iWay Software How-to's



Configuring LDAP Authentication in iWay Service Manager

LDAP authentication in iWay Service Manager (iSM) allows iSM to authenticate against LDAP and associate an LDAP iSM role to the user.

iSM includes a built-in role for an administrator that allows for complete management and control of iSM from the iSM Administration Console. Other roles may be added using the iSM Administration Console to limit access and management of iSM.

To implement LDAP authentication for the iSM Administration Console, each of these roles must be added to an LDAP/Active Directory configuration as Groups and then associated to users. Optionally, an LDAP attribute like *title*, can be associated to a role like *ism.admin*.

The built-in administrator role is *ism.admin*.

Additional roles must be defined in the iSM Administration Console and also in LDAP. This how-to describes the required configuration for LDAP and iSM.

Configuring LDAP Groups

This section describes how to configure LDAP groups for iSM roles. The following steps describe how to create an LDAP group based on the iSM role and a Common Name (CN), which is the iSM role, then adding LDAP members to the group. For example, in the LDAP group for the built-in iSM administrator, *ism.admin* will have *CN=ism.admin*.

1. Create a new LDAP Group for *ism.admin* and then set *cn=ism.admin*, as shown in the following image.

Entry Creation Wizard - Step 3			8 23
Entry RDN Please specify an RDN for the entry.			$\overline{\mathbf{z}}$
Please specify the entry RDN. You can spec	ify a	multi-valued RDN by clicking on the 'Add Value' li	nk.
Type:		Value:	
= m 🔻	=	ism.admin	
<u>Add Value</u>			
RDN Preview: cn=ism.admin			
	<	Back Next > Cancel	Help

2. Add LDAP users as members to the LDAP group (*ism.admin*), as shown in the following image.

CN=ism.admin Properties	ि <mark>४</mark>
Entry Displayed Attribute	s Paging Policy Group Membership
Members Member of	
Name	Parent DN
🧟 Bob Hittner	CN=Users,DC=aethni,DC=ibi,
Search completed. 2 memb	per(s Add or Remove Members
t <u>Configure Settings</u>	Refresh
ОКС	ancel Apply Help

The LDAP group (*ism.admin*) and the associated members of this group are shown in the following image.

Softerra LDAP Administrator 2013.1		OF industry is 200," to the inner infrare and Reality	Manual Inc.		0 0 -8
😋 🕢 👻 🗜 Local Servers 🔸 AETHNE 🔸 OU-Data C	Center + OU=Groups + ON=ism.admin			🔅 😯 Quick Search	P x
File Edit View Favorites Server Entry Schema	Reports Tools Window Help				
🔁 New - 🗔 🕊 🗙 🐇 🖕 🙇 😤 🙁 🏘 .	17.202.12.12.12002	🖉 🖓 🛺 👩 👌 % (objectClass=") 🔹 🚦 🌛 🖏 😭	100 60 Ing.		
Scope Pane 🔹 🔻 🕸 🗙	Name	Value	Туре	Size	0 -
Image: South Servers Image: South Servers Image: South Servers	ObjectClas ObjectClas objectClas objectClas objectClas objectSla objectSla objectSla objectSla objectSla objectSla objectSla objectSla	top group imadm CN-bab Https://Cl-ubers.pC=asthr.pC=ab.pC=com CN-bab Https://Cl-ubers.pC=asthr.pC=ab.pC=com CN-bab Https://Cl-ubers.pC=asthr.pC=ab.pC=com CN-bab Https://Cl-ubers.pC=asthr.pC=asthr.pC=ab.pC=com Y15/2013 3:07:39 PM 9(15/2013 1:158:38 PM 30387 201275 imadmin im.admin c samthrofecutrify/GroupCliptct > [GlobalEcoce] CN=Group.Ol-Schma.CN=Configuration.pC=ast%rLC=4 1/1/1601 CDCMBMD=505 S-1-5-21:20076:12042-1577500245-5020214353-1204	Attribute Attribute	3 5 9 47 45 61 1 17 17 6 6 9 9 9 9 9 9 9 9 9 9 9 1 59 17 15 38	

The following image shows LDAP user *Bob Hittner* as a member of the *ism.admin* LDAP group.

