RSA ClearTrust Ready Implementation Guide
for Portal Servers and Web-Based Applications

Last Modified March 15, 2005

1. Partner Information

| Partner Name	IBM Corporation
Web Site	www.ibm.com
Product Name	IBM Lotus Team Workplace
Version & Platform	6.5.1, Windows 2003 Enterprise
Product Description	IBM Lotus Team Workplace (QuickPlace) is a business-ready, self-service work space expressly designed for team collaboration. With Lotus Team Workplace, users can instantly create secure work spaces on the Web, providing them with a "Place" to coordinate, collaborate and communicate on any project or ad hoc initiative.
Product Category	Internet / Intranet

2. Contact Information

	Sales contact	Support Contact
Phone	800-IBM-4YOU	800-IBM-SERV
Web	www.lotus.com/products	www.ibm.com/software/lotus/support

3. Solution Summary

Feature	Details
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	No
API-level Authorization Support (RuntimeAPI)	No
User Management (AdminAPI)	No

4. Integration Overview

To achieve single-sign-on with Lotus Team Workplace, the RSA ClearTrust Agent for Domino is installed on the Domino server. The agent is then configured to protect all Team Workplace pages, as well as any other desired pages. The Domino server is configured for multi-server single-sign-on, and authentication enabled. After this, users authenticated via either a ClearTrust authentication mechanism, or Domino's internal authentication, will be able to access all protected Domino assets.
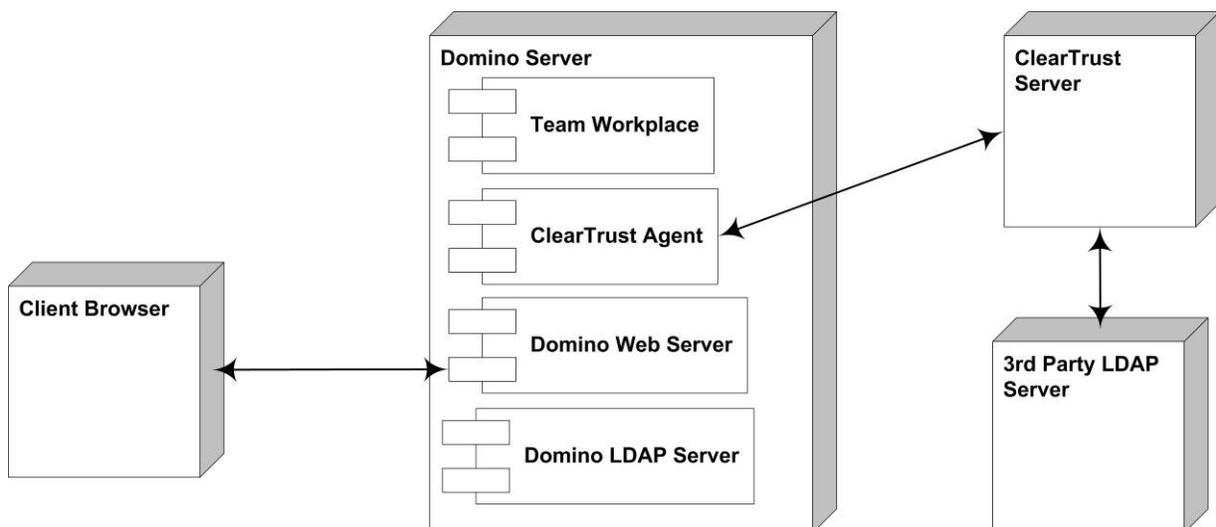
5. Product Requirements

Hardware requirements

Component Name: Lotus Domino	
Memory	256Mb
Hard Drive	1Gb (1.5Gb recommended)

Software requirements

Component Name: Lotus Domino	
Operating System	**Version (Patch-level)**
AIX	5.1, 5.2
OS/400	VSR1, VSR2, i5OS VSR3
Windows 2000	Server, Advanced Server
Windows 2003	Server, Enterprise
Solaris	8, 9
Red Hat Enterprise Linux	2.1

