

IBM® Security Identity Manager™ New Features in 6.0 and 7.0

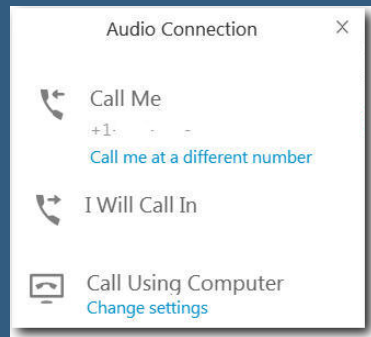
IBM SECURITY SUPPORT OPEN MIC

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

You will not hear sound until the host opens the audio line.

For more information, visit:

http://ibm.biz/WebExOverview_SupportOpenMic



NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.




IBM® Security Identity Manager™ New Features in 6.0 and 7.0

IBM SECURITY SUPPORT OPEN MIC

SOKE-WAN CHUA & SHARWARI MORE

6 December 2017





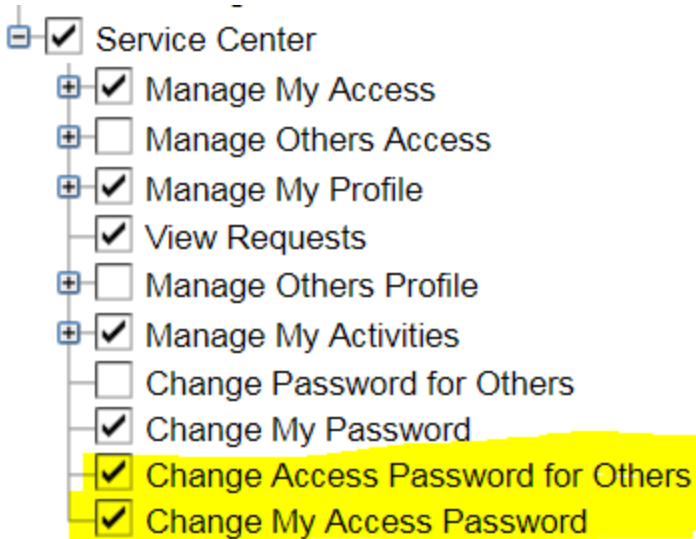
IBM Security Identity Manager

6.0 Fixpack 19

7.0 Fixpack 8

Change Access Password task in ISC

- New tasks in Manage View to change password for self and others on accesses (accounts) that are excluded from password synchronization:
 - Enable them to show tasks in ISC



Change Access Password task in ISC (cont.)

- ISC View :

IBM Security Identity Manager

System Administrator Log Out

IBM

Identity Service Center

Manage Access Manage Activities View Requests Manage Profiles

My Activities

View and act on my activities.

View Requests

View my requests.

View and Edit Profile

View and edit profile for myself and others

Change Password

Change password for myself and others.

Change Access Password

Change password for my and other access that are excluded from password synchronization.

Delegate Activities

Delegate my activities.

Change Access Password task in ISC (cont.)

- If login user is manager, gets to select subordinates

IBM Security Identity Manager

System Administrator Log Out

IBM

Change Access Password

Manage Access Manage Activities View Requests Manage Profiles

Select User




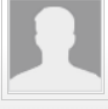
Search users

Quick Select

Select me

1 to 8 of 8

Sort by: Name | Contact Information

	divya	View Accesses
	Greg Heffley	View Accesses
	Role1 Approver	View Accesses
	Role2 Approver	View Accesses

Change Access Password task in ISC (cont.)

- Showing accesses that are excluded from password synch

IBM Security Identity Manager

System Administrator Log Out

IBM

Change Access Password

Manage Access Manage Activities View Requests Manage Profiles

Back

Change Access Password: Sachin Babar

Search accounts

☒ Generate a password for me

☐ Allow me to type a password

Submit

Password Requirements:

The minimum number of characters in the password is 1.

