

Agenda Key: 23FK

Session #: 570493

Going Mobile with Notes and Domino

Kim Greene

kim@kimgreene.com

507-367-2888

Skype/Twitter: iSeriesDomino

Amy Hoerle

ahoerle@kimgreene.com

507-775-2174

Skype/Twitter: iLotusDomino

Amy Hoerle - Introduction

- 1st “real” job was as an AS/400 administrator in 1997
- Worked on IBM Lotus Domino support team for 11 ½ years
- Specializing in Lotus products on IBM i & Windows since 1999
 - Installing, configuring, tuning, debugging and troubleshooting
- DAOS expert
- Xpages development
- Author of numerous technotes, articles and the “Optimizing Domino Administration” IBM Redbooks Wiki
- Blog: www.bleedyellow.com/blogs/ilotusdomino
- Twitter: [iLotusDomino](#)

Kim Greene - Introduction

- Owner of Kim Greene Consulting, Inc.
- Extensive iSeries background
- Services offered include:
 - System and application performance optimization
 - Administration
 - Upgrades
 - Troubleshooting
 - Health, performance, security, etc. checks
 - Migrations
 - Custom development
 - Enterprise integration
- Technical writer for Systems Magazine, IBM i Edition
- Blog: www.bleedyellow.com/blogs/dominodiva
- Twitter: [iSeriesDomino](#)

Agenda

- Getting started with Traveler
- Planning
- Traveler 8.5.3
- Security
- Managing Traveler
- Customizing Traveler
- When you need more than mail
 - Other applications your users may want/need

What is Lotus Notes Traveler?

- Server that provides real-time synchronization to mobile devices
 - Mail
 - Contacts
 - Calendar
 - Notebook entries (Windows Mobile & Nokia)
- Data accessed from the server
 - Company Directory
 - Secondary Directories (requires directory assistance configured on the Traveler server)

Devices supported by Lotus Traveler

Device Family	Supported Devices
Android	Android 2.x 3.x*. 4.x**
Apple	iPad iPhone (OS2 or higher) iPod (3G or higher)
Nokia	Nokia Series 60 – 3 rd and 5 th edition Symbian3
Microsoft	Windows Mobile 6.x

*Android 3.x requires Lotus Traveler 8.5.2.2 or above

**Android 4.x requires Lotus Traveler 8.5.3.2

Detailed device list: <http://www-01.ibm.com/support/docview.wss?uid=swg27022506>

Installing Traveler

- Install Domino
 - Install Domino 8.5.3 & 8.5.3 FP1
- Configure Domino Server
 - Configure Directory Assistance (if required)
 - Create required connection documents for replication
 - Configure SSL
 - Configure session authentication (Single or multi-server)
 - Test HTTP connectivity
- Install Traveler
 - Configure Traveler default device settings and/or policies

Accessing the traveler servlet from a browser



User Status (Amy Hoerle/Kim Greene Consulting)

Lotus Notes Traveler server is available.

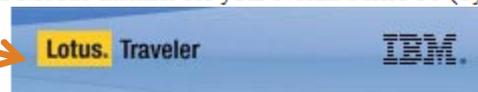
SPH-D700: Online and no sync requests from the server are pending.

Configure your Device

Your device could not be automatically identified, so you need to download IBM Lotus Mobile Installer for your Nokia Series 60 (Symbian OS), Touch/iPad device.

[Select an IBM Lotus Mobile Installer.](#)

[Generate an Apple Profile.](#)



Manage Security

Manage security for the user's devices.

Manage the Notes ID

Your Notes ID, a file that your administrator creates, allows you to encrypt, decrypt, : [Android](#)

Report a Problem

Report a problem with Lotus Notes Traveler to your server administrator.

Download IBM Lotus Mobile Installer

[Nokia Series 60 \(Symbian OS\)](#)

[Windows Mobile 6.0/6.1/6.5](#)

[Android](#)

Configuring the Device / Installing Traveler

Tip: Upgrade the firmware of the device before you start

- Installing on an Apple Device:

http://www-10.lotus.com/ldd/dominowiki.nsf/dx/Demo_Installing_Lotus_Notes_Traveler_on_Apple_devices

- Installing on an Android Device:

http://www-10.lotus.com/ldd/dominowiki.nsf/dx/Video_Installing_IBM_Lotus_Notes_Traveler_on_your_Android_device

- Installing on a Windows Mobile Device:

<http://www-10.lotus.com/ldd/dominowiki.nsf/dx/installing-lotus-notes-traveler-on-a-windows-mobile-device>

- Installing on a Nokia Device:

<http://www.youtube.com/watch?v=YQnpmZHzn5k>

Traveler 8.5.3

Apple Traveler Enhancements

- 8.5.3
 - Apple iOS partial wipe of traveler only
 - Group name and Mail-in database lookup
 - Select which applications are allowed to sync to Apple devices
 - Reply and Forward indicators from Apple devices
- 8.5.3.1 & iOS 5
 - Ability to create, rename, move and delete mail from folders
 - Requires `AS_ALLOW_DS_FOLDER_CHANGES` set to **true** in `NTSConfig.xml`
 - Follow up flags

Android Traveler Enhancements

- 8.5.3
 - Home Page widgets for mail and calendar
 - Invite, creation, quick switch days/weeks, week view hints
 - Copy/paste & send button when composing messages
 - Android OS 3.x support
 - Android OS 4.x support (8.5.3.2)
- Nokia Symbian 3 support

Upgrading to 8.5.3

- Simple to upgrade the server
 - Traveler will defrag during the process
- The 8.5.2 Traveler application on the client will be removed and replaced (data will be replaced)
 - Installer can now perform automatic updates

Company Mobile Policies

Planning A Company Mobile Policy

- What to include in a Mobile policy
 - Company devices or Bring Your Own Device (BYOD)
 - Agree to secure devices
 - Agree to remote wipe
 - Anti-virus



Example Mobile Policy

1. Purpose

The purpose of this policy is to help you understand how mobile devices should be used at XYZ. It applies to:

- Laptops;
- Tablets (e.g. iPads);
- Mobile/cellular phones;
- PDAs;
- Any other mobile device capable of storing corporate data. We'll refer to these devices as "mobile devices." This policy applies to any mobile device connected to the XYZ network, whether it's owned by XYZ or the employee. The goal of this policy is to protect XYZ's data, and to set out our expectations of employees who access that data from mobile devices.

2. Relation to Other Policies

This document is not intended to replace the Electronic Media Systems policy or the Overtime policy. We have just put everything relating to the use of mobile devices together into this one handy document.

3. Access

Before you can access XYZ data on your mobile device, you need to register it with the IT Department. If you do anything that puts XYZ data at risk, the IT Department may turn off your access to the network without notice.

Example Mobile Policy

4. Security

The IT department sets standards for passwords, encryption and other security measures. You must agree to abide by these standards in order to access corporate data from your device. Any jailbroken device needs special permission in writing from the head of the employee's region to be allowed to access the XYZ network..

5. Loss or Theft of Mobile Devices

If your mobile device is lost or stolen, you must immediately tell your manager as well as your local IT manager. IT staff will remotely wipe the data on the mobile device as soon as possible and within 8 hours at the most. If you bring a personal mobile device to the office or on a business trip, XYZ is not liable if you lose it or if it is damaged or stolen.

6. Loss of Data

If your mobile device is lost or stolen and data is wiped, XYZ can't guarantee to preserve your personal data such as photographs, music, address book contacts or applications that you have downloaded. XYZ is not responsible for backing up your personal data. It is your responsibility to back up any personal data on your mobile device.