Component Name: Lotus Team Workplace	
Operating System	**Version (Patch-level)**
AIX	5.1, 5.2
OS/400	VSR1, VSR2, i5OS VSR3
Windows 2000	Server, Advanced Server
Windows 2003	Server, Enterprise
Solaris	8, 9

Component Name: RSA ClearTrust Agent for Domino	
Operating System	**Version (Patch-level)**
AIX	5.1, 5.2
Windows 2003	Server
Domino	6.5.1IF1

6. Product Configuration

This section provides instructions for integrating the partners' product with RSA ClearTrust. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components, including the ClearTrust servers and Entitlements Manager, need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

In order to achieve this integration, the following steps are necessary:

- Install & Configure Domino Server
- Install & Configure RSA ClearTrust Agent for Domino
- Install & Configure Lotus Team Workplace

### Installation & Configuration of the Domino Server

Using the Domino 6.5.1 installation media, start the setup program. During the setup process, customize as necessary for your requirements, but be sure to choose to install the **Domain Enterprise Server**.

After the installation of the base server, install the Interim FixPack 1. Lotus Team Workplace (LTWP) requires Domino 6.5.1 IF1. Also, if you do not already have a Domino Administrator client already installed, you should install one at this time.
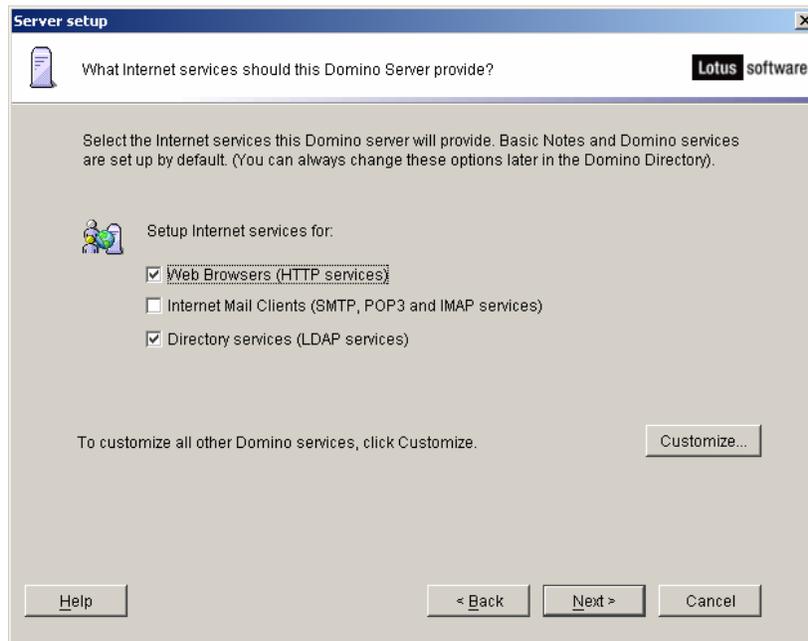
Configuration

Once the basic server and IF1 are installed, start the Domino server. When you start it for the first time, you will be prompted to configure the server. Unless you have a pre-existing Domino installation that you are integrating this server into, select the stand-alone server option.

During the setup process, if you save an external copy of the administrator's id file, it will be easier to find from the client.
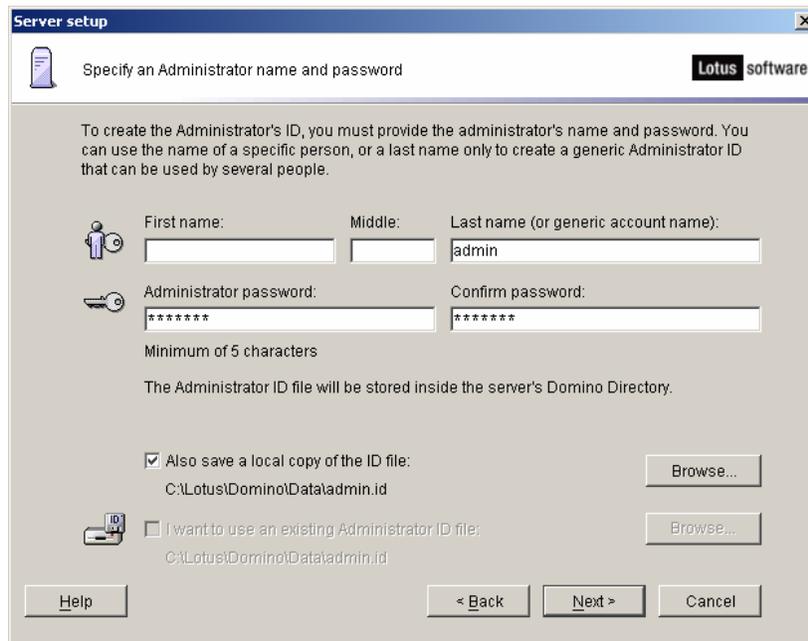
Also, be sure to select the **Web Browsers (HTTP services)** option, since it is not selected by default.