1 to 2 of 2

Sort by: Name | Description | User ID

☒

ITIM Service (User ID: sachin1)

☒

Test Ldap (User ID: sachin1)

- Showing accesses that are excluded from password sync

- Showing accesses that are excluded from password sync

IBM Security Identity Manager

Configure ISC approval justification

- Ulconfig.properties

This property decides whether the justification field is mandatory while approving the activity.

Allowed Values: (true|false)

By default this property will be set to 'true'.

ui.activities.approve.justificationRequired=true

This property decides whether the justification field is mandatory while rejecting the activity.

Allowed Values: (true|false)

By default this property will be set to 'true'.

ui.activities.reject.justificationRequired=true

This property decides whether justification field is to be

displayed on Manage Activities and Decisions page or not.

Allowed Values: (true|false)

By default this property will be set to 'true'

ui.activities.displayJustification=true

Configure ISC approval justification (cont.)

IBM Security Identity Manager

Role2 ApproverLog Out

IBM

My Activities

Manage Access

Manage Activities1

View Requests

Manage Profiles

Manage Activities and Decisions

Select Multiple

Search in: Current Activities

Search activities

Sort by: Date | Requested for

accOwnerApprv: w3 access for Greg Heffley

* Justification for this decision (mandatory for rejection):

Provide justification for this decision.

Approve

Reject

Due Date: Nov 20, 2017, 3:10:51 PM

Configure SMTP Authentication

- enRoleMail.properties

Host, example: 192.168.6.204

mail.host=

mail.smtp.port=

Since 6.0 FP 19, the following properties are introduced to support SMTP authentication while sending email notification within ISIM.

mail.smtp.starttls.enable enables TLS session with the mail server.

mail.smtp.auth enables authentication with the mail server.

#runConfig mail Test also depends on this setting to establish authenticated or non-authenticated session to send mail

mail.smtp.auth.user is the user id used by ISIM to authenticate with the smtp server.

mail.smtp.auth.password is the password for mail.smtp.auth.user.

#Password entered as plain text directly will be encrypted by running runConfig utility.

