Configuring a Lotus single sign-on environment

Add security to a collaborative environment

Skill Level: Advanced

Jeffrey Slone (jeffrey_slone@us.ibm.com)
Senior Curriculum Developer
IBM

William Tworek (william_tworek@us.ibm.com)
Project Leader
IBM

16 Sep 2003

This tutorial shows how to enable single sign-on in collaborative environments that include Domino and WebSphere Portal Server technologies.

Section 1. About this tutorial

Should I take this tutorial?

This tutorial is recommended for system administrators who wish to configure single sign-on (SSO) in a collaborative environment that includes several IBM software products. It is recommended that you have some experience with the following:

- Lotus Domino administration (both 5.x and 6.x versions)
- Lotus Domino Web Access (iNotes) administration
- Lotus Instant Messaging and Web Conferencing (Sametime) administration
- Lotus Team Workplace (QuickPlace) administration
- WebSphere Portal (version 5) administration

What is this tutorial about?

Configuring single sign-on across a number of existing systems can be a challenging task. This tutorial discusses the configuration of SSO in a Lotus collaborative environment containing servers running several IBM software products.

The tutorial is divided into two parts. Part one demonstrates the configuration of SSO in a Domino-only environment. Part two demonstrates the configuration of SSO in a collaborative environment containing WebSphere Portal and several Lotus software products. Both parts demonstrate the configuration of SSO using Lightweight Third Party Authentication (LTPA) tokens.

Because of the scope of this software environment, no attention is given to installation or basic configuration of these products. The tutorial demonstrates SSO configuration with the assumption that each product mentioned has been correctly installed and configured. More detailed requirements on the software used to develop this tutorial are provided at the beginning of each section.

The topics covered in this tutorial include:

- An overview of SSO methods
- Creating a Web SSO Configuration document (and the accompanying LTPA key) in Domino
- Enabling multi-server session authentication in the Server document
- Confirming FQDN settings in Domino
- Verifying your Domino LTPA configuration
- Exporting a WebSphere LTPA key
- Importing a WebSphere LTPA key into Domino
- Verifying your Domino/WebSphere Portal LTPA configuration

Section 2. Overview of single sign-on (SSO) methods

Introduction

Simply put, single sign-on gives end users the ability to access several different applications across servers in a domain without forcing the user to authenticate with each server individually. This requires a common framework with the ability to authenticate a user, to assign the correct access controls to the user, and to pass authentication information to different applications running on different machines.

There are several mechanisms for achieving a single sign-on framework in an environment involving Lotus and WebSphere technologies, including:

- HTTP headers
- LTPA
- X.509 certificates
- DSAPI

Before discussing the various methods of achieving single sign-on, some mention of the difference between SSO and single password authentication is in order. Single password authentication involves having the same credentials (user ID and password) stored in multiple places for use by different applications. In this scenario, the user is prompted to authenticate for each different application they access, but uses the same ID and password at each authentication prompt. Such a single password scenario usually involves careful, and sometimes troublesome, synchronization of multiple directories -- including the synchronization of passwords. The difficulty in setting up such synchronization, combined with the impact of multiple authentication prompts on the end user, often influences the implementation of a full single sign-on solution.

Implementing such a full SSO solution in an IBM Lotus environment is the focus of the rest of this tutorial.

SSO Option 1 - HTTP headers

HTTP headers is the first method of implementing SSO. Domino 6 supports the use of HTTP headers for passing user ID and password information, allowing you to use a third-party Web server as a front end to a Domino server. This feature is often described as the WebSphere Application Server (WAS) plug-in for Domino.

Plug-in is a somewhat misleading term because the feature is enabled using a Domino notes.ini setting. This is not the same as an authentication plug-in for WebSphere, and it does not involve a plug-in on Domino. Enabling the notes.ini setting simply tells Domino to accept the WebSphere-style user ID and password in the HTTP headers. The actual plug-in to support this SSO method is installed on the front-end Web server.

SSO Option 2 - LTPA tokens

IBM Light-Weight Third Party Authentication (LTPA) is the next method of implementing SSO. LTPA tokens, or cookies, provide a means to share authentication information among Lotus, WebSphere, and Tivoli application (Web) servers. A user authenticated by an application server will be authenticated automatically on other application servers in the same DNS domain providing the LTPA keys have been shared by all the applications.

LTPA utilizes a token that is stored as a cookie in the user's browser. The LTPA token contains data that uniquely identifies the user, such as the user's Distinguished Name (DN) and session expiration.

SSO Option 3 - X.509 certificates

X.509 certificates are another method of implementing SSO. Client authentication using X.509 certificates provides for two-way authentication between a browser user and a server using SSL and an LDAP directory. The LDAP client, specifically the browser installed on the user's workstation, must have a digital certificate (based on the X.509 standard). The X.509 certificate, which contains the user's credentials, is passed to the different Web servers that require the same X.509 authentication.

In order to authenticate users, the LDAP directory must contain the root certificate from the certificate authority and the client's public SSL certificate (key). This digital certificate is used to authenticate the LDAP client (browser) against the LDAP directory.

In order to use X.509 certificates, there must be an Internet certificate (PKI) infrastructure implemented where users can obtain X.509 certificates that are trusted by the LDAP directory service.

