



Secure and Seamless integration of iNotes, Sametime, and Quickr with SSL and SSO

Acadia Services & Solutions, LLC



A Lotus Technical and Professional Virtual Conference

Presentation Goals

- Configure SSL on a Domino Server
- Configure SSO on a Domino Server
- Configure both SSL & SSO for seamless function of iNotes, Sametime, and Quickr
- Review gains of this configuration



A Lotus Technical and Professional Virtual Conference

Configure SSL

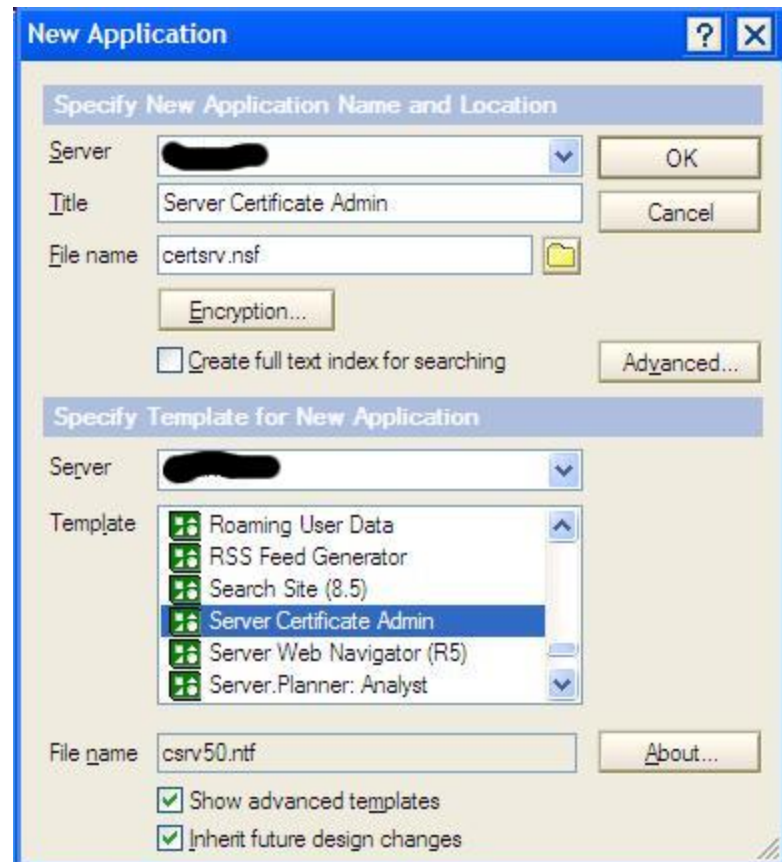
- What type of Certificate?
 - Single Domain Certificate
 - Wildcard Certificate
- What authority to use?
 - Self Cert
 - Verisign/Thwate
 - Others like GoDaddy

Configure SSL (cont'd)

- Purchase Certificate
- Create Key Ring on Domino
 - Step-by-step in CertSrv.nsf
- Submit CSR with chosen Authority
- Merge Authority Certs with Key Ring
- Add files to Domino Server
 - .kyr and .sth files in Data directory

Create Key Ring on Domino

Make sure the database exists (usually called certsrv.nsf) if not, create it



Create Key Ring (cont'd)

Open the CertServ.nsf file (once created) and select the first option



Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring

2. Create Certificate Request

3. Install Trusted Root Certificate into Key Ring

4. Install Certificate Into Key Ring

Create Key Ring (cont'd)

Enter the location of the KYR and
STH files and the password

Key Ring Information	
Key Ring File	⌈ C:\Program
Name:	Files\IBM\Lotus\Notes\Data\keyfile.kyr ⌋
Key Ring	⌈ ***** ⌋
Password:	
Confirm	⌈ ***** ⌋
Password:	

Create Key Ring (cont'd)

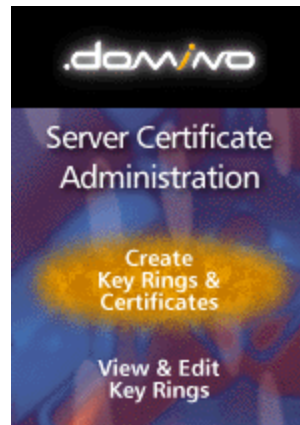
Enter the key strength and
organizational information