Softerra LDAP Administrator 2013.1		200 propagates in \$200 to the local behaviour field by	Contract Contract		0 0 8
COO - 2 + Local Servers + AETHNE + CN+Users	ON+Bob Hittner			🕸 🔯 Quick Search	P,
i File Edit View Favorites Server Entry Schema	Reports Tools Window Help			-	-
📴 New - 🗔 🛷 🗙 🐇 🍟 🖄 🕅 🙄 k? 🖕	19202.12.9999	월 🖉 🖓 🖓 🎝 👌 💥 (objectClass=*) 🔹 🚦 🥥 🦓 😘	100 IOO 100 IN	9.	
Scope Pane 🗢 🗘 🗙	Name	Value	Туре	Size	e
💼 📲 Local Servers 🔹	objectClass	top	Attribute	3	
i Aethna	☑ objectClass	person	Attribute	6	
E CN=BI	☑ objectClass	organizationalPerson	Attribute	20	
🐵 🧱 CN=B1.ocalAdmn	objectClass	user	Attribute	4	
🛞 📴 CN=Buith	(F) (F)	Sob Hittper	Attribute	11	
E CN+Computers	(F) (D)	billion and	Attribute	7	
😑 - 📴 OU =Data Center	a) title	and admin	Attribute		
OU-Disabled Users		Bub.	Allele de	,	
🖻 🔯 OU=Groups	(i) gversare		All built		
I Description CN+BBLocalAdmins	(a) astropolytication	Evaluation 7	All the design of the design o	40	
- 💭 ON=channeler	Consumer ype	[writible]	Attribute		
🕀 💯 CN+ism.admin	I when created	5/21/2013 9:06:55 PM	Attribute	12	
- 20 CN=ReadOnly	(iii) whenChanged	9/10/2013 4:25:20 PM	Attribute	17	
OU+Domain Controllers	 displayName 	Bob Hitther	Attribute	11	
E OU-Foreign	 uSNCreated 	180829	Attribute	6	
E CN-ForeignSecurityPrincipals	I memberOf	ON-ism.admin,OU=Groups,OU=Data Center,DC=aethni,DC	Attribute	61	
B CO OU-HPHS	I member Of	CN=Administrators,CN=Builtin,DC=aethni,DC=bi,DC=com	Attribute	52	
① CNwInfrastructure	I uSNChanged	197879	Attribute	6	
I CN-ESM	🗟 name	Bob Hitther	Attribute	11	
ON=LostAndFound	userAccountControl	[NormalAccount]	Attribute	3	
OU+miscellaneous	B badPwdCount	0	Attribute	1	
ONWNTDS Quotas	CodePage	0	Attribute	1	
E CN=pop o	📧 countryCode	0	Attribute	1	
R CN=Program Data	badPaspwordTime	9/15/2013 11:41:06 AM	Attribute	18	
CN=System	(F) last oroff	unspecified	Attribute	ĩ	
E CN=testContainer		Q/16/2013 10:45:45 AM	Attribute	50	
⊖ GN=Users	C court action	D/10/2013 4/24 E0 PM	Allegede	10	
B-∑ CN=Administrator	(i) processes	5/10/2013 1121/33 PM	Allebote	28	
IN Alan Tsang IN Alan Tsang IN IN IN I	Contrary ar output	313	Alleboye		
E CN=Allowed RODC Password Replication C	admin.count	1	Attribute		
(8)-22 CN-barney ruble	(e) account(xpires	unspecified	Altribute	1	
2 CN-Bob Hitther	(it) logonCount	34	Attribute	2	
Ovebportnoy01 Oveb	sAMAccountriame	rh10241	Attribute	7	
OinCert Publishers	sAMAccountType	< samUserAccount >	Attribute	9	
H- 2 CN=david hunter	UserPrincpalName	rh10241@aethni.bi.com	Attribute	22	
- 1 CN-Denied RODC Password Replication Gr	objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=aethni,DC	Attribute	60	
	ADT waDrinsansKunftata	1/1/10/14	Amilyan	12	

Configuring iWay Service Manager (iSM)

This section describes how to configure iSM to access and authenticate against LDAP. The following steps will create an iSM Directory Provider, an Authentication Realm, and define additional iSM roles.