Example Mobile Policy

7. Reimbursement

Because of the nature of their work, certain employees are entitled to reimbursement of specified fees for their personal mobile devices. For those employees, XYZ will reimburse them as follows:

Purchase of a mobile device (Android, iPhone or Blackberry smartphones or iPad tablets):

NALA: 50% of the cost of the device, up to a maximum purchase price of \$1,000

EMEA: 50% of the cost of the device, up to a maximum purchase price of 1,000 euros

APAC: 50% of the cost of the device, up to a maximum purchase price of JPY100,000

Monthly voice/data charges:

All Regions: 50% of the monthly voice tariff fixed cost and 50% of the monthly data tariff fixed cost, or 50% of a combined voice + data tariff fixed cost In addition, XYZ will reimburse 100% of any qualifying business-related charges that are additional to the fixed monthly cost (these need to be separately identified from fixed costs in your expenses claim). Qualifying charges include:

- Business-related international roaming mobile calls (please use Skype over WiFi though, if it's convenient and if you can get good enough quality, it's cheaper)

Example Mobile Policy

- Business-related normal international mobile calls (please use Skype over WiFi though, if you can, it's cheaper)
- 50% of data roaming charges (please use public or private WiFi in preference to data roaming, if you can find it, it's a LOT cheaper!) Qualifying charges don't include:
 - Premium rate numbers
 - Premium SMS services
 - Personal international calls

The maximum number of devices per employee (e.g. Android phone + iPad) will be determined by your manager based on your job role. Reimbursement for these charges must be approved in advance by your manager and, for recurring charges, must be submitted on a monthly basis using XYZ's expense reimbursement procedures. XYZ may change these reimbursement amounts at any time.

The mobile devices covered by this reimbursement policy are and remain your personal property. XYZ carries no responsibility for repairing or replacing these devices if lost, damaged or stolen at any time. If you leave the company for any reason, XYZ's obligation to reimburse you as specified above will end on the last day of your employment. If you leave in the middle of a month, you will be paid pro-rata for that month up until the day you leave. If you leave the company within 3 months of purchasing and being reimbursed for a new device, then you agree to repay XYZ the full amount of the reimbursement. If you leave the company, XYZ Company will remove all company data from the device. Out-of-hours contact information for local IT managers is available in the XYZ Phone Directory.

Security

Security Considerations

- Network location of Traveler server
 - In DMZ
 - Require VPN Access?
- Will device access be via HTTP or HTTPS (SSL)
- Is this Domino server available from the Internet?
 - Don't let changes to names.nsf replicate into the environment
 - Which databases can anonymous access?

Lotus Mobile Connect

- VPN solution for mobile devices
- Supported across networks so application is not interrupted when switching networks (for example, WiFi to 3G)
- Integrates with Traveler
- For more details:

<http://www.ibm.com/software/lotus/products/mobileconnect/>

SSL

- It is strongly recommended to use SSL when implementing your Traveler server
 - Just want to pilot Traveler? Use a self-signed certificate
- What if you change your mind?
 - User must manually update the configuration on their device

Traveler Server Security

- Can anyone register a device on the server?
- How many devices is each user allowed to use?
- What to know about device and data security
- Will passwords be required on the device?

Device Security Capabilities at 8.5.3

	Apple iOS 3.x and higher	Android 2.0.1 and higher	Nokia Symbian	Windows Mobile 6.x
Connect via HTTPS	Yes	Yes	Yes	Yes
Read/Compose encrypted mail	Yes with Traveler Companion	Yes	Yes	Yes
Remote Wipe (Full or Traveler only)	Yes	Yes	Yes	Yes
Data stored encrypted on device	Yes	Yes	Yes	No
Allow/deny access based on password	Yes	Yes	Yes	Yes

Restricting access to Traveler

- Ways to restrict access
 - By user
 - By requiring approval for each device accessing traveler
 - By device type

Server: AmyKGCI/akh

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail | DAOS | Lotus Traveler

Basics	
Maximum Memory Size:	1024 MB
IPC Socket Ports:	50125 50126
External Server URL:	http://AmyKGCI/servlet/traveler
Lotus Traveler Access	
Access server:	All users can access this server
Not access server:	
Remote user commands:	Disabled
User managed security:	Enabled

Setting Default Device Settings:

- Open Domino Administrator
- Messaging → Mail Tab
- IBM Lotus Traveler → Device Settings

Note: Only 1 default document for the Traveler server

Basics | Preferences | Assignment

Sync | Filter Settings | Device Settings | Security Settings

Windows Mobile | Nokia | Apple | Android

Device Security	Violation Action
<input type="checkbox"/> Require device password	Report
<input type="checkbox"/> Storage card encryption	Report
<input type="checkbox"/> Prohibit devices incapable of security enablement	Enforce

Lotus Traveler Device Settings : Default

Basics | Preferences | Assignment

Sync | Filter Settings | Device Settings | Security Settings

Mail Filters:

Email Body Truncation: Enabled KB

Maximum Email Attachment Size Allowed - Administrator KB

Email Attachments: Enabled

Email Attachment Size: KB

Email Date Filter: Enabled

Email Importance: High Importance Only

Other Filters

Calendar Date Filter:

Past Events: Enabled

Future Events: Enabled

Journal Date Filter: Enabled

ToDo Status: Incomplete Status Only

Approving Devices

- Force device approval in the Device settings document

Lotus Traveler Device Settings : Default

Basics | **Preferences** | Assignment

Sync | Filter Settings | Device Settings | Security Settings | **Device Access**

Restrict Device Access

Require approval for device access

Number of devices to allow per user before approval is required: 0

Optional: Addresses to notify when approval action is pending: Domino Admin/akh@akh

- Approve Devices in the Traveler Database

Deny Access	Wipe Device	Clear Wipe / Allow Access	Change Approval	Update SMS Address		
Device Name	User	Approval	Security Policy	Access	Wipe Options	
Domino Admin/akh						
Apple-iPod4C1	Domino Admin/akh	Approved	No policy	Allow	None	
iPod touch	Domino Admin/akh	Approved	No policy	Allow	None	

The Approval Process

- User connects to Traveler web page to configure profile or install Traveler application
- After install mail messages are sent to:
 - The user notifying them a device is waiting to be approved
 - The administrator notifying them a device is pending approval
- The Administrator then approves the device
- The User receives an e-mail that the device has been approved
- Data begins to sync to the device

The Approval Process - Example

User Domino Admin/akh has registered the following device with the Lotus Notes Traveler server AmyKGCI/akh.

The device will be unable to sync data until approved by a Lotus Notes Traveler Administrator.

Device access can be approved or denied in the Lotus Traveler administration database. 

User ID	Domino Admin/akh
Server	AmyKGCI/akh
Device ID	CIKNTD-136E7083E89-I-099FB479-F26F-48E7-9A8B-FC94A89145B6
Device Name	Cikado - NotesF1 To Do Free 1.5.2 (Apple-iPhone 5.1)
Device Type	Cikado - NotesF1 To Do Free 1.5.2 (Apple-iPhone 5.1) (OS 3)

Lotus Notes Traveler product documentation:

<http://www.lotus.com/idd/dominowiki.nsf/xpViewCategories.xsp?lookupName=Product%20Documentation>

Message auto sent by the Lotus Notes Traveler server AmyKGCI/akh.

The Approval Process - Example



Device access approved for Domino Admin/akh on Lotus Notes Traveler server AmyKGCI/akh.
Domino Admin to: Domino Admin

Device access has been approved by a System Administrator.

