



AdminCamp 2013

Single Login/Sign On – Reloaded

Workshop Track 1 – Session 5

Christian Henseler, 24.09.2013

Christian Henseler, 24.09.2013

Agenda

- ▶ Introduction
 - What are we coming from
 - Yet another SSO mechanism!?
 - SAML basics
 - Domino 9 requirements and limitations
- ▶ SAML use cases
 - SAML based Web Server SSO
 - Notes Federated Login (Notes client)
 - Web Federated Login (iNotes)
- ▶ Troubleshooting
- ▶ Wrap Up



Introduction – What is it all about!?

- ▶ Users don't want to enter their credentials multiple times
- ▶ Wouldn't it be nice to have a SSO solution that

is user friendly

works cross platform

supports both IBM Notes & Web clients

can be used internally and externally

is easily to configure and maintain

is based on open standards



Introduction – Situation pre 9.0

We already have

- Notes Single Login
- Notes Shared Login
- Domino Multi-session server Authentication
- SPENEGO/Kerberos

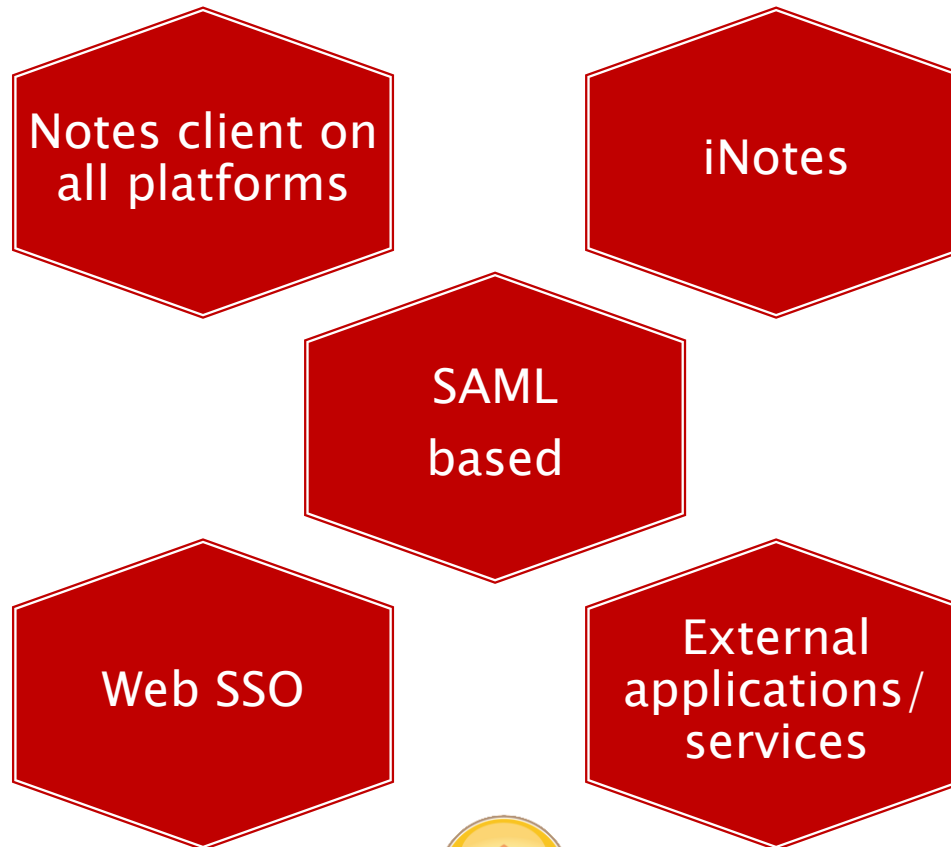
But all these mechanisms have limitations:

- Platform specific
- Not across DNS domains
- Missing flexibility
- Notes xor Web Client



Introduction – SSO in 9.0

IBM Domino 9.0 promises a new single SSO-mechanism:



Introduction – SAML

- ▶ Security Assertion Markup Language (sam-el)
 - XML based open standard
 - used for Authentication and Authorization
 - Roles
 - Principal
 - Notes 9.0/Web clients
 - Service Provider (SP)
 - Domino 9.0
 - Identity Provider (IdP)
 - Tivoli Federated Identity Manager (TFIM)
 - Microsoft Active Directory Federation Services (ADFS) 2.0

SAML 2.0 is recommended, but 1.1 is also supported (only by TFIM)



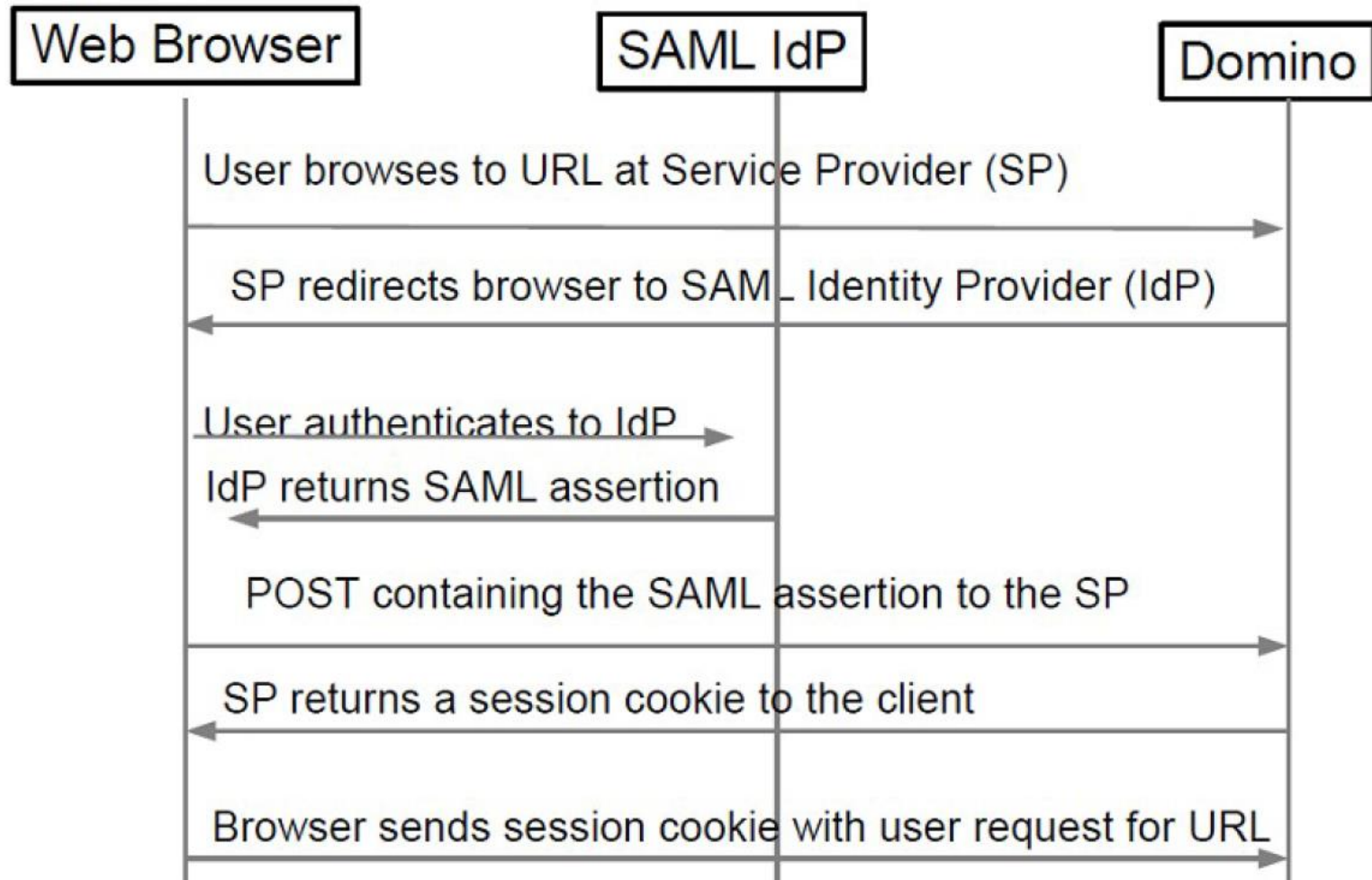
Introduction – SAML Assertions

```
<samlp:Response ID="_93e965fe-d658-4fe3-83b4-e21c9eec825f" Version="2.0"
  IssueInstant="2013-08-27T00:04:19.705Z"
  Destination="https://demail01.henseler.org/names.nsf?SAMLLogin"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" xmlns:samlp="urn:oasi
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  http://dc.henseler.org/adfs/services/trust
</Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<Assertion ID="_ae4d2a14-6406-4a9a-b503-bc88cbb1a02b" IssueInstant="2013-08-
27T00:04:19.660Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
<Subject>
  <NameID>
    christian.henseler@henseler.org
  </NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData NotOnOrAfter="2013-08-27T00:09:19.707Z"
      Recipient="https://demail01.henseler.org/names.nsf?SAMLLogin" />
  </SubjectConfirmation>
</Subject>
```

Assertions are using time stamps, IDP and SP must be **time sync'ed**!
Assertions can be encrypted, if sensitive data is exchanged.