- 1. Create an iSM Directory Provider to access the LDAP directory.
- 2. Logon to the iSM Administration Console, click *Server*, and then *Directory Provider* in the left pane.
- 3. Enter the LDAP URL and Base DSN.

8 4 1 4 F 8 F		OF Separate Red Market Institution and All Res Result for a	0 0 - X
CC	rFormLdap?configuration=basel 🔎 + 🖒 👔	🔋 InfoResponse Online - Inform 🕅 Inbox (532) - bhittner@gmail	<u>ଲି ଜି ହ</u> ି
👍 🔼 LDAP Troubleshooting 🕘 Secure Vendor	Portal Acc 🔍 Concur Expense (2) 🥑 abo	ut.com http://www.njt 🥑 SSL VPN Service 💟 db2utor SQL 🧧 CONTENTS DB2 V9.3 for z 🎬 BIM DB2 for z-OS - Techni 😮 Citrix XenApp - Logen 🥫 RAD 0, RAD 1, RAD	5, RA **
iWay Service Mana	ger	Management 🔤 🔽 🖉 😨 sp8.41391	^
<u>Server</u> Registry Deploym			
Properties D General Properties ar Java Properties W M	irectory Providers: LDAP ghtweight directory access pro d other resources such as file Vay Service Manager allows the anager's use of LDAP follows a	tocol or LDAP a software protocol that enables standard program accessibility to locate organizations, individuals, s and devices in a network, whether on the public Internet or on a corporate intranet. Enabling LDAP for use with e value of configuration parameters to be retrieved directly from an LDAP-enabled directory. Way Service all security rules for LDAP use and does not permit any changes to be made to the LDAP directory.	
Settings	DAP Server Definition		
General Settings	lame	ldap_console	
Console Settings	Description	Enter a description of the use of this directory server.	
Java Settings		^	
Register Settings		×	
Trace Settings	DAP Initial Context Factory	Fully gualified class name of the LDAP Initial Context Factory, default is com.sun.indi.ldap.LdapCtxFactory	
Log Settings	,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Path Settings			
Backup Settings	JRL *	URL to reach LDAP directory. LDAP URL's are in the form idap://host[:port] or idaps://host[:port]. When used as a CertStore, consider adding the base DN to the URL, for example idap://host[:port]/o=Company.c=US	
Providers		ldap://iwserv18.ibi.com:389/DC=aethni,DC=ibi,DC=com	
Data Provider	Pool Size	A pool of connections to the LDAP server reduces contention but increases memory use. iWay suggests a range of 2-	
Services Provider		10 for a normally loaded system.	
Directory Provider		2	
Security Provider			
XML Namespace Map Provider	Authentication Mechanism	Specifies the authentication mechanism to use. Choose Not Specified to use UNDIs detault, if the User ID and Password are absent, the default is none, otherwise the default is simple. When using an LDAPS URL, the default is always simple. You can also type a space separated list of mechanisms to try in order of preference.	
Pooling Providers		and the second	· ·

- 4. Update the required fields for the LDAP Directory Provider.
- 5. Select *simple* from the Authentication Mechanism drop-down list. Enter the user ID and password for LDAP in the corresponding fields.