After this configuration process ends, start your Domino server, and ensure that it starts up correctly. You should also use the admin.id file created above to enable you to administer the server from a Domino Administrator.

Installation & Configuration of the RSA ClearTrust Agent for Domino

Prior to beginning installation of the RSA ClearTrust Agent, stop the Domino server. Then, start the agent setup program. Ensure that the agent detects the correct installation directory for Domino.

Make sure that the SSL settings entered in this process match the settings in your RSA ClearTrust servers' configuration files. For more information, consult the RSA ClearTrust Agent for Domino's Installation & Configuration Guide.

During the installation procedure you will be prompted for the address of a Dispatcher server, and an Entitlements server. While the dispatcher's address is required, the Entitlements server's address is required only if it is not connected to a dispatch server.

Remember the web server name you enter during the setup, as you will need to enter the exact same name into the Entitlements manager.

Installation & Configuration of Lotus Team Workplace

To begin installation, stop the Domino server, and then run the LTWP setup program. Ensure that it detects the correct Domino installation directory. After the installation concludes, a setup program will run. During the configuration, you will be asked for credentials for an administration account.

Note: Ensure that this user name is unique among user names from any LDAP stores you will attach LTWP to. LTWP authenticates to a separate data store by default, and will not be able to distinguish between users if there is overlap.


Once LTWP is installed and configured, restart Domino, and ensure that it starts successfully. Next, Domino must be configured for multi-server single-sign-on according to the instructions in the Lotus Team Workplace *Administrator's Guide.*

Disable ClearTrust DSAPI Filter

Note: There is a known issue with authenticating via the QuickPlaceLoginForm while the agent is installed. While using RSA ClearTrust Agent v4.6 for Domino, authenticating a user via QuickPlaceLoginForm may cause the Domino server to exit. See Known Issues for more information.

Because of this issue, disable the RSA ClearTrust DSAPI filter for further configuration (it will be re-enabled later). To do this, start the Domino Administrator, and open up the server document for the server you created for LTWP. Under Internet Protocols, on the HTTP tab, you will see the DSAPI section halfway down on the right hand side of the document. Remove the ct_domino65_agent.dll entry, but make note of it, as you will replace it later. Then restart the Domino server.
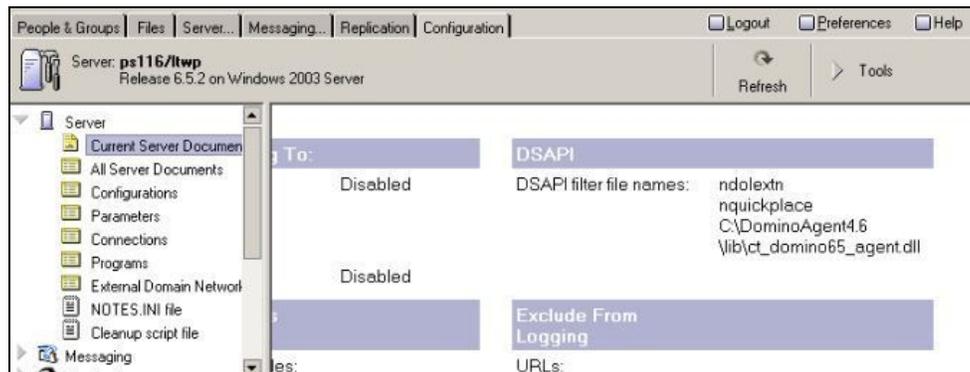
Enable Domino SSO

Once the server restarts, start configuring the LTWP installation.