Introduction – SAML protocol flow



Introduction – SAML Requirements

To use SAML based SSO mechanisms you need:

- Notes 9.0 Clients for Notes Federated Login
- Domino 9.0 Vault-Servers
- Domino 9.0 for Service Provider servers
- Domino Directory 9.0 Design for security settings
- User credentials hosted on IdP, e.g. Active Directory user account (and computer account)
- SAML compatible Web-browsers
- IdP – ADFS 2.0 or TFIM are currently supported
- A good relationship to your IdP Administrators!



Limitations

- ▶ You can't use SAML, when you are using
 - Smartcard protected ID
 - Roaming users with ID files in PAB
 - Notes on a USB device
 - Notes user IDs with multiple passwords
 - Notes Single Login
 - Basic Client & Admin Client
 - Lotus Notes Traveler (for LNT authentication)

- ▶ Password management settings should be disabled:
 - Check password on Notes id file
 - Update Internet Password When Notes Client Password Changes
 - Enforce Internet Password Lockout



SAML use cases

SAML is used in 9.0 for the following use cases:

- ▶ SAML-based Web SSO
 - Web Access with SAML-based SSO
- ▶ Notes federated Login
 - Notes client with SAML SSO
- ▶ Web federated Login
 - iNotes (with mail encryption, ID access)

Not covered here:

- ▶ Federated Login to externally-based services
(see Andrews Pollack's session on Wednesday)



SAML based Web SSO

Used as SSO mechanism for Web Application servers.

1. ADFS Trust Relationship
2. Attribute Mapping Domino vs. ADFS
3. IDP–Catalog on SP
4. IDP–Document for Web Server working as SP
5. Authentication method in Server or Internet Site documents
6. Optional: Integrated Windows Authentication (SPNEGO/Kerberos)

ID–Vault and security policies are **not** involved!



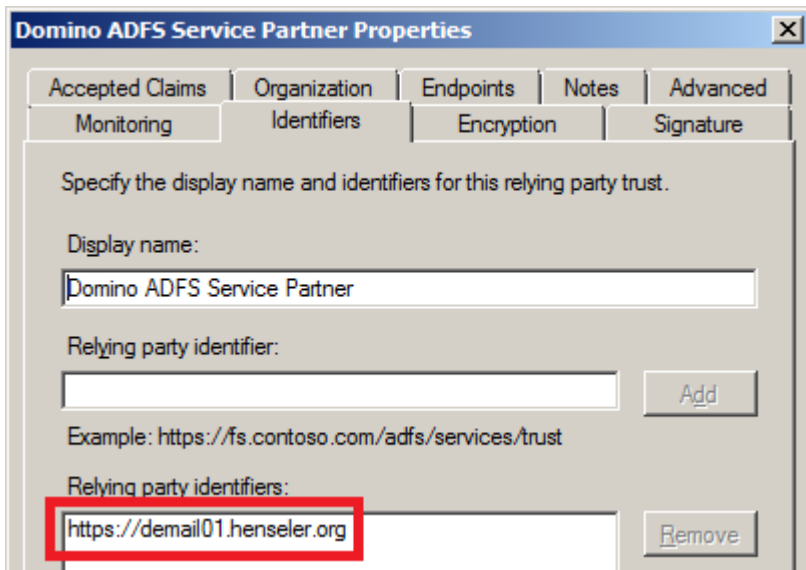
IdP Configuration – ADFS 2.0

- ▶ Separate download for Windows Server 2008 R2!
- ▶ User account must be available in Active Directory
- ▶ AD user and Domino Person document must have an attribute used for matching, usually the Internet Address
- ▶ SSL must be configured
- ▶ For Integrated Windows Authentication:
 - User Account and computer must be Active Directory members
 - Integrated Windows Authentication configuration of the ADFS-servers
 - Extended Protection must be turned off for Notes Federated Login and Non-IE-Browsers
- ▶ Very well documented in the Lotus Notes and Domino Wiki

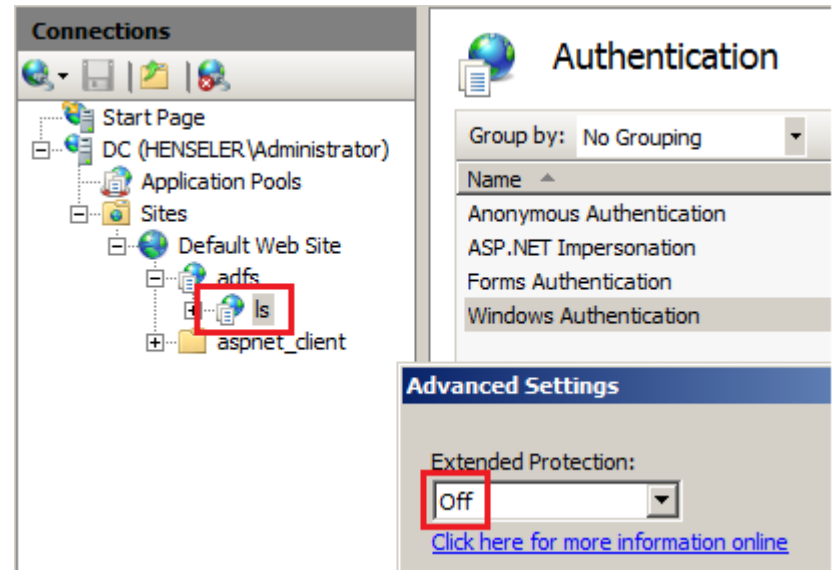


ADFS Trust Relationship

Important ADFS 2.0 configuration details:



The Relying party identifier is used in the IdP configuration document

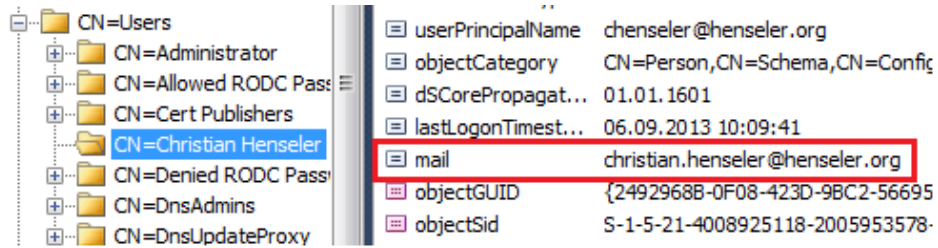


Extended Protection must be turned off
NFL and Non-IE-Browsers



SAML attribute matching

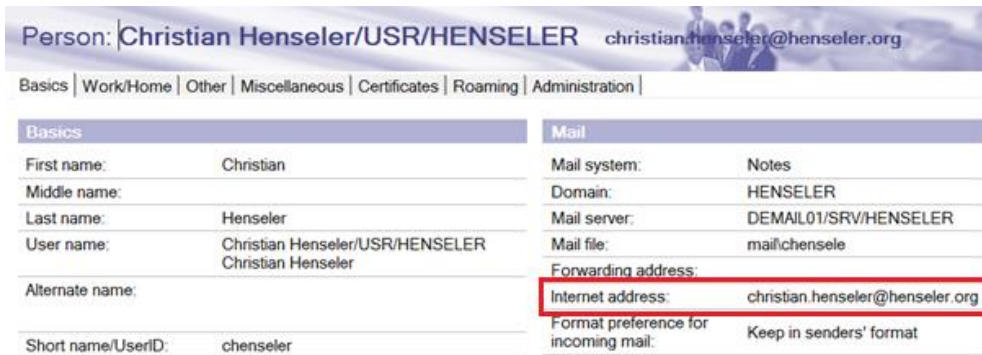
The E-Mail Address in Active Directory...