mail.smtp.starttls.enable=false

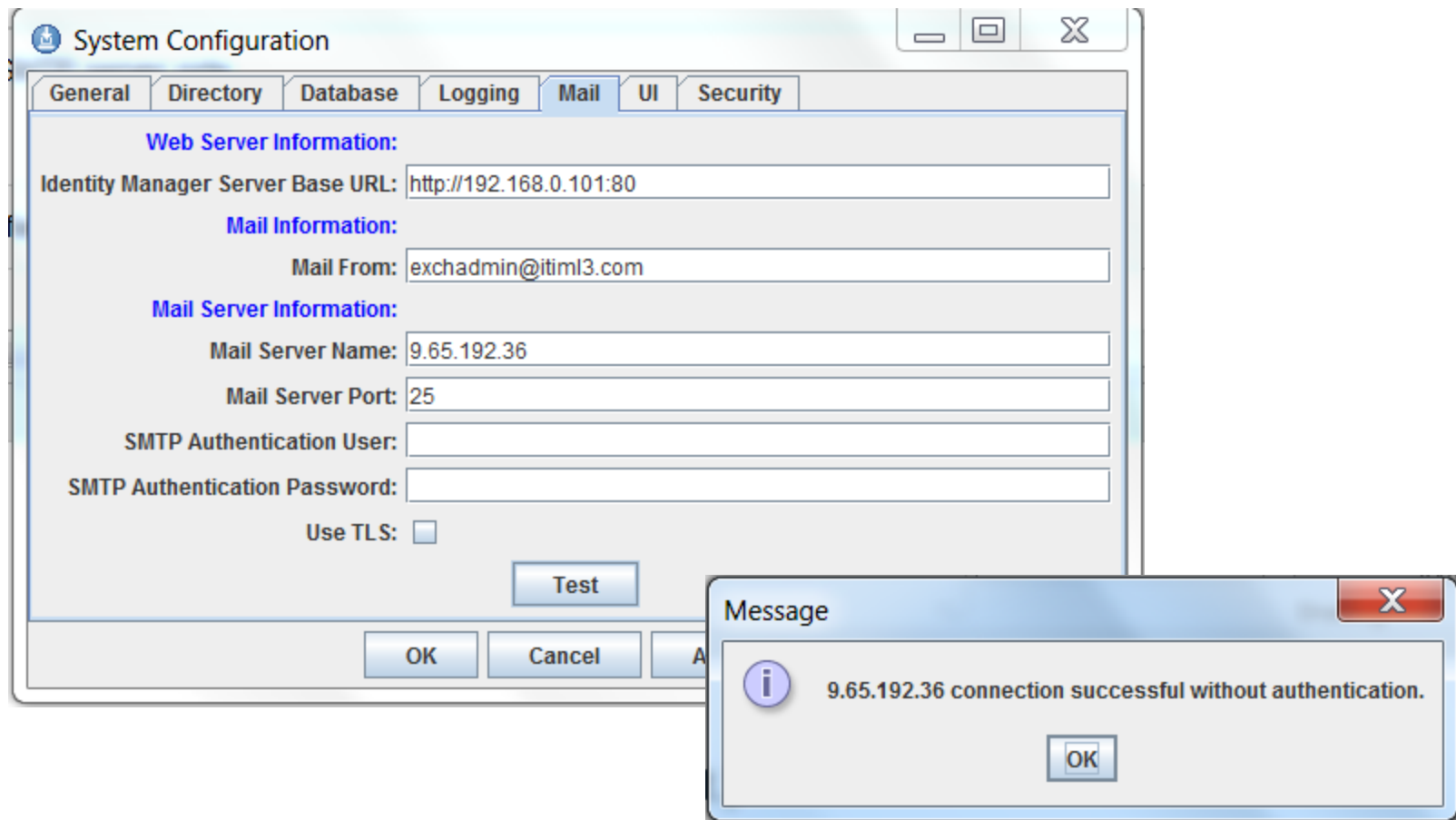
mail.smtp.auth=false

mail.smtp.auth.user=

mail.smtp.auth.password=

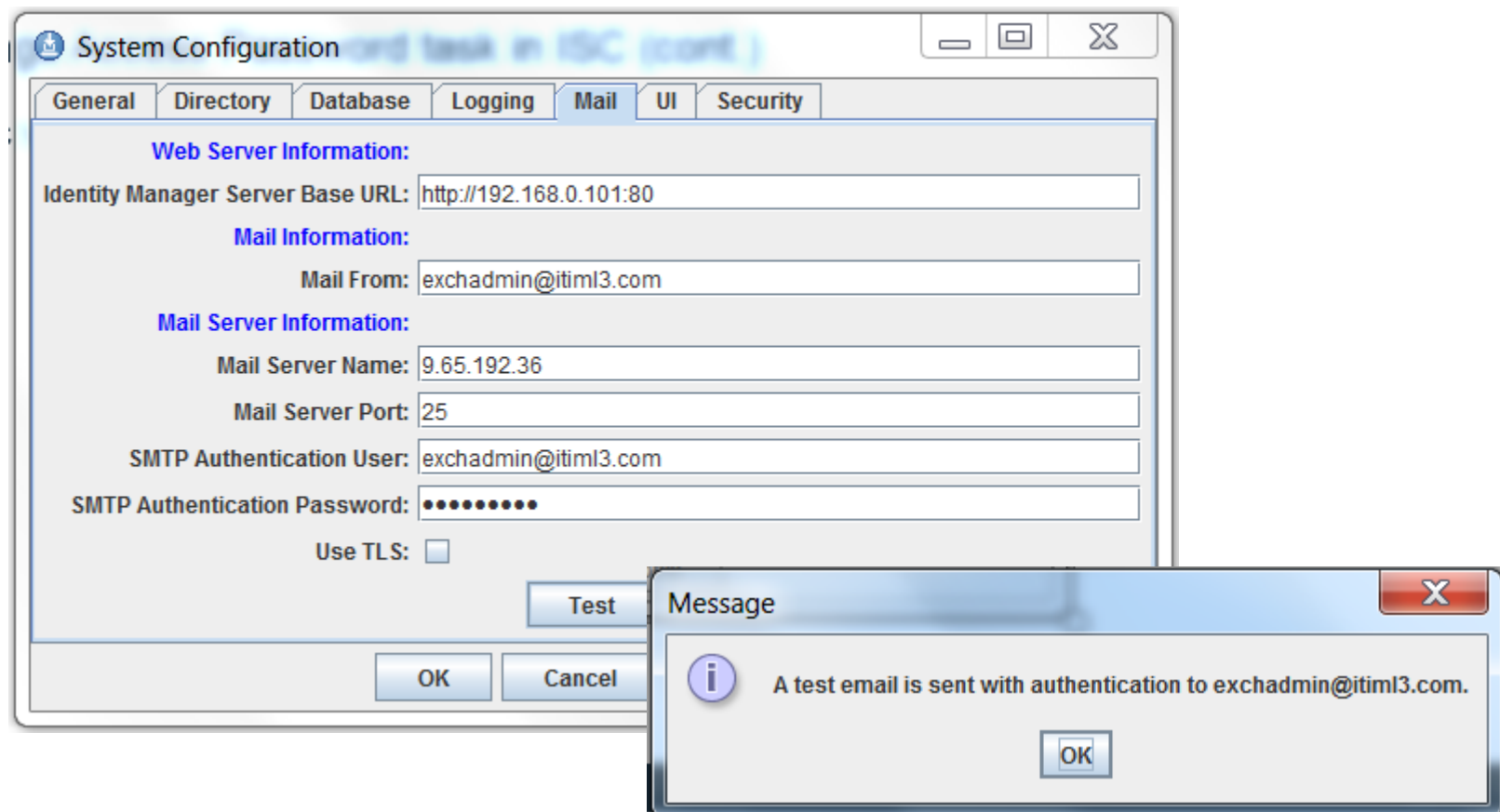
Configure SMTP Authentication

- runConfig – example showing no SMTP authentication, no TLS communication



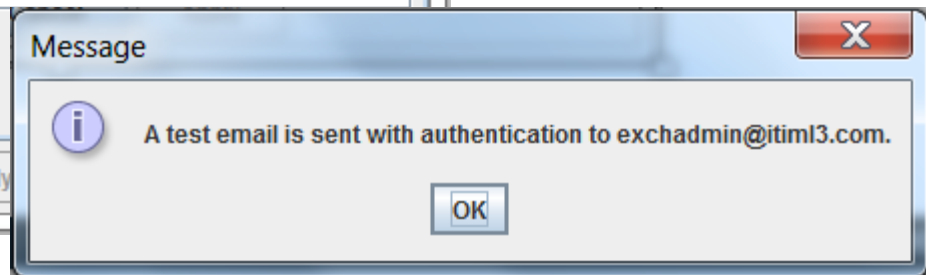
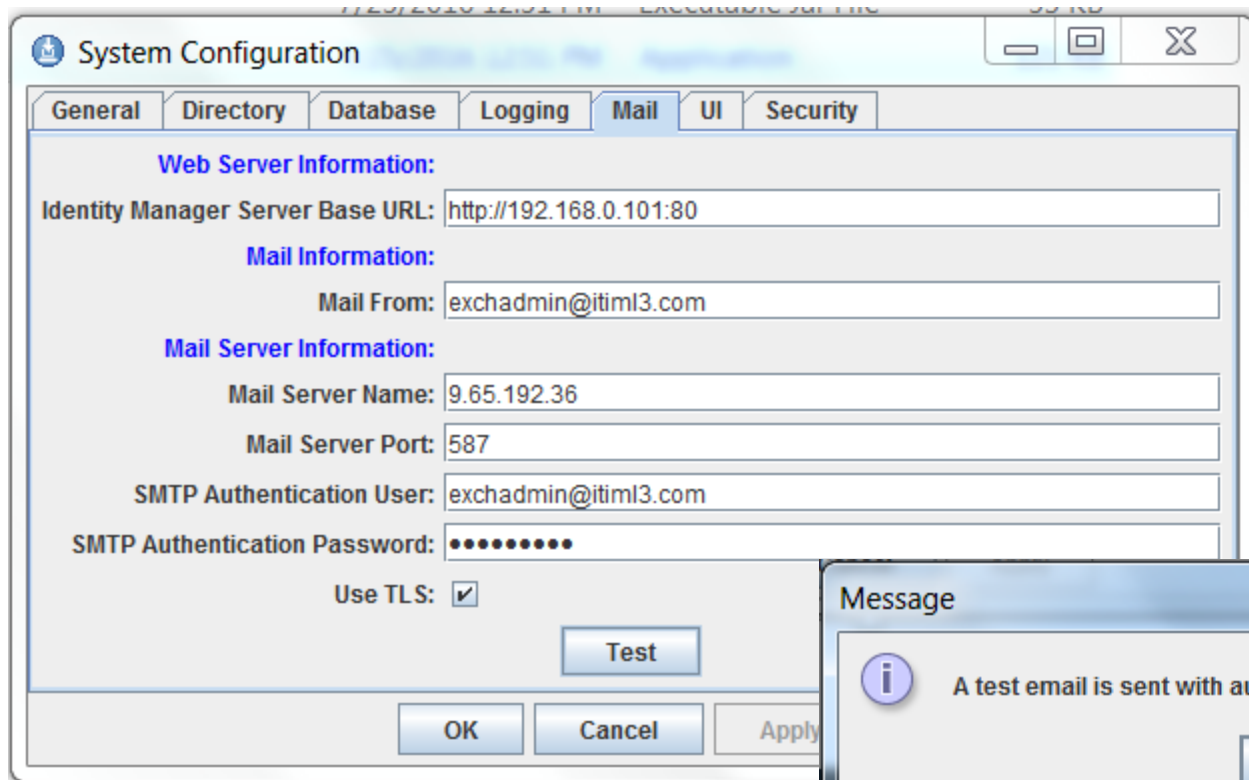
Configure SMTP Authentication (cont.)

- runConfig – example showing SMTP authentication, no TLS communication



Configure SMTP Authentication (cont.)

- runConfig – example showing SMTP authentication, TLS communication
- REMEMBER – must import mail server's SSL certificate



Workflow Time-Out setting

- LIMIT setting in workflow can now be changed via UI

The screenshot shows a 'Properties' dialog box with the following sections:

- Operation Type:** Radio buttons for 'Static' (selected) and 'Non Static'.
- Escalation Limit:** Input fields for '0' Days, '12' Hours, '0' Minutes, and '0' Seconds.
- Input Parameters:** A table with columns 'ID', 'ID', and 'Type'. It contains three rows: 'R' with 'owner' (Person), 'service' (Service), and 'S' with 'account' (Account). A 'Details' button is to the right.
- Legend:** 'S: Subject R: Requestee B: Both'.
- Output Parameters:** A section with a 'Map Relevant Data' button and 'Add', 'Modify', and 'Delete' buttons.
- Table:** A table with columns 'ID', 'Type', and 'Relevant Data ID'.
- Relevant Data:** A section with 'Add', 'Modify', and 'Delete' buttons.
- Table:** A table with columns 'ID' and 'Type'.
- Legend:** 'S: Subject R: Requestee B: Both'.
- Buttons:** 'Ok' and 'Cancel' at the bottom.