The following device will now be able to sync with the Lotus Traveler server AmyKGCI/akh.

User ID	Domino Admin/akh
Server	AmyKGCI/akh
Device ID	CIKNTD-136E7083E89-I-099FB479-F26F-48E7-9A8B-FC94A89145B6
Device Name	iPod touch
Device Type	iphone/5.1
Client Level	8.5.2.1.201011181900

Lotus Notes Traveler product documentation:

<http://www.lotus.com/ldd/dominowiki.nsf/xpViewCategories.xsp?lookupName=Product%20Documentation>

Message auto sent by the Lotus Notes Traveler server AmyKGCI/akh.

Restricting Device Types by Customizing NTSConfig.xml

- **AS_PROTOCOL_VERSIONS:** specifies the ActiveSync Protocol versions that the server supports (choices are 2.5, 12.0, 12.1).
 - For example, to prohibit Apple 2.x devices specify :
`<PROPERTY NAME="AS_PROTOCOL_VERSIONS" VALUE="12.0,12.1"/>`
- **AS_PROVISION_EXEMPT_USER_AGENT_REGEX:** devices that are exempt from using the ActiveSync Provision command
 - Provision command required to enforce security and allow remote wipe (Default is that none are exempt)
- **ALLOWED_USER_AGENT_REGEX:** The User-Agent HTTP headers that are allowed to sync data
 - For example, to allow only Apple and Android specify:
`<PROPERTY NAME="ALLOWED_USER_AGENT_REGEX" VALUE="(Lotus Traveler Android)|(Apple)"/>`

Traveler device settings & policies

- Use to override the defaults
 - Executive team does not need to go through device approval?
- Settings you may want to enable
 - Attachment synchronization
 - Increasing the Email Body Truncation size
- Settings you may not want to enable
 - Wiping the device after X incorrect password attempts
 - Email Importance

Example Traveler Settings Document

Lotus Traveler Settings

Basics | Preferences | Comments | Administration

Sync | Filter Settings | Device Settings | Security Settings | Device Access

Mail Filters:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies
Email Body Truncation:	<input checked="" type="checkbox"/> Enabled [100K]	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Maximum Email Attachment Size Allowed - Administrator	[4000] KB	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Email Attachments:	<input checked="" type="checkbox"/> Enabled	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Email Attachment Size:	[100] KB	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Email Date Filter:	<input checked="" type="checkbox"/> Enabled [1 Week]	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Email Importance:	<input type="checkbox"/> High Importance Only	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Other Filters		How to apply this setting:	Inherit from parent policy:	Enforce in child policies
Calendar Date Filter:				
Past Events:	<input checked="" type="checkbox"/> Enabled [1 Week]	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Future Events:	<input checked="" type="checkbox"/> Enabled [3 Months]	Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Policy Settings vs. Device Settings

- The device settings will be used unless they will violate a server setting
- Example:
 - Device sets the *Date filter* for mail to 1 month
 - Server sets the *Date filter* for mail to 1 week

Winner: The Server with 1 week

Removing Data from the Device

- Being able to remove data or “wipe” a device is critical
 - Lost or stolen device
 - Employee resignation or termination
- Wipe options
 - Full or Traveler only (requires 8.5.3 for some devices)
 - User or server initiated

Lotus Traveler Access	
Access server:	All users can access this server
Not access server:	
Remote user commands:	Disabled
User managed security:	Enabled

User can only initiate a wipe if enabled in the server document, Traveler tab

User Initiated Wipe

<https://mytravelerserver.com/servlet/traveler>



User Status for Amy Hoerle/Kim Greene Consulting

Lotus Notes Traveler server is available.

Apple-iPod4C1: Online and no sync requests from the server are pending.

Samsung SPH-D700: Online and no sync requests from the server are pending.

Configure your Device

Your device could not be automatically identified, so you need to download IBM Lotus Mobile Installer or IBM Lotus Notes Traveler

[Download IBM Lotus Notes Traveler for Android.](#)

[Download IBM Lotus Mobile Installer for Nokia Symbian^3/Series 60.](#)

[Download IBM Lotus Mobile Installer for Windows Mobile 6.0/6.1/6.5.](#)

[Generate an Apple Profile.](#)

Manage Security

Manage security for the user's devices.

Manage Security for Amy Hoerle/Kim Greene Consulting

Device: Apple-iPod4C1 which has Device ID ApplC3LH1K9HDNQW

Status

No security actions are pending.

Request Security Action

[Wipe Device](#) - Resets the device to the factory default state by erasing everything on the device and prevents the device from synchronizing with the server.

[Wipe Application](#) - Erases all Lotus Notes Traveler client software and data on the device and prevents the device from synchronizing with the server.

[Deny Access](#) - Prevents the device from synchronizing with the server.

Device: Samsung SPH-D700 which has Device ID Android_57a7a27d46bdaf84

Status

No security actions are pending.

Request Security Action

[Wipe Device and Storage Card](#) - Resets the device to the factory default state by erasing everything on the device, erases everything on the storage card, and prevents the device from synchronizing with the server.

[Wipe Application and Storage Card](#) - Erases all Lotus Notes Traveler client software and data on the device, erases everything on the storage card, and prevents the device from synchronizing with the server.

[Wipe Device](#) - Resets the device to the factory default state by erasing everything on the device and prevents the device from synchronizing with the server.

[Wipe Application](#) - Erases all Lotus Notes Traveler client software and data on the device and prevents the device from synchronizing with the server.

[Wipe Storage Card](#) - Erases everything on the storage card and prevents the device from synchronizing with the server.

[Deny Access](#) - Prevents the device from synchronizing with the server.

Administrator Initiated Wipe

Domino Administrator, Messaging -> Mail tab
IBM Lotus Notes Traveler -> Device Security

The screenshot shows the Domino Administrator interface with a 'Select wipe device options' dialog box open. The dialog box contains the following text and options:

Select wipe device options

Select one or more options for this request.

- Hard reset device (selected)
- Lotus Traveler application and data

Buttons: OK, Cancel

In the background, the 'Wipe Device' button is highlighted, and a red arrow points from it to the dialog box. Below the dialog box, a table lists devices and their security settings:

Device Name	User	Policy	Access	Wipe
Domino Admin/akh				
Apple-iPod4C1	Domino Admin/akh	Approved	No policy	Allow
iPod touch	Domino Admin/akh	Approved	No policy	Allow

Sending/Receiving Encrypted Mail

- Sending and receiving encrypted mail can be done just as it is today on the Notes client!
 - Can be done within the mail application on Android
 - Requires Traveler Companion app on Apple devices
- Requires the Notes.id be imported into the user's mail file
 - Can be pulled from the ID Vault
 - Be aware the vault download settings
 - Failed to authenticate with server AmyKGCI/akh: This server does not have the vault. A referral was returned.
 - Server domserver1/akh reported the following problem causing authentication to fail: ID in vault has download count of zero

Traveler Companion



- Requires Server Configuration Update
 - Edit NTSConfig.xml on the Traveler server

and add the following into the TrueSyncServer section

```
<PROPERTY NAME="TSS_APPLE_ENCRYPT_ENABLED" VALUE="true"/>
```

- Ensure the external host URL is entered correctly in the Traveler server document

<https://mytravelerserver.mycompany.com/servlet/traveler>

- Restart the Traveler server



- Users must manually update their passwords on the device
- How can you minimize the pain for your users?