Active Directory Users and Groups console showing the properties of the user 'Christian Henseler'. The 'mail' attribute is highlighted with a red box, showing the value 'christian.henseler@henseler.org'.

Attribute	Value
userPrincipalName	chenseler@henseler.org
objectCategory	CN=Person,CN=Schema,CN=Config
dSCorePropagat...	01.01.1601
lastLogonTimeSt...	06.09.2013 10:09:41
mail	christian.henseler@henseler.org
objectGUID	{2492968B-0F08-423D-9BC2-56695}
objectSid	S-1-5-21-4008925118-2005953578-

... is mapped to the Internet Address of the Person document



Person: Christian Henseler/USR/HENSELER christian.henseler@henseler.org

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming | Administration

Basics		Mail	
First name:	Christian	Mail system:	Notes
Middle name:		Domain:	HENSELER
Last name:	Henseler	Mail server:	DEMAIL01/SRV/HENSELER
User name:	Christian Henseler/USR/HENSELER Christian Henseler	Mail file:	mail/chensele
Alternate name:		Forwarding address:	
Short name/UserID:	chenseler	Internet address:	christian.henseler@henseler.org
		Format preference for incoming mail:	Keep in senders' format

Alternatively: DA to AD with Domino Distinguished name mapping



IdP Catalog & Configuration docs

The IdP Catalog is used to define trust relationship on the domino side

- Filename must be **idpcat.nsf**
- Database must be located on Service Provider
- Use **IdP Catalog** template
- Admin must have the rights
 - „Full Access administrators“
 - „Sign or run unrestricted methods and operations“
 - ACL should be restricted to SP servers and IdP admins

Manual process using *certmgmt* if

- Server.id is password protected
- Admin does not have appropriate rights



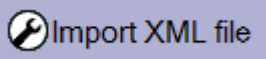
IdP Configuration – Basics

IdP Configuration : ADFS 2.0

Basics | Client Settings | Certificate Management | Administration

Basics

Host names or addresses mapped to this site:	demail01.henseler.org; 192.168.152.153
IdP name:	ADFS 2.0
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	ADFS
Service provider ID:	https://demail01.henseler.org
Artifact resolution service URL:	https://dc.henseler.org/adfs/services/trust/artifactresolution
Single sign-on service URL:	https://dc.henseler.org/adfs/ls/IdpInitiatedSignOn.aspx
Signing X.509 certificate:	MIIC2jCCAcKgAwIBAgIQPkYCEYnLfKhALeg/tAPyTTANBgkqhkiG
Encryption X.509 certificate:	MIIC4DCCAciGAwIBAgIQKBHftkJCVKBFvxjrj8ZoBzANBgkqhkiG
Protocol support enumeration:	urn:oasis:names:tc:SAML:2.0:protocol
Comment:	

- ▶ Add IP address if ADFS 2.0 is used (because of SSL)
- ▶ ADFS needs SAML 2.0 protocol version
- ▶ *Service Provider ID* must match *Relying party identifiers* in the ADFS configuration!
- ▶ Other fields are imported using the  button
- ▶ Imported IdP X.509 certificates are used for SAML Assertion Verification & optionally for Encryption



IdP Configuration – Client settings

IdP Configuration : ADFS 2.0

Basics | Client Settings | Certificate Management |

Notes Client Settings

<u>Enable Windows single sign-on:</u>	Yes
---------------------------------------	-----

Sites that are trusted:	
-------------------------	--

Enforce SSL:	Yes
--------------	-----

- ▶ *Enable Windows single sign-on* is needed for Notes federated Login
- ▶ Enforce SSL is used for ADFS 2.0



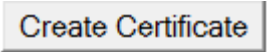
IdP Configuration – Certificate Management

IdP Configuration : ADFS 2.0

Basics | Client Settings | Certificate Management | Administration

Certificate Management Settings

Company name:	DEMAIL01 SAML Signing Certificate
Domino URL:	https://demail01.henseler.org
Single logout URL:	https://dc.henseler.org/adfs/ls/?wa=woutcleanup1.0
Certificate public hash value (base 64):	WYHjiB1qh94bQW1IIDguyA==

- ▶ Company name is used to create the SAML Signing Certificate using the  button
- ▶ Domino URL is (in most cases) the same as the Service Provider ID (on Basics tab)



IdP – SAML Signing Certificate

Create Certificate is creating a X.509 certificate in the server.id:

Examine Internet Certificate

Certificates issued by

1. CN=DEMAIL01 SAML Signing Certificate

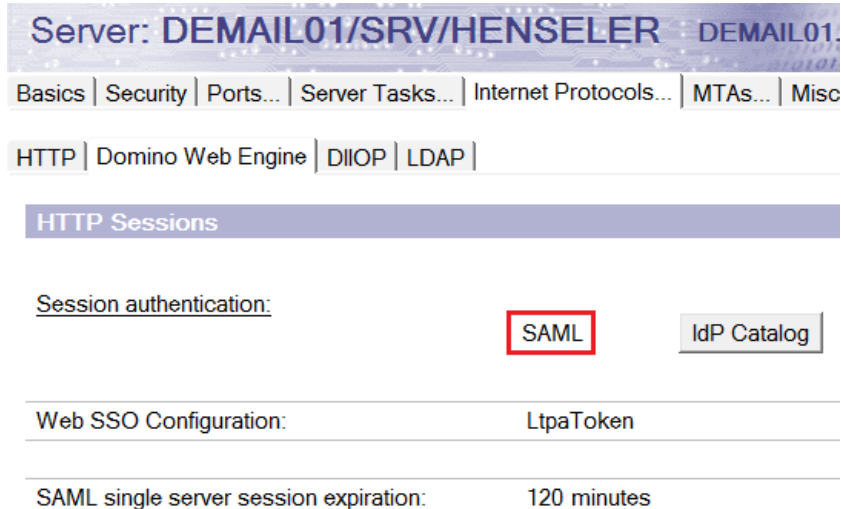
Issued to	CN=DEMAIL01 SAML Signing Certificate
Activated	10.09.2013 21:31:24
Expires	29.08.2063 21:31:24
Serial number	75:CE:F0:42:BA:C0:E5:15:70:55:46:6D:93:5A:C2:E2
Fingerprint	F576 22A0 B6FA 158A 9261 AA1C C4ED 061B
Key Strength	2048 bits

- ▶ Is used for SAML Assertion encryption.
- ▶ Is exported to idp.xml by using the  **Export XML** button



Authentication configuration

Select SAML in the Server or Internet site document:



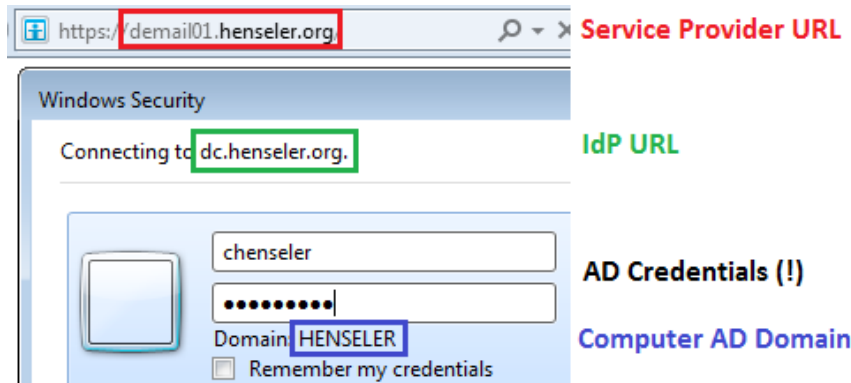
The screenshot shows the Domino configuration console for the server 'DEMAIL01/SRV/HENSELER'. The 'HTTP' tab is selected, and the 'HTTP Sessions' sub-tab is active. Under 'Session authentication', the 'SAML' button is highlighted with a red box, while the 'IdP Catalog' button is unselected. Below this, the 'Web SSO Configuration' field is set to 'LtpaToken'. At the bottom, the 'SAML single server session expiration' is set to '120 minutes'.

