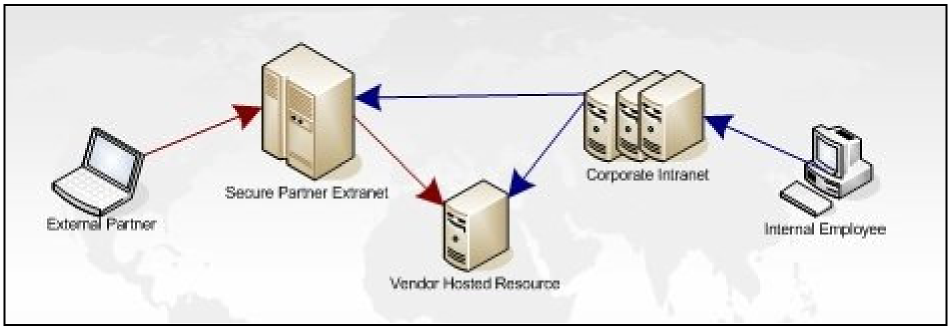
NCT SIMPLE SIGNON

INTEGRATION WITHOUT AGGRAVATION



Quick Start Guide

This document is designed for an experienced administrator or developer to get up and running as quickly as possible without all the detail. If the steps listed here are too broad, please see the full documentation. We strongly recommend you also read the more complete documentation – it's mostly pictures, we promise it won't take long.

NORTHERN Collaborative TECHNOLOGIES

THE QUICKEST POSSIBLE START

SECURITY CONSIDERATIONS WITH NCT SIMPLE SIGNON

At Northern Collaborative Technologies, we've worked hard to make NCT Simple Signon a robust, stable, and secure product for your environment. With any authentication related product, however, there are dangers.

THERE IS NO SUCH THING AS PERFECT SECURITY

If you absolutely, positively, never, ever can allow something to be shared; do not put it on a web site or a server. There are techniques which can be used to watermark items individually and thus trace leaked documentation, but even these are only good at cleaning up after the fact. This tool, like most others, is designed to provide a reasonable level of security to prevent the casual or even modest attempts to circumvent authorized use procedures. If NCT Simple Signon is used correctly, it provides one part of a security solution – but only one part. Application design best practices are still required, as is the localized encryption and other security measures required in modern applications.

Authentication is not the same thing as Authorization. NCT Simple Signon is designed to enable you to pass authentication credentials among disparate sources and maintain a reasonable level of surety that those credentials are authentic. Once you have authenticated a user, however, you must still control that user's authorization to view, add, create, change, or delete data.

NCT Simple Signon is powerful medicine. In fact, more than 90% of the development effort associated with this product has gone into providing the necessary controls to allow its safe use.

SYSTEM REQUIREMENTS

NCT Simple Signon requires a Lotus Domino version 6 or higher server. NCT Simple Signon has been tested and shown to work properly on IBM Lotus Domino version 7 servers as well.

Although the schema itself is not application server, operating system, or machine specific; if you wish to use NCT Simple Signon for inbound user access you will need at least one Win32 based IBM Lotus Domino server. Future versions will support other CAPI compatible versions of Lotus Domino for this purpose. For use with servers other than Win32 based, you can set up a single Win32 server to generate session tokens in a Domino Shared Session environment.

NCT Simple Signon is not browser specific, and should work for users on nearly any modern web browser including both Microsoft Internet Explorer and Mozilla Firefox.

Administrators of NCT Simple Signon should have an IBM Lotus Notes Client version 6.0 or higher, and must have sufficient rights to install databases to the server.

To function properly, the NCT Simple Signon Application Database will have to be "Signed" with an ID file having sufficient rights to run Unrestricted LotusScript agents.

INSTALL THE PRODUCT

1. Make a backup of your entire server, all the servers in the organization, your workstation, the other workstations in the office, and all your machines at home. Don't forget your cell phone. You might want to back your car up too. – Kidding aside, this is a program which works at the API level. Problems, if they occur, could be serious. We recommend having valid backups and using a test environment.

2. Read and pay attention to the security warnings throughout this product. Your biggest danger is leaving an authentication method too open, and allowing someone else to pretend to be someone they are not. We've taken steps to minimize this danger, but you have the power to open things right up.

3. Copy the DLL file and License Key file you received the Lotus Domino Server's program directory.

4. Sign a copy of the Application Database using an ID which is authorized to run Unrestricted LotusScript Agents on your server.