Managing Passwords

- Synchronize Notes.id password with internet password via a security policy

Basics	Password Management	Execution Control List	Keys and Certificates	S
	Password Management Basics	Custom Password Policy	Notes Shared Login	

Password Management Options	
Use Custom Password Policy for Notes Clients	Yes
Check password on Notes id file	Yes
Allow Users to Change Internet Password over HTTP	Yes
Update Internet Password When Notes Client Password Changes	Yes

Managing Passwords

- Use ID Vault to synchronize the password for the notes.id stored in the mail file

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | **ID Vault**

ID Vault Options:		How to apply this setting:
Assigned vault:	akhVault	<input type="checkbox"/> Don't set value
Forgotten password help text:	Please contact the helpdesk at 555-HELP for password assistance	<input type="checkbox"/> Don't set value
Enforce password change after password has been reset:	Yes	<input type="checkbox"/> Don't set value
Allow Notes-based programs to use the Notes ID Vault:	Yes	<input type="checkbox"/> Don't set value

Attachment security

- Do you want to allow users to download encrypted attachments to the device where they may no longer be encrypted?
- If not, disable with the notes.ini setting:
TS_COMPANION_POLICY= noexport
- Encryption of attachments or mail data in the Traveler application
 - Refer to the device settings policy document
 - Always encrypted by Android, optionally encrypted on other devices

Remote User Commands

- What does it give you?

User Commands for Domino Admin/akh

Show - Display all the information for a user and the user's devices

Dump - Dump the information for a user to a file on the server

Device Commands

Device: Apple-iPod4C1 which has Device ID ApplC3LH1K9HDNQW

Delete - Delete the Lotus Traveler data for the device

Reset - Force a sync reset for the device

Stop Sync - Stops any active syncs for the device

- Optionally enabled via the Server document
 - Recommended to leave this setting disabled

Managing Traveler

Traveler Releases

- Staying current is important!
 - New devices, new features..
- 8.5.2 – Released August 2010
 - 8.5.2.1 – December 2010, support for Android 2.0.1+
 - 8.5.2.2 – March 2011, support for Android 3.0
 - 8.5.2.3 – June 2011, support for iOS partial wipe
 - 8.5.2.4 – October 2011, database defrag support
- 8.5.3 – Released October 2011
 - 8.5.3.1 – November 2011, support for iOS5
 - 8.5.3.2 – February 2012, support for Android 4.0

Synchronizing Contacts

- Make sure the user's contacts get to their device (before they call you!)

The screenshot shows the 'Desktop Settings' window with the 'Basics' tab selected. The 'Contacts' section is expanded, showing two settings: 'Enable "Synchronize Contacts" on the Replicator:' with a checked 'Yes' radio button and a dropdown menu set to 'Set value and prevent changes'; and 'Do not automatically add names to the Recent Contacts view:' with a 'No' radio button selected and a dropdown menu set to 'Don't set value'.

Desktop Settings	
Basics Smart Upgrade Applications Widgets Dial-up Connections Accounts Name Servers SSL Applet Sec	
Basics	
Name:	<input type="text"/>
Description:	<input type="text"/>
Homepage/Welcome Page Options	
How to apply this setting: Inherit from parent pol	
Contacts	
How to apply this setting:	
Enable "Synchronize Contacts" on the Replicator:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="text" value="Set value and prevent changes"/>
Do not automatically add names to the Recent Contacts view:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="text" value="Don't set value"/>

Basic Traveler Commands

- Invoking Traveler command help
tell traveler help
- Starting the Traveler server
load traveler
- Stopping the Lotus Traveler server
tell traveler shutdown
 - Waits for any pending syncs to complete**tell traveler quit**
 - Ends immediately
- Restarting the Traveler server
restart task traveler

Basic Traveler Commands

- View information for a specific user
tell traveler show firstname lastname
- Display users currently synchronizing with the server
tell traveler showActive
- Show number and list of registered users
tell traveler showUsers
- Show Lotus Traveler server statistics
tell traveler stat show
- Display status of all users and devices
tell traveler security allstatus

Example

tell traveler show HTC Thunderbolt

Lotus Traveler has validated that it can access the database mail/hthunder.nsf.

Encrypting, decrypting and signing messages are enabled because the Notes ID is in the mail file or the ID vault.

Canonical Name: CN=HTC Thunderbolt/O=KGCI

Internet Address: HThunderbolt@kimgreene.com

Mail Server (Home): CN=Mail1/O=KGCI

Mail File (Home): mail/hthunder.nsf

Mail Server (Current): CN=Mail1/O=KGCI Release 8.5.2FP1

Mail File (Current): mail/hthunder.nsf

Mail File Replicas: [CN=Mail1/O=KGCI, mail/hthunder.nsf]

Notes ID: Mail File does not contain the Notes ID.

Auto Sync User State: Online

Last Prime Synchronization: Wednesday, August 17, 2011 1:55:58 PM EDT

Banned Documents: 0

Devices:

Device ID: Android_d3d8f5322bd41ab8

Device Description: DROID X2:2.3.3:1.0.0.1

Removing a Traveler User

- Deleting a Traveler user
 - tell traveler delete * username**
 - tell traveler security delete * username**

Lotus Traveler	User Name ◇	User State ◇	Mail Server ◇	Mail File
Device Security	Apple iPad/	Online		mail/airpad.nsf
Device Settings	htc droid/	Offline		mail/hdroid.nsf
Devices	HTC Thunderbolt/	Online		MAIL/hthunder.nsf
Users		Online		mail/

- **Note:** Do not delete documents directly from the traveler database (LotusTraveler.nsf).
- **Note:** Users automatically removed after 30 days without a sync request.

Data Usage (new for 8.5.3.2)

Remote console command issued by Amy Hoerle/Kim Greene Consulting: tell traveler dbusage

tell traveler dbusage

Lotus Traveler Database Statistics

Accounts : 1

Devices : 2

Device documents: 94

Domino documents: 48

Highest Total Usage	Documents	Percentage
Domino Admin/akh	48	100.00

Domino Admin/akh	48	100.00
------------------	----	--------

Mail documents: 40

Highest Mail usage	Documents	Percentage	EMail filter
Domino Admin/akh	40	100.00	unlimited

Domino Admin/akh	40	100.00	unlimited
------------------	----	--------	-----------

Calendar documents: 0

Contacts documents: 0

To Do documents: 2

Highest To Do usage	Documents	Percentage	Task filter
Domino Admin/akh	2	100.00	incomplete only

Domino Admin/akh	2	100.00	incomplete only
------------------	---	--------	-----------------

Notebook documents: 0

Folder documents: 4

Highest Folder usage	Documents	Percentage	Folder filter
Domino Admin/akh	4	100.00	unlimited

Domino Admin/akh	4	100.00	unlimited
------------------	---	--------	-----------

Command DbUsage complete.