- ▶ If Web SSO Configuration is empty: Single Server authentication
 - IdP vs. SP Trust relationship configuration for every server using SAML
- ▶ As soon as an IdP Config document exists, it takes precedence:
HTTP Server: Error processing authentication configuration for
demail01.henseler.org: Active IdP catalog entry found. **Overriding
configuration and enabling SAML authentication at demail01.henseler.org**

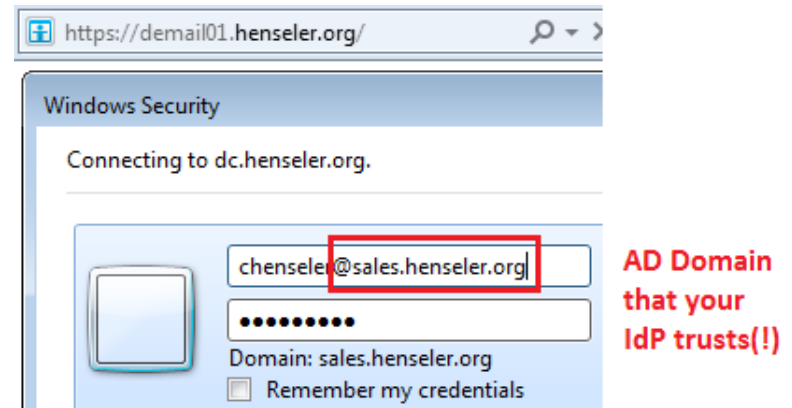


Integrated Windows Authenticoitin

If not configured, the user is prompted for IdP(!) login credentials:



or cross(!) domain:



Integrated Windows Authentication

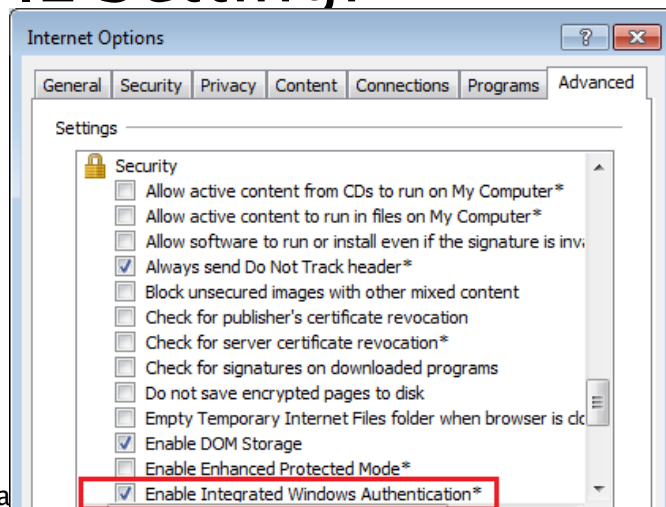
- ▶ SPNEGO/Kerberos available since 8.5.1
- ▶ Use *setspn* utility on ADFS server side
- ▶ Disable Windows Single Sign-on integration in the Web SSO configuration document:

Participating Servers

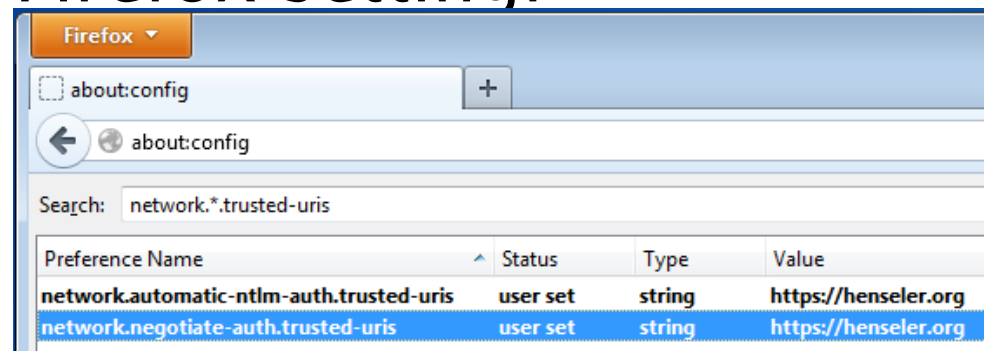
Domino Server Names:

Windows single sign-on integration (if available): **Disabled**

- ▶ IE Setting:

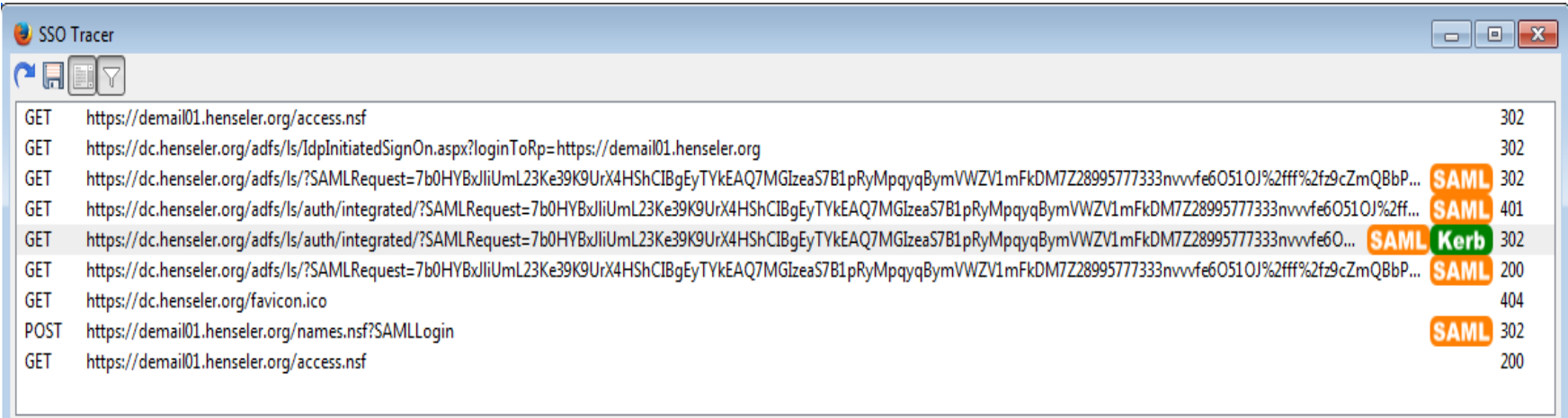


- ▶ Firefox setting:



Putting all together

Web-based access to a Domino resource using SAML & Integrated Windows Authentication



The SSO Tracer window displays the following sequence of requests and responses:

Method	URL	Status	Protocol
GET	https://demail01.henseler.org/access.nsf	302	
GET	https://dc.henseler.org/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=https://demail01.henseler.org	302	
GET	https://dc.henseler.org/adfs/ls/?SAMLRequest=7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIZEaS7B1pRyMpqqqBymVWZV1mFkDM7Z28995777333nvvfe6051OJ%2fff%2fz9cZmQBbP...	302	SAML
GET	https://dc.henseler.org/adfs/ls/auth/integrated/?SAMLRequest=7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIZEaS7B1pRyMpqqqBymVWZV1mFkDM7Z28995777333nvvfe6051OJ%2fff...	401	SAML
GET	https://dc.henseler.org/adfs/ls/auth/integrated/?SAMLRequest=7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIZEaS7B1pRyMpqqqBymVWZV1mFkDM7Z28995777333nvvfe60...	302	SAML Kerb
GET	https://dc.henseler.org/adfs/ls/?SAMLRequest=7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIZEaS7B1pRyMpqqqBymVWZV1mFkDM7Z28995777333nvvfe6051OJ%2fff%2fz9cZmQBbP...	200	SAML
GET	https://dc.henseler.org/favicon.ico	404	
POST	https://demail01.henseler.org/names.nsf?SAMLLogin	302	SAML
GET	https://demail01.henseler.org/access.nsf	200	



Notes Federated Login

1. ADFS Trust Relationship
 2. Attribute Mapping Domino vs. ADFS
 3. ID Vault & Vault Configuration
 4. IDP-Catalog on Vault-Server
 5. IDP-Document for SP
 6. Internet Cross Certificate IdP
 7. Security Settings document
 8. Integrated Windows Authentication is mandatory
-
- ▶ SP is not necessarily the Vault-Server!
 - ▶ HTTP task is neither on SP nor on Vault-Server necessary!



