```

Description of the argument values:

- disable: This command indicates that OMNIbus ObjectServer authentication will be disabled for Impact. The options are “enable” or “disable”.

- username: This is the name of the new Impact administrative user that will be created in the new file-based repository.

  We will use impactadmin as the Impact administrative user for this example.

- userpassword: This is the password for the new Impact administrative user account in the new file based repository. Use the existing password for the impactadmin user unless you have a reason to change it.

  You will use this password to logon to Impact as impactadmin after running this script.

  You will need to know this password to run the script to enable Active Directory authentication later.

  You will also need to know this password if something goes wrong when you run the confAuth4OMNIbus script with the disable option, and you need to attempt to revert to OMNIbus authentication.

- currentpassword: This is the ObjectServer-based password of the impactadmin user. This is the password that the impactadmin user currently uses to logon to Impact.

__4. The script must complete with a **BUILD SUCCESFUL** message.

__a. If the script does not complete successfully, you can try to revert to the previous ObjectServer authentication configuration, correct any issues, and try again.

Since this script simply sets up a local file based repository, it is unlikely to fail unless it cannot authenticate to Impact to make the required changes. Be sure the ObjectServer is up and the correct impactadmin password for ObjectServer authentication was supplied.

__i. To attempt to revert to (re-enable) ObjectServer authentication, execute the command:

```
./confAuth4OMNIbus.sh enable <username>
<userpassword> <password> <currentpassword>
```

Description of the argument values:

- username: The ObjectServer-based user for the Impact administrator account.
- userpassword: The ObjectServer-based user password for the Impact administrator account.
- password: The ObjectServer administrator user password for repository connections. This will be the ObjectServer password for the user specified by the **username** property in the <IMPACT_HOME>/install/security/impactncos.properties file.

- Currentpassword: The current Impact user administrator password for Impact. This will be the new password you specified for the new file based repository user in the previous failed invocation of the confAuth4OMNIbus script.

__5. After the configAuth4Omnibus script completes successfully in disable mode, verify that you can logon to Impact as the impactadmin user using the new password you specified (the **userpassword** argument).

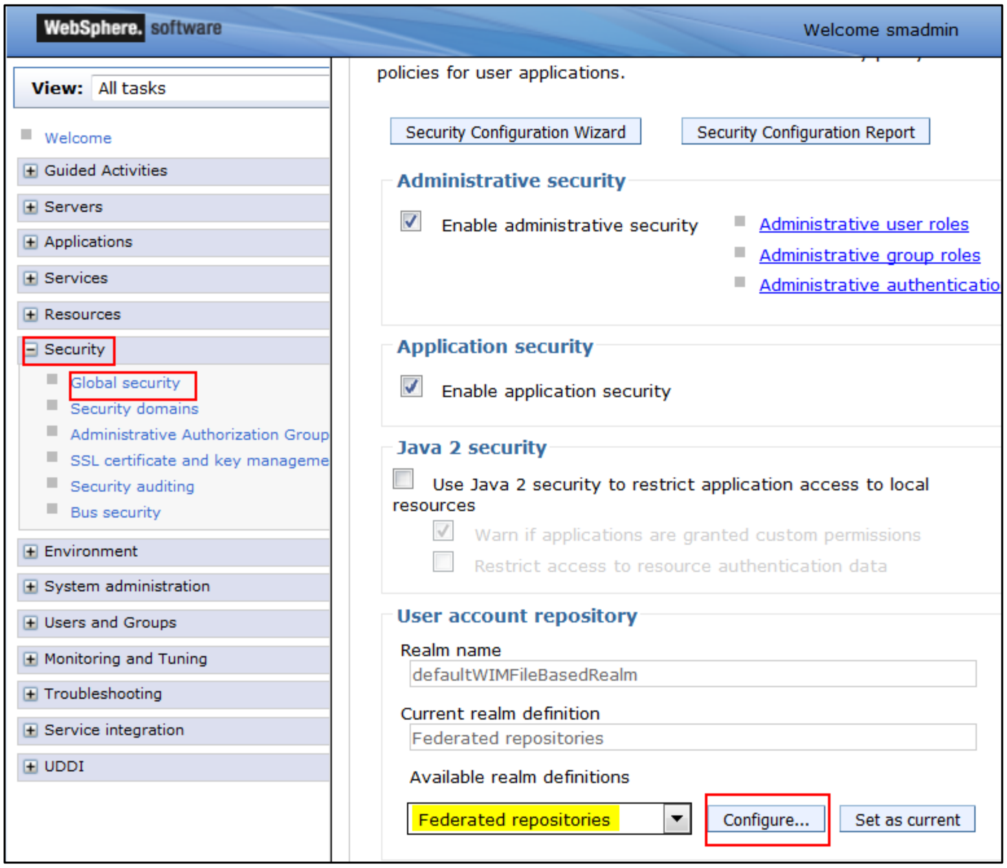
2.5 Determine the SSO realm value

This work is performed on the DASH server.

__1. Logon to the DASH GUI as the smadmin user and launch the WebSphere administrative console.

__2. Navigate to **Security->Global Security**.

__3. Under the **User account repository** section, verify that **Federated repositories** is selected in **Available realm definitions** and click the **Configure** button.



policies for user 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

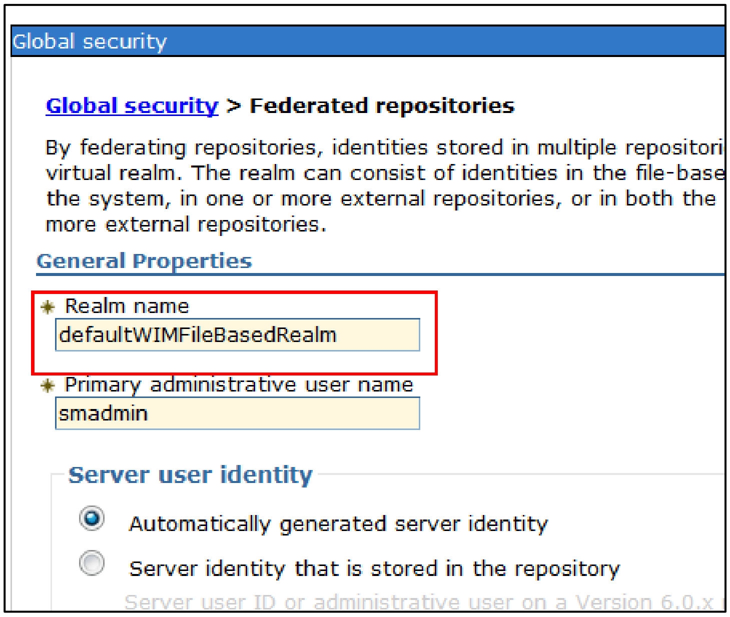
Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

__4. Note the value of **Realm name** in the **General Properties** section.

This value will be used as the **SSORealm** property value when editing the Impact configuration files for Active Directory authentication. The spelling and capitalization used in Impact must exactly match the value shown in DASH.



Global security

Global security > Federated repositories

By federating repositories, identities stored in multiple repositori
virtual realm. The realm can consist of identities in the file-base
the system, in one or more external repositories, or in both the
more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
smadmin

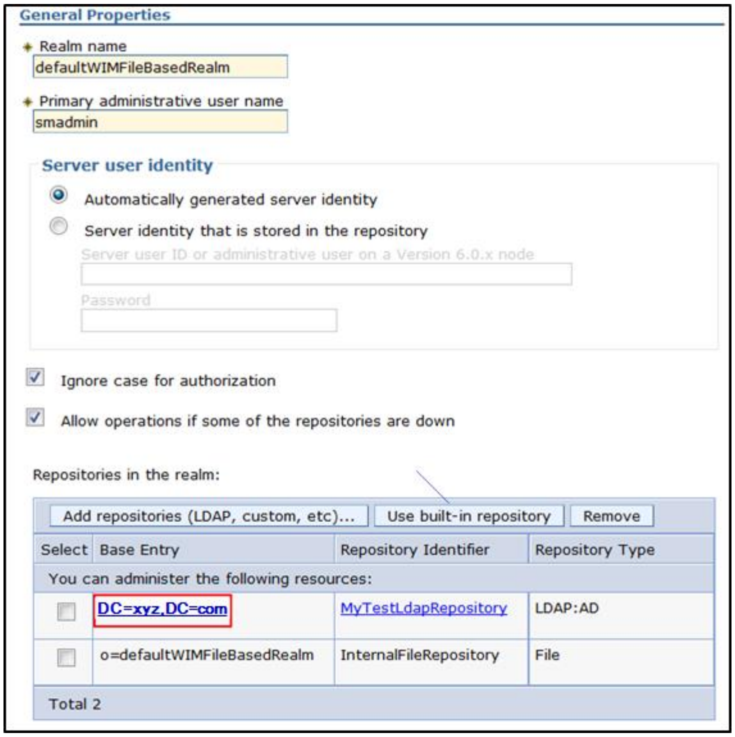
Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

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

__5. On the current panel (General Properties), in the **Repositories in the realm** table click on the **Base Entry** for your Active Directory repository.



General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
smadmin

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

☑ Ignore case for authorization

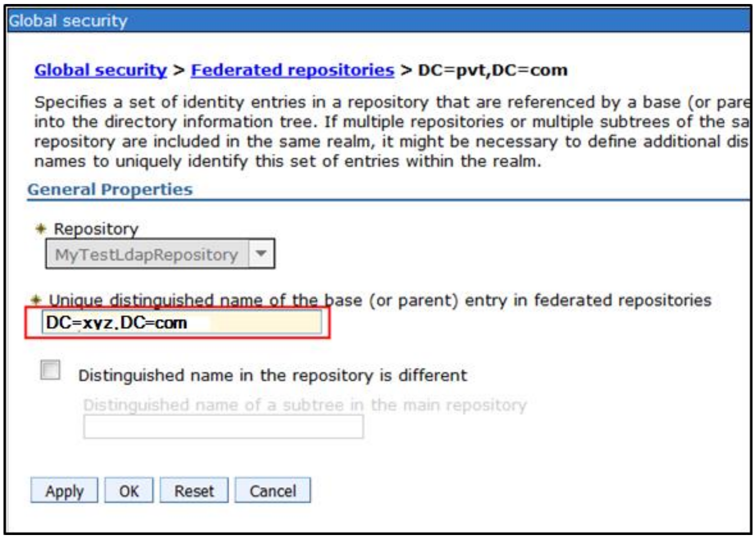
☑ Allow operations if some of the repositories are down

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	DC=xyz,DC=com	MyTestLdapRepository	LDAP:AD
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 2			

__6. Note the value of the field **Unique distinguished name of the base (or parent) entry in federated repositories**.

This value will be used as the value of the **LDAPBaseEntry** property when editing Impact configuration files for Active Directory authentication. The value used in Impact must match exactly the value shown in DASH.



Global security

Global security > Federated repositories > DC=pvt,DC=com

Specifies a set of identity entries in a repository that are referenced by a base (or pare into the directory information tree. If multiple repositories or multiple subtrees of the sa repository are included in the same realm, it might be necessary to define additional dis names to uniquely identify this set of entries within the realm.

General Properties

* Repository: MyTestLdapRepository

* Unique distinguished name of the base (or parent) entry in federated repositories: DC=xyz,DC=com

□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository

__7. Exit the WebSphere administration console without making any changes.

__8. Verify that the data collected in this section is the same on all DASH servers used in your installation.

2.6 Import the Active directory SSL certificate into the Impact server

Do this step only if you are using a secure connection to the Active Directory server

If you do not use a secure connection for your initial install and later change to a secure connection, you can perform this step later when you change to a secure connection.

This work must be performed on all Impact servers.

__1. Copy the Active Directory SSL certificate provided by your Active Directory administrator to the Impact server.

For this example, the Active Directory SSL certificate is named **certnew.cer** and it is copied to the /tmp/ directory on the Impact server.

__2. Import the SSL certificate into the Impact server trust.jks keystore using the keytool utility (the command is all on one line):

__a.
```
<IPACT_HOME>/sdk/jre/bin/keytool -import -alias ldap -file
/tmp/certnew.cer -keystore
/opt/IBM/tivoli/impact/wlp/usr/servers/<SERVER-
NAME>/resources/security/trust.jks
```

__b. When prompted for a keystore password, use the password that was configured for the Impact administrator (for instance impactadmin) during the installation of Netcool/Impact.

__i. If you using these instructions for updating / adding a certificate rather than for initial LDAP authentication setup:

(1) Use the Impact administrator’s current password.

(2) You may need to supply a new alias name.

__c. Respond **yes** to the prompt: **Trust this certificate? [no]:**

__3. Import the SSL certificate into the Impact GUI server trust.jks keystore using the keytool utility (the command is all on one line):

__a.
```
<IPACT_HOME>/sdk/jre/bin/keytool -import -alias ldap -file
/tmp/certnew.cer -keystore
/opt/IBM/tivoli/impact/wlp/usr/servers/ImpactUI/resources/s
ecurity/trust.jks
```

__b. When prompted for a keystore password, use the password that was configured for the Impact administrator during the installation of Netcool/Impact.

__i. If you using these instructions for updating a certificate rather than initial LDAP authentication setup, see the notes in the previous step about the password and alias values.

__c. Respond **yes** to the prompt: **Trust this certificate? [no]:**

__4. Restart the Impact server so that the changes will take effect.

2.7 Edit impactdap.properties to use the target Active Directory settings

This work is performed on all Impact servers and Impact GUI servers. If the Impact server and Impact GUI server are installed on the same host, this file will be used for both the Impact server and Impact GUI server on that host.

__1. Open the file <IMPACT_HOME>/install/security/impactdap.properties in a text editor.

__2. Set the value of the **LDAPRepositoryName** property to a unique identifier for this repository in the Impact server realm. This can be a string of your choice. It does not need to be the same repository name that was used when configuring Active Directory authentication for DASH earlier in this document.

__3. Set the value of the **LDAPServerType** property to **Microsoft Active Directory**.

Be sure this is spelled exactly as shown in the list of LDAP Server Types listed in the file.

__4. Set the value of the **LDAPHost** property to the fully qualified hostname of your Active Directory server.

__5. Set the value of the **LDAPPort** property to the LDAP port value that your LDAP administrator provided.

> **Important! This port number is different for secure and non-secure communications**
>
> If you are using secure communications, you must have already imported the Active Directory server's SSL certificate by completing the step: **Import the Active directory SSL certificate into the Impact server**.

__a. If you are using non-secure communications, enter the non-SSL port number that your Active Directory administrator gave you. The default non-secure port is 389.

__b. If you are using secure communications, enter the SSL port number that your Active Directory administrator gave you. The default SSL port is 636.

__6. Set the value of the **LDAPBindDN** property to the "bind user" that you obtained from your LDAP administrator.

For this example, the value is: **CN=Administrator,CN=Users,DC=xyz,DC=com**.

__7. Set the value of the **LDAPBaseEntry** to the base entry DN you obtained from the DASH WebSphere administrative console earlier in this section.

For this example, the value is: **DC=xyz,DC=com**.

__8. Set the value of **LDAPSSLEnabled** to **false** if you are not using a secure connection to Active Directory.

__a. Set the value to **true** if you are using a secure connection to Active directory.

> ⚠ **Important! This requires using the correct port and importing the Active Directory SSL certificate**
>
> If you are using secure communications, you must have:
>
> - Already entered the Active Directory SSL port as the value of the **LDAPPort** property.
> - Already imported the Active Directory server's SSL certificate by completing the step: **Import the Active directory SSL certificate into the Impact server**.

__9. Set the value of the **LDAPSSORealm** to the realm value that you obtained from the DASH WebSphere administrative console earlier in this section.

For this example, the value is: **defaultWIMFileBasedRealm**.

__10. For this example, do not change the property values in **the Advanced LDAP Repository Settings** section.

__11. For this example, do not change the property values in the **Custom LDAP Search Filtering** sections.

__12. Save your changes to the file and exit the text editor.

2.8 Enable LDAP (Active Directory) authentication for Impact

This work is performed on all Impact servers and Impact GUI servers. If the Impact server and Impact GUI server are installed on the same host, performing this work once on that host will enable LDAP authentication for both the Impact server and Impact GUI server.

__1. Change to the directory <IMPACT_HOME>/install/security.

__2. Execute the confAuth4LDAP.sh script, passing in the following argument values:

```
./confAuth4LDAP.sh  enable <impactadmin> <impactpassword>
<ldappassword> <currentpassword>
```

Argument details:

- enable or disable (**enable** for this example): Enables or disables LDAP authentication.
- impactadmin: The username of the "new" administrative user for Impact.

  This user will be set as the Impact administrative user as part of this script execution.

We will use the impactadmin user for this example

This user must exist in Active Directory; be sure that the impactadmin user (or the user you are using for this purpose) has been created in Active Directory.

- impactpassword: The password for the “new” impact administrative user.

  Note that this is the impactadmin user’s password in Active Directory.
- ldappassword: The Active Directory bind user’s password.
- currentpassword: The current Impact administrative user’s file based repository password.

  This is the password that you provided for the new file based repository Impact administrator account (impactadmin for this example) that was created when disabling OMNIbus ObjectServer based authentication.

> **Use single quotes around any passwords with special characters.**
>
> Enclose the impactpassword, ldappassword and /or currentpassword in single quotes if they contain special characters.

Example script invocation:

```
./confAuth4LDAP.sh enable impactadmin Passw0rd Object00 password
```

For this example, (yours will use different passwords and potentially a different user account):

- The Impact admin account is **impactadmin**.
- The impactadmin user’s Active Directory password is **Passw0rd**.
- The Active Directory bind user’s password is **Object00**.
- The impactadmin user’s current password for local file based authentication is **password**.

__3. The confAuth4LDAP.sh script must complete with the message **BUILD SUCCESSFUL** before you can continue with the next steps.

If the script fails, you can try to revert to file-based authentication, correct the problem, and then try again:

```
./confAuth4LDAP.sh disable impactadmin <file-based-password>
<current-Active-Directory-password-for-impactadmin>
```

__4. Verify that you can logon to the Impact GUI as impactadmin, using the Active Directory password for impactadmin.

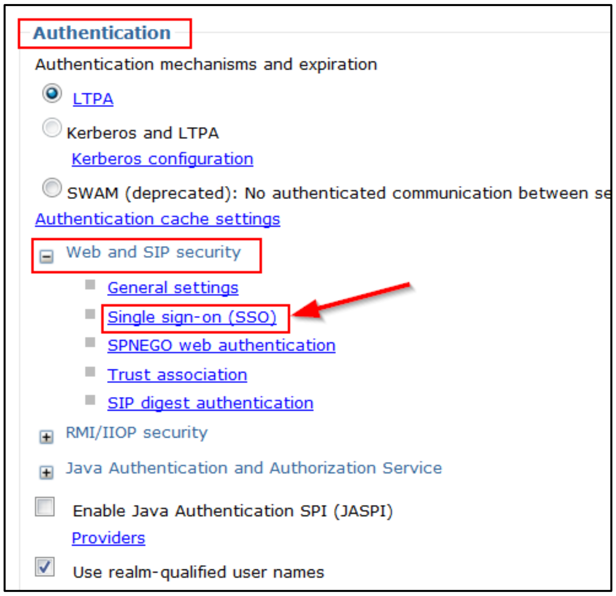
2.9 Configure SSO settings in DASH

This work is performed on all DASH servers, and the settings must be the same on all DASH servers.

__1. Logon to the DASH GUI as smadmin and launch the WebSphere administrative console.

__2. In the WebSphere administrative console, navigate to **Security->Global Security**.

__3. Under the **Authentication** section, expand the **Web and SIP Security** entry, then click on **Single sign-on (SSO)**.



Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

○ SWAM (deprecated): No authenticated communication between se

Authentication cache settings

⊟ Web and SIP security

- General settings
- Single sign-on (SSO)
- SPNEGO web authentication
- Trust association
- SIP digest authentication

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

□ Enable Java Authentication SPI (JASPI)

Providers

☑ Use realm-qualified user names

__4. In the **Single sign-on (SSO)** panel:

__a. Verify that the **Enabled** box is checked.

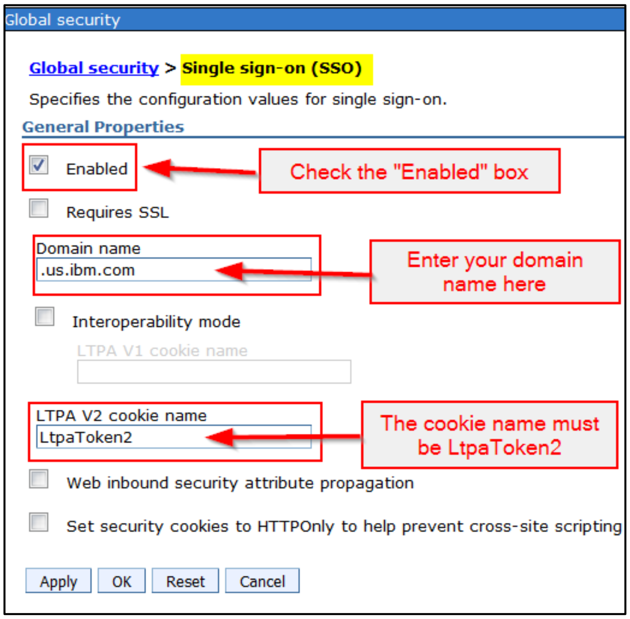
__b. Leave **Requires SSL** unchecked.

__c. Enter the domain name that your Impact and DASH servers use in the **Domain name** field.

For instance, if your Impact server's fully qualified host name is impactsrv1.mycompany.com, you would enter **.mycompany.com** in the **Domain name** field.

__d. Enter **LtpaToken2** in the **LTPA V2 cookie name** field.

__e. Leave the remaining checkboxes un-checked.



Global security

Global security > Single sign-on (SSO)

Specifies the configuration values for single sign-on.

General Properties

☑ Enabled

Check the "Enabled" box

□ Requires SSL

Domain name: .us.ibm.com

Enter your domain name here

□ Interoperability mode

LTPA V1 cookie name:

LTPA V2 cookie name: LtpaToken2

The cookie name must be LtpaToken2

□ Web inbound security attribute propagation

□ Set security cookies to HTTPOnly to help prevent cross-site scripting

__f. Click **OK**.

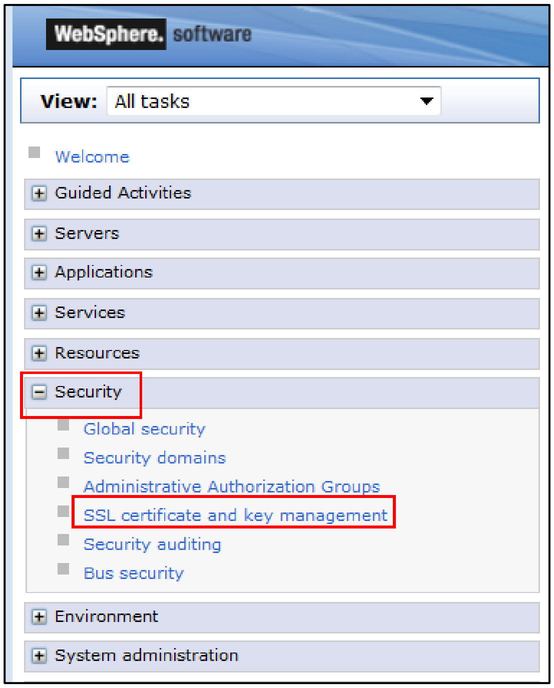
__g. Save directly to the master configuration.

__5. Restart DASH so that the changes take effect.

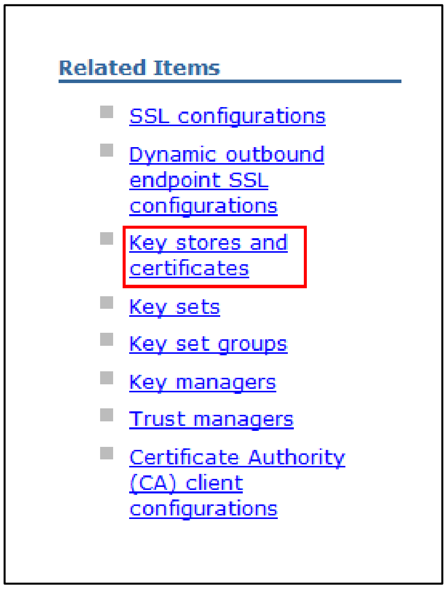
2.10 Add the Impact SSL certificate to the DASH truststore

This work is performed on all DASH servers.

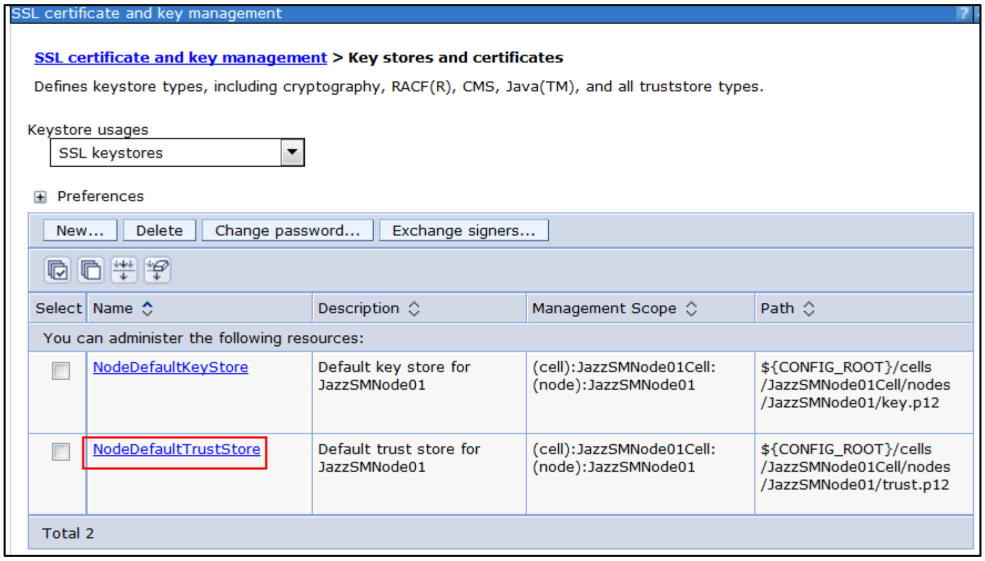
__1. From the main menu of the WebSphere administrative console, navigate to **Security->SSL certificate and key management**.



__2. Under the **Related Items** section, click **Key stores and certificates**.


Related Items
SSL configurations
Dynamic outbound endpoint SSL configurations
Key stores and certificates
Key sets
Key set groups
Key managers
Trust managers
Certificate Authority (CA) client configurations

__3.   Click the **NodeDefaultTrustStore** link.



SSL certificate and key management

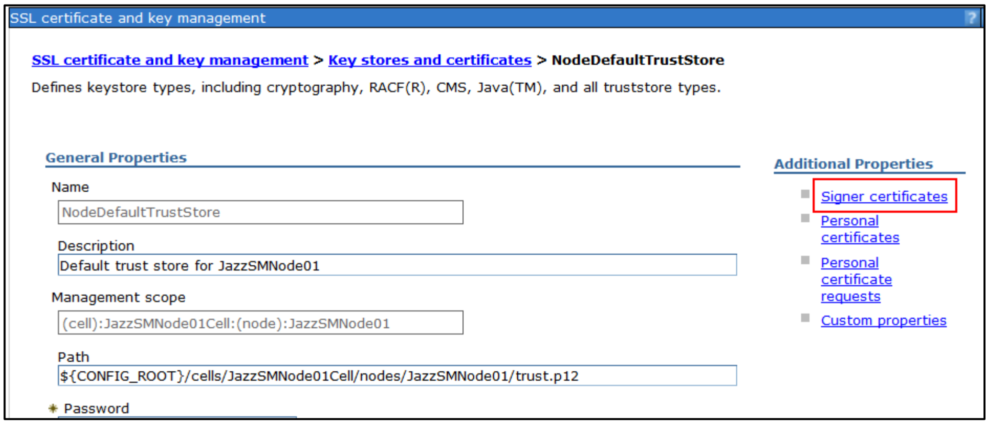
SSL certificate and key management > Key stores and certificates

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

Keystore usages: SSL keystores

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
□	NodeDefaultKeyStore	Default key store for JazzSMNode01	(cell):JazzSMNode01Cell:(node):JazzSMNode01	${CONFIG_ROOT}/cells/JazzSMNode01Cell/nodes/JazzSMNode01/key.p12
□	NodeDefaultTrustStore	Default trust store for JazzSMNode01	(cell):JazzSMNode01Cell:(node):JazzSMNode01	${CONFIG_ROOT}/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12
Total 2				

__4.   Under the **Additional Properties** section, click **Signer certificates**.



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

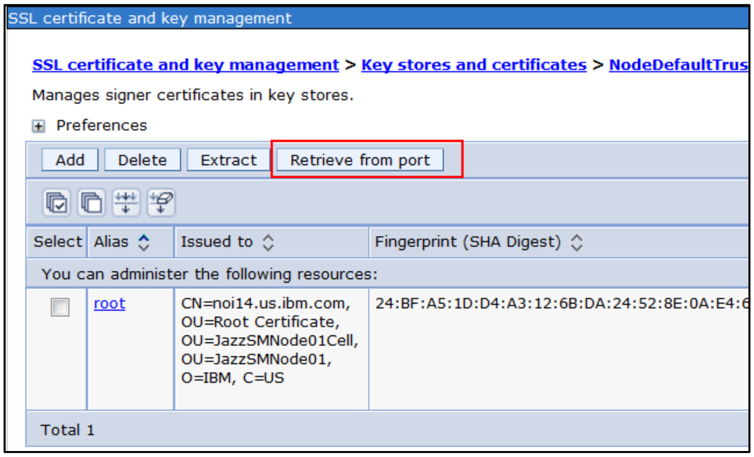
Name: NodeDefaultTrustStore

Description: Default trust store for JazzSMNode01

Management scope: (cell):JazzSMNode01Cell:(node):JazzSMNode01

Path: ${CONFIG_ROOT}/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12

__5.   Click the **Retrieve from port** button.



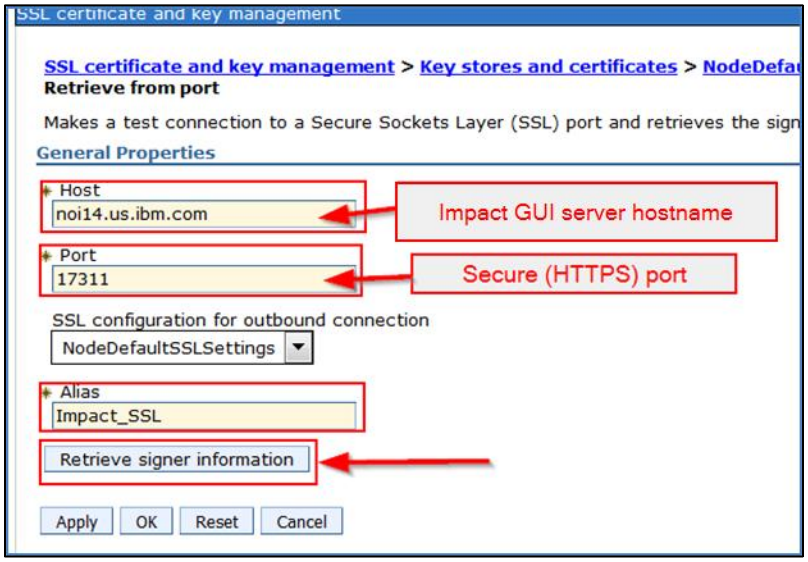
SSL certificate and key management

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

Manages signer certificates in key stores.

Select	Alias	Issued to	Fingerprint (SHA Digest)
You can administer the following resources:			
□	root	CN=noi14.us.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	24:BF:A5:1D:D4:A3:12:6B:DA:24:52:8E:0A:E4:6
Total 1			

__6. Enter the hostname of your first Impact GUI server in the **Host** field, the secure port that the Impact GUI server listens on in the **Port** field, and an alias name such as **Impact_SSL** in the **Alias** field. Then click the **Retrieve signer information** button.



SSL certificate and key management

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

Retrieve from port

Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the sign

General Properties

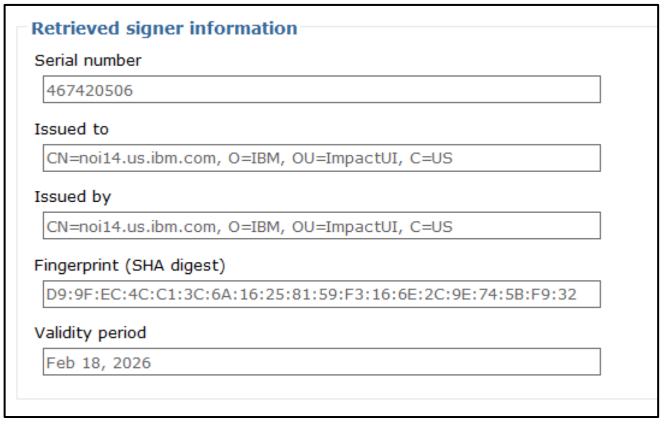
Host: noi14.us.ibm.com

Port: 17311

SSL configuration for outbound connection: NodeDefaultSSLSettings

Alias: Impact_SSL

__7. Verify that the signer information was retrieved.



Retrieved signer information

Serial number: 467420506

Issued to: CN=noi14.us.ibm.com, O=IBM, OU=ImpactUI, C=US

Issued by: CN=noi14.us.ibm.com, O=IBM, OU=ImpactUI, C=US

Fingerprint (SHA digest): D9:9F:EC:4C:C1:3C:6A:16:25:81:59:F3:16:6E:2C:9E:74:5B:F9:32

Validity period: Feb 18, 2026

Important! You must successfully retrieve the signer information before continuing

Correct any issues and retrieve the signer information before continuing.

__8. Click **OK**.

__9. Save directly to the master configuration.

__10. Repeat steps 1 through 9 on this DASH server for all other Impact GUI servers.

Important! Use a different SSL certificate alias name for each server when performing step 6

__11. Repeat steps 1 through 10 on all other DASH servers.

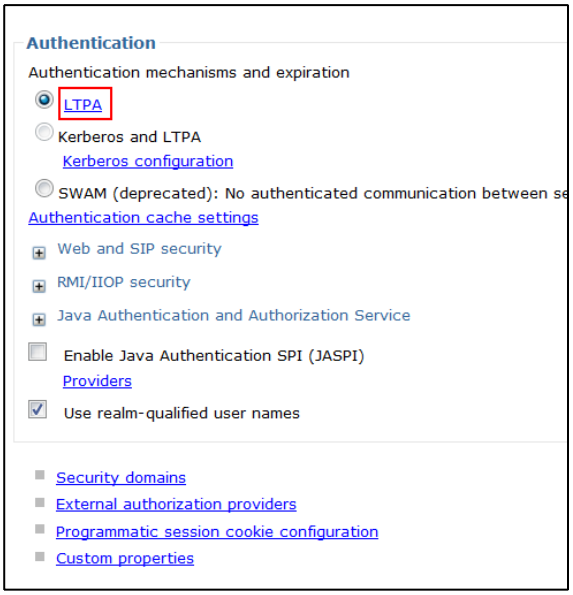
2.11 Export the DASH LTPA keys.

This work is done on only one of the DASH servers.

The exported DASH LTPA keys will later be imported into all Impact servers, and will also be imported into any other DASH servers. All servers must use the same LTPA keys for SSO to work correctly.