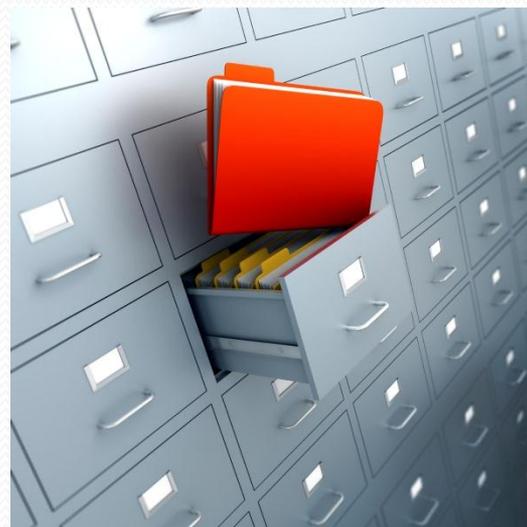
Traveler Performance

- Memory
 - NSF_BUFFER_POOL_SIZE_MB=256
- Threads
 - HTTP threads = # of devices X 1.2
- Authentication
 - Enable session authentication
 - Prevents authentication for every device to server communication
 - Could cause install problems on the device

www-10.lotus.com/ldd/dominowiki.nsf/dx/Lotus_Notes_Traveler_and_Domino_Session_Authentication
www-10.lotus.com/ldd/dominowiki.nsf/dx/Tuning_performance_of_the_server_LNT8521

Derby Database Defrag

- Over time Traveler performance can deteriorate
 - Defrag the Derby database to restore performance
- Steps to start a Defrag:
 - Tell traveler shutdown
 - Tell http quit
 - Load traveler -defrag



Traveler Defrag Enhancement

- Requires Traveler 8.5.2.4 or 8.5.3.1
- New Notes.ini parameters
 - **NTS_DEFRAG_INTERVAL_DAYS=<# of days>**
 - **NTS_LAST_DEFRAG=<timestamp of last defrag>**
- Defrag will automatically run if NTF_LAST_DEFRAG doesn't exist or if the # days past the last run is greater than the defined interval
- Defrag a minimum of every 30 days for optimal traveler server performance

Multiple Traveler Servers?

- Be aware of the Map databases
 - Always created with the same replica ID
- Why do you care?
 - Mapping databases are used to customize mapping for contacts
 - Useful for custom user directories
 - Pick the correct field (For example: email instead of MailAddress)

<http://www-10.lotus.com/ldd/dominowiki.nsf/dx/o8252009121253PMWEBM24.htm>

Troubleshooting

- Oops while trying to modify Traveler configuration?
 - Rename NTSConfig.xml
 - Restart server and a new file will be automatically created
- Need to send data to IBM?
 - tell traveler pmr <pmr_number> [log file list]
 - performs a systemdump
 - collects the requested log files into an archive
 - uploads them to IBM support

Customizing Traveler

Corporate Lookup Options

- Finding contacts from Domino Directory or other secondary directories (configured via Directory assistance)
- Note: The lookup application is not automatically used by the phone for caller id purposes when phone rings
 - This is a limitation of the mobile OS
 - Only local contacts are searched

Corporate Lookup Customizations

- Where should lookups be done
 - Prior to 8.5.3 it was always the Traveler server
 - At 8.5.3, lookups are performed on the user's mail server
 - Revert back to Traveler with Notes.ini setting of
 - **NTS_TRAVELER_AS_LOOKUP_SERVER=true**
- Lookup should be done as who?
 - By default will be completed as the server
 - If restricting access to some directories, switch to user based lookups with Notes.ini setting of
 - **NTS_LOOKUP_ENFORCE_ACL=1**

Folder Management for iOS devices!

- Create, rename, move and delete folders!!
- Not enabled by default
 - New to 8.5.3.1
- Modify TrueSyncServer section of NTSSConfig.xml
 - `AS_ALLOW_DS_FOLDER_CHANGES = true`
- ****Only works when the device is on-line (No off-line support for folder operations)**

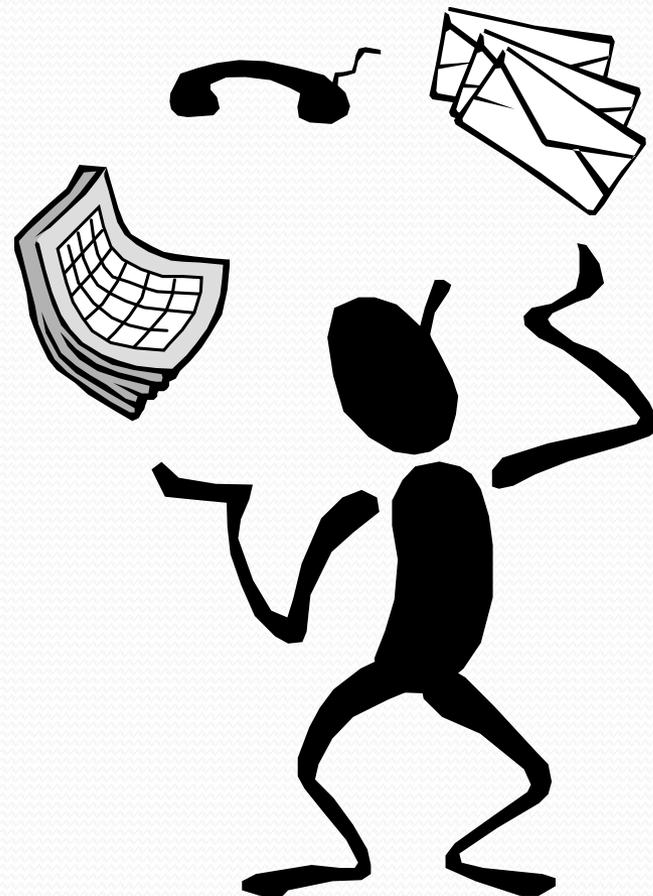
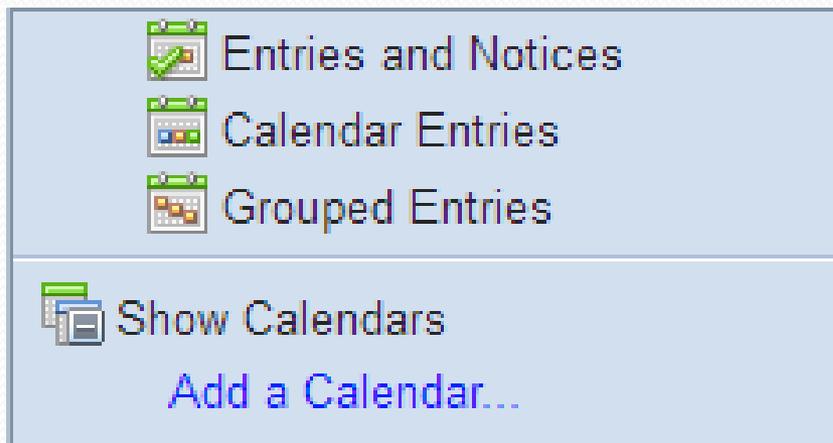
Anti-virus / Outbox