- Create a Web SSO Configuration document, or add the LTWP server onto an existing one. When creating the SSO document, this guide used a Domino SSO Key.
- Create a mapping form to map authentication to the QuickPlaceLoginForm.
- Restart the server.

1. Use the Domino Administrator and open the hub server:
   a. Select the Configuration tab.
   b. In the navigation pane, choose Server.
   c. Click the Web button, and select Create Web SSO Configuration.
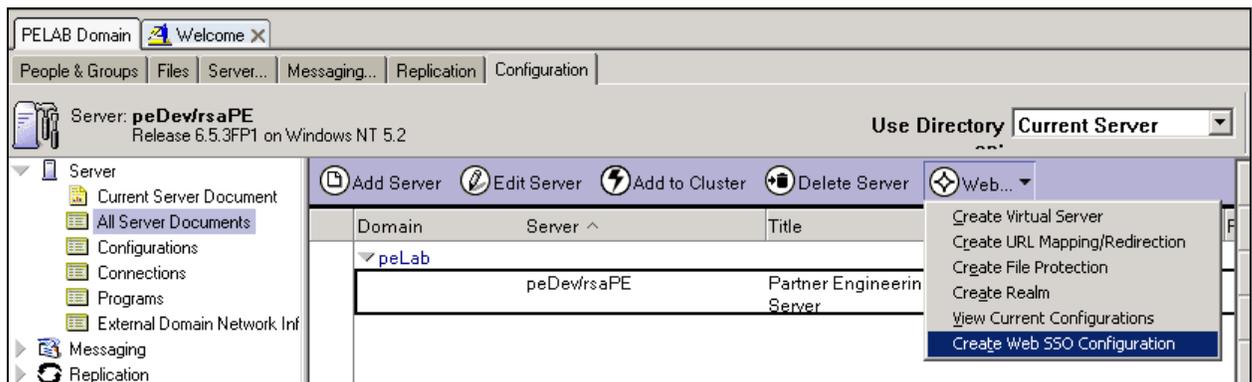
Note: If you have a mixed R5/D6 environment, you will need to use the **Create Web R5 (SSO configuration)** button found in the action bar of Server documents. If you have a pure D6 environment, you can use the method outlined here or use Internet Site documents. For more information, see the IBM Redbook.

2. In the SSO Configuration document, make the following entries

   a. Select LtpaToken.

   b. Leave the Organization field empty.

   c. Select and add all of the servers from the directory to the Domino Server Names field (this uses the proper hierarchical name for each server).

   d. Enter the Internet domain that all of your servers share (you should precede this name with a leading period; Domino 6 will insert it when the document is saved if you forget).

   e. Select **Keys** from the action bar and click **Create Domino SSO Key**. You will receive a confirmation when it has been successfully created.


   f. Save and close the Web SSO document.

> **Note:** The Web SSO document is automatically encrypted with the user's ID that created it. If another administrator subsequently needs to edit the document, the administrator will receive a warning about the document being encrypted and will not be able to edit it.
>
> If this happens, delete the document and create a new one so that you can add all the servers to the document.

3. Open each Server document and make the following changes to the Internet Protocols - Domino Web Engine tab:

    a.   Session authentication: Multiple Servers (SSO)

    b.   Web SSO Configuration: LtpaToken.

    c.   Then Click Save and Close.