🗲 💿 🛯 http://mktrjhiway64.9999/isn	n/serverFormLdap?configuration=baset P = C	😰 InfoResponse Online - Inform. Minbox (532) - bhittner@gmail TN Object Naming 🚽 Way Service Manager Ad 🗴 🌻 In Microsoft Active Directory,
🎪 💦 LDAP Troubleshooting 🧃 Secure 1	Vendor Portal Acc 🗯 Concur Expense (2) 🧃 al	bout.com http://www.njt 🧃 SSL VPN Service 💟 db2utor SQL 🏧 CONTENTS DB2 V9.1 for z 🏧 IBM DB2 for z-OS - Techni 🕐 Citrix XenApp - Logon 🥫 RAID 0, RAID 1, RAID 5, RA.
Data Provider Services Provider Directory Provider	Pool Size	A pool of connections to the LDAP server reduces contention but increases memory use. IWay suggests a range of 2- 10 for a normally loaded system.
Security Provider XML Namespace Map Provider Pooling Providers Authentication Realms Data Quality Providers	Authentication Mechanism	Specifies the authentication mechanism to use. Choose Not Specified to use JNDI's default. If the User ID and Password are absent, the default is none, otherwise the default is simple. When using an LDAPS URL, the default is always simple. You can also type a space separated list of mechanisms to try in order of preference. simple Pick one V
Schedule Provider SNMP Provider Facilities	Authentication Realm	For some SASL authentication mechanisms, this is the domain from which the user ID should be chosen. If you do not specify a reaim, then any one of the realms offered by the server will be used.
Activity Facility Correlation Facility	User ID	User ID registered for appropriate access to this LDAP directory. [waydp01
	Password	Password for access to the LDAP directory.
	SSL Context Provider	Way Security Provider for SSL Context. This parameter is required when using an Idaps: URL. When an SSL Context is given with an Idap: URL, this will upgrade the normal LDAP connection to one protected by TLS/SSL using the LDAP StarTLS extension. DAP StarTLS extension. Pick one or enter value
	Quality of Protection	Some SASL mechanisms support integrity and privacy protection of the communication channel after successful authentication. Choose Not Specified to rely on JNDI's default.

6. Click *Add* and then test the Directory Provider for successful connectivity.

🚕 🔼 LDAP Troubleshooting 🗿 Secu	re Vendor Portal Acc 🚨 Concur Expense (2) 🕘 ab	out.com http:-www.njt 🕘 SSL VPN Service 🔚 db2utor SQL 🧱 CONTENTS DB2 VP.1 for z 🜃 BIM DB2 for z-OS - Techni 🕲 Citrix XenApp - Logon 😭 RAED 6, RAID 1, RAED 5, A	RA_
iWay Service M Server Registry De	anager ployments Tools	Management <mark>base v </mark> Ø Ø op 41391 Restart Licenses About Logout	
Properties General Properties Java Properties	Directory Providers: LDAP Lightweight directory access pr and other resources such as fill Way Service Manager allows th Manager's use of LDAP follows	extraction of LDAP a software protocol that enables standard program accessibility to locate organizations, individuals, es and devices in a network, whether on the public Internet or on a corporate intranet. Enabling LDAP for use with he value of configuration parameters to be retrieved directly from an LDAP-enabled directory. Way Service all security rules for LDAP use and does not permit any changes to be made to the LDAP directory.	
Settings	Test Result		
General Settings	Success	success	
Console Settings	PROBLEM		
Java Settings	Success	SUCCESS	
Register Settings	LDAP Server Definition		
Log Settings	Name	ldap_console	
Path Settings	Description	Enter a description of the use of this directory server.	
Data Settings Backup Settings		0	
Providers Data Provider	LDAP Initial Context Factory	Fully qualified class name of the LDAP Initial Context Factory, default is com.sun.jndi.idap.LdapCtxFactory	
Services Provider			
Directory Provider	URL	CertStore, consider adding the base DN to the URL, for example Idap://host[:port]/o=Company.c=US	
Security Provider		Idap://iwserv18.ibi.com:389/DC=aethni.DC=ibi.DC=com	
XML Namespace Map Provider			
Pooling Providers	Pool Size	A pool of connections to the LDAP server reduces contention but increases memory use. IWay suggests a range of 2-	

- 7. Add the Authentication Realm by clicking on *Authentication Realm* under Providers in the left pane.
- 8. Click *New*.