Mail Server Configuration

Mail Server Configuration

Configure | Reconfigure | Unconfigure

Mail Server Configuration

Mail Configuration

Edit Mail Configuration Details

Mail server (FQDN, IPv4, or IPv6):
9.118.38.119

Port:
25 **TLS** ☐

Mail from:
admin@ibm.com

Mail base URL (Optional):

Mail User (Optional):

Mail Password (Optional):

Save Configuration

Cancel

Changes in Mail Server Configuration

- New fields to enable authentication:
 - Mail User
 - Mail Password
- Changed the label for SSL to TLS

Also...

- Reduce exception stack output in ISIM trace.log file from password change request when new password value does not conform to password rule (from this)

```
<Trace Level="MIN">
<Time Millis="1468335015903"> 2016.07.12 07:50:15.903-07:00</Time>
<Server Format="IP">win2k8r2cw</Server>
<ProductId>CTGIM</ProductId>
<Component>com.ibm.itim.policy</Component>
<ProductInstance>server1</ProductInstance>
<LogText><![CDATA[Validation failed for Account cweber on the Service ITIM Service;CTGIME012E The password does not meet the
requirements of the password rule. The following error occurred.
Error: CTGIMH011E The password does not adhere to the minimum number of characters. ]]></LogText>
<Source FileName="com.ibm.itim.policy.PasswordPolicyAuthority" Method="checkPassword"/>
<Thread>WebContainer : 26</Thread>
<Exception><![CDATA[com.ibm.passwordrules.InvalidPasswordException: CTGIMH011E The password does not adhere to the minimum
number of characters.
    at com.ibm.passwordrules.standard.LengthConstraint.validate(LengthConstraint.java:129)
    at com.ibm.passwordrules.standard.RuleSet.validate(RuleSet.java:498)
    at com.ibm.itim.policy.PasswordPolicyAuthority.checkPassword(PasswordPolicyAuthority.java:334)
    at com.ibm.itim.policy.PasswordPolicyAuthority.checkPassword(PasswordPolicyAuthority.java:245)
    at com.ibm.itim.apps.ejb.organization.account.PasswordManagerBean.isValidPassword(PasswordManagerBean.java:2197)
    at com.ibm.itim.apps.ejb.organization.account.PasswordManagerBean.submitToWorkflow(PasswordManagerBean.java:1887)
    at com.ibm.itim.apps.ejb.organization.account.PasswordManagerBean.submitToWorkflow(PasswordManagerBean.java:1853)
    at com.ibm.itim.apps.ejb.organization.account.PasswordManagerBean.submitPasswordChange(PasswordManagerBean.java:1170)
    at com.ibm.itim.apps.ejb.organization.account.PasswordManagerBean.submitPasswordChange(PasswordManagerBean.java:1266)
    at
com.ibm.itim.apps.ejb.organization.account.EJSLocalStatelessenrolejb_PasswordManagerHome_702d2dff.submitPasswordChange(Unknown
Source)
    at com.ibm.itim.ui.impl.ejb.PasswordManager$14.run(PasswordManager.java:538)
    at java.security.AccessController.doPrivileged(AccessController.java:452)
```

Also...

- Reduce exception stack output in ISIM trace.log file from password change request when new password value does not conform to password rule (to this)

```
<<Trace Level="MIN">
<Time Millis="1468335015918"> 2016.07.12 07:50:15.918-07:00</Time>
<Server Format="IP">win2k8r2cw</Server>
<ProductId>CTGIM</ProductId>
<Component>com.ibm.itim.ui.impl</Component>
<ProductInstance>server1</ProductInstance>
<LogText><![CDATA[CTGIMU017E The password specified for the selected accounts does not comply with all of the password rules defined for
these accounts.]]></LogText>
<Source FileName="com.ibm.itim.ui.impl.PersonImpl" Method="changeAccountPasswords(Collection, String)"/>
<Thread>WebContainer : 26</Thread>
<Exception><![CDATA[com.ibm.itim.apps.identity.InvalidPasswordException: CTGIME012E The password does not meet the requirements of
the password rule. The following error occurred.
Error: CTGIMH011E The password does not adhere to the minimum number of characters.
]]></Exception>
```

Also...