Notes Federated Login

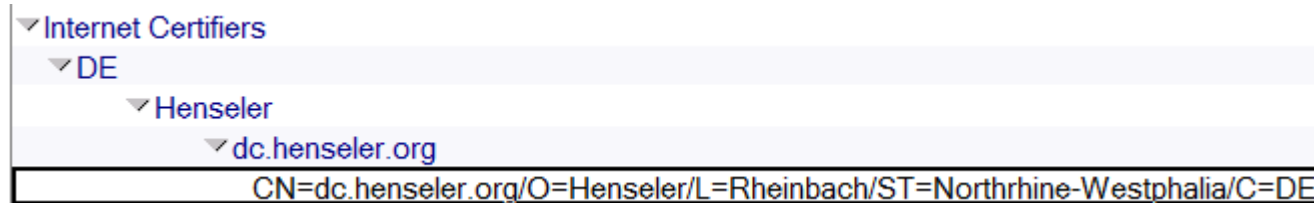
- ▶ ADFS Relying Party Trust configuration for SP as explained
- ▶ Users IDs must be in the ID Vault
 - Automatic download should be enabled
- ▶ IdP Catalog must reside on Vault server
 - Replica of SP's idpcat.nsf



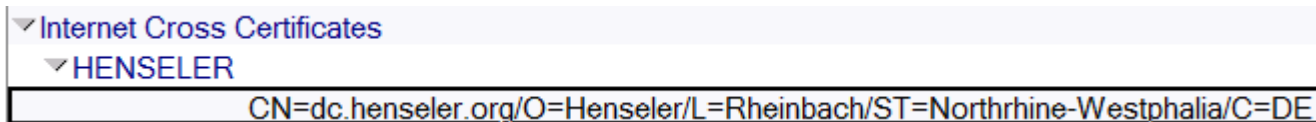
IdP Internet Cross Certificate

An Internet cross certificate for the IdP is necessary in the Domino directory:

1. Import Internet Certificate

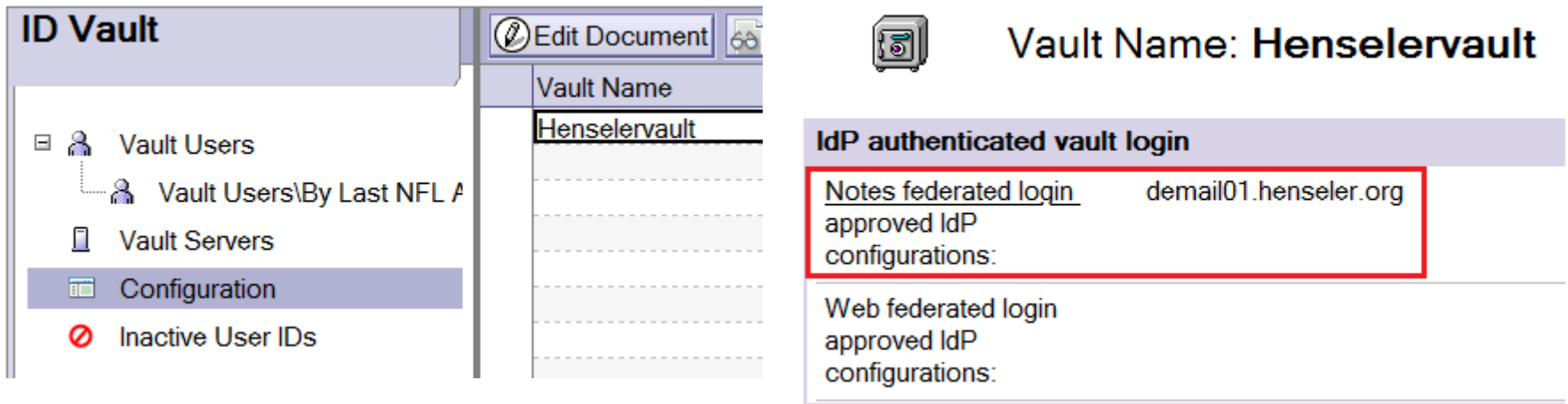


2. Create Internet Cross Certificate



ID Vault configuration

Add all IdP configurations used for NFL to the Vault configuration:



The screenshot displays the 'ID Vault' configuration window. On the left, a tree view shows 'Vault Users', 'Vault Users\By Last NFL A', 'Vault Servers', 'Configuration' (selected), and 'Inactive User IDs'. The main area shows the 'Vault Name' as 'Henselervault'. To the right, a summary box titled 'Vault Name: Henselervault' contains a safe icon and a section 'IdP authenticated vault login'. This section lists 'Notes federated login' with the value 'demail01.henseler.org' and 'approved IdP configurations:'. Below this, 'Web federated login' and 'approved IdP configurations:' are also listed.

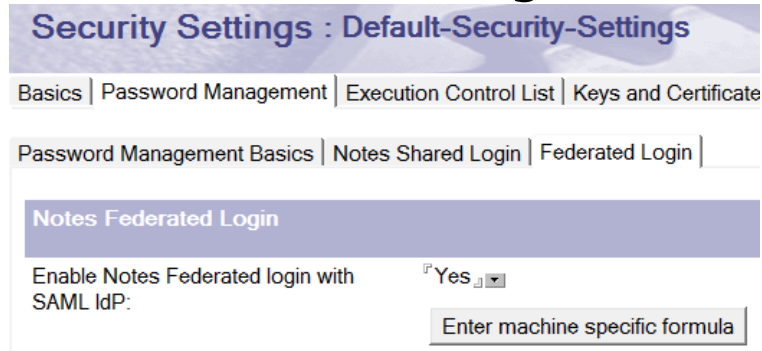
IdP authenticated vault login	
<u>Notes federated login</u>	demail01.henseler.org
approved IdP configurations:	
Web federated login	
approved IdP configurations:	

The Vault server must be able to find the IdP configuration document in the local idpcat.nsf



Security Settings document

- ▶ Notes Federated Login must be activated



Security Settings : Default-Security-Settings

Basics | Password Management | Execution Control List | Keys and Certificate

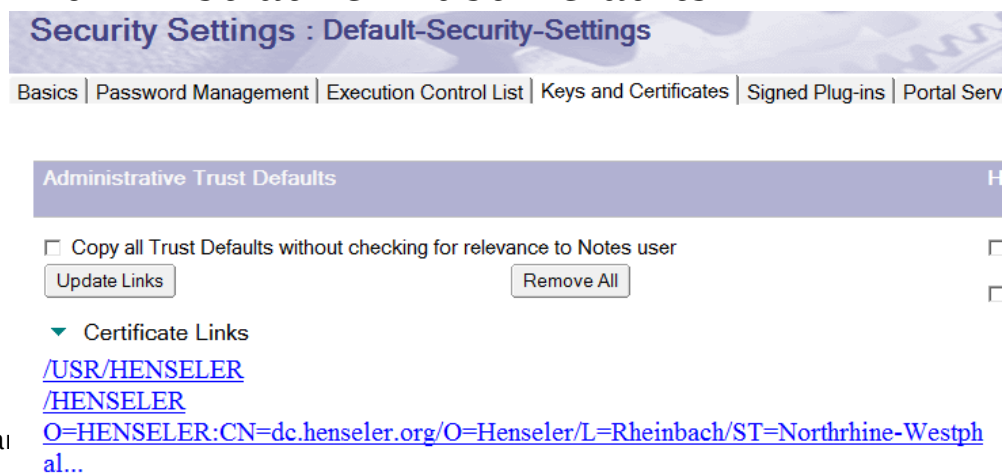
Password Management Basics | Notes Shared Login | Federated Login |

Notes Federated Login

Enable Notes Federated login with SAML IdP: ☒ Yes

You should use Machine specific formulas to exclude Notebooks

Internet Cross Certificate & Notes certifier must be added to Administrative Trust Defaults