9. Select *ldaprealm* from the Realm Type drop-down list, enter a name in the Name field, and then select the configured directory provider for LDAP in the LDAP Provider field.

iWay Service N	lanager	Management base	~		0 0	
Server Registry D	eployments Tools					
Properties General Properties	Authentication Realn Configure an authentic	ation realm to manage access to NHTTP and NAS2 channels.				
Java Properties	Realm Parameters					
Jurg Tropando	Realm Type	Select the type of realm you want to create.				
General Settings		Idaprealm	~			
Console Settings	Name *	Name to identify this realm				
Java Settings		console_authentication_realm				
Trace Settings	Description	Enter a description of the use of this realm.				
Log Settings Path Settings				\bigcirc		
Data Settings	LDAP Provider *	Name of the Directory Provider describing the connection to the LDAS	P server.			
backup secongs		Idap_console	×			
Providers		Pick one or enter value	~			

10. Enter the user-based LDAP information by selecting *true* from the Search User Subtree dropdown list, and then entering *sAMAccountName={0}* in the User Search Filter field.

User Base Context	The base of the subtree containing users. Each user that can be authenticated must be represented by an individual entry that corresponds to an element in this DirContext. If not specified, the top level element in the directory context will be used.
User Pattern	A pattern for the distinguished name (DN) of the user's directory entry. Use {0} to substitute the username. For example, (cn={0}). LDAP OR syntax is also supported ((cn={0})(cn={0}),o=myorg)). You can use this property instead of User Search Filter, Search User Subtree and User Base Context when the distinguished name contains the username and is otherwise the same for all users.
Search User Subtree	The search scope. Set to true if you wish to search the entire subtree rooted at the User Base Context entry. The default value of false requests a single-level search including only the top level. true Pick one
User Search Filter	The LDAP filter expression to use when searching for a user's directory entry, with {0} marking where the actual username should be inserted. Use this property (along with the Search User Subtree property) instead of User Pattern to search the directory for the user's entry.
User Password Attribute	Name of the attribute in the user's entry containing the user's password. If you specify this value, this realm will retrieve the corresponding attribute for comparison to the value specified by the user being authenticated. If you do not specify this value, this realm will attempt a simple bind to the directory using the DN of the user's entry and password specified by the user, with a successful bind being interpreted as an authenticated user.

11. Enter the role-based information by adding the Role Base Context, selecting *true* from the Search role Subtree drop-down list, specifying values for the Role Search Filter and Role Attribute parameters. Click *Add* when finished.

The base directory entry for performing role searches. If not specified, the top level element in the directory context will be used. OU=Groups,OU=Data Center
Set to true if you want to search the entire subtree of the element specified by the Role Base Context for role entries associated with the user. The default value of false causes only the top level to be searched. true Pick one
The LDAP filter expression used for performing role searches. Use {0} to substitute the distinguished name (DN) of the user, and/or {1} to substitute the username. If not specified a role search does not take place and roles are taken only from the attribute in the user's entry specified by the User Role Attribute. member={0}
The name of the attribute that contains role names in the directory entries found by a role search. In addition you can use the User Role Attribute property to specify the name of an attribute, in the user's entry, containing additional role names. If Role Attribute is not specified a role search does not take place, and roles are taken only from the user's entry.
The name of an attribute in the user's directory entry containing zero or more values for the names of roles assigned to this user. In addition you can use the Role Attribute property to specify the name of an attribute to be retrieved from individual role entries found by searching the directory. If User Role Attribute is not specified all the roles for a user derive from the role search.

12. Click Management.



13. Click Servers.

2	
iWay Service M Server Registry De	
Application Management	
Deployments	
Applications	
Templates	
Events	
Server Management	
Servers	
Users	
Server Roles	
Test Servers	
Remote Servers	

14. Click the configuration name that will be using the LDAP authentication (for example, *base*).

Servers Server creation and ma components.	nagement. Server - a tradi	cional ISM runtime configuratic	on that allows non-atomic deployment and managemen	it of
Name	Port	Secure	Description	
base	9999	No		
Add Delete				

- 15. Under Console Attributes, update the Authentication Realm parameter to use the Authentication Realm that you configured earlier.
- 16. Enter the LDAP user ID and password that was associated to the LDAP group (*ism.admin*). Optionally, enable the Console Tracing option for debugging LDAP authentication issues, as shown in the following image.