Key Size	
Key Size:	2048 ▼

Distinguished Name	
Common Name:	subdomain.yourcompany.com
Organization:	Your Company
Organizational Unit:	(optional)
City or Locality:	Nowhere (optional)
State or Province:	Alabama (no abbreviations)
Country:	US (two character country code)

Create Key Ring (cont'd)

Make a CSR Request from the
selected Certificate Authority



Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

Create Key Rings & Certificates

Create Key Ring (cont'd)

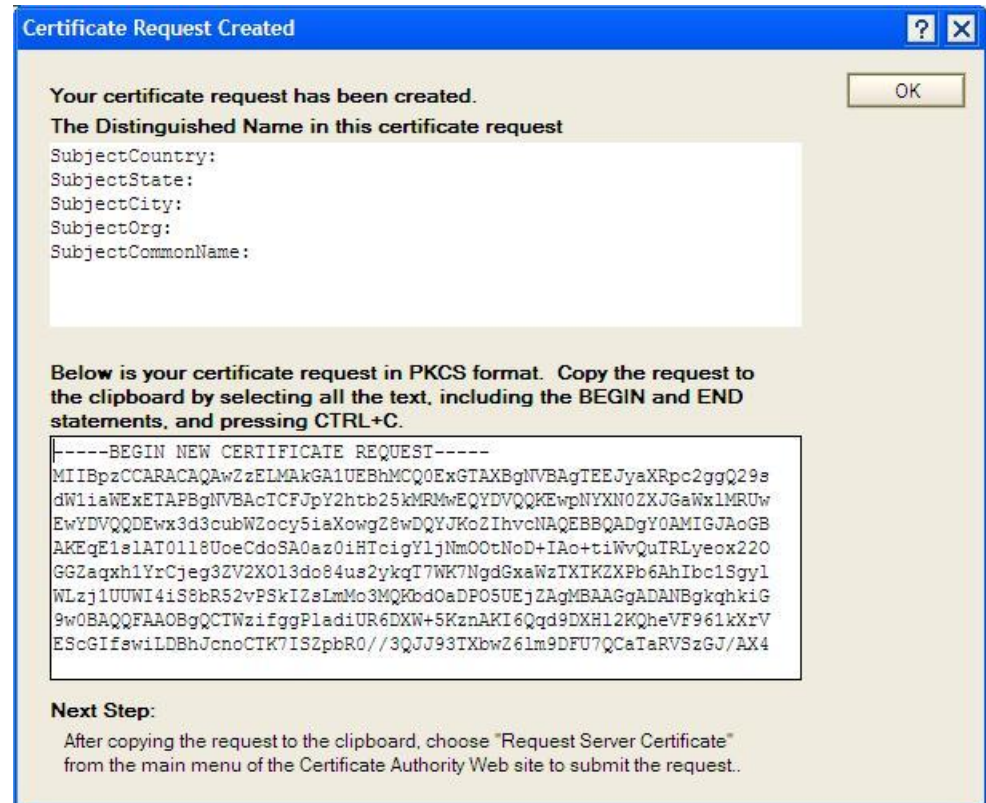
Certificate Authority CSR Request options

Key Ring Information	
Key Ring File Name	C:\Program Files\IBM\Lotus\Notes\Data\keyfile.kyr

Certificate Request Information	
Log Certificate Request	Yes
Method	☒ Paste into form on CA's site ☐ Send to CA by e-mail

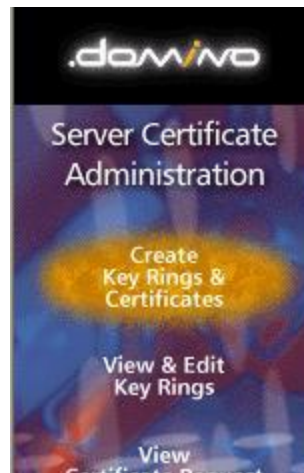
Create Key Ring (cont'd)

Key to paste to Certificate Authority



Create Key Ring (cont'd)

Merge Trusted Root Certificate(s)



Click on the steps below to create an SSL key ring and populate it with certificates.

1. [Create Key Ring](#)
2. [Create Certificate Request](#)
3. [Install Trusted Root Certificate into Key Ring](#)
4. [Install Certificate Into Key Ring](#)

Create Key Ring (cont'd)

Merge CA provided Certificates with KeyRing (may do more than once)

Key Ring Information	
Key Ring File Name	C:\Program Files\IBM\Lotus\Notes\Data\keyfile.kyr

Certificate Information	
Certificate Label	MySubdomain-SSL-CERT
Certificate Source	☒ File ☐ Clipboard
File Name	c:\certificate\authority\domain.crt
File Format	☒ Base 64 encoding ☐ Binary file format

Create Key Ring (cont'd)

Merge CA provided Server Certificate



Click on the steps below to create an SSL key ring and populate it with certificates.