__1. From the main WebSphere administrative console menu, navigate to **Security->Global Security**.

__2. Under the **Authentication** section, click **LTPA**.



Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

○ SWAM (deprecated): No authenticated communication between se

Authentication cache settings

⊞ Web and SIP security

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

☐ Enable Java Authentication SPI (JASPI)

Providers

☑ Use realm-qualified user names

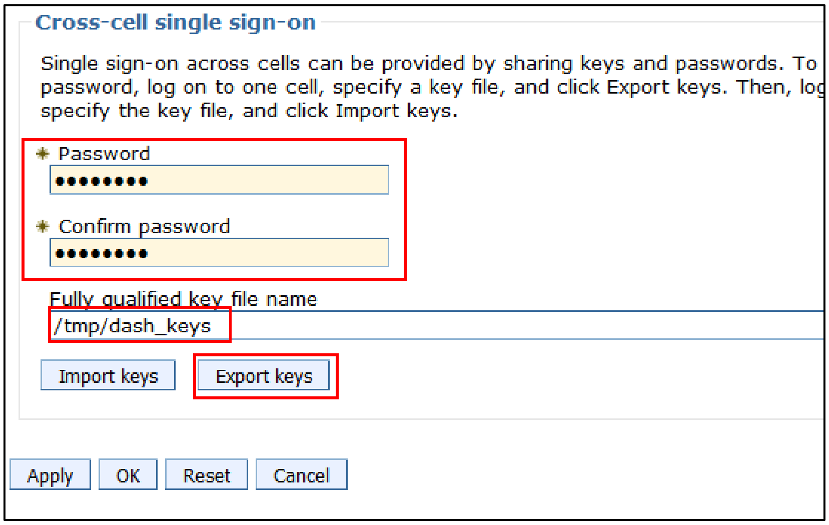
- Security domains
- External authorization providers
- Programmatic session cookie configuration
- Custom properties

__a. Under the **Cross-cell single sign-on** section:

__i. Enter and confirm a password for the key file. Remember the password since you will need it later to import the LTPA keys into Impact and the other DASH servers.

__ii. Enter a fully qualified name for the key file. We will use /tmp/dash_keys for this example.

__iii. Click **Export keys**.



Cross-cell single sign-on

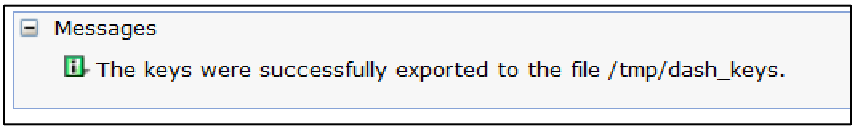
Single sign-on across cells can be provided by sharing keys and passwords. To password, log on to one cell, specify a key file, and click Export keys. Then, log specify the key file, and click Import keys.

* Password: ••••••••

* Confirm password: ••••••••

Fully qualified key file name: /tmp/dash_keys

__iv. You should see a message indicating that the keys were successfully exported.



Messages

The keys were successfully exported to the file /tmp/dash_keys.

2.12 Import the exported DASH LTPA keys into any additional DASH servers

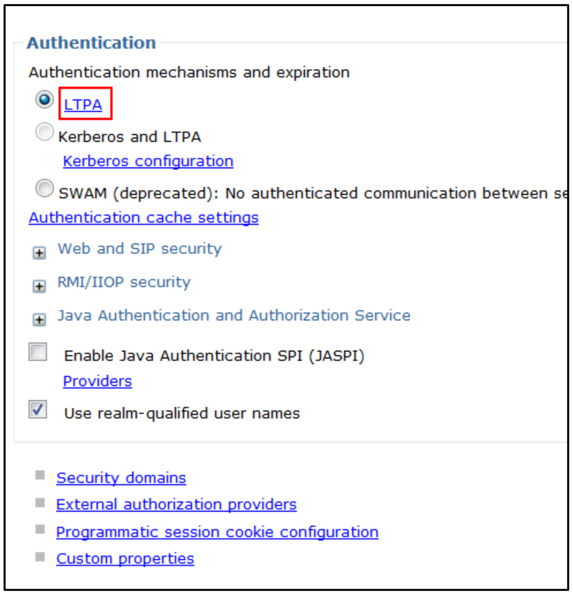
This work is performed on all additional DASH servers (all DASH servers other than the one that the LTPA keys were exported from). All servers must use the same LTPA keys for SSO to work correctly.

__1. Copy the file containing the exported LTPA keys to the target DASH server.

__2. Logon to the target DASH GUI as smadmin and launch the WebSphere administrative console.

__3. From the main WebSphere administrative console menu, navigate to **Security->Global Security**.

__4. Under the **Authentication** section, click **LTPA**.



Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

○ SWAM (deprecated): No authenticated communication between se

Authentication cache settings

□ Enable Java Authentication SPI (JASPI)

Providers

☑ Use realm-qualified user names

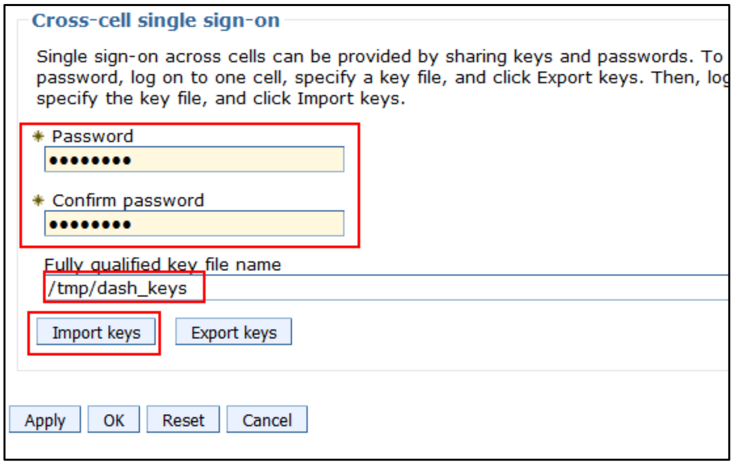
Web and SIP security
RMI/IIOP security
Java Authentication and Authorization Service
Security domains
External authorization providers
Programmatic session cookie configuration
Custom properties

__a. Under the **Cross-cell single sign-on** section:

__i. Enter and confirm the password that you used when you exported the key file from the "first" DASH server.

__ii. Enter the fully qualified path and file name to the location where you copied the key file on this DASH server.

__iii. Click **Import keys**.



Cross-cell single sign-on

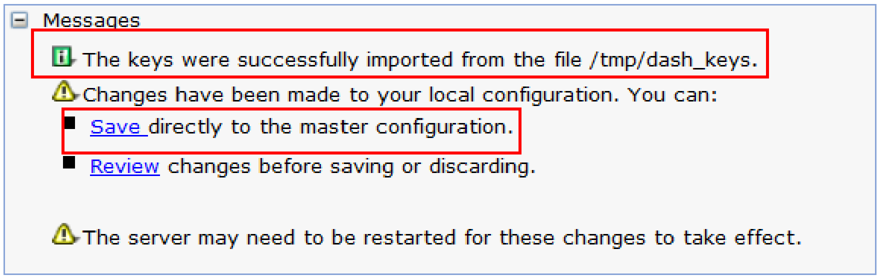
Single sign-on across cells can be provided by sharing keys and passwords. To password, log on to one cell, specify a key file, and click Export keys. Then, log specify the key file, and click Import keys.

* Password
••••••••

* Confirm password
••••••••

Fully qualified key file name
/tmp/dash_keys

__iv. You should see a message indicating that the keys were successfully imported.



Messages

The keys were successfully imported from the file /tmp/dash_keys.

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.

__v. Save directly to the master configuration.

2.13 Import the DASH LTPA keys into Impact and configure SSO on Impact.

Unless otherwise noted, all work in this section is performed on all Impact servers and Impact GUI servers. If the Impact server and Impact GUI server are installed on the same host, performing this work once on that host will import the DASH LTPA keys and configure SSO for both the Impact server and Impact GUI server.

Important! You must set up SSO again if you ever change the authentication mechanism after completing this step

After performing this step, if you ever re-execute the confAuth4LDAP or the confAuth4OMNibus script on an Impact server, then you will need to set up SSO again on that server by re-executing the configImpactSSO.sh script.

__1. Copy the file containing the exported LTPA keys from the DASH server to the Impact server.

__2. On the Impact server, copy the DASH LTPA key file to the location and file name used by the SSO configuration script, as shown in this step.

Note that the LTPA keys are copied to the directory structures for both the Impact server and the Impact GUI server.

Be sure to name the destination file **ltpa.keys**.

__a.
```
cp dash_keys
<IMPACT_HOME>/wlp/usr/servers/ImpactUI/resources/security/l
tpa.keys
```

__b.
```
cp dash_keys <IMPACT_HOME>/wlp/usr/servers/<IMPACT-SERVER-
NAME>/resources/security/ltpa.keys
```

__3. Execute the Impact SSO configuration script:

Important! If your passwords contain special characters, you may need to apply a fix pack or edit the configImpactSSO.sh script.

For Impact versions up to and including v7.1.0.6, the configImpactSSO.sh script does not properly handle passwords that contain the **$** character. You must either apply a fix pack with a fix for APAR IV86146 if one is available for your Impact version, or edit the configImpactSSO.sh script using the directions in the appendix **Editing configImpactSSO.sh**.

IBM Tivoli Netcool/Impact V7.1.0 Fix Pack 7(7.1.0-TIV-NCI-FP0007) which is available from IBM Fix Central includes this fix.

Applying a fix pack is the preferred and supported solution.

__a.
```
cd <IMPACT_HOME>/install/security
```

__b.
```
./configImpactSSO.sh "<SSO-realm-from-DASH>" "LtpaToken2"
"<DASH-SSO-domain>" <LTPA-key-password> <Impact-admin-
password>
```

Note the use of double quotes around some of the values

Enclose the SSO realm name, the word LtpaToken2, and the SSO domain name in double quotes.

Use single quotes around any passwords with special characters

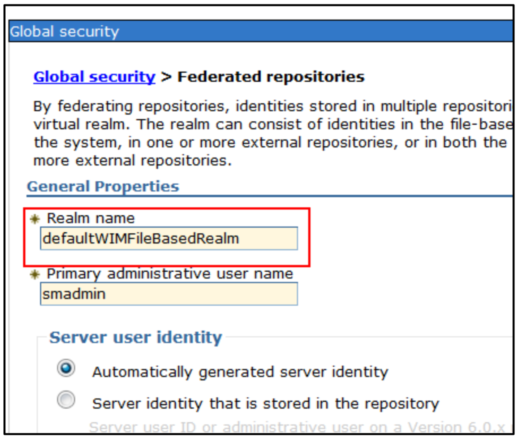
Enclose the LTPA-key-password and Impact-admin-password in single quotes if they contain special characters.

An example invocation of the script is shown here:

```
./configImpactSSO.sh "defaultWIMFileBasedRealm" "LtpaToken2"
".mycompany.com" myLtpaKeyPw myImpactAdminPw
```

Details regarding the argument values for the configImpactSSO.sh script:

- The value of <SSO-realm-from-DASH> is the **Realm name** that you noted earlier in the WebSphere administrative console for DASH (shown here for reference only).



Global security

Global security > **Federated repositories**

By federating repositories, identities stored in multiple repositori virtual realm. The realm can consist of identities in the file-base the system, in one or more external repositories, or in both the more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
smadmin

Server user identity

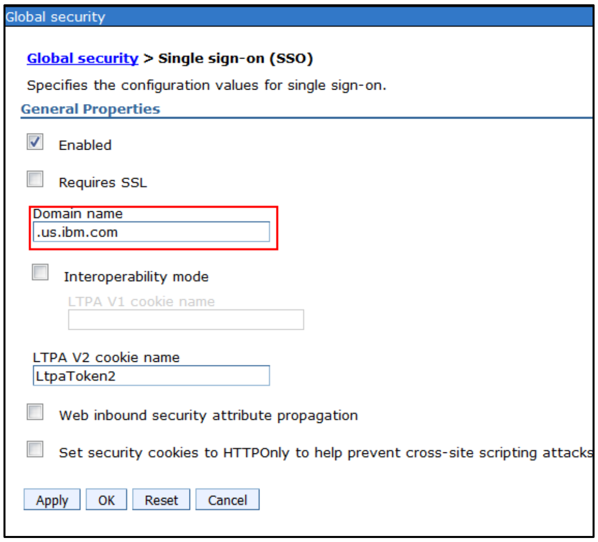
● Automatically generated server identity

○ Server identity that is stored in the repository

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

- **LtpaToken2** is the default LTPA cookie name, and you must use this value since it is the value that was configured in DASH.

- The value of <DASH-SSO-domain> is the value noted earlier in the **Domain name** field of the **Single sign-on (SSO)** panel in the WebSphere administrative console for DASH (shown here for reference only).



Global security

Global security > **Single sign-on (SSO)**

Specifies the configuration values for single sign-on.

General Properties

☑ Enabled

☐ Requires SSL

Domain name
.us.ibm.com

☐ Interoperability mode

LTPA V1 cookie name

LTPA V2 cookie name
LtpaToken2

☐ Web inbound security attribute propagation

☐ Set security cookies to HTTPOnly to help prevent cross-site scripting attacks

- The value of <LTPA-key-password> is the password you used when exporting the LTPA keys from DASH.

- The value of <Impact-admin-password> is the password (for Active Directory authentication at this point) of your Impact administrative user, typically the impactadmin user.

__4. The script must complete indicating **BUILD SUCCESSFUL**.

__5. Clear your browser cache.

__6. Verify that the impactadmin user can still logon and access Impact using the Impact GUI.

2.14 Integrating the Impact GUI console with DASH

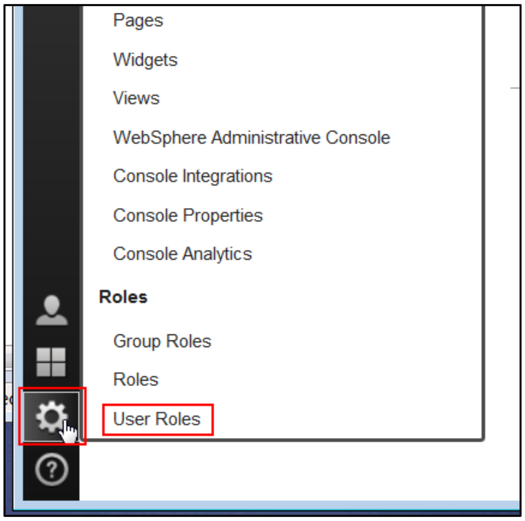
This work is performed on all DASH servers.

This will allow an Impact user to logon to DASH and then access Impact from the DASH GUI.

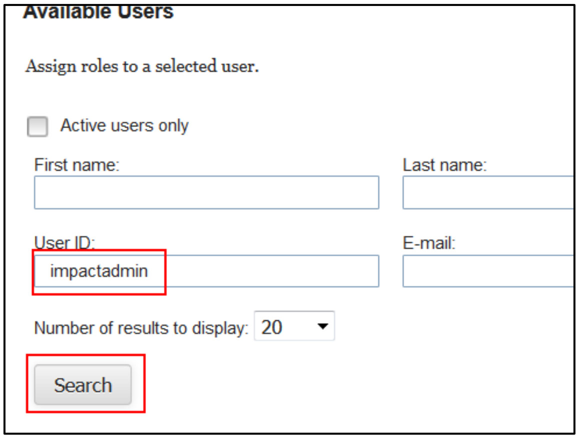
__1. The steps in this section must be done as a valid Impact user who also has administrative privileges for DASH. One way to setup a user for this task is to logon to DASH as the smadmin user and grant the **iscadmins** role to the Impact administrative admin user (typically impactadmin).

__a. Logon to the DASH GUI as the smadmin user.

__b. Navigate to the **User Roles** menu.



__c. Enter **impactadmin** (or your Impact administrative user) as the **User ID** and click the **Search** button. We will use the **impactadmin** user for this example.



Available Users

Assign roles to a selected user.

□ Active users only

First name:

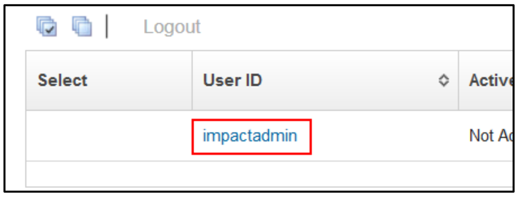
Last name:

User ID: impactadmin

E-mail:

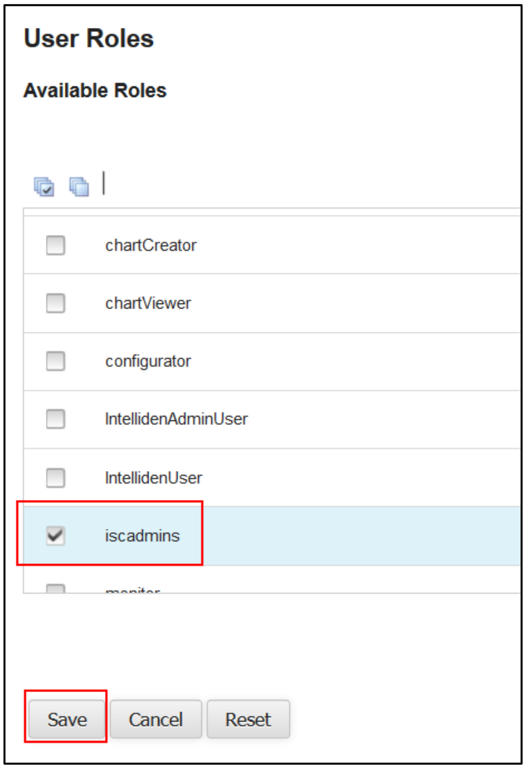
Number of results to display: 20

__d. Click on the impactadmin user in the resulting list.



Select	User ID	Active
	impactadmin	Not Ac

__e. Locate the **iscadmins** role in the list of available user roles and select it by checking the box beside that role.



User Roles

Available Roles

□ chartCreator
□ chartViewer
□ configurator
□ IntellidenAdminUser
□ IntellidenUser
☑ iscadmins
□ monitor

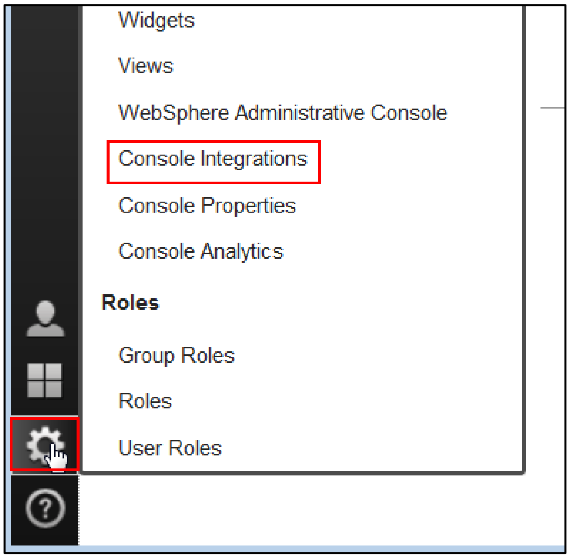
__f. Click the **Save** button.

__g. Log out of the DASH GUI.

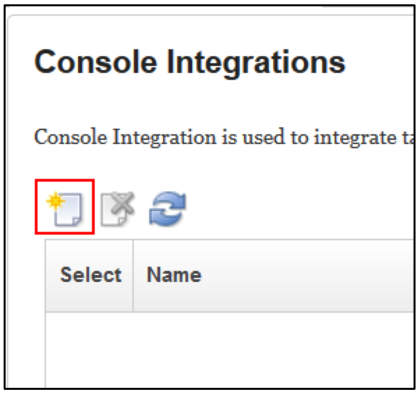
__2. Logon to the DASH GUI as the impactadmin user.

> ⚠ **Important! Use fully qualified host names in URLs to connect with your browser when using SSO**
>
> For SSO to work correctly, you must use the fully qualified domain name of the DASH server in the URL for the DASH GUI when logging on to DASH.

__3. Navigate to the **Console Integrations** menu.



__4. Click the **New** icon to create a new console integration.



Console Integrations

Console Integration is used to integrate t

Select	Name

__5. Fill out the fields in the resulting panel:

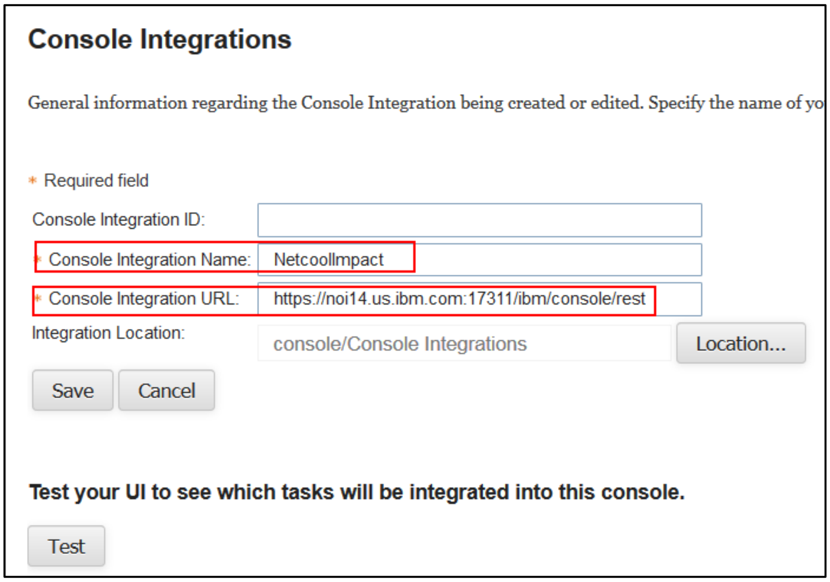
__a. Leave the **Console Integration ID** field empty.

__b. Enter **NetcoolImpact** for the **Console Integration Name** value.

Important! Use unique names if you add additional Impact Console Integrations

If you later add additional Console integrations for additional Impact GUI servers, you must use different Console Integration Names for them.

__c. Enter https://<impact-hostname>:<impact-https-port>/ibm/console/rest as the **Console Integration URL** value, providing the correct fully qualified host name and the HTTPS port for one of your Impact GUI servers.



Console Integrations