Console Tracing	Should console components output traces to the system log at levels specified in the system trace settings? Default is to output only error and warning level trace messages. Change requires restart of ISM.	
Authentication Realm	FISM Security Ism_console_ldap console_authentication_realm	
Console Admin ID	User ID to be used for internal communication with the iSM console. Must be valid in the specified authentication realm and should have iSM admin authority. rh10241	
Console Admin Password	Password for the console admin account	
<- Back Finish		

17. Restart iSM and logon to the iSM Administration Console.

To debug any potential LDAP authentication issues, start iSM from a Windows Command Prompt using the following command:

c:\> iway61 base -u

Configuration of an LDAP connection and authentication for iSM is complete.

Adding Additional Server Roles in iWay Service Manager (iSM)

- 1. To add additional iSM roles, click *Management* and then click *Server Roles* in the left pane.
- 2. Click *Add*, provide a name for the role, and assign permissions.

Server Registry De	anager ployments Tools	Management base	Restart Licenses About Lo	
Application Aanagement Deployments	Server Roles Server role management Server Roles			-
Applications Templates Events	Name ReadOnly	Description		
erver Management Servers Users Server Roles	Add Delete			

- 3. Click Add.
- 4. In the Server Roles section, enter *ReadWrite* in the Name field, and then select the allowable permissions, as shown in the following image.

An external authentication realm assigns one or more roles to an authenticated user. Roles are authorized to perform actions on the server.				
Role				
Name *	ReadWrite			
Description				
General iSM Permissions				
Can Add Configurations	Permit the holder of this role to create new configurations on the server			
	On			
Can Delete Configurations	Permit the holder of this role to delete any existing configuration			
	On			
Can Stop Configurations	Permit the holder of this role to stop configurations and components deployed in those configurations			
	V On			
Can Restart Configurations	Permits the user to restart configurations			
	V On			
Can Access Server Settings.	Permits the user to view and edit general server settings. Requires write permission for the configuration.			
	V On			
Can Access Channels	Permits the user to view, manage, and deploy channels and services. Requires write permission for the configuration			
	✔ On			
Configuration Specific Permissions				
base	Read Write Monitor			

- 5. Perform the steps in *Configuring LDAP Groups* to add the LDAP group for the *ReadWrite* role.
- 6. Restart iSM and verify the new role.

The name of the iSM role must match the name of the LDAP group. For example:

- iSM role = ReadWrite
- LDAP group = ReadWrite

They are mapped by using the same name.

Troubleshooting LDAP Authentication Using the iWay Service Manager Configuration Log (Tracing)

- 1. Enable Console Tracing. For more information, see step 16 in *Configuring iWay Service Manager (iSM)*.
- 2. Click Server, navigate to Trace Settings, and then enable Deep and Debug.
- 3. Log on to the iSM Administration Console (configuration).
- 4. Examine the log file from the iSM log directory (*iway_home*\config\base\log) and look for the most recent log file. For example:

DEEP (console) LDAP Realm, entry found for csswxz with dn CN=CSSWXZ,CN=Users,DC=eda,DC=csseda,DC=com

DEEP (console) LDAP User role name cn search

DEEP (console) LDAP Realm, retrieving values for attribute cn

DEBUG (console) LDAP Realm, csswxz authenticated successfully

DEEP (console) LDAP Realm, getRoles(CN=CSSWXZ,CN=Users,DC=eda,DC=csseda,DC=com)

DEEP (console) LDAP Realm, retrieving values for attribute cn

DEEP (console) LDAP Realm, Returning roles: CSSWXZism.admin

DEEP (console) LDAP Realm, Closing directory contex

The *ism.admin* role may seem joined to another role (CSSWXZism.admin), which is the expected behavior. It is important to ensure that the *ism.admin* role (or any other role you assign) exists within the *Returning roles* entry in the log file.