Security Settings : Default-Security-Settings

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Serv

Administrative Trust Defaults

☐ Copy all Trust Defaults without checking for relevance to Notes user

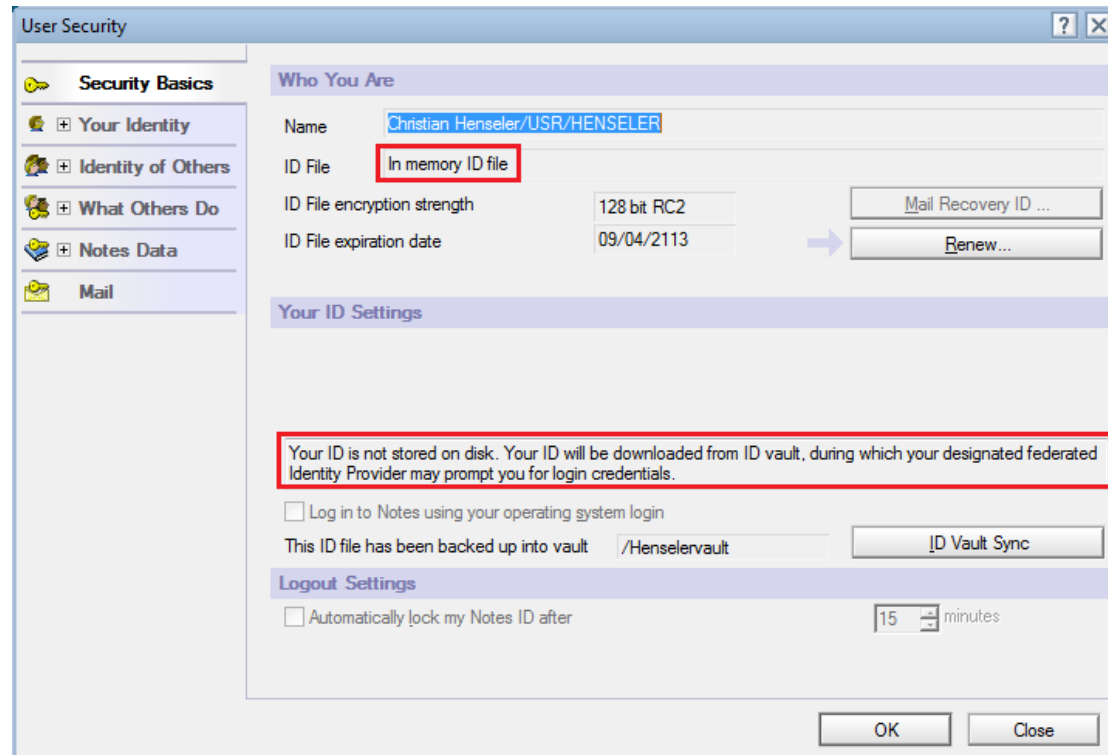
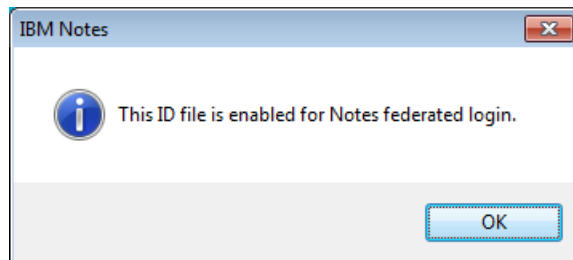
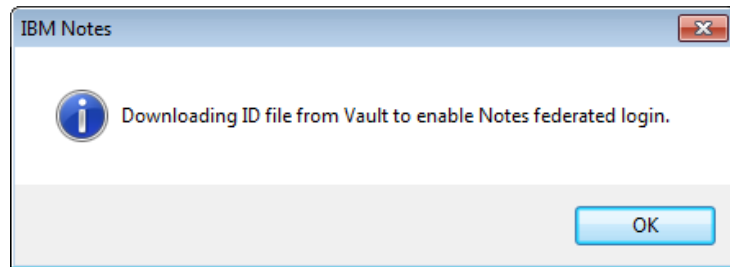
▼ Certificate Links

[/USR/HENSELER](#)

[/HENSELER](#)

[O=HENSELER:CN=dc.henseler.org/O=Henseler/L=Rheinbach/ST=Northrhine-Westphal...](#)

Notes Federated Login enablement



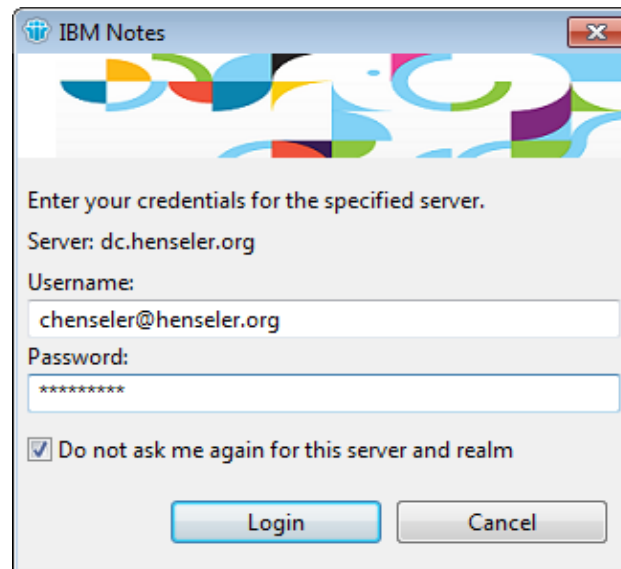
Please note:

- User.ID password is still **required** for First time setup
- User.id **remains** on disk (not automatically deleted)



NFL vs. IWA

The previous slide omitted one step if Integrated Windows Authentication is not available:

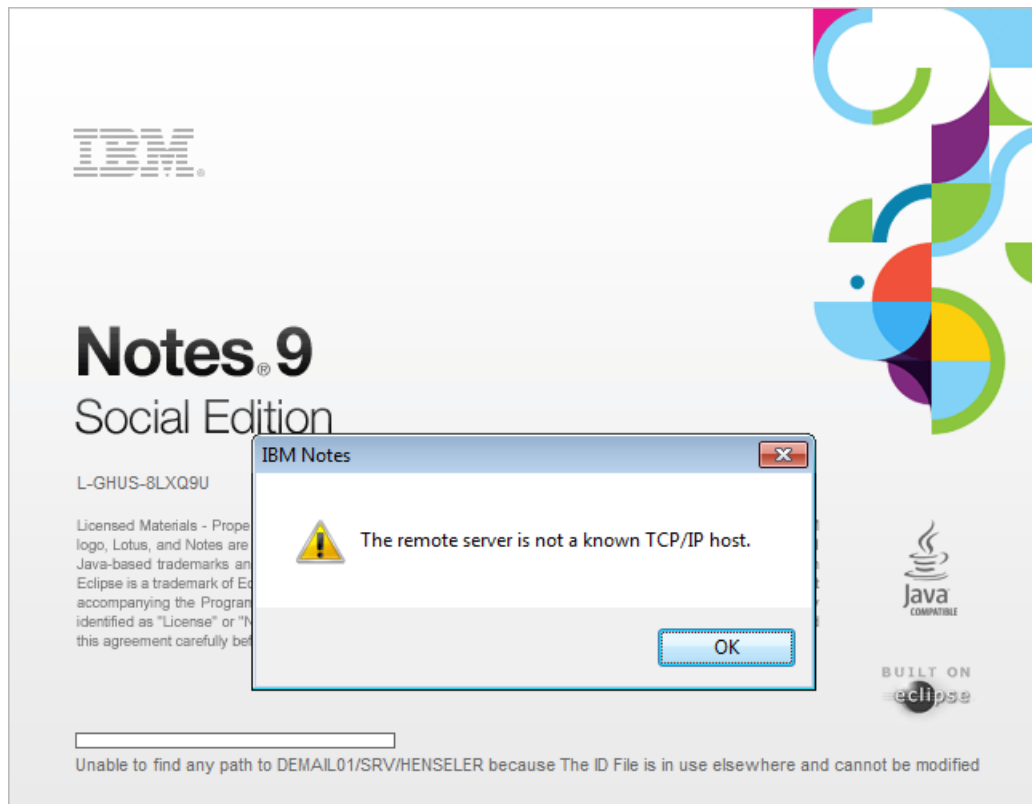


If Notes 9.0 is used on Windows AD integrated computers, IWA should be used for user convenience