- Provide object info during decryption exception

Caused by: com.ibm.itim.util.EncryptionException: CTGIMO047E An error occurred while processing a decryption request on object or property value `erglobalid=6337939778805454869,ou=services,erglobalid=00000000000000000000,ou=org,dc=ISIM`. The following error occurred.

Error: Input length (with padding) not multiple of 16 bytes

at com.ibm.itim.util.EncryptionManager.decrypt(EncryptionManager.java:1004)

at com.ibm.itim.util.EncryptionManager.decrypt(EncryptionManager.java:951)

at com.ibm.itim.remoteservices.ServiceProviderUtil.getPropertiesFromAttributes(ServiceProviderUtil.java:417)

at com.ibm.itim.remoteservices.ejb.mediation.ServiceProviderInfoLoader.readResourceInfo(ServiceProviderInfoLoader.java:116)

at com.ibm.itim.remoteservices.ejb.mediation.ServiceProviderInfoLoader.<init>(ServiceProviderInfoLoader.java:75)

at com.ibm.itim.remoteservices.ejb.mediation.ConnectorFactory.getConnector(ConnectorFactory.java:66)

at com.ibm.itim.workflowextensions.RemoteServicesAdapter.createAccount(RemoteServicesAdapter.java:340)

at com.ibm.itim.workflowextensions.AccountExtensions.createAccount(AccountExtensions.java:557)

... 21 more

Caused by: javax.crypto.IllegalBlockSizeException: Input length (with padding) not multiple of 16 bytes

at com.ibm.crypto.provider.AESCipher.a(Unknown Source)

at com.ibm.crypto.provider.AESCipher.engineDoFinal(Unknown Source)

at com.ibm.crypto.provider.AESCipher.engineDoFinal(Unknown Source)

at javax.crypto.Cipher.doFinal(Unknown Source)

at com.ibm.itim.util.EncryptionManager.decrypt(EncryptionManager.java:994)

... 28 more

]]></Exception>

</Trace>

Also...

- DB2 11.1 support
- Latest browser versions
 - FireFox 52.3.0 ESR
 - Chrome 61.0.3163.79

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

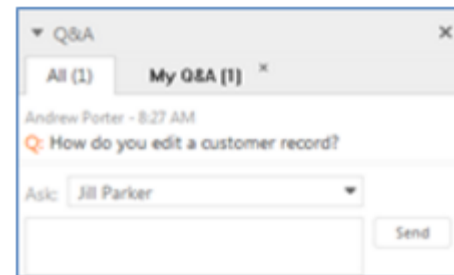
Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.

To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum:

<<https://developer.ibm.com/answers/topics/isim.html>>



IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content
published daily!



Learning at no
cost!

Learning Videos • Hands-on Labs • Live Events

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

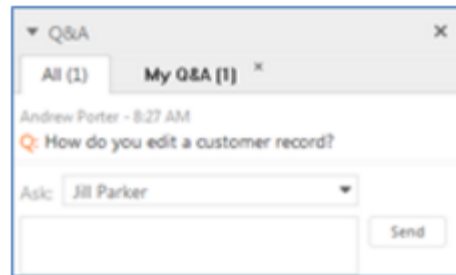
Type a question in the box below the Ask drop-down menu in the Q&A panel.

Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.

To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum:
<<https://developer.ibm.com/answers/topics/isim.html>>





THANK YOU

FOLLOW US ON:



facebook.com/IBMSecuritySupport



youtube/user/IBMSecuritySupport



[@askibmsecurity](https://twitter.com/askibmsecurity)



SecurityLearningAcademy.com



securityintelligence.com



xforce.ibmcloud.com

© Copyright IBM Corporation 2017. All rights reserved. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.