1. [Create Key Ring](#)
2. [Create Certificate Request](#)
3. [Install Trusted Root Certificate into Key Ring](#)
4. [Install Certificate Into Key Ring](#)

Create Key Rings & Certificates

Create Key Ring (cont'd)

Merge CA provided Server Certificate into KeyRing

Key Ring Information	
Key Ring File Name	C:\Program Files\IBM\Lotus\Notes\Data\keyfile.kyr

Certificate Information	
Certificate Source	☒ File ☐ Clipboard
File Name	c:\certificate\authority\server.crt

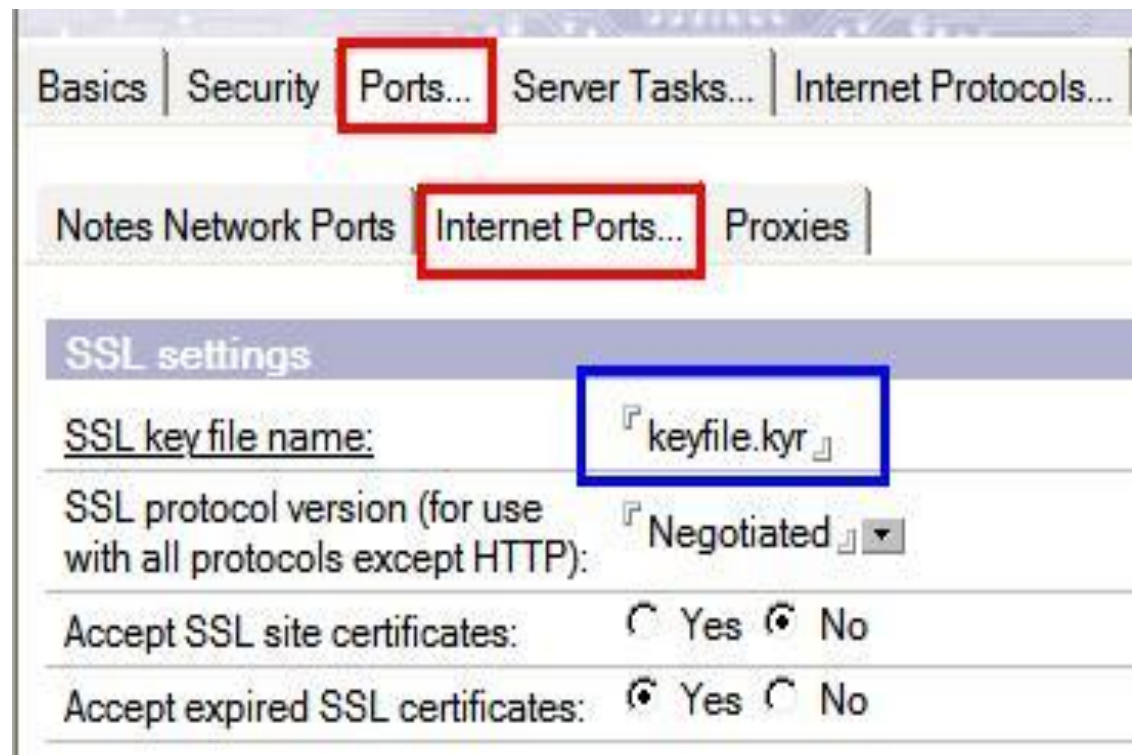
SSL on the Domino Server

- The KYR and STH Files
 - Locate KYR and STH files and copy to server's Data directory
- Server Configuration items
 - Server doc
 - Internet Site doc
 - Web Configuration doc
- Restart HTTP

SSL – Server Doc Items

Setting SSL KYR file on Server

Document – use your file name



The screenshot shows the 'Ports...' tab in the 'Security' section of the IBM Notes configuration window. The 'Internet Ports...' sub-tab is selected. Under the 'SSL settings' section, the 'SSL key file name' is set to 'keyfile.kyr'. The 'SSL protocol version' is set to 'Negotiated'. The 'Accept SSL site certificates' option is set to 'No', and the 'Accept expired SSL certificates' option is set to 'Yes'.