SSO Option 4 - DSAPI

The Domino Web Server Application Programming Interface (DSAPI) is the fourth (and final) method of implementing SSO discussed in this tutorial. DSAPI is a C API that allows you to create extensions to the Domino Web server.

DSAPI extensions, or filters, are notified whenever a particular event occurs during the processing of an HTTP request. The HTTP stack notifies the DSAPI filter(s) of the event, and the logic created by the DSAPI developer decides how to handle it. DSAPI is not actually an SSO method. It is part of a development toolkit that can be used to develop a custom SSO mechanism for Domino.

Choosing an SSO method

Choosing an SSO method can be a difficult task as each method has its own advantages and disadvantages. Pros and cons of the various SSO methods include:

- LTPA has the advantage of being supported by virtually all Lotus, WebSphere, and Tivoli Access Manager products. It is dependent on a common, trusted directory used for user credentials.
- X.509 certificates have the advantage of providing a two-factor authentication, but their drawback is the requirement to implement a Certificate Authority or pay a third party for the service. Managing

certificates on the client workstations can also be a challenge if users work from multiple machines.

- DSAPI has the advantage of complete flexibility in determining the manner of user authentication, however, it is specific to Domino. It allows for integration into any existing custom authentication scheme in any environment, but requires a good deal of expertise to develop the complex filters in a secure and scalable manner.
- HTTP headers have the advantage of relative ease of implementation, but they present a high degree of security risk if the channel between the front-end HTTP server and the back-end Domino server is not secure. They are most commonly implemented in conjunction with an enterprise access management system that centrally controls all Web resource access for an entire enterprise.

Because of its considerable strengths (and few weaknesses) LTPA is the most common SSO method utilized in mixed Lotus/WebSphere environments. Therefore, it is the method demonstrated in this tutorial.

Section 3. Enabling SSO for Domino-based technologies

Introduction

The first part of this tutorial discusses enabling SSO (using LTPA) in a collaborative environment based on Lotus Domino technologies. Specifically, this tutorial was created using the following software environment:

- A Lotus Instant Messaging and Web Conferencing 3.1 server running on Domino 6.0.2 CF1
- Lotus Instant Messaging and Web Conferencing 3.1 configured to use Domino-based LDAP (including the necessary Directory Assistance document)
- A Lotus Team Workplace 3.0.1 server running on Domino 5.0.12
- Lotus Team Workplace 3.0.1 configured to use Domino-based LDAP
- A Domino 6.0.2 CF1 server running Lotus Domino Web Access

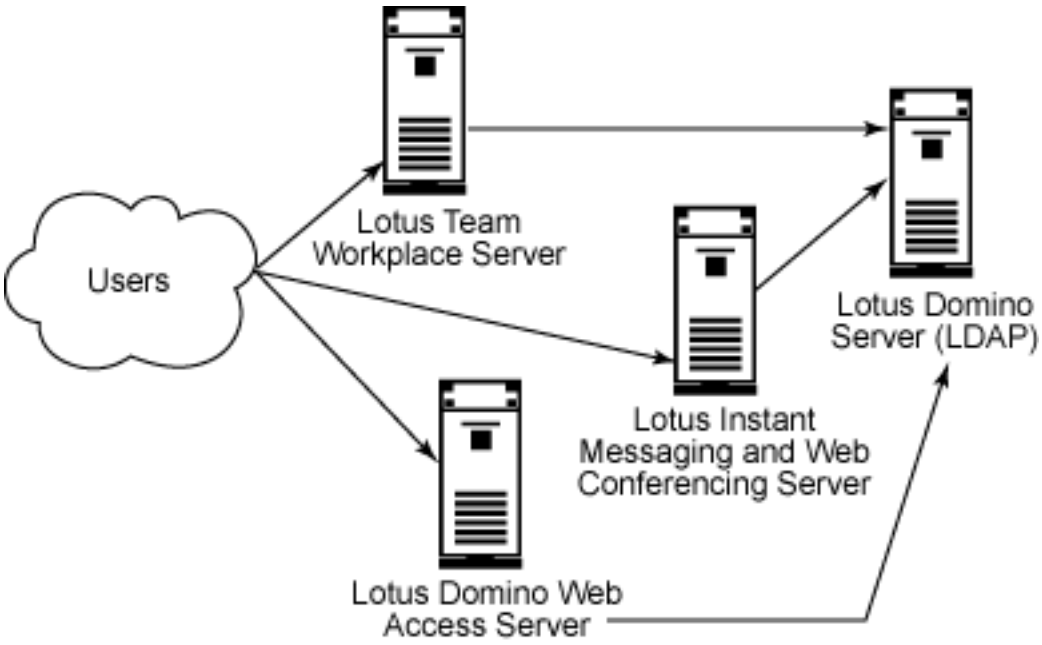
All servers are in the same DNS domain and are using the same Domino LDAP directory.

Implementing SSO in Domino using LTPA involves the following steps:

- Creating a Web SSO Configuration document and an LTPA key
- Enabling multi-server session authentication
- Verifying your FQDN settings
- Verifying your Domino LTPA configuration

Server topology diagram

The following diagram represents the server topology for this portion of the tutorial. There are three Domino application servers, all of which authenticate against a fourth Domino LDAP server.