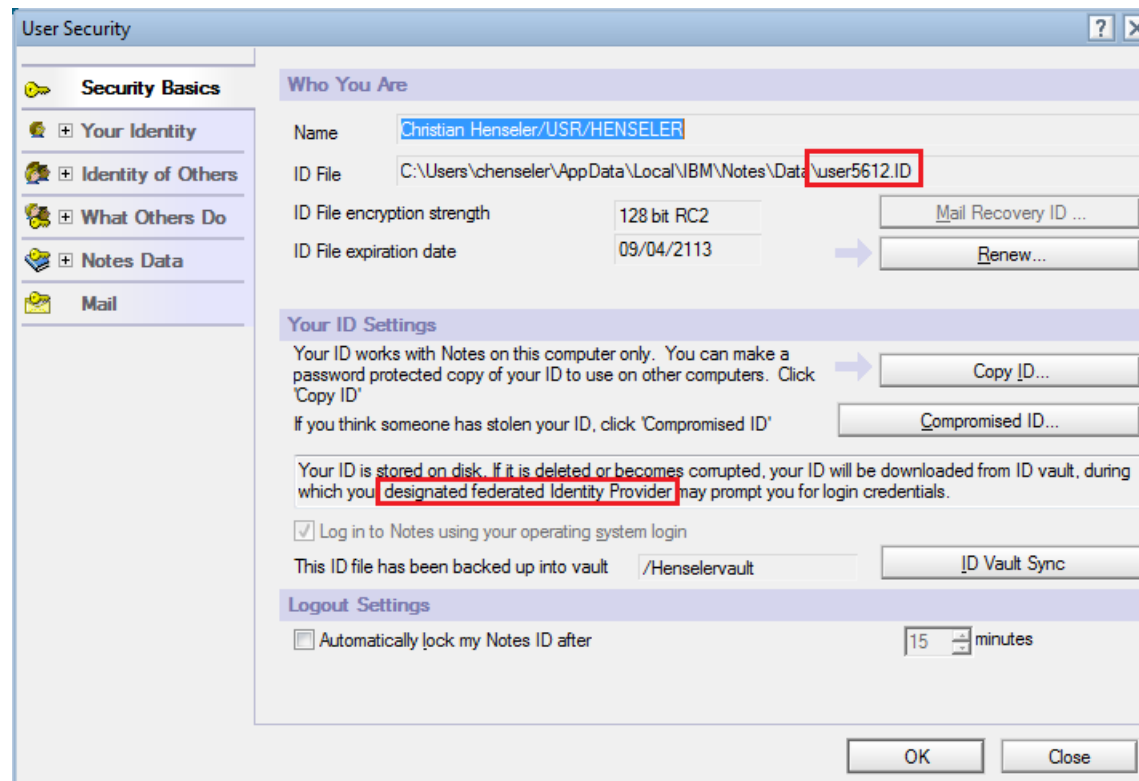
...and Notebook users !?

What happens with NFL enabled users when they are working without connection to the IdP?



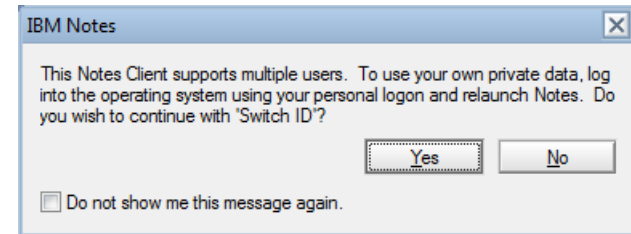
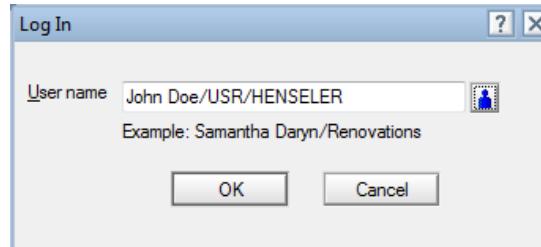
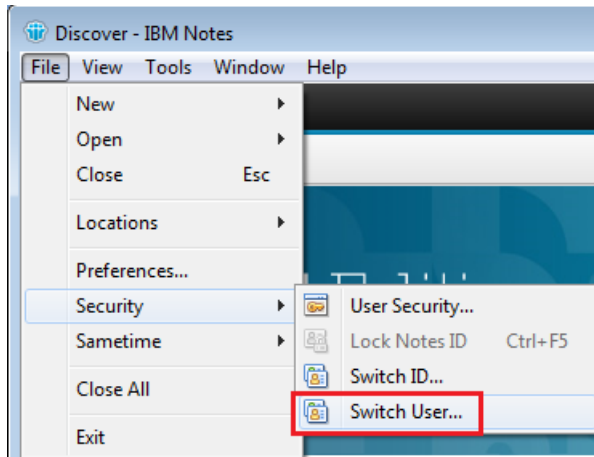
NFL vs. NSL

- ▶ Use standard Notes Shared Login for users that need to work disconnected from the IdP:



Switching users ...

- ▶ In theory, because no ID is stored on disk, you have to use Switch User...

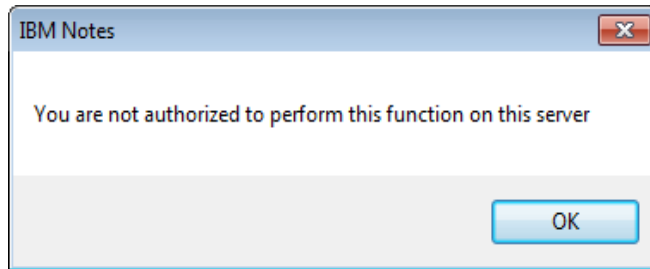


but



Switching users...

...when IWA is configured, you will most probably run into:



The problem is that you cannot map a unique matching attribute to different accounts and IWA is handing over the OS credentials

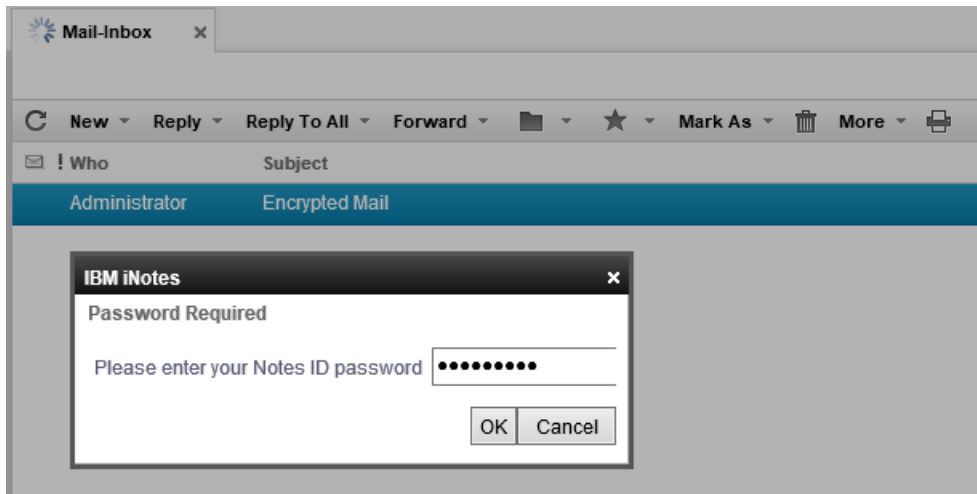


Web Federated Login

Web Federated Login combines

- ▶ SAML-based SSO for Webservers (iNotes)
- ▶ SAML-based access to ID files (ID-Vault)

Major goal is to eliminate:



Web Federated Login

Based on a SAML-based SSO Web configuration you need additionally:

- ▶ Security Policy Settings
- ▶ iNotes vs. ID Vault Server Trust
- ▶ ID Vault configuration

Still no HTTP-Task on ID-Vault(!)



WFL – Security Settings

Web Federated Login must be enabled in the Security Settings document:

Security Settings : Default-Security-Settings

Basics | Password Management | Execution Control List | Keys and Certificates

Password Management Basics | Notes Shared Login | Federated Login |

Web Federated Login

Enable Web Federated login with SAML IdP: ☒ Yes

It must be activated in the ID Vault configuration:

Security Settings : Default-Security-Settings

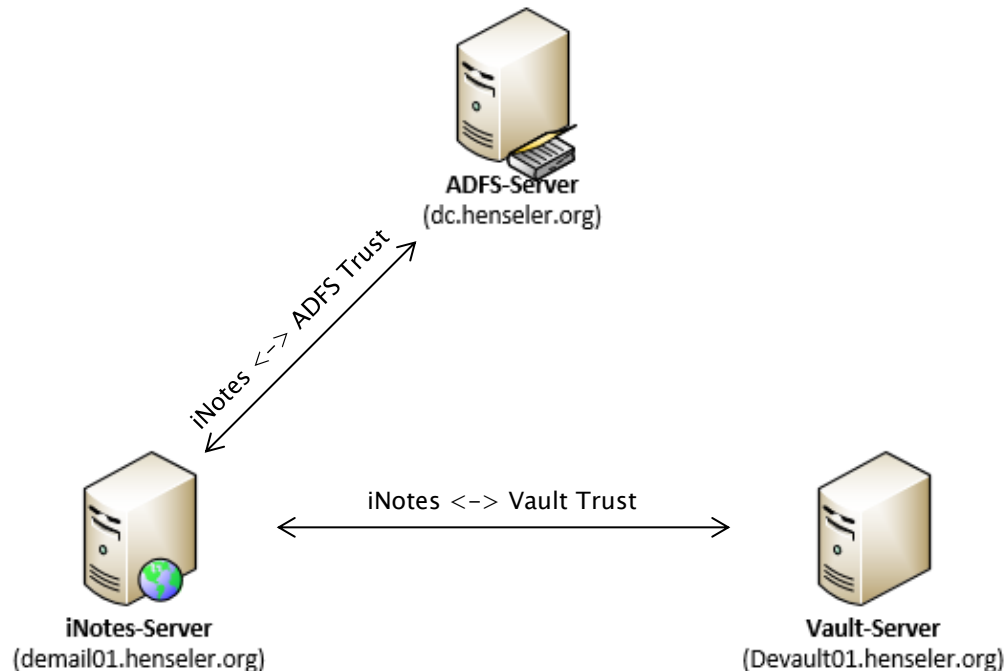
Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | ID Vault |