SSL settings	
SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	☐ Yes ☒ No
Accept expired SSL certificates:	☒ Yes ☐ No

SSL – Server Doc Items

Turn SSL on – Server Document

Web	Directory	Mail	DIIOP	Remote Debug
Web (HTTP/HTTPS)				
TCP/IP port number:	80			
TCP/IP port status:	Enabled			
Enforce server access settings:	No			
Authentication options:				
Name & password:	Yes			
Anonymous:	Yes			
SSL port number:	443			
SSL port status:	Enabled			
Authentication options:				
Client certificate:	No			
Name & password:	Yes			
Anonymous:	Yes			

SSL – Web Config Doc

Setting SSL KYR file on Web
Config Doc – use your file name



The screenshot shows the 'Security' tab of the Web Config Doc interface. The 'Security' tab is highlighted with a red box. Below it, the 'SSL key file:' field is highlighted with a blue box and contains the text 'keyfile.kyr'. The 'Redirect TCP to SSL:' dropdown is set to 'No'. The 'TCP/IP Authentication options:' section has 'Name & password:' set to 'Yes' and 'Anonymous:' set to 'Yes'. The 'SSL Authentication options:' section has 'Client certificate:' set to 'No', 'Name & password:' set to 'Yes', and 'Anonymous:' set to 'Yes'.

Security	
SSL key file:	keyfile.kyr
Redirect TCP to SSL:	No
TCP/IP Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL Authentication options:	
Client certificate:	No
Name & password:	Yes
Anonymous:	Yes

SSL – Web Config Doc

Turn SSL on – Server Document

Web	Directory	Mail	DIIOP	Remote Debug
Web (HTTP/HTTPS)				
TCP/IP port number:	80			
TCP/IP port status:	Enabled			
Enforce server access settings:	No			
Authentication options:				
Name & password:	Yes			
Anonymous:	Yes			
SSL port number:	443			
SSL port status:	Enabled			
Authentication options:				
Client certificate:	No			
Name & password:	Yes			
Anonymous:	Yes			

SSL – Internet Site Doc

Setting SSL KYR file on Internet Site Doc – use your file name

Basics | Configuration | Domino Web Engine | **Security** | Comments

TCP Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Redirect TCP to SSL: ☐ Yes ☒ No

SSL Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Client certificate: ☐ Yes ☒ No

SSL Options

Key file name:

Protocol version:

Accept SSL site certificates: ☐ Yes ☒ No

Accept expired SSL certificates: ☒ Yes ☐ No

SSL – Internet Site Doc

Turn SSL on – Server Document

Basics | Security | **Ports...** | Server Tasks... | Internet Protocols

Notes Network Ports | **Internet Ports...** | Proxies

Web | Directory | Mail | DIIOP | Remote Debug Manager

Web
(HTTP/HTTPS)

TCP/IP port number:	80
TCP/IP port status:	Enabled
Enforce server access settings:	Yes
SSL port number:	443
SSL port status:	Enabled

NOTE: This server uses Internet Site documents to configure S
Internet Site documents are located in the Servers\Int

SSL Complete

- If more than 1 server, repeat the above for each server
- Replicate Domino Directory changes to all servers
- Restart HTTP Task on each affected server to enable SSL (can wait for SSO to restart task)

SSO on the Domino Server

- Create SSO document
 - Internet Site Docs
 - Web Configuration Docs
- Server document / Web Configuration docs / Internet Site documents
- Restart HTTP Task
- iNotes database settings

SSO on the Domino Server

Creating an SSO Configuration Doc



SSO on the Domino Server

SSO Configuration Doc Settings

Basics | Comments | Administration

Token Configuration	
Configuration Name:	LtpaToken
Organization:	
DNS Domain:	yourcompany.com
Map names in LTPA tokens:	Disabled
Require SSL protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Disabled

Token Expiration	
Expiration (minutes):	600
Idle Session Timeout:	☒ Enabled
Minimum Timeout (minutes):	65

Participating Servers	
Domino Server Names:	
Windows single sign-on integration (if available):	Disabled

SSO on the Domino Server

Internet Site Docs vs. Web Config

Basics	Comments	Administration
Token Configuration		
Configuration Name:		LtpaToken
Organization:		
DNS Domain:		yourcompany.com
Map names in LTPA tokens:		Disabled
Require SSL protected communication (HTTPS):		Disabled
Restrict use of the SSO token to HTTP/HTTPS:		Disabled
Token Expiration		
Expiration (minutes):		600
Idle Session Timeout:		☒ Enabled
Minimum Timeout (minutes):		65
Participating Servers		
Domino Server Names:		
Windows single sign-on integration (if available):		Disabled