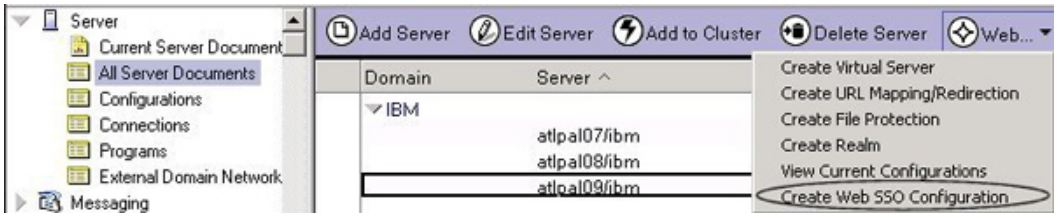
Creating a Web SSO Configuration document and an LTPA key

The first step in enabling SSO in a Domino environment is to create a Web SSO Configuration document (and the corresponding LTPA key). You should note that in Domino 6, you can configure SSO using only Internet Site documents. However, since Lotus Team Workplace 3.0.1 requires Domino 5.0.x, you must configure SSO using Web SSO Configuration documents. To create a Web SSO Configuration document in the Domino Directory:

1. Use the Domino 6 Administrator client to connect to the domain's primary directory server (this should be a Domino 6 server).
2. Select the Configuration tab.

3. Expand Server and select All Server Documents.

4. Click Web and select Create Web SSO Configuration:



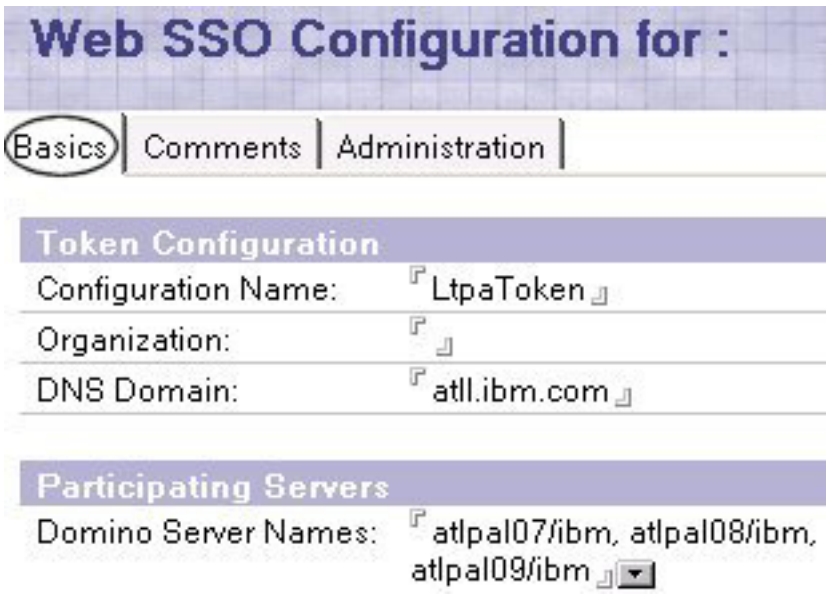
5. Enter values in the following fields in the Token Configuration section of the document:

	Field label	Sample value	Description
	Configuration Name	LtpaToken	SSO configuration name **Note**: The Configuration Name field is editable in Domino 6. Changing the name of the token in this field does not change the token name when it is generated by Domino. For compatibility with Lotus Team Workplace, use the default name of LtpaToken.
	Organization	blank	Organization name **Note**: In order for the Web SSO document to appear in the Web SSO Configurations view, you must leave this field blank.
	DNS domain	.atll.ibm.com	Enter the DNS domain for which the tokens will be generated. The servers enabled for single sign-on must all belong to the same DNS domain.

6. Enter values in the following field in the Participating Servers section of the document:

Field label	Sample value	Description
Domino server names	atlpal07/ibm, atlpal08/ibm, atlpal09/ibm	Enter the names of the servers that will be participating in single sign-on. **Note**: Groups, wildcards, and the names of WebSphere servers are not allowed in this field. Only Domino servers can be listed as participating servers in the Server Names field.

Your completed Web SSO Configuration document should resemble the following:



7. Click Keys and choose Create Domino SSO Key:

Once the SSO key has been successfully generated, you will receive a

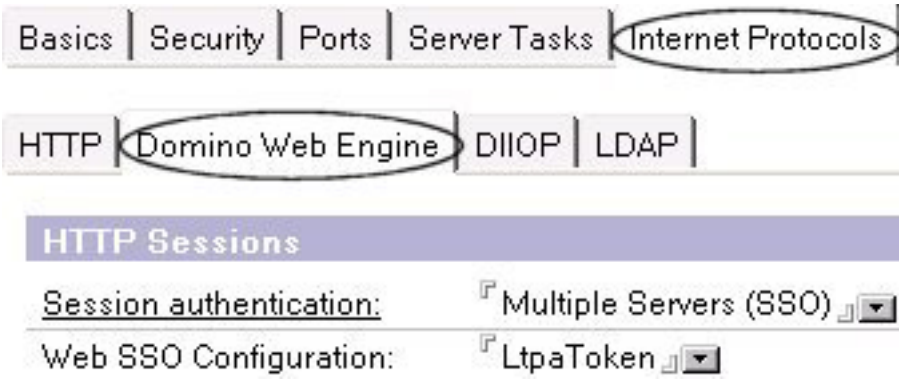
confirmation dialog:

8. Save and close the Web SSO Configuration document.

Enabling multi-server session authentication in the Server document

Once you've created your Web SSO Configuration document, you must enable multi-server authentication in each server's Server document. To enable multi-server authentication:

1. Use the Domino 6 Administrator client to connect to the domain's primary directory server (this should be a Domino 6 server).
2. Select the Configuration tab.
3. Expand Server and select All Server Documents.
4. Choose an applicable Server document and click Edit Server.
5. Select Internet Protocols - Domino Web Engine:



6. Enter values in the following fields in the HTTP Sessions section of the document:

	Field label	Sample value	Description
	Session authentication	Multiple Servers (SSO)	Multiple Servers allows a Web user to log on once to a Domino server,

			then access any other Domino server in the same domain without logging on again. Groups, wildcards, and the names of WebSphere servers are not allowed in this field. Only Domino servers can be listed as participating servers in the Server Names field.
	Web SSO Configuration	LtpaToken	Enter the name of the Web SSO configuration document created previously.

7. Save and close the Server document.

8. Replicate the Domino directory with the other servers in your domain. **Important note**: Because Lotus Team Workplace relies on the Domino 5.0.x directory template, the replication settings for the servers in your domain should be adjusted so that your servers do not receive design elements from, or send design elements to, the Lotus Team Workplace server. The Lotus Team Workplace server should also be configured not to replicate Domino directory design elements with any server in your domain. For more information on adjusting replication settings, see the Domino Administrator help database (help6_admin.nsf).

9. Restart the HTTP task on each of your servers using the command: `tell http restart`.

Verifying FQDN settings in Domino

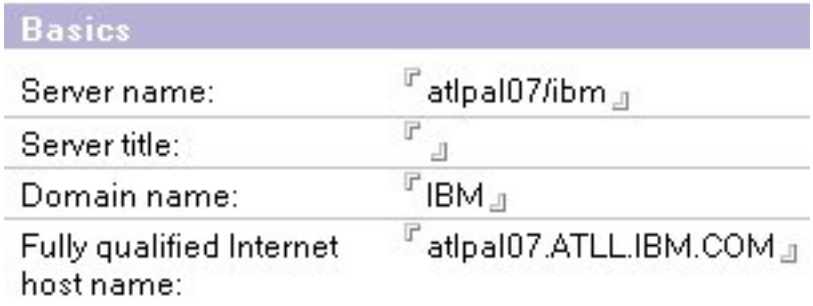
Since SSO relies on domain names in order to function properly, the final step in configuring SSO for a Domino-based environment is to verify your FQDN settings. In order for Lotus collaborative applications to share credentials across servers in a domain, all of your applications must be aware of the fully qualified domain name of each server. To verify FQDN settings in Domino:

1. From the Domino 6 Administration client, select the Configuration tab.

2. Expand Server and select All Server Documents.

3. Select an applicable Server document and click Edit Server.

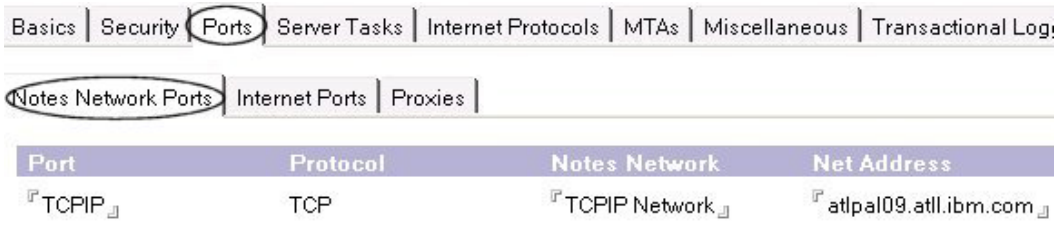
4. On the Basics tab of the Server document, verify that Fully qualified Internet host name is correct:



Note:The domain suffix in this field (and all other fields in this section of the tutorial) must match the domain name entered in the Web SSO Configuration document you created previously.

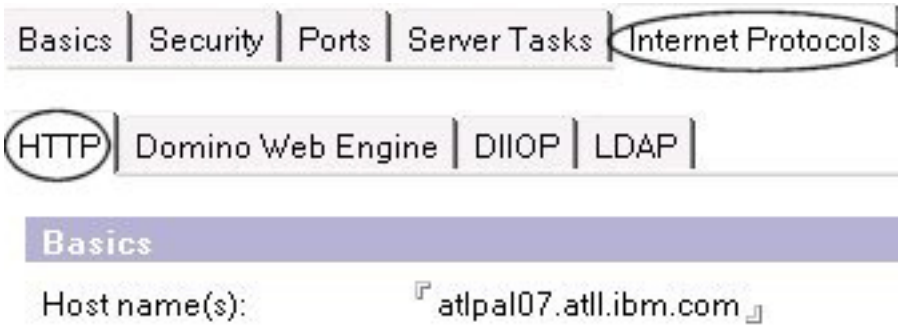
5. Switch to the Ports tab of the Server document.