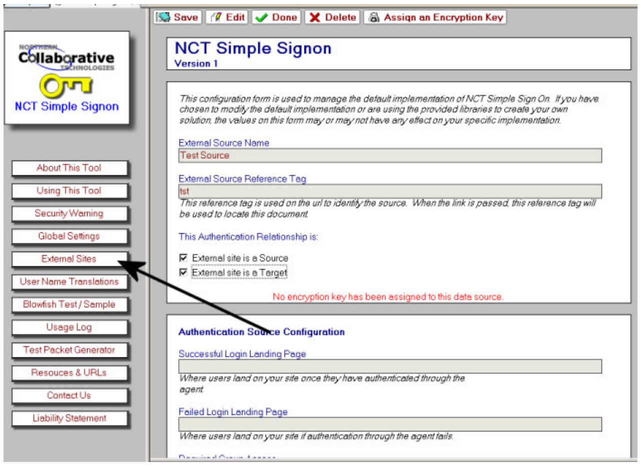
5. Check that the ACL settings are correct. (Full Documentation Page 8)

6. Verify that your server is correctly configured for session based login (Full Documentation Page 9)

CHECK YOUR INSTALLATION TO SEE IF IT WORKS

The Slightly Longer, much safer method

A more patient, much wiser administrator or developer would find that it doesn't really take long at all to create a Remote Site Reference in the Application Database. Just create the document, assign it a reference id, and select the checkbox for "External Site is a Source". Once you've done that, click to assign it an encryption key. Remember this key.



NCT Simple Signon
Version 1

This configuration form is used to manage the default implementation of NCT Simple Sign On. If you have chosen to modify the default implementation or are using the provided libraries to create your own solution, the values on this form may or may not have any effect on your specific implementation.

External Source Name
Test Source

External Source Reference Tag
tst
This reference tag is used on the url to identify the source. When the link is passed, this reference tag will be used to locate this document.

This Authentication Relationship is:

☑ External site is a Source
☑ External site is a Target

No encryption key has been assigned to this data source.

Authentication Source Configuration

Successful Login Landing Page

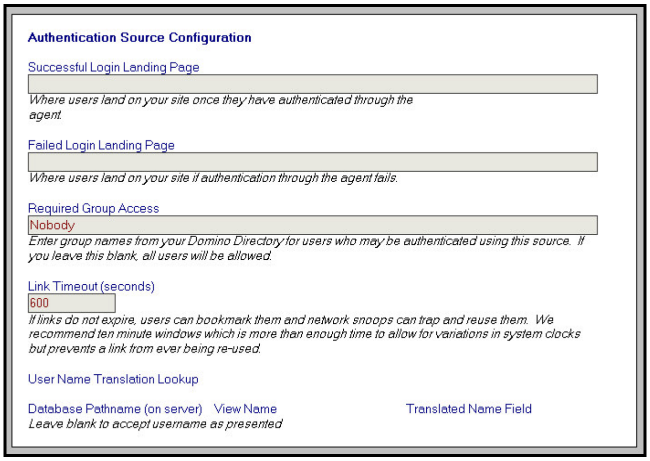
Where users land on your site once they have authenticated through the agent

Failed Login Landing Page

Where users land on your site if authentication through the agent fails.

Next you should make sure to create a group in your Domino Directory which contains a few test user names who will be allowed to login. Put that group in the field called

"Required Group Access". This will prevent someone from using your name, or your boss's name.



Authentication Source Configuration

Successful Login Landing Page

Where users land on your site once they have authenticated through the agent.

Failed Login Landing Page

Where users land on your site if authentication through the agent fails.

Required Group Access

Nobody

Enter group names from your Domino Directory for users who may be authenticated using this source. If you leave this blank, all users will be allowed.

Link Timeout (seconds)

600

If links do not expire, users can bookmark them and network snoops can trap and reuse them. We recommend ten minute windows which is more than enough time to allow for variations in system clocks but prevents a link from ever being re-used.

User Name Translation Lookup

Database Pathname (on server) View Name Translated Name Field

Leave blank to accept username as presented

Now, you've got a remote site reference document created, assigned it an encryption key, and you are ready to test. Simply select the menu item "Test Packet Generator", and enter a username the same encryption key you assigned to the remote site reference. The tool will generate a packet as if it came from that remote site.

The URL below will log you in if you've set things up correctly. Of course, you'll need to use your own server name and Application Database pathname. Then substitute the reference ID you assigned to the External Site Configuration document where the "NNNN" is, and the packet you've just greated where the "XXXX" is. You knew that already though.

http://servername/path/yourAppDatabase.nsf/SimpleUserAuth?Openagent& ref=NNNN&pkt=XXXX

The Simple, dangerous method

Within the Application Database there waits an agent named "SimpleUserAuth". This agent is disabled right now. To enable it – which you should never ever do – a risk-taking admin or developer could go to the initialize subroutine and (ignoring all the warnings not to do this) comment out the line which says "exit sub".

If one were careless enough to take this drastic and reckless step, and that one saved the agent, and that careless person had sufficient access rights to run unrestricted LotusScript agents on the server (what a temptation of fate!) then that one should realize that simply using the URL which follows would cause an LTPA token to be created for the user "Bob Smith" and assigned to whomever was to use the URL in their browser! Be warned, however, they could just as easily put your name or your bosses name in there.

Remember, you MUST have that ability to run unrestricted LotusScript agents in order for this to work. That is not an authority to be given out lightly under any circumstances.

http://servername/path/yourAppDatabase.nsf/SimpleUserAuth?Openagent& user=BOB_SMITH&login=0

You should not, under any circumstances, EVER leave this test agent enabled.