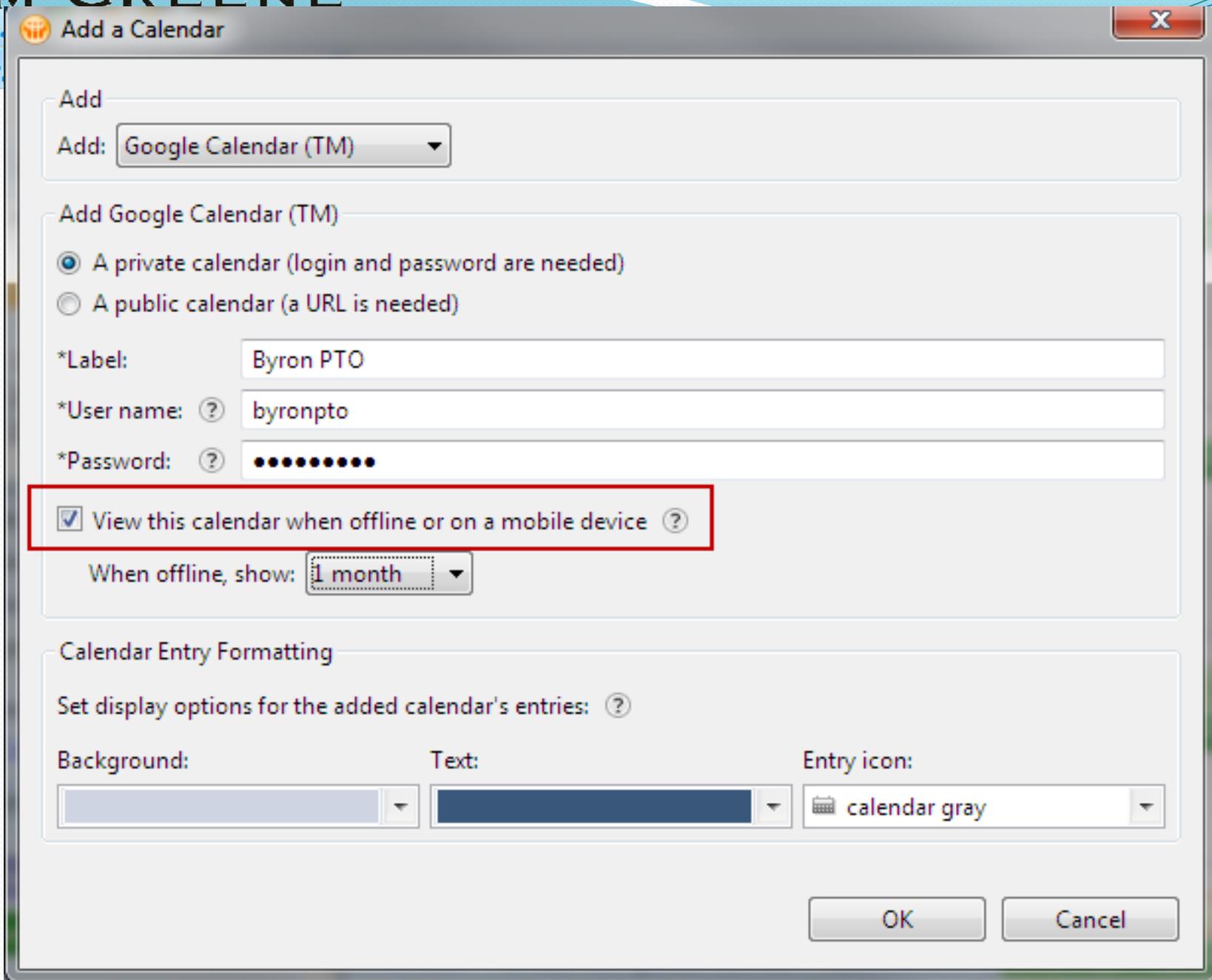
- Do all outbound emails need to be delivered to a gateway server?
- Do you need to run anti-virus on all outbound mail?
- Force traveler to send mail to a specific gateway or anti-virus server rather than directly to the mail server
 - TrueSyncServer section of NTSConfig.xml
 - OUTBOX_MAIL_SERVERS
 - Value = server1/akh, server2/akh

**When you need
More than Mail**

What's on your calendar?

- Personal calendar, work calendar, sports calendar, ...
- Bring them together and optionally on your device!



A screenshot of a Windows-style dialog box titled "Add a Calendar". The dialog has a close button (X) in the top right corner. It is divided into several sections: "Add", "Add Google Calendar (TM)", "Calendar Entry Formatting", and "When offline, show:". The "Add" section contains a dropdown menu set to "Google Calendar (TM)". The "Add Google Calendar (TM)" section has two radio buttons: "A private calendar (login and password are needed)" which is selected, and "A public calendar (a URL is needed)". Below these are three text input fields: "*Label:" with "Byron PTO", "*User name:" with "byronpto", and "*Password:" with a masked password of ten dots. A checkbox labeled "View this calendar when offline or on a mobile device" is checked and highlighted with a red rectangle. Below the checkbox is a dropdown menu for "When offline, show:" set to "1 month". The "Calendar Entry Formatting" section has a label "Set display options for the added calendar's entries:" followed by three dropdown menus: "Background:" (light blue), "Text:" (dark blue), and "Entry icon:" (calendar icon and "calendar gray"). At the bottom right are "OK" and "Cancel" buttons.

Add a Calendar

Add

Add: Google Calendar (TM)

Add Google Calendar (TM)

A private calendar (login and password are needed)

A public calendar (a URL is needed)

*Label: Byron PTO

*User name: ? byronpto

*Password: ? ●●●●●●●●●●

View this calendar when offline or on a mobile device ?

When offline, show: 1 month

Calendar Entry Formatting

Set display options for the added calendar's entries: ?

Background: Text: Entry icon:

calendar gray

OK Cancel

To Dos

- Not available yet for Apple or Android devices
- 3rd Party option available
 - NotesF1 To Do
 - Apple and Android devices
- Free and Paid versions available



Journal/Notebook synchronization

- No option for Android Devices
- Notebook app for Apple Devices
 - \$5.99, product by YouAtNotes
- Synchronizes Journal entries to the device
 - Journal must be available on the server!



Out of Office

- Out of Office functionality currently not supported with Traveler
- 3rd party option available for iPhone
 - <http://www.extracomm.com/TravelerOOO>
- Requires server side component which you must purchase
 - Also provides Out of Office management to the browser
 - Allows other users to enable Out of Office for another employee



Dealing with Notes document links

- Document links do not work with Traveler and are stripped out by the Traveler server
- Can optionally be sent to the device with the notes.ini:
 - `DominoHTMLOptions=OfferNotesURLInLink=1`
- iDocLink app provides a way to map a Domino server name to a hostname
 - Will allow access to documents for any web enabled Domino application
 - \$2.99 to purchase in the App Store
 - Not available for Android devices



Offline access to Notes Applications

- XPages applications can be replicated to a mobile device using Team Studio's Unplugged
 - Unplugged server is a chargeable feature
 - Not all XPages controls are supported
 - Still need an application that is suitable for a mobile device
 - Cannot be used with iDocLink
 - Supported on Blackberry, Apple and Android devices



Allowing other apps to connect to Traveler

- If its out there, a user will find it!!
- Can the app connect?
 - ALLOWED_USER_AGENT_REGEX in NTSCConfig.xml allows the user agent
 - If you approve the device for that application when requiring approval for device access
 - Each application is different
 - May not specify a different user agent or device id
 - May access Traveler without you as the admin aware!

Managing your Mobile Devices

- Are there standard applications you want to deploy?
- Are there applications you need to prohibit?
- You need Mobile Device Management (MDM)
 - Air Watch
 - IBM Endpoint Manager
 - Mobile Iron



Questions

Thank you for attending



Please fill out your session evaluations.

Appendix

Detailed steps to install Traveler
in your Domino Domain

Server Requirements

- Domino Server (32 or 64 bit) running on
 - Windows 2003 or 2008
 - Red Hat Linux
 - SUSE Linux
- Minimum additional hardware requirements
 - 500MB Disk
 - 512MB RAM

Server Requirements

- Network connectivity
 - DMZ placement recommended
 - Requires high speed network
 - Port 80/443 must be available or open on the firewall
- Licensing
 - Included in Notes Messaging CAL and Enterprise CAL
 - Requires a Lotus Domino Server License

Domino Preparations

- Domino requirements:
 - Register an additional server
 - <http://www-10.lotus.com/ldd/dominowiki.nsf/dx/1.6> Expanding the Domino Domain
 - Domino Directory using 8.5.3 template version
 - Users must have an internet address and password specified in their person document
 - Review existing DA configuration
 - Traveler will perform directory lookups on the mail server unless default configuration is modified
 - Review existing mail server Security
 - New Traveler server must be able to access mail server
 - New Traveler server must have manager + delete access to mail files

Security Planning

- Decisions to make...
 - Require VPN into network to access or use SSL connection?
 - Use a self-signed certificate or purchase a 3rd party certificate?
 - Which users will be allowed to access?
 - Device password requirements?