General information regarding the Console Integration being created or edited. Specify the name of yo

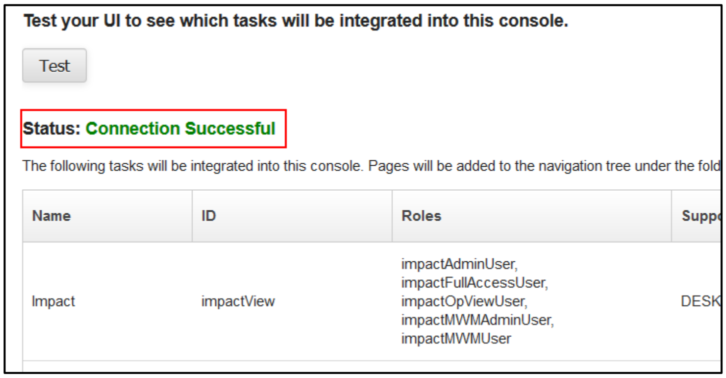
* Required field

Console Integration ID:	
* Console Integration Name:	NetcoolImpact
* Console Integration URL:	https://noi14.us.ibm.com:17311/ibm/console/rest
Integration Location:	console/Console Integrations

Test your UI to see which tasks will be integrated into this console.

__6. Click the **Test** button to verify the connection.

You should see a “Connection Successful” message.



Test your UI to see which tasks will be integrated into this console.

Status: Connection Successful

The following tasks will be integrated into this console. Pages will be added to the navigation tree under the fold

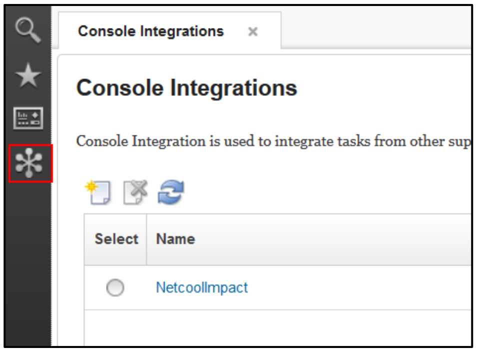
Name	ID	Roles	Supp
Impact	impactView	impactAdminUser, impactFullAccessUser, impactOpViewUser, impactMWMAdminUser, impactMWMUser	DESK

Important! The test must indicate "Connection Successful" before continuing.
Correct any issues and test again before continuing.

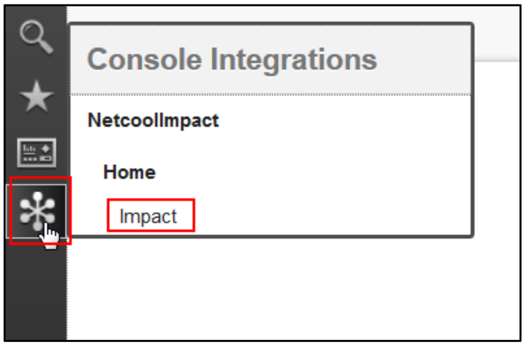
__7. Click the **Save** button.

__8. You should see a new "snowflake" icon on the DASH main menu.

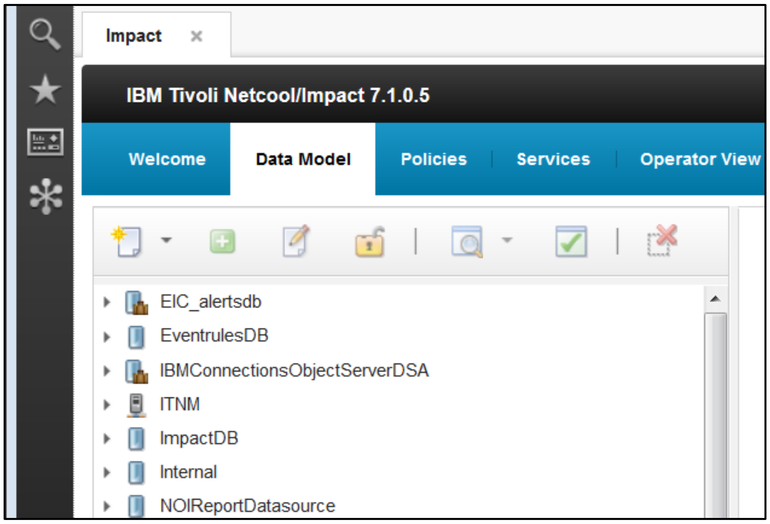
This "snowflake" menu item will only be visible to for valid Impact users.



__9. Click the new "snowflake" menu item, and then click **Impac**t.



__10. Verify that the Impact GUI console opens and that you can access Impact functionality in the Impact GUI.



SSO Troubleshooting

If you are prompted for credentials when clicking on the new Impact console integration menu, check that you have restarted DASH since configuring SSO in the WebSphere administrative console in previous steps. A restart of DASH is necessary so that DASH will recognize the new SSO settings.

__11. You can repeat steps 4 – 10 to add console integration menu selections for additional Impact GUI servers.

__a. Use a different **Console Integration Name** in step 5 for each additional Impact GUI server.

__b. Note that you will see the new menu items under the **Console Integration**s menu shown in step 9.

__c. For an Impact Cluster, all Impact GUI servers will point to whichever Impact server is currently acting as the primary Impact server.

__12. Log out of DASH.

2.15 Enabling users to access the Impact GUI from DASH

Perform this work on all Impact servers.

If the Impact server and Impact GUI server are installed on the same host, performing this work once on that host will set up the Impact user and group roles for both the Impact server and Impact GUI server.

Access to Impact features is controlled via Impact roles that are managed from Impact (not from DASH), using the mapRoles.sh command line utility in Impact.

One approach to controlling access to Impact is to create groups in Active Directory, assign Impact roles to those groups from Impact with the mapRoles.sh utility, and then put users in those groups from Active Directory or from the WebSphere administrative console. You may already have existing groups set up for that purpose.

For this section, we will consider the situation where the existing ncoadmin user does not have access to Impact, and we want to allow the ncoadmin user to have administrative access to Impact.

Use users and groups that will work in your environment

If your ncoadmin user already has administrative access to Impact, select a user without Impact access to use for this example. If you already have a group set up for this purpose, then use that group.

We will use the following approach:

- Have the LDAP administrator create a new group in Active Directory named **impact_admins**.
- Have the LDAP administrator add the **ncoadmin** user to the **impact_admins** group.
- Using the mapRoles.sh command line utility from Impact, add the **impactAdminUser** role to the **impact_admins** group.

Note that another approach is to simply to add the impactAdminUser role to an existing group that the ncoadmin user already belongs to such as netcool_admin, if you want all users in that group to have administrative access to Impact.

This example starts at the point where the impact_admins group has been created in LDAP and the ncoadmin user has been added to that group by the LDAP administrator.

__1. Verify that the ncoadmin user does not currently have Impact access from DASH.

__a. Logon to the DASH GUI as ncoadmin and note that the “snowflake” menu item that contains the Impact menus is not visible.

__b. Log out of the DASH GUI.

__2. From a terminal window on the Impact Server, list the available Impact roles using the mapRoles.sh script.

For a description of the roles, see http://www.ibm.com/support/knowledgecenter/SSSHYH_7.1.0.5/com.ibm.netcoolimpact.doc/common/dita/imug_assigning_roles_to_impact_users.html