SSO on the Domino Server

Internet Site Docs vs. Web Config

Basics	Comments	Administration
Token Configuration		
Configuration Name:	LtpaToken	
Organization:	YourOrg	
DNS Domain:	yourcompany.com	
Map names in LTPA tokens:	Disabled	
Require SSL protected communication (HTTPS):	Disabled	
Restrict use of the SSO token to HTTP/HTTPS:	Disabled	
Token Expiration		
Expiration (minutes):	600	
Idle Session Timeout:	☒ Enabled	
Minimum Timeout (minutes):	65	
Participating Servers		
Domino Server Names:		
Windows single sign-on integration (if available):	Disabled	

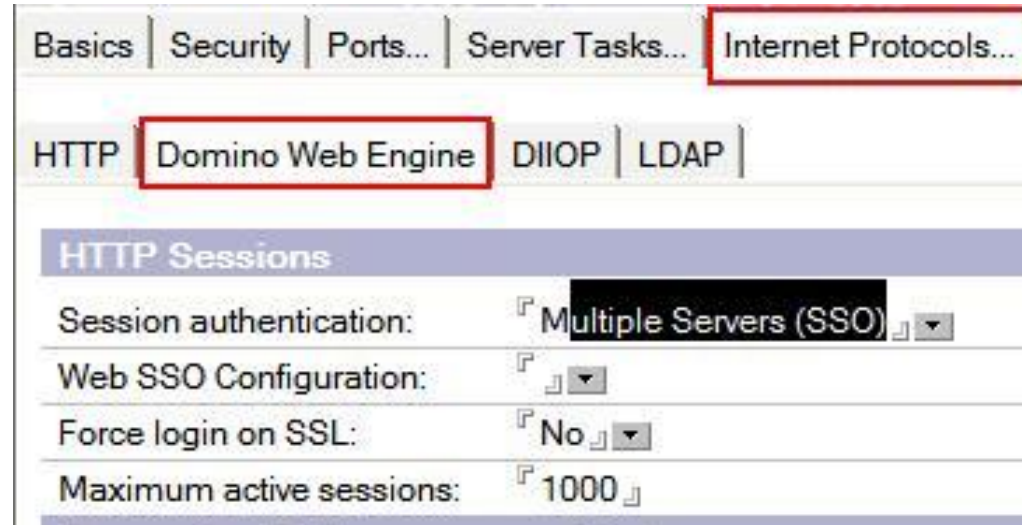
SSO on the Domino Server

Finally, create the SSO Keys



SSO on the Domino Server

Add SSO Parameters to Server



Basics | Security | Ports... | Server Tasks... | Internet Protocols...