4. Open domcfg.nsf. If domcfg.nsf does not exist you will need to create it. See the Domino documentation for information on how to do this.
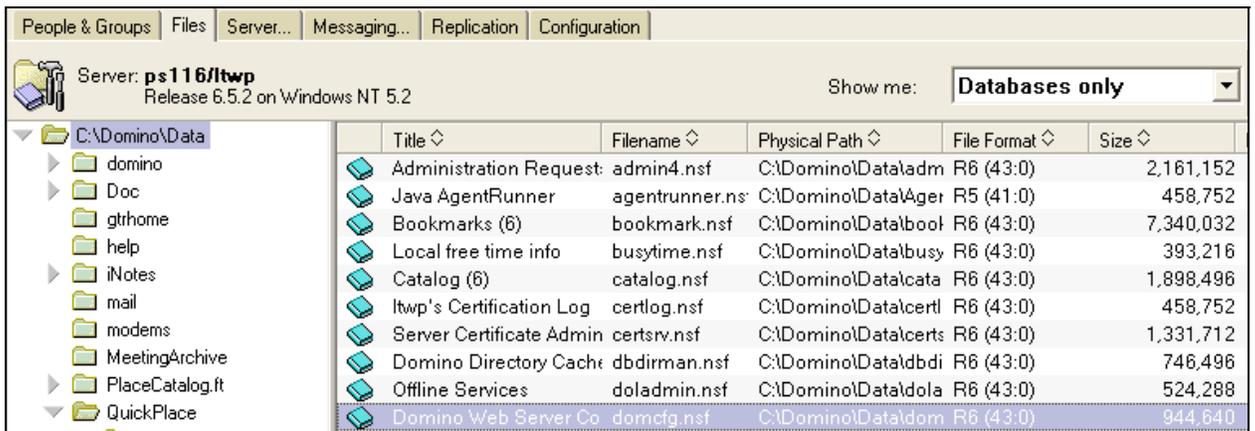
5. Create a mapping form to map authentication to the QuickPlaceLoginForm.
   a. Applies To: All Web Sites/Entire Server
   b. Target Database: QuickPlace/resources.nsf
   c. Target Form: QuickPlaceLoginForm
   b. Then Click Save and Close.

6. Open the notes.ini file located in the Domino install directory and add the following parameter QuickPlaceUseDSAPIDNs=1

7. Restart both servers.

Point Team Workplace at Domino User Store

Open up LTWP home page in a browser, and login as the LTWP administrator created during installation. Under **Server Settings**, select **User Directory**, then **Change Directory**. Select Domino Server as the type, and point it at your Domino server. Then, select to disallow new users. Save your changes, and log out of LTWP. This is necessary so LTWP will pick up the Domino users.
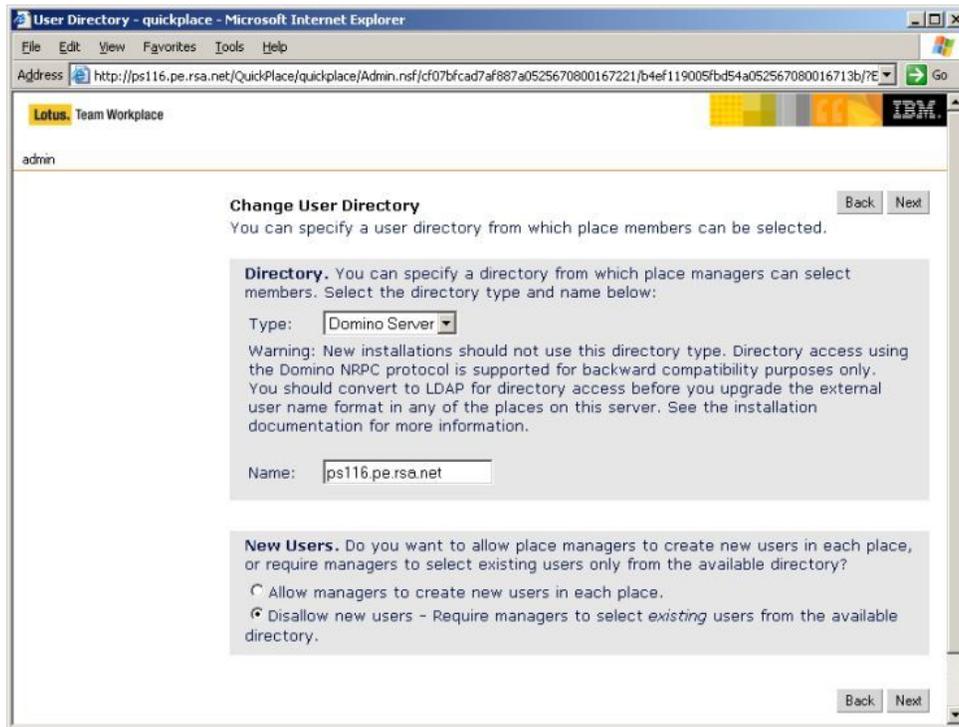
By default, LTWP uses Cloudscape as its user repository. To ease the SSO process, it should be using only Domino users. By pointing LTWP at Domino, and not allowing new user creation, the only user in Cloudscape will be the LTWP administrator created during installation. The RSA ClearTrust repository, for the purposes of this implementation guide, will be kept separate from the Domino user repository, so those two will need to be separately synchronized.