```
__a.  cd <IMPACT_HOME>/install/security/

__b.  ./mapRoles.sh -list -all
```

Results of the command:

```
Roles:
      ConsoleUser
      ReadAdmin
      WriteAdmin
      impactAdminUser
      impactFullAccessUser
      impactMWMAdminUser
      impactMWMUser
      impactOSLCDataProviderUser
      impactOpViewUser
      impactRBAUser
      impactSelectedOpViewUser
      impactUIDataProviderUser
      impactWebServiceUser
```

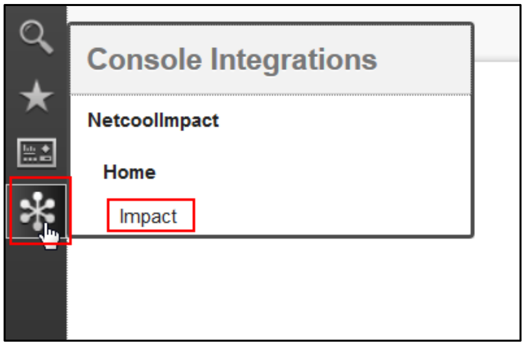
__3. Add the **impactAdminUser** role to the **impact_admins** group. From the terminal window used in the previous step, execute the command:

```
./mapRoles.sh -add -group impact_admins -roles "impactAdminUser"
```

__4. Logon to the DASH GUI as ncoadmin.

__5. Verify that the “snowflake” icon is visible, that you can launch the Impact GUI from DASH, and that you have full access to the Impact menus.

If you are unable to access Impact: logoff, clear your browser cache, and then try again.



About Impact administrative access

Administrative access allows you to unlock policies, services and data models locked by other users if they are not open for editing.

__6. You can use this approach to assign Impact roles to group or to individual users as needed. For this example, we mapped Impact roles to groups. If you want to map Impact roles to individual users, the syntax of the command is:

```
./mapRoles.sh -add -user <username> -roles "<role>"
```

Appendix A. Editing configImpactSSO.sh to handle passwords that include the $ character

In versions of Impact up to and including v7.1.0.6, passwords that include the **$** character are not properly handled by the configImpactSSO.sh script. Using passwords that include the $ character will result in an error during the last step of the script similar to the following:

```
updateCOOKIE:
     [echo] Updating REST API with cookie name
     [echo] Run command java -jar
/opt/IBM/tivoli/impact/install/../cli/cli.jar -addCustomCookieName
'LtpaToken2' -consoleRest https://localhost:16311/ibm/console/rest -
username impactadmin -svc -password xxxxxx
     [java] Authenticating against REST with username:immpactadmin-svc
Password: ********
     [java] Authorization failed.  Please check user and password.


BUILD FAILED
/opt/IBM/tivoli/impact/install/security/cfg_scripts/configImpactSSO.xm
l:49: The following error occurred while executing this line:
/opt/IBM/tivoli/impact/install/security/cfg_scripts/configImpactSSO.xm
l:136: Java returned: 1


Total time: 1 minute 6 seconds
netcool@impact01:/opt/IBM/tivoli/impact/install/security>
```

To avoid this error, you can apply a fix pack that includes a fix for APAR IV86146, such as IBM Tivoli Netcool/Impact V7.1.0 Fix Pack 7 (7.1.0-TIV-NCI-FP0007) which is available from IBM Fix Central. Using a fix pack to correct the issue is the preferred and supported solution.

If a fix pack is not available for your installation, the following work around may work for you, although it has only been tested with Impact V7.1.0.5 and is an unsupported work around:

__1. Make a backup copy of the file <IMPACT_HOME>/install/security/configImpactOSS.sh.

__2. Open configImpactOSS.sh in a text editor.

__3. Locate the line:

```
"$IMPACT_HOME/bin/nc_ant" -buildfile
"$IMPACT_HOME/install/security/cfg_scripts/configImpactSSO.xml"
-Denable=true -Dimpact.home="$IMPACT_HOME" -DPASSWORD="$4" -
DREALMNAME="$1" -DCOOKIENAME="$2" -Dtype=".sh" -Dtype2="" -
Dtype3="" -DDOMAINNAME="$3" -DADMINPASSWORD="$5"
```

Note that this should be the next to last line of the script.

__4. Replace the line with the following three lines. The text starting with **"$IMPACT_HOME/bin/nc_ant" -buildfile** and ending with **DADMINPASSWORD="${passwordAdmin}"** should all be on one line:

```
passwordLtpa=$(echo $4 | sed s/[$]/\\\\\$/g)

passwordAdmin=$(echo $5 | sed s/[$]/\\\\\$/g)

"$IMPACT_HOME/bin/nc_ant" -buildfile
"$IMPACT_HOME/install/security/cfg_scripts/configImpactSSO.xml"
-Denable=true -Dimpact.home="$IMPACT_HOME" -
DPASSWORD="${passwordLtpa}" -DREALMNAME="$1" -DCOOKIENAME="$2" -
Dtype=".sh" -Dtype2="" -Dtype3="" -DDOMAINNAME="$3" -
DADMINPASSWORD="${passwordAdmin}"
```

__5. Save the file.

Appendix B. Example confAuth4LDAP.sh error

This is an example of the error that is returned if you attempt to enable LDAP authentication for Impact while OMNIbus ObjectServer authentication is still enabled.

```
[netcool@noi14 security]$ ./confAuth4LDAP.sh enable impactadmin
Passw0rd Object00 password
Buildfile:
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP.xml

init:
     [echo] Creating backup directory:
/opt/IBM/tivoli/impact/install/../backup
    [mkdir] Created dir: /opt/IBM/tivoli/impact/backup/etc
     [echo] Loading LDAP properties file:
/opt/IBM/tivoli/impact/install/../install/security/impactdap.propertie
s

checkFilters:

enableLDAPWithFilter:

checkFilters:

enableLDAPWithoutFilter:
     [echo] Encrypted LDAP bind DN password: {xor}ED01Ojwrb28=
     [move] Moving 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/shared/config
     [xslt] Processing
/opt/IBM/tivoli/impact/backup/wlp/usr/shared/config/ldapRegistry.xml.0
6142016123821 to
/opt/IBM/tivoli/impact/wlp/usr/shared/config/ldapRegistry.xml
     [xslt] Loading stylesheet
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP-
enable.xsl

removeRegistries:

enableFeature:
     [move] Moving 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/shared/config
     [xslt] Processing
/opt/IBM/tivoli/impact/backup/wlp/usr/shared/config/features.xml.06142
016123821 to /opt/IBM/tivoli/impact/wlp/usr/shared/config/features.xml
     [xslt] Loading stylesheet
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP-
enableFM.xsl

disableFeature:

checkServerEnabled:
```

```
enableLDAP_Server:
     [echo] Located Impact Server Profile

stopNCI:
     [echo] Attempting to stop the Impact NCI Server...
     [exec] Stopping server NCI.
     [exec] Server NCI stopped.

enableLDAP:
     [echo] Enabling LDAP configuration
     [echo] Encrypted Impact password:
{aes}55C2ED520E9E05ECB1D5A67BE23604C9
     [echo] Encrypted Impact bootstrap password:
{aes}ADJTO1mHwW8WOU1fXrNXaggBQLf/UNWLagUar8GaA8nH
     [exec] Password change successful for alias <mykey>
     [exec] Password change successful for alias <default>
     [copy] Copying 1 file to /opt/IBM/tivoli/impact/backup/etc
     [copy] Copying 1 file to /opt/IBM/tivoli/impact/backup/etc
     [copy] Copying 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/NCI
     [move] Moving 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/NCI
     [xslt] Processing
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/NCI/server.xml.061420161
23821 to /opt/IBM/tivoli/impact/wlp/usr/servers/NCI/server.xml
     [xslt] Loading stylesheet
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP-
enableServer.xsl
     [copy] Copying 1 file to /opt/IBM/tivoli/impact/backup/etc
     [copy] Copying 1 file to /opt/IBM/tivoli/impact/backup/etc

startNCI:
     [echo] Attempting to start the Impact NCI Server...
     [exec] Starting server NCI.
     [exec] Server NCI started with process ID 8772.
     [exec] [FATAL   ] Unable to start the Netcool/Impact server due
to authentication problems
     [exec] Unable to successfully start NCI

checkServerDisabled:

disableLDAP_Server:

checkGUIEnabled:

enableLDAP_GUI:
     [echo] Located Impact GUI Server Profile

stopGUI:
     [echo] Attempting to stop the Impact GUI Server...
     [exec] Stopping server ImpactUI.
     [exec] Server ImpactUI stopped.

enableLDAP:
     [echo] Enabling LDAP configuration
     [echo] Encrypted Impact password:
{aes}55C2ED520E9E05ECB1D5A67BE23604C9
     [echo] Encrypted Impact bootstrap password:
{aes}AAqOUF7Rh9K+T6Pe9HznSuxrndEz5HpmOr8JBcrnAQRW
     [exec] Password change successful for alias <mykey>
     [exec] Password change successful for alias <default>
     [copy] Copying 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/ImpactUI
     [move] Moving 1 file to
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/ImpactUI
     [xslt] Processing
/opt/IBM/tivoli/impact/backup/wlp/usr/servers/ImpactUI/server.xml.0614
2016123821 to
/opt/IBM/tivoli/impact/wlp/usr/servers/ImpactUI/server.xml
     [xslt] Loading stylesheet
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP-
enableServer.xsl

startGUI:
     [echo] Attempting to start the Impact GUI Server...
     [exec] Starting server ImpactUI.
     [exec] Server ImpactUI started with process ID 9179.
     [exec] [FATAL   ] Unable to start the Netcool/Impact server due
to authentication problems
     [exec] Unable to successfully start GUI Server ImpactUI

updatePLUGINS:
     [echo] Updating plugin registration
     [echo] Run command java -jar
/opt/IBM/tivoli/impact/install/../cli/cli.jar -deletePlugin
Preferences -pluginurl_username impactadmin -pluginurl_password xxxxxx
-consoleRest https://localhost:17311/ibm/console/rest -username
impactadmin -password xxxxxx
     [java] Deleting a plugin.
     [java] java.net.ConnectException: Connection refused
     [java]      at java.net.PlainSocketImpl.socketConnect(Native
Method)
     [java]      at
java.net.AbstractPlainSocketImpl.doConnect(AbstractPlainSocketImpl.jav
a:370)
     [java]      at
java.net.AbstractPlainSocketImpl.connectToAddress(AbstractPlainSocketI
mpl.java:231)
     [java]      at
java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:
213)
```