Lotus Traveler Device Settings : Default

Basics | Preferences | Assignment

Sync | Filter Settings | Device Settings | Security Settings

Windows Mobile | Nokia | Apple | Android

Device Security	Violation Action
<input type="checkbox"/> Require device password	Enforce
<input type="checkbox"/> Prohibit camera	Enforce
<input type="checkbox"/> Prohibit devices incapable of security enablement	Enforce

Implementation: Phase 1

- Install Operating System / prepare server
- Add host name to DNS
- Download the required code:
 - Domino 8.5.3
 - Domino 8.5.3 Fix Pack 1
 - Traveler 8.5.3
 - Traveler 8.5.3 Fix Pack 2

Implementation: Phase 2

- Install Domino
 - Install Domino 8.5.3 & 8.5.3 FP1
- Configure Domino Server
 - Verify server starts properly
 - Configure Directory Assistance (if required)
 - Create required connection documents for replication
 - Configure SSL (if required)
 - Configure session authentication (Single or multi-server)
 - Test HTTP connectivity

Implementation: Phase 2

- Install Traveler
 - End the Domino Server
 - Install Traveler 8.5.3
 - Install Traveler 8.5.3 Fix Pack 2

Required Connection Document(s)

- Pull From Hub/Mail/Administration server
 - Names.nsf
 - Secondary directory
 - Directory Assistance
- Pull-Push from Hub/Mail/Administration server
 - Admin4.nsf

Configuring SSL / Creating the Keyring

- Configuration done from a “Server Certificate Administration” application (csrv50.ntf template)



Create Key Ring

The first step in setting up SSL on a server is to create the key ring. When the key ring is created, a public/private keypair is automatically generated and stored in the key ring.

SSL

- Step #1
Create the
keyring file

Key Ring Information	Quick Help
Key Ring File Name: <input type="text" value="keyfile.kyr"/>	Specify the name and password for the key ring file. Note: You'll be referring to the key ring information you enter here in subsequent steps as you create and install certificates into the key ring.
Key Ring Password: <input type="password" value="*****"/>	
Confirm Password: <input type="password" value="*****"/>	
Key Size	
Key Size: <input type="text" value="2048"/>	Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength.
Distinguished Name	
Common Name: <input type="text" value="traveler.kimgreene.com"/>	The Distinguished Name is the information about your site that will appear in any certificates you create. Note: Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.
Organization: <input type="text" value="Kim Greene Consulting, Inc."/>	
Organizational Unit: <input type="text" value=" (optional)"/>	
City or Locality: <input type="text" value=" (optional)"/>	
State or Province: <input type="text" value="Minnesota"/> (no abbreviations)	
Country: <input type="text" value="US"/> (two character country code)	
<input type="button" value="Create Key Ring"/>	

SSL

- Step #2a
Create the certificate request
- Step #2b
Work with vendor to obtain certificate

Create Server Certificate Request

A certificate is required for the public key in the key ring you created. To obtain a certificate, you create a certificate request, and provide it to a Certificate Authority for signing. Use this form to create the certificate request.

Note: Before proceeding you should read the documentation provided by the Certificate Authority you are using to see how they require the certificate request to be delivered.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="keyfile.kyr"/>	Specify the key ring file. Note: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information	Quick Help
Log Certificate Request <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Log certificate requests for future reference. Note: Choose "View Certificate Request Log" in the main menu page to see a listing of all logged requests.
Method <input checked="" type="radio"/> Paste into form on CA's site <input type="radio"/> Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority. Note: The "Paste" method is recommended if it is supported by the Certificate Authority you are using.

SSL

- Step #3

Install Trusted root certificate into your keyring file

Install Trusted Root Certificate

Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. **Note:** This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="keyfile.kyr"/>	Specify the key ring file.
Certificate Information	
Certificate Label <input type="text"/>	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source <input type="radio"/> File <input checked="" type="radio"/> Clipboard	
Certificate from Clipboard: <input type="text"/>	Paste clipboard contents into this field.
<input type="button" value="Merge Trusted Root Certificate into Key Ring"/>	

SSL

- Step #4
Install the certificate for your server

Install Certificate into Key Ring

The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority, but typically you will receive an e-mail specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. **Note:** Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority In Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.

Key Ring Information	Quick Help
Key Ring File Name <input style="width: 100%;" type="text" value="keyfile.kyr"/>	Specify the key ring file.
Certificate Information Certificate Source <input type="radio"/> File <input checked="" type="radio"/> Clipboard Certificate from Clipboard: <input style="width: 100%;" type="text" value="Paste your certificate here"/>	The source of the certificate can be from a file or from the clipboard. Paste the clipboard contents into this field. Note: The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.
<input type="button" value="Merge Certificate into Key Ring"/>	

Configuring HTTP

- Copy .kyr and .sth file to server
- Redirect to SSL
- Enforce Server access
- Enable SSL port
- Tip: Allow anonymous authentication to prevent some device authentication failures

Basics	Security	Ports...	Server Tasks...	Internet Protocols...	MTAs...	Miscellaneous
Notes Network Ports Internet Ports... Proxies						
SSL settings						
SSL key file name:		mykeyring.kyr				
SSL protocol version (for use with all protocols except HTTP):		V3.0 only				
Accept SSL site certificates:		<input type="radio"/> Yes <input checked="" type="radio"/> No				
Accept expired SSL certificates:		<input checked="" type="radio"/> Yes <input type="radio"/> No				
SSL ciphers:		RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC				
<input type="button" value="Modify"/>						
Enable SSL V2: (SSL V3 is always enabled)		<input type="checkbox"/> Yes				
Web Directory Mail DIIOP Remote Debug Manager Server Controller						
Web (HTTP/HTTPS)						
TCP/IP port number:		80				
TCP/IP port status:		Redirect to SSL				
Enforce server access settings:		Yes				
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				

Configuring HTTP (cont'd)