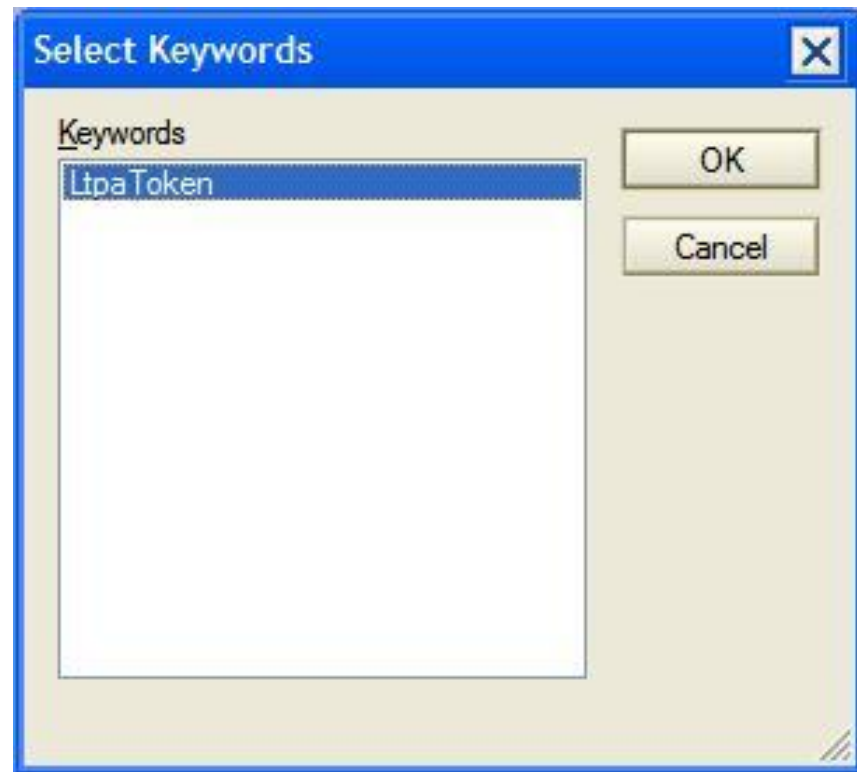
HTTP | Domino Web Engine | DIIOP | LDAP

HTTP Sessions

Session authentication:	Multiple Servers (SSO)
Web SSO Configuration:	
Force login on SSL:	No
Maximum active sessions:	1000

SSO on the Domino Server

Add SSO Token for Use



SSO on the Domino Server

Final SSO setting on Server Doc

Basics | Security | Ports... | Server Tasks... | **Internet Protocols...** | MTAs... | M

HTTP | **Domino Web Engine** | DIIOP | LDAP |

HTTP Sessions

Session authentication:	Multiple Servers (SSO)
Web SSO Configuration:	LtpaToken
Force login on SSL:	No
Maximum active sessions:	1000

SSO on the Domino Server

Add SSO to Internet Site Docs

Basics | Configuration | **Domino Web Engine** | Security | Comments

HTTP Sessions

Session authentication: ☐ Multiple Servers (SSO) ☐ Single Server

Web SSO Configuration: ☐ LtpaToken ☐ LtpaToken2

Force login on SSL: ☐ Yes ☐ No

When overriding session authentication, generate session cookie: ☐ Yes ☐ No

SSO Complete – What's next

- Replicate Domino Directory if multiple servers involved
- Restart HTTP task on all servers involved
- Make iNotes changes for integration

iNotes Settings affected

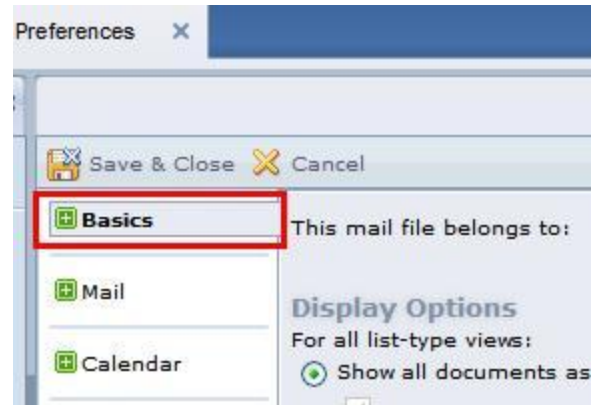
- Enable Instant Messaging
- Lotus Quickr
 - Needs Lotus Quickr Connectors installed
 - Add Places
 - Configure attach/save actions
- Seamless due to SSO