```
     [java]       at
java.net.SocksSocketImpl.connect(SocksSocketImpl.java:404)
     [java]       at java.net.Socket.connect(Socket.java:643)
     [java]       at com.ibm.jsse2.qc.connect(qc.java:223)
     [java]       at com.ibm.jsse2.pc.connect(pc.java:57)
     [java]       at
sun.net.NetworkClient.doConnect(NetworkClient.java:193)
     [java]       at
sun.net.www.http.HttpClient.openServer(HttpClient.java:462)
     [java]       at
sun.net.www.http.HttpClient.openServer(HttpClient.java:557)
     [java]       at
com.ibm.net.ssl.www2.protocol.https.c.<init>(c.java:176)
     [java]       at
com.ibm.net.ssl.www2.protocol.https.c.a(c.java:177)
     [java]       at
com.ibm.net.ssl.www2.protocol.https.d.getNewHttpClient(d.java:50)
     [java]       at
sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnec
tion.java:947)
     [java]       at
com.ibm.net.ssl.www2.protocol.https.d.connect(d.java:60)
     [java]       at
sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLCon
nection.java:1105)
     [java]       at
com.ibm.net.ssl.www2.protocol.https.b.getOutputStream(b.java:31)
     [java]       at
com.ibm.tivoli.dashcli.Main.postToServer(Main.java:928)
     [java]       at
com.ibm.tivoli.dashcli.Main.postToServer(Main.java:652)
     [java]       at
com.ibm.tivoli.dashcli.arguments.DeletePlugin.process(DeletePlugin.jav
a:64)
     [java]       at com.ibm.tivoli.dashcli.Main.process(Main.java:536)
     [java]       at com.ibm.tivoli.dashcli.Main.main(Main.java:96)
     [java] Error during request:

BUILD FAILED
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP.xml:
109: The following error occurred while executing this line:
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP.xml:
291: The following error occurred while executing this line:
/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4LDAP.xml:
154: Java returned: 1

Total time: 1 minute 27 seconds
[netcool@noi14 security]$
```

Appendix C. Steps to recover from attempting to enable LDAP authentication for Impact while OMNIbus ObjectServer authentication is still enabled

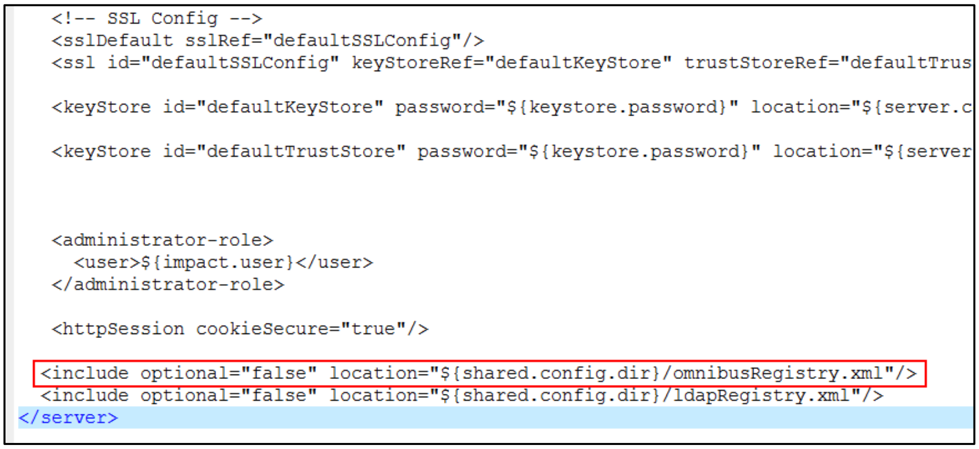
If you attempted to enable LDAP authentication when OMNIbus ObjectServer authentication was still enabled, your confAuth4LDAP.sh script probably terminated with the error shown in the previous Appendix entry. If you are not able to revert to OMNIbus ObjectServer authentication using the confAuth4LDAP.sh script with the “disable” option, you can attempt to edit the underlying WebSphere Liberty Profile configuration files to remove the references to OMNIbus ObjectServer user registries to correct this error.

The authentication error for this example is caused by issues due to multiple available types of user registry implementation services. You will remove the ObjectServer registry from the Impact security configuration, leaving only the LDAP user registry

__1. Make a backup copy of <IMPACT_HOME>/wlp/usr/servers/NCI/server.xml.

__2. Edit <IMPACT_HOME>/wlp/usr/servers/NCI/server.xml.

__a. Remove the line that references the ObjectServer registry (omnibusRegistry.xml).



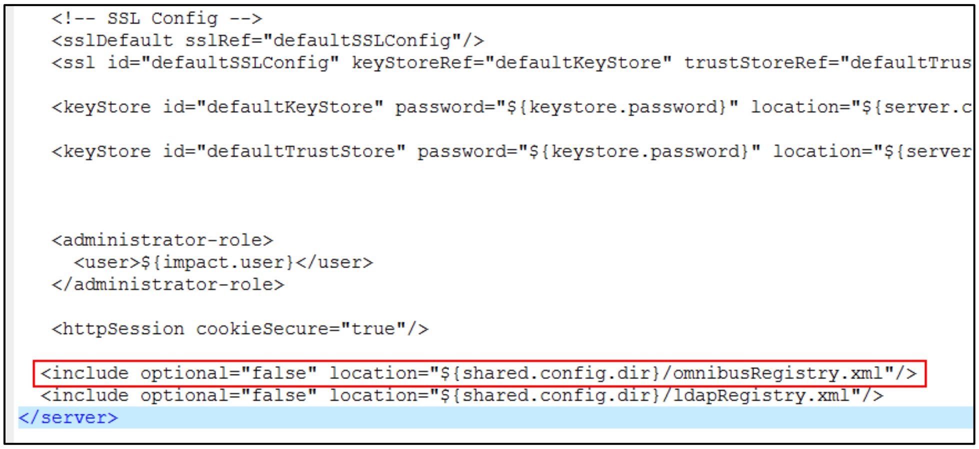
```
   <!-- SSL Config -->
   <sslDefault sslRef="defaultSSLConfig"/>
   <ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrus

   <keyStore id="defaultKeyStore" password="${keystore.password}" location="${server.c

   <keyStore id="defaultTrustStore" password="${keystore.password}" location="${server



   <administrator-role>
     <user>${impact.user}</user>
   </administrator-role>

   <httpSession cookieSecure="true"/>

  <include optional="false" location="${shared.config.dir}/omnibusRegistry.xml"/>
  <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
</server>
```

__b. Save the file.

__3. Make a backup copy of <IMPACT_HOME>/wlp/usr/servers/ImpactUI/server.xml.

__4. Edit <IMPACT_HOME>/wlp/usr/servers/ImpactUI/server.xml.

__a. Remove the line that references the ObjectServer registry (omnibusRegistry.xml).



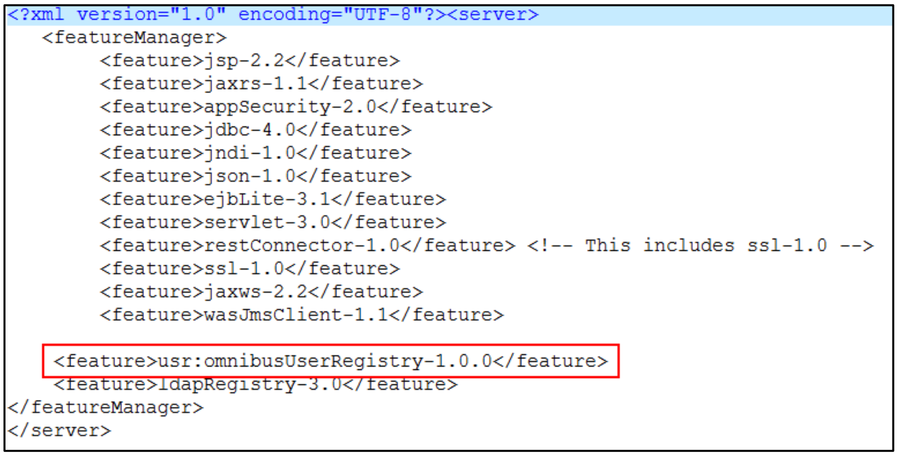
```
   <!-- SSL Config -->
   <sslDefault sslRef="defaultSSLConfig"/>
   <ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrus

   <keyStore id="defaultKeyStore" password="${keystore.password}" location="${server.c

   <keyStore id="defaultTrustStore" password="${keystore.password}" location="${server



   <administrator-role>
     <user>${impact.user}</user>
   </administrator-role>

   <httpSession cookieSecure="true"/>

  <include optional="false" location="${shared.config.dir}/omnibusRegistry.xml"/>
  <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
</server>
```

__b. Save the file.

__5. Make a backup copy of <IMPACT_HOME>/wlp/usr/shared/config/features.xml.

__6. Edit <IMPACT_HOME>/wlp/usr/shared/config/features.xml.

__a. Remove the line that references the ObjectServer registry (usr:omnibusUserRegistry-1.0.0).



```
<?xml version="1.0" encoding="UTF-8"?><server>
   <featureManager>
        <feature>jsp-2.2</feature>
        <feature>jaxrs-1.1</feature>
        <feature>appSecurity-2.0</feature>
        <feature>jdbc-4.0</feature>
        <feature>jndi-1.0</feature>
        <feature>json-1.0</feature>
        <feature>ejbLite-3.1</feature>
        <feature>servlet-3.0</feature>
        <feature>restConnector-1.0</feature> <!-- This includes ssl-1.0 -->
        <feature>ssl-1.0</feature>
        <feature>jaxws-2.2</feature>
        <feature>wasJmsClient-1.1</feature>

    <feature>usr:omnibusUserRegistry-1.0.0</feature>
    <feature>ldapRegistry-3.0</feature>
</featureManager>
</server>
```

__b. Save the file.

__7. Test starting the Impact Server and the Impact GUI Server to be sure that Active Directory authentication is working.

__a. <IMPACT_HOME>/bin/startImpactServer.sh

__b. <IMPACT_HOME>/bin/startGUIServer.sh

Appendix D. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Appendix E. Trademarks and copyrights

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	AIX	CICS	ClearCase	ClearQuest	Cloudscape
Cube Views	DB2	developerWorks	DRDA	IMS	IMS/ESA
Informix	Lotus	Lotus Workflow	MQSeries	OmniFind	
Rational	Redbooks	Red Brick	RequisitePro	System i	
System z	*Tivoli*	*WebSphere*	*Workplace*	*System p*	

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.