Log back into LTWP as the LTWP administrator. This time, select **Security** under **Server Settings**. In the administrator section, click **Add**, and add a Domino user as LTWP administrator.
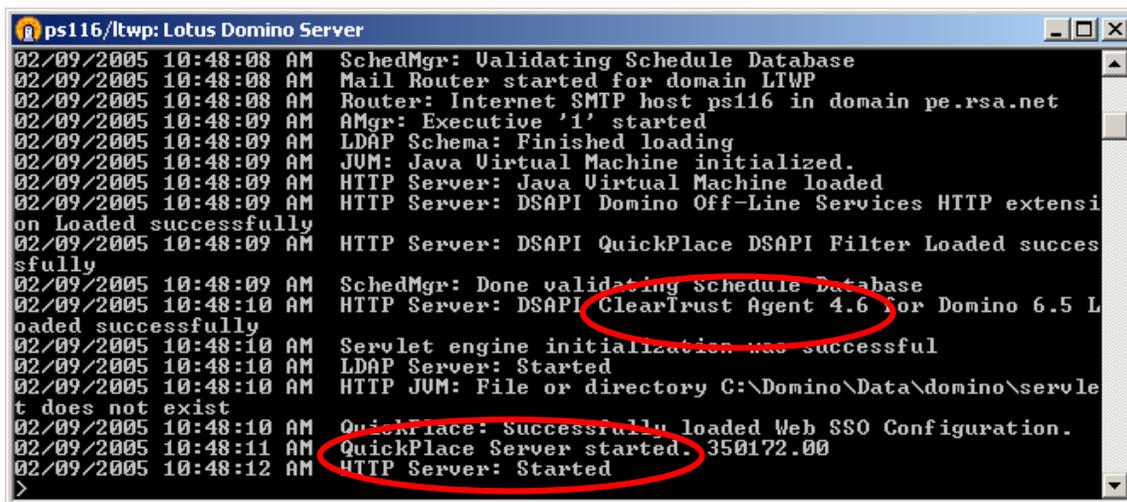
Cleaning Up

Now, re-insert the ClearTrust DSAPI filter in the server document. Then, restart the server one last time.

> Note: The RSA ClearTrust DSAPI filter should be the last filter in the list. Authentication will not behave correctly otherwise.

Testing the Setup

When Domino starts, you should be able to see startup notices for LTWP and RSA ClearTrust DSAPI filters. Note that the LTWP message will show up as QuickPlace.


Using the RSA ClearTrust Entitlements Manager, create entries for the Domino server, and a sample Domino user. Then define resources for /*homepage.nsf*, and */QuickPlace* on that server, and entitlements for your sample user. Remember that in Domino, you must protect the database and views separately (e.g. /abc, and /abc/*). Finally, add entitlements for the sample user for the Domino server resources.