ID Vault Options:	How to apply this setting:
Assigned vault: /Henselervault	☐ Don't set value
Forgotten password help text:	☐ Don't set value
Enforce password change after password has been reset: Yes	☐ Don't set value
Allow Notes-based programs to use the Notes ID Vault: Yes	☐ Don't set value



WFL – IdP Configuration

- ▶ If the iNotes server is separated from the Vault server:
 - 1st document for iNotes as SP
 - 2nd document for iNotes „interfacing“ the vault server



WFL – IdP Configuration

IdP config field	iNotes vs. IdP	iNotes vs. Vault-Server
Host names or addresses mapped to this site	https://demail01.henseler.org; 192.168.152.153	vault .demail01.henseler.org
Service provider ID	https://demail01.henseler.org	https:// vault .demail01.henseler.org
Company Name	DEMAIL01 SAML Signing Certificate	DEVAULT01 SAML Signing Certificate
Domino URL	https://demail01.henseler.org	https://demail01.henseler.org

- The virtual FQDN for the Vault-server should **not** exist in DNS!
- IP address is not necessary for the Vault-server



WFL – ID Vault configuration

The virtual FQDN of the Vault-server is used:



Vault Name: **Henselervault**

IdP authenticated vault login

Notes federated login
approved IdP
configurations:



Web federated login
approved IdP
configurations:

vault.demail01.henseler.org



Debug_SAML

- 0x0001 (1) – Debug output contains information from http side.
- 0x0002 (2) – Debug output contains SAML parse information.
- 0x0004 (4) – Debug output only contains errors.
- 0x0008 (8) – Debug to dump decoded assertion.
- 0x0010 (16) – Debug to trace idpcat activity
- 0x0020 (32) – Trace replay prevention
- 0x0080 (128) – Dump the entire XML tree
- 0x0100 (256) – Dump canonicalized buffers
- 0x0200 (512) – Debug for the library sort
- 0x0800 (2048) – Debug for namespace use
- 0x2000 (8192) – Debug output for certificate management



Client side debugging

Notes.ini

DEBUG_SAML=31

DEBUG_CONSOLE=1

DEBUG_CLOCK=32

DEBUG_OUTFILE=<outfile>

DEBUGGINGWCTENABLED=4294967295

CONSOLE_LOG_ENABLED=1

DEBUG_DYNCONFIG=1

DEBUG_TRUST_MGMT=1

DEBUG_IDV_TRACE=1

DEBUG_TRUSTCERT=1

DEBUG_ROAMING=4

DEBUG_BSAFE_IDFILE_LOCKED=8

STX9=2



Client side debugging

Java logging with rcpininstall.properties

`com.ibm.rcp.internal.security.auth.samlSso.level=FINEST`

`com.ibm.rcp.internal.security.auth.dialog.level=FINEST`

`com.ibm.rcp.core.internal.launcher.level=FINEST`

`com.ibm.notes.internal.federated.manager.level=FINEST`

`com.ibm.notes.java.api.internal.level=FINEST`

`com.ibm.notes.java.init.level=FINEST`

`com.ibm.notes.java.init.win32.level=FINEST`

`com.ibm.workplace.noteswc.level=FINEST`

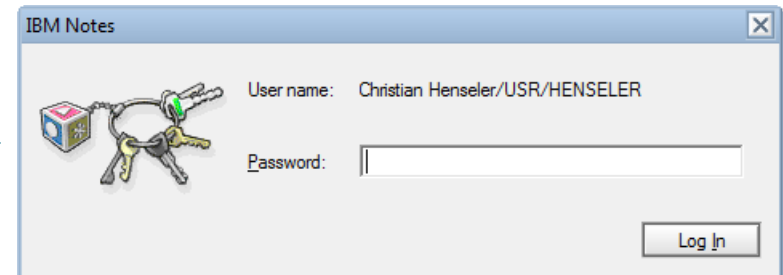
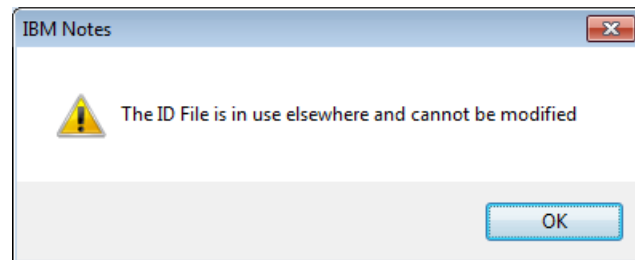
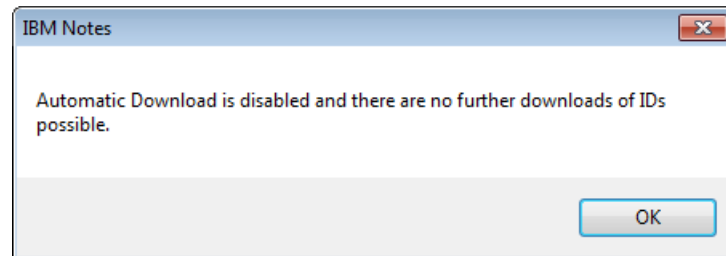
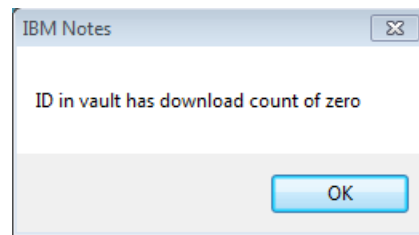
`com.ibm.workplace.internal.notes.security.auth.level=FINEST`

`com.ibm.workplace.internal.notes.security.level=FINEST`



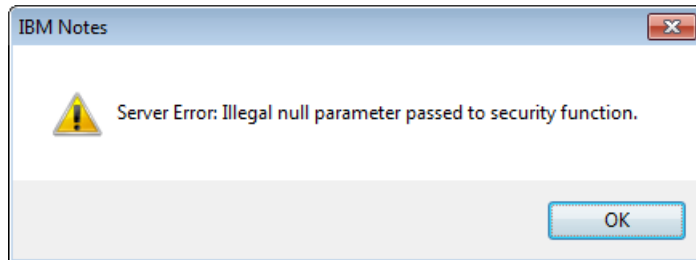
Troubleshooting – NFL Examples

- ▶ If ID Vault Automatic download is disabled and Download counter is 0:



Troubleshooting – Examples

- ▶ NFL enablement: If idpcat.nsf is not on Vault server:



- ▶ Saml configured for server, but no Idpcat.nsf or idp config document:

HTTP Server: Error reading IdP configuration for server :**Entry not found in index**

HTTP Server: SAML configuration error. SAML is enabled for server [], but **no active IdP configuration could be loaded.**



Troubleshooting – Examples

- ▶ Problem when using Create Certificate:

SECMakeInetSAMLCert> **SAML signing key already exists** in ID file:
Cannot accept internet certificate because the certificate is already in the ID file.

- ▶ If the cross certificate is not included in the security settings document for NFL:

com.ibm.rcp.internal.security.auth.samlso.SAMLBrowser HandleSSLCrossCertValidationFailed	CWPST0117E: Certificate chain of SSL server dc.henseler.org is not trusted.
---	---



Wrap Up

SAML-based authentication

- Provides a cross platform SSO mechanism
- Frees users from managing credentials in Notes
- Reduces administrative costs

You may not use SAML for

- Notebook users (exclude per machine specific policy)
- Administrators (because Ids cannot be extracted from ID Vault)
- Developers

Thank you very much!



Resources

Links

- [Supplementary information on Security Assertion Markup Language \(SAML\) configuration combinations of IBM Domino and other products](#)
- [Configuring an IBM Domino Web server to use SAML-based single sign-on \(Open Mic\)](#)

AdminCamp 2013

- [Workshop Track 1 – Session 8: SAML OAUTH and Session sharing \(Andrew Pollack\)](#)