- Enabling Session authentication

Basics	Security	Ports...	Server Tasks...	Internet Protocols...	MTAs...	Miscellaneous	Transactional Logging	Shared Mail	DAOS																												
<table border="1"> <tr> <td>HTTP</td> <td>Domino Web Engine</td> <td>DIIOIP</td> <td>LDAP</td> </tr> </table>										HTTP	Domino Web Engine	DIIOIP	LDAP																								
HTTP	Domino Web Engine	DIIOIP	LDAP																																		
<table border="1"> <thead> <tr> <th colspan="2">HTTP Sessions</th> </tr> </thead> <tbody> <tr> <td>Session authentication:</td> <td>Single Server</td> </tr> <tr> <td>Idle session timeout:</td> <td>30 minutes</td> </tr> <tr> <td>Force login on SSL:</td> <td>Yes</td> </tr> <tr> <td>Maximum active sessions:</td> <td>1000</td> </tr> <tr> <td colspan="2">Generating References to this Server</td> </tr> <tr> <td colspan="2">Does this server use IIS?</td> </tr> </tbody> </table>					HTTP Sessions		Session authentication:	Single Server	Idle session timeout:	30 minutes	Force login on SSL:	Yes	Maximum active sessions:	1000	Generating References to this Server		Does this server use IIS?		<table border="1"> <thead> <tr> <th colspan="2">Java Servlets</th> </tr> </thead> <tbody> <tr> <td>Java servlet support:</td> <td>Domino Servlet Manager</td> </tr> <tr> <td>Servlet URL path:</td> <td>/servlet</td> </tr> <tr> <td>Class path:</td> <td>domino\servlet</td> </tr> <tr> <td>Servlet file extensions:</td> <td></td> </tr> <tr> <td>Session state tracking:</td> <td>Enabled</td> </tr> <tr> <td>Idle session time-out:</td> <td>30 minutes</td> </tr> </tbody> </table>					Java Servlets		Java servlet support:	Domino Servlet Manager	Servlet URL path:	/servlet	Class path:	domino\servlet	Servlet file extensions:		Session state tracking:	Enabled	Idle session time-out:	30 minutes
HTTP Sessions																																					
Session authentication:	Single Server																																				
Idle session timeout:	30 minutes																																				
Force login on SSL:	Yes																																				
Maximum active sessions:	1000																																				
Generating References to this Server																																					
Does this server use IIS?																																					
Java Servlets																																					
Java servlet support:	Domino Servlet Manager																																				
Servlet URL path:	/servlet																																				
Class path:	domino\servlet																																				
Servlet file extensions:																																					
Session state tracking:	Enabled																																				
Idle session time-out:	30 minutes																																				

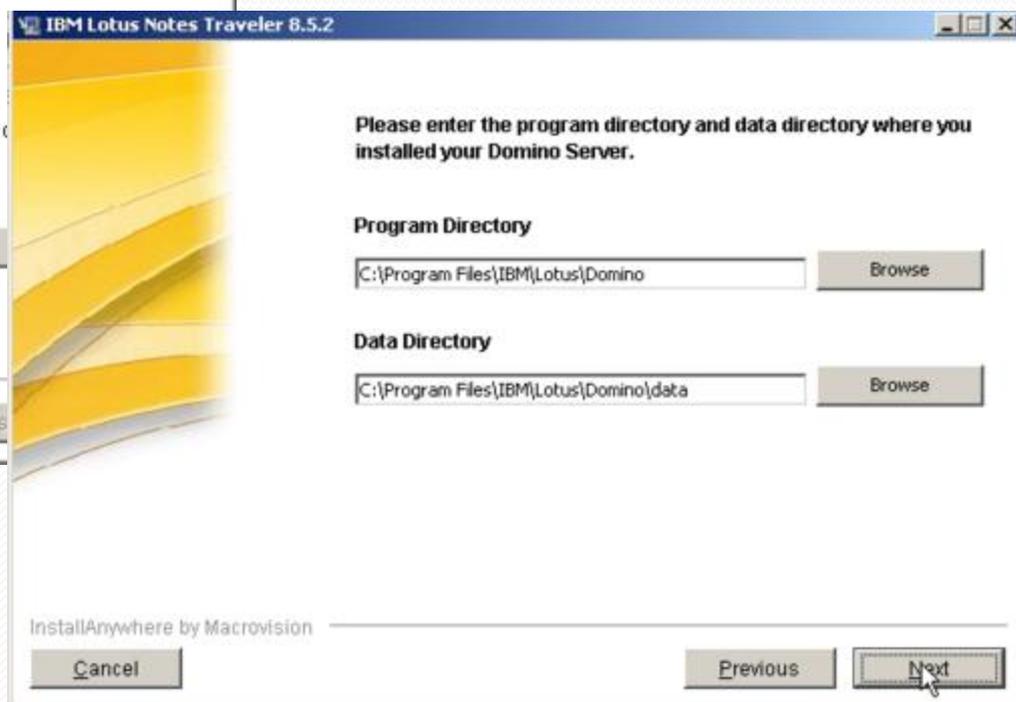
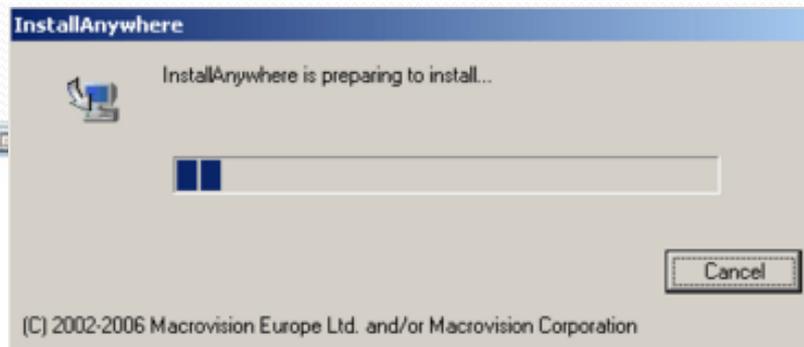
Testing

- Test accessing via HTTP
 - <http://traveler.kimgreene.com/names.nsf>
 - Do you get redirected to SSL?
 - Can you log in?
- Verify Directory Assistance
 - “Show xdir” console command

DomainName	DirectoryType	ClientProtocol	Replica/LDAP Server
1 KIMGREENE	Primary-Notes	Notes & LDAP	names.nsf
2 KGCIEXTERNAL	Secondary-Notes	Notes	edc.nsf

Directory Assistance Database 'da.nsf' in use

Installing Traveler



Set /servlet/traveler as the home URL

Installing Traveler

Traveler data and server changes

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared M

HTTP | Domino Web Engine | DIIOP | LDAP

Basics		Mapping	
Host name(s):	traveler.kimgreene.com	Home URL:	/servlet/traveler
Bind to host name:	Enabled	HTML directory:	domino/html
DNS lookup:	Disabled	Icon directory:	domino/icons

HTTP | Domino Web Engine | DIIOP | LDAP

HTTP Sessions		Java Servlets	
Session authentication:	Single Server	Java servlet support:	Domino Servlet Manager
Idle session timeout:	30 minutes	Servlet URL path:	/servlet
Force login on SSL:	Yes	Class path:	domino/servlet
Maximum active sessions:	1000	Servlet file extensions:	

servlets.properties file automatically updated via the install

Implementation: Phase 3

Starting the Server:

```
HTTP Server: Using Web Configuration View
JVM: Java Virtual Machine initialized.
HTTP Server: Java Virtual Machine loaded
Lotus Traveler: Server starting...
HTTP Server: DSAPI Domino Off-Line Services HTTP extension
Loaded successfully
Servlet engine initialization was successful
HTTP JVM: com.lotus.sync.servlet.TravelerServlet: init
HTTP JVM: Traveler 8.5.2.3 Build 201107280608
Starting replication with server MyServer/KimGreene
Pulling customers.nsf from MyServer/KimGreene customers.nsf
Lotus Traveler: Server started.
```

Basics

Maximum Memory Size:	512 MB
IPC Socket Ports:	50125 50126
External Server URL:	https://traveler.kimgreene.com/servlet/traveler

Lotus Traveler Access

Access server:	<input checked="" type="checkbox"/> users listed in all trusted directories
Not access server:	Terminations
Remote user commands:	Disabled
User managed security:	Enabled

Log Settings

Logging Level:	Informational
Obsolete as of Domino 8.5.2	Off
SyncML Logging:	
Package Log Filter:	*
Maximum File Size:	50 MB
Maximum Number of Activity Log Files:	10
Fields Logged - Privacy:	Subject; Location; Address; Phone Number

Auto Sync Settings

Monitor Polling Interval:	3 seconds
Port for TCP Connections:	8642
Heartbeat Algorithm:	Indefinite Detection

Server Document Changes

1. Set External URL
2. Define user access