From a new browser, browse to http://servername.domainname. You should see the Domino homepage. Then go to /homepage.nsf, which should show you the same page, after authentication via RSA ClearTrust.
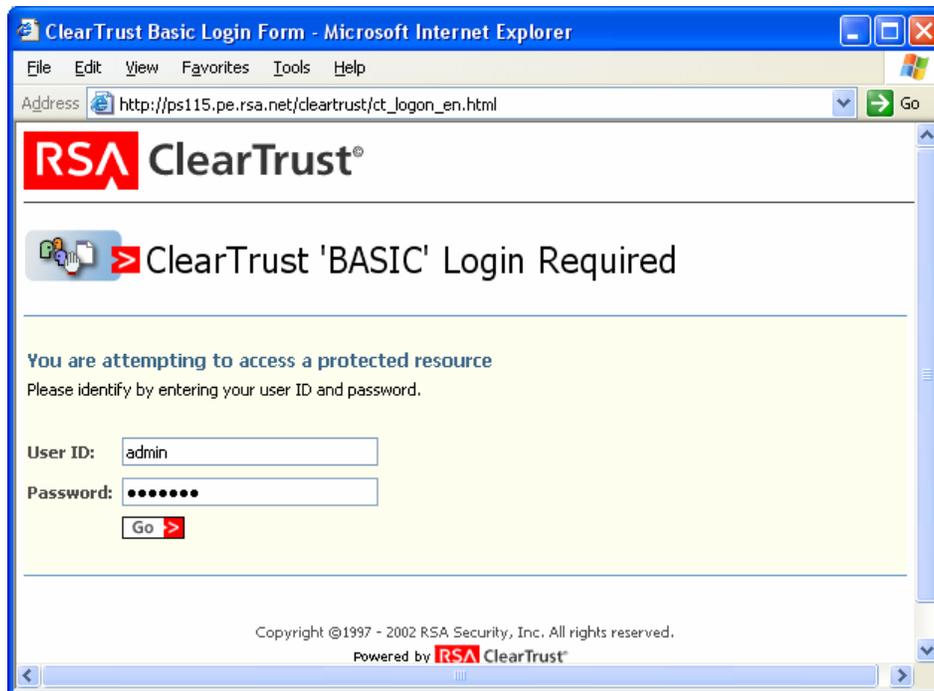
When you navigate from there to the QuickPlace home page (/QuickPlace), you can see that you are automatically recognized by the RSA ClearTrust agent.
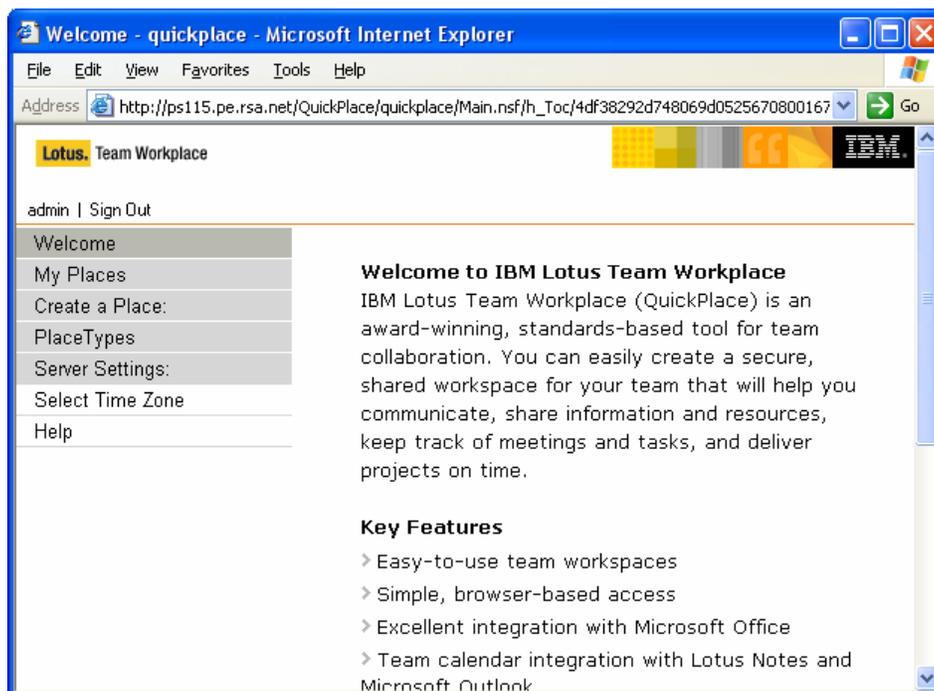
As a last check, navigate to the web administration database (/webadmin.nsf). You will Notice that even though the web admin database is protected by Domino, and not by RSA ClearTrust, the Domino agent supplies the credentials to Domino's native authentication, and the user is recognized from his RSA ClearTrust SSO cookie.
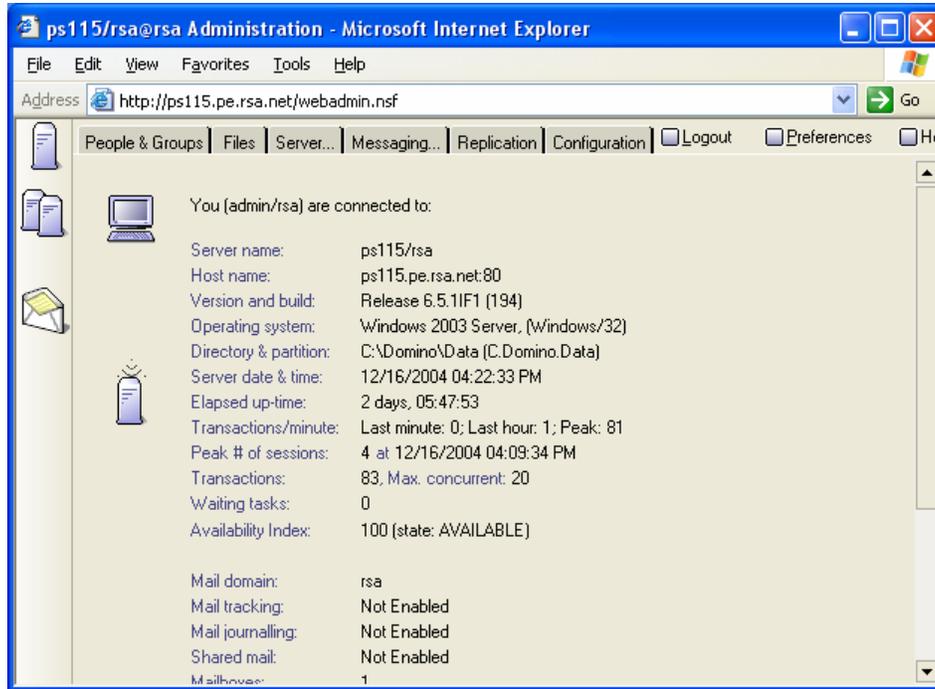
7. Certification Checklist for Portal Servers and Web-Based Apps