iNotes – Enable IM

- Go to Preferences

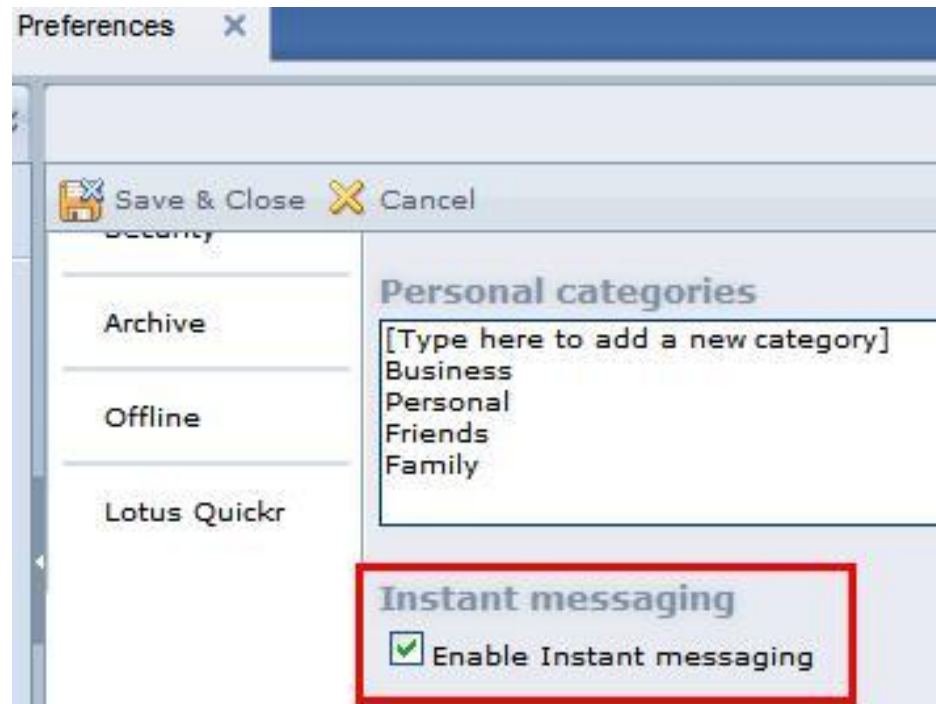


- Basic Tab



iNotes – Enable IM (cont'd)

- Select Enable Instant Messaging (from Basics tab)

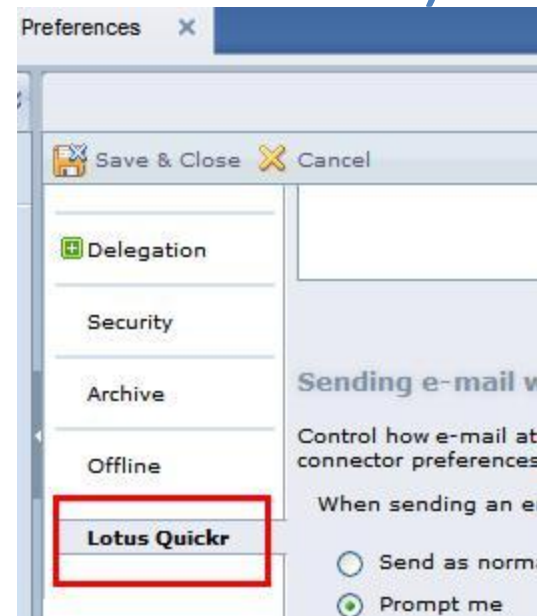


iNotes – Enable Quickr

- Go to Preferences



- Lotus Quickr Tab (requires Connectors be installed)



iNotes – Quickr Settings

- Add Places for faster access when using Quickr



iNotes – Quickr Settings

- Set how Quickr Actions should be initiated for better integration

Sending e-mail with attachments

Control how e-mail attachments are handled in Lotus iNotes, and edit connector preferences.

When sending an email with attachments:

- ☒ Send as normal (always send attached files)
- ☐ Prompt me
- ☐ Always send links (save attachments to a Lotus Quickr place default location)

Save attachments in (default location):

Browse...

Benefits / Caveats

- Accessing iNotes or Quickr, Sametime awareness is automatic
- Moving between iNotes and Quickr is seamless
- Not perfect – some issues in Quickr

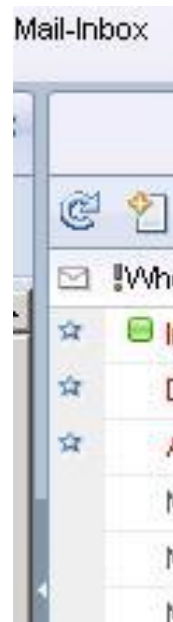
Benefits – IM Awareness

- IM login status in iNotes



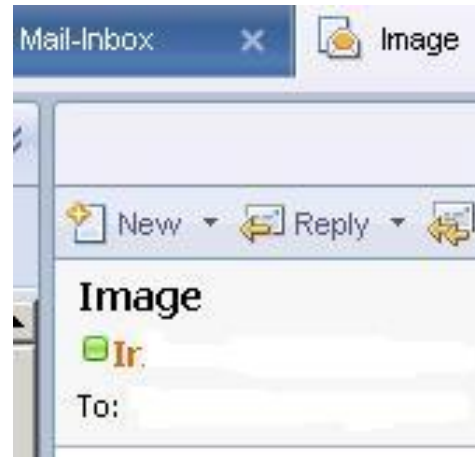
Benefits – IM Awareness

- IM Awareness in Inbox



Benefits – IM Awareness

- IM Awareness in Messages



Benefits – IM Awareness

- IM Login status and Chat initiation in Quickr



Conclusion

Questions????

Please email Mike Kinder
mkinder@acadiasolutions.com