6. On the Notes Network Ports tab, verify that the Net Address for the TCPIP port contains the fully qualified server name:



7. Switch to the Internet Protocols tab of the Server document.

8. On the HTTP tab, verify that Host name(s) contains the fully qualified name of the server:



9. Save and close the Server document.

10. Repeat the steps above for each server in your domain participating in SSO.

11. Replicate the Domino directory changes to each server in your domain.

12. If you only changed the Host name(s) field on the Internet Protocols tab of the Server documents, restart the HTTP task on each affected server. If you changed other fields as well, restart each server.

Verifying your Domino LTPA configuration

Once you have completed your SSO configuration, you should verify that SSO is working as expected. To verify your SSO settings:

1. Launch your browser and enter the fully qualified URL for accessing one of your application servers. Since SSO relies on domain names in order to correctly pass authentication credentials, you must enter the fully qualified name of the server for each URL you enter or SSO will not function properly. For example, to open a Lotus Domino Web Access mail file enter: `http://atlpal09.atll.ibm.com/mail/jdoe.nsf`, or to open a Lotus Team Workplace, enter: `http://atlpal08.atll.ibm.com/qptestdb`.

2. Instead of receiving the application's login dialog, your browser should display the Server Login form:

Note: If you first log into the Lotus Team Workplace server, you will receive the QuickPlaceLoginForm you mapped in domcfg.nsf.

3. After entering your credentials and logging into the server, enter the following command in your browser's address line:

```
JavaScript:alert(document.cookie)
```

You should receive a pop-up window displaying your LTPA token:

4. Enter the URL to access another of the servers participating in SSO. You should be logged into the server automatically.

5. If you receive the Server Login form again, you can use the command in step 3 to verify that each server in your domain in generating LTPA tokens. Simply close and reopen your browser after each login (to start a new session) and enter the JavaScript command to display the token. If each server is correctly generating tokens, you should see LtpaToken= in the dialog.

Section 4. Enabling SSO integration with WebSphere Portal

Introduction

The second part of this tutorial discusses enabling SSO in a collaborative environment that includes both Lotus software and WebSphere Portal. Specifically, this second part of the tutorial was created using the following software environment:

- A Lotus Instant Messaging and Web Conferencing 3.1 server running on Domino 6.0.2 CF1
- Lotus Instant Messaging and Web Conferencing 3.1 configured to use Domino-based LDAP (including the necessary Directory Assistance document)
- A Lotus Team Workplace 3.0.1 server running on Domino 5.0.12
- Lotus Team Workplace 3.0.1 configured to use Domino-based LDAP
- A Domino 6.0.2 CF1 server running Lotus Domino Web Access
- **Note**: All servers are in the same domain
- A WebSphere Portal version 5 server installed and configured to use

either a Domino LDAP directory or a non-Domino LDAP server (this includes the installation of WebSphere Application Server and WebSphere Application Server Enterprise)

- Lotus Instant Messaging and Web Conferencing, Lotus Team Workplace, and Lotus Domino Web Access portlets configured on the Portal Server
- Each Lotus product has the necessary Directory Assistance documents in place to authenticate with the LDAP server used by Portal (if your using a non-Domino LDAP directory)
- The Portal Server has security properly configured so that SSO has been enabled and an LTPA key has been created (see Resources for a link)

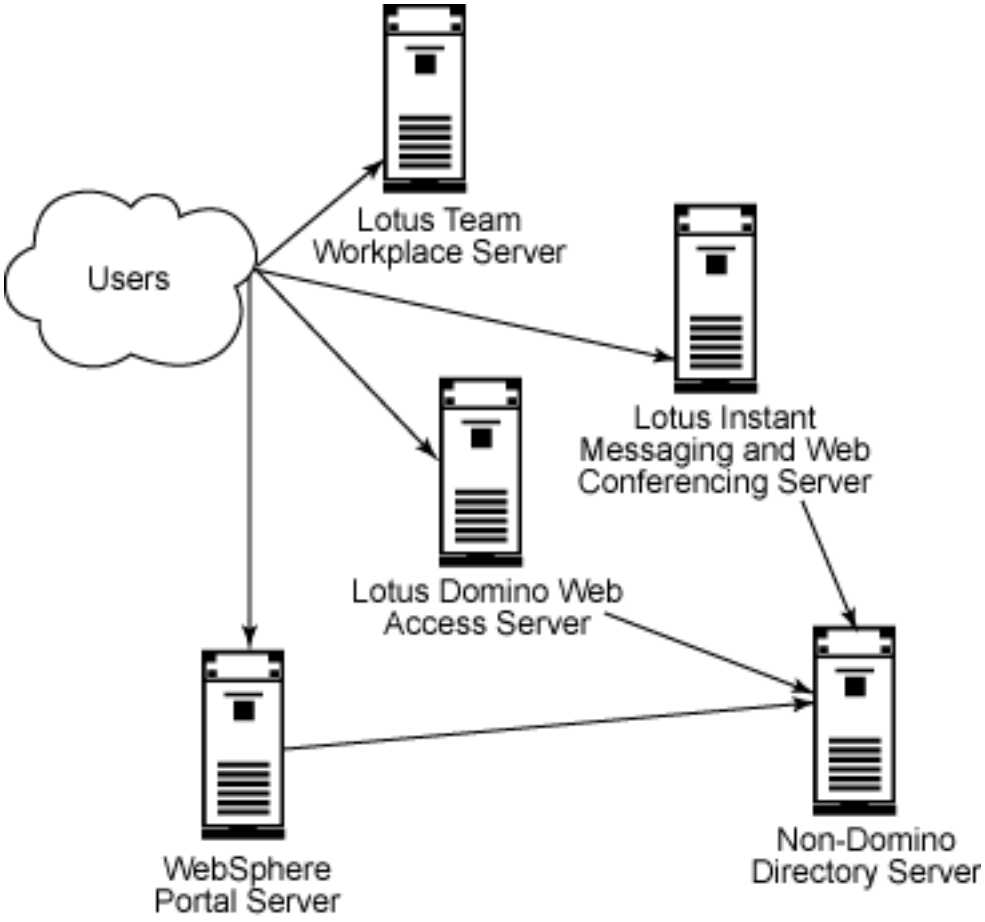
Implementing SSO in a Domino/WebSphere Portal collaborative environment (using LTPA) involves the following steps:

- Exporting the LTPA key from WebSphere
- Importing the LTPA key into Domino
- Verifying your Domino/WebSphere Portal LTPA configuration

Server topology diagram

The following diagram represents the server topology for this portion of the tutorial. A WebSphere Portal Server, which authenticates against a non-Domino LDAP directory, has been added. Directory Assistance documents have also been added to the Domino directory to allow the Domino servers to authenticate against the non-Domino LDAP directory as well as the normal Domino directory.

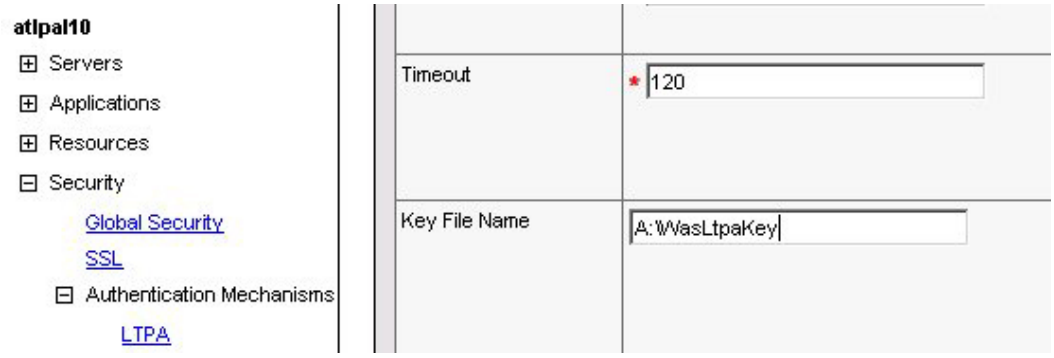
It is important to note that the user IDs within the new non-Domino LDAP directory must map to user IDs in the original Domino directory used in the first part of this tutorial. This is needed so that users who authenticate against the non-Domino LDAP directory will still have access to Domino-based resources that have the Domino user ID listed in their Access Control Lists. Alternatively, these Domino Access Control Lists can be updated to allow the new LDAP user IDs access. If the Domino LDAP directory was utilized by WebSphere Portal instead of introducing a new LDAP directory, such a name mapping effort would not be required.



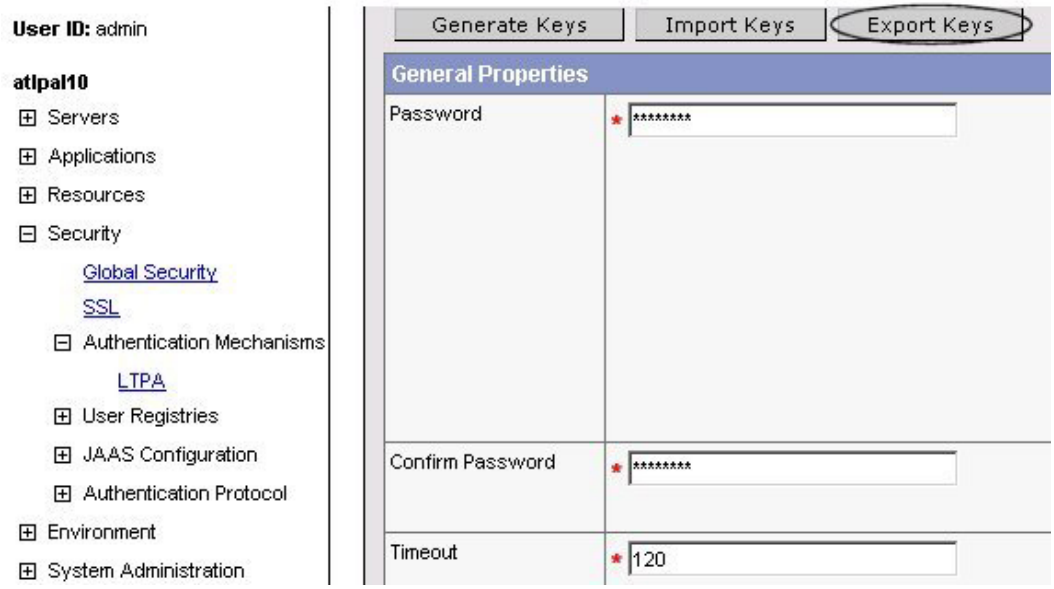
Export the LTPA key from WebSphere

Because Domino and WebSphere create LTPA keys differently, you must ensure that all the servers in your environment will pass LTPA-based credentials in a compatible manner. Domino can create LTPA tokens using a WebSphere LTPA key, however, the reverse is not true. Therefore, before configuring your collaborative environment for SSO using the LTPA key from your WebSphere Portal environment, you must first export the key for use by Domino. To export the LTPA key from WebSphere:

1. From the WebSphere Application Server version 5 Administrative console, expand Security - Authentication Mechanisms and select LTPA.
2. Enter a value in KeyFileName, for example: `A:\wasLTPAKey`:



3. Insert a floppy disk and click Export Keys:



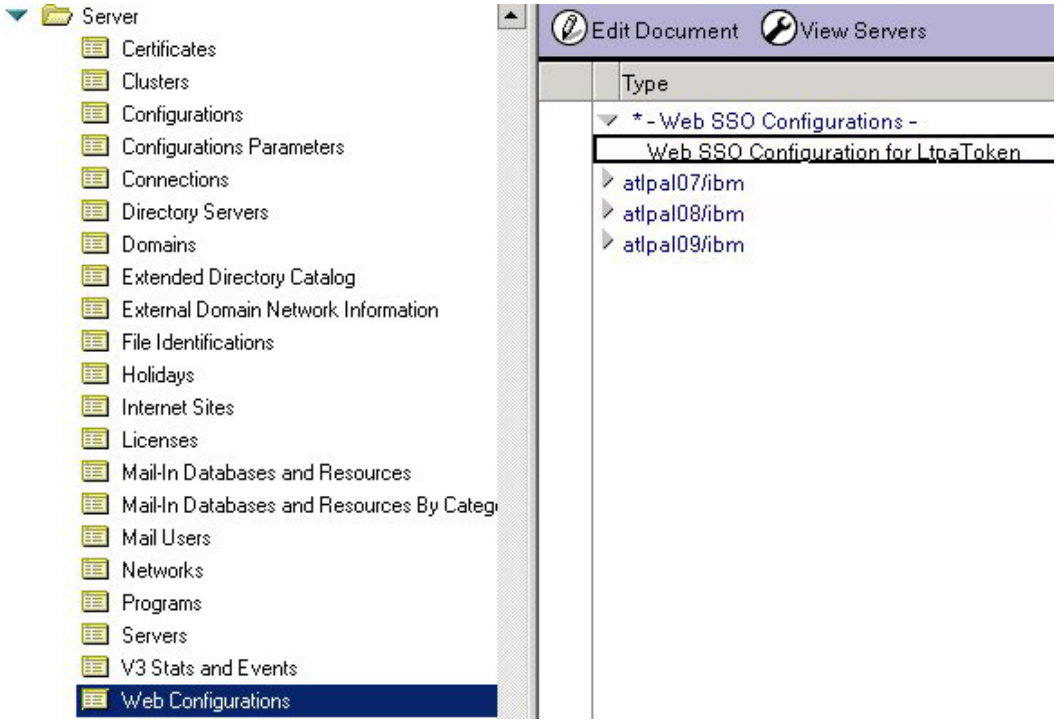
4. Remove the floppy disk and insert it into the drive on the Domino 6 primary directory server.

Import the LTPA key into Domino

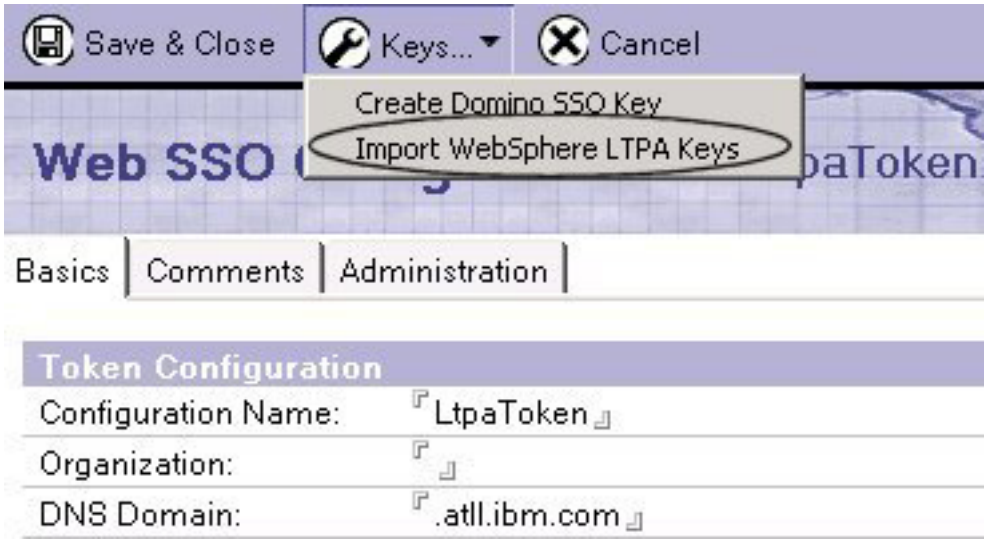
After exporting the LTPA key from WebSphere, your next step is to import the key into the Domino directory. To import the LTPA key:

1. From the Domino 6 Administration client, select the Configuration tab.
2. Expand Server and select All Server Documents
3. Click Web and choose View Current Configurations:

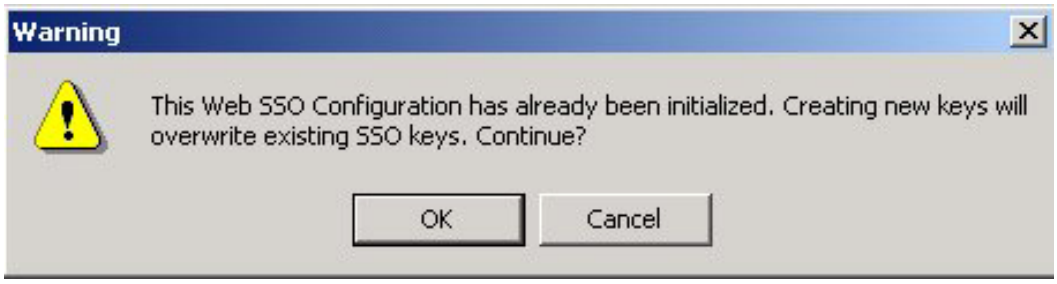
4. In the Web Configurations view, expand Web SSO Configurations, select your Web SSO Configuration document, and click Edit Document:



5. Click Keys and select Import WebSphere LTPA Keys:



6. When prompted to overwrite your existing key, click OK:



7. Enter the path to the LTPA key you saved to the floppy in Section 3, for example: `A:\wasLTPAKey`.

8. When prompted, enter the password for the LTPA key and click OK.

9. When the key has been successfully imported, you will receive a confirmation dialog:

10. Save and close the Web SSO Configuration document.

11. Replicate the Domino directory with the other servers in your domain.

12. Restart the HTTP task on each server configured for SSO by entering the command: `tell http restart`.

Verifying your Domino/WebSphere Portal LTPA configuration

Once you have completed your SSO configuration, verify that SSO is working as expected. To verify your SSO settings:

1. Launch your browser and enter the fully qualified URL for accessing your WebSphere Portal. For example: `http://atlpal08.atll.ibm.com:80/wps/myportal`.

2. Log into the Portal Server as a user with a page containing at least one Lotus collaborative portlet.

3. After entering your credentials and logging into the Portal Server, enter the following command in your browser's address line:

```
JavaScript:alert(document.cookie)
```

   You should receive a pop-up window displaying your LTPA token. This LTPA token should differ from the token created by using the Domino LTPA key:

4. After logging into the Portal Server, switch to the page containing the Lotus portlet(s). You should see the portlet information display without being prompted to enter your credentials again.

Section 5. Wrap up

Summary

Implementing single sign-on in a collaborative software environment can be a challenge to administrators, but the ease provided to users greatly outweighs the administrative burden. This tutorial showed you how to implement single sign-on in a Domino collaborative environment and in a Lotus/WebSphere Portal collaborative environment.

Enabling LTPA-based SSO in a Domino environment consisted of:

- Creating a Web SSO Configuration document (and the accompanying LTPA key) in Domino
- Enabling multi-server session authentication in the Server document
- Confirming FQDN settings in Domino
- Verifying your Domino LTPA configuration

Enabling LTPA-based SSO in a WebSphere Portal/Domino environment consisted of:

- Exporting a WebSphere LTPA key
- Importing a WebSphere LTPA key into Domino
- Verifying your Domino/WebSphere Portal LTPA configuration

Resources

Learn

- For more information on single sign-on, see the Open Group's Web site.
- For more detailed information on single sign-on in IBM software products, see the Redbook, "Lotus Security Handbook."
- For more information on configuring security in WebSphere Portal, and on enabling SSO and creating an LTPA key, see the WebSphere Portal product documentation.
- For more information on security in WebSphere Application Server version 5, see the Redbook, "IBM WebSphere V5.0 Security WebSphere Handbook Series"
- Stay current with developerWorks technical events and Webcasts.

Get products and technologies

- Build your next development project with IBM trial software, available for download directly from developerWorks.

Discuss

- Participate in the discussion forum for this content.

About the authors

Jeffrey Slone
Jeffrey Slone is a Senior Curriculum Developer with the Lotus Software Performance and Learning Group. As a part of the Lotus Engineering Test, Product Introduction, and Technical Support group at IBM, Mr. Slone has developed and delivered training on Lotus products ranging from Domino to Lotus Workplace Messaging. Mr. Slone is a CLP in Notes and Domino System Administration. Contact him at jeffrey_slone@us.ibm.com

---

William Tworek
William Tworek is a Project Leader with the International Technical Support Organization, working out of Westford, Massachusetts. He provides management and technical leadership for projects that produce technical materials (including IBM Redbooks) on various topics involving IBM Software technologies. Prior to joining the ITSO, he was an IT Architect in the consulting industry working for Andersen Consulting/Accenture, followed by IBM Software Services for Lotus. His areas of expertise include collaborative technologies and business portals, system integration, and systems infrastructure design. Contact him at william_tworek@us.ibm.com.