Date Tested: February 7, 2005

Product	Tested Version
RSA ClearTrust	5.5.2, 5.5.3
Team Workplace	6.5.1
Domino	6.5.1IF1, 6.5.2, 6.5.3
ClearTrust Agent for Domino	4.6

Test Case	Result
Product Characteristics for SSO Support	
Application/Portal is web-based, and supports access by a standard HTTP-based browser	P
Application/Portal runs on Web Server Platform supported by RSA ClearTrust	P
Application/Portal login interface can be modified or replaced	P
Application/Portal can extract user information from RSA ClearTrust session cookie	P
Application/Portal can extract user information from HTTP Headers	N/A
Application/Portal can extract authentication type from RSA ClearTrust session cookie	N/A
Application/Portal can extract authentication type from HTTP Headers	N/A
Application/Portal can perform SSO with other RSA ClearTrust-supported Web Server	P
Login - General	
HTTP basic authentication	P
Forms based	P
Forms based w/ URI retention	P
Login – Basic Authentication	
Access Denied for unauthorized user	P
Successful login for authorized user	P
Successful recognition of identity/personalization in 3rd Party Product	P
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	P
Login –Graded Authentication	
Access Denied for unauthorized user	N/A
Successful login for authorized user	N/A
Successful recognition of identity/personalization in 3rd Party Product	N/A
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	N/A

SWA / ATB   P=Pass or Yes   F=Fail   N/A=Non-available function

8. Known Issues

Authentication Via QuickPlaceLoginForm May Cause Domino Server Exit

While using RSA ClearTrust Agent v4.6 for Domino, authenticating a user via QuickPlaceLoginForm when the ClearTrust DSAPI filter is in place may cause the Domino server to exit. There is a fix available for this behavior from RSA technical support. To acquire this, ask for RSA ClearTrust Agent Hotfix 4.6.0.17.

This issue can also be worked around by deleting the login mapping created in the Web Configuration Database, and protecting the Team Workplace resources with ClearTrust.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com