Home | Community Articles | Product Documentation | Learning Center

Community Articles | Search for... | Advanced Search

Home > Deployments > Scenario 3: Setting up SiteMinder Single Sign-On (SSO) with Lotus Connections 3.0

(0 ratings)

Scenario 3: Setting up SiteMinder Single Sign-On (SSO) with Lotus Connections 3.0

Abstract

Introduction

This document explains how to set up integration between Lotus Connections 3.0 and Computer Associates SiteMinder. This article looks at this integration almost entirely from the Lotus Connections perspective. For a fuller policy server, refer to the Lotus Connections 3.0 product documentation topic entitled [Enabling single sign-on for SiteMinder: lc3].

Prerequisites

Before beginning SiteMinder enablement with Lotus Connections 3.0 ensure that the following items are complete:

- Lotus Connections 3.0 is setup and working with the IBM HTTP Server without issue.
- The J2C Authentication Alias "connectionsAdmin" is a user who exists on the LDAP and has administrative rights on the WebSphere Administration Console.

What is SiteMinder

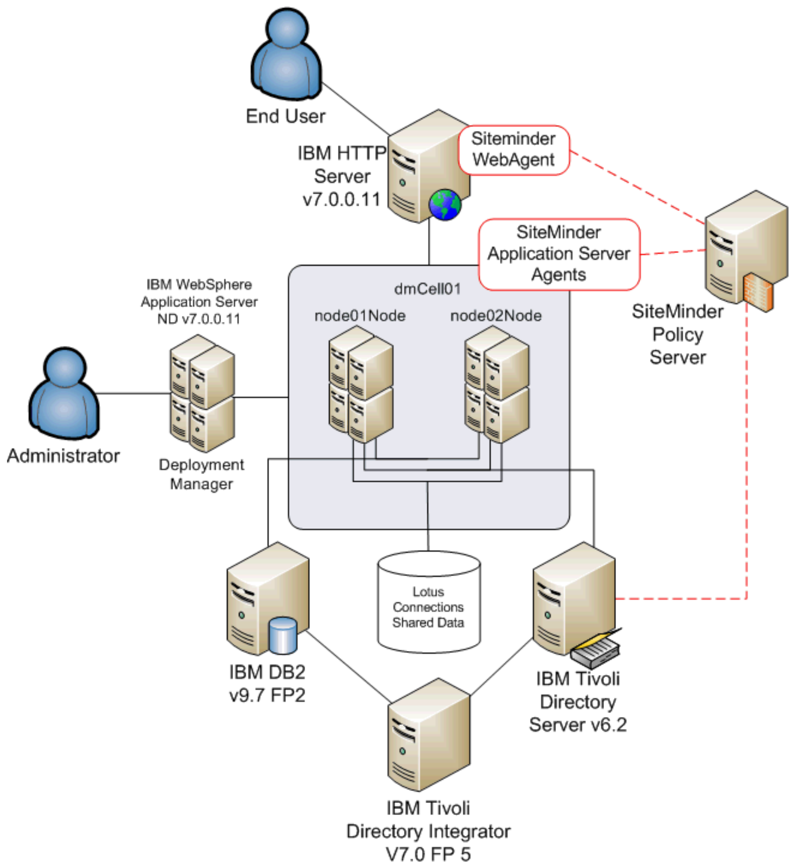
Computer Associates is a Web access control product providing web single sign-on (SSO), centralized policy management for authentication, authorization, auditing and user entitlement.

A SiteMinder Web Agent is a software component that controls access to any resource that can be identified by a URL. The Web Agent resides on a web server and intercepts requests for a resource to determine whether o Server to authenticate and authorize users who request access to the protected web server resources.

When a user requests a page that is protected by SiteMinder, the Web Agent on the HTTP server intercepts the request and prompts the user for authentication. If the user provides valid credentials, the user is authenticated WebSphere Application Server. The SiteMinder Trust Association Interceptor (TAI) -also known as Application Server Agent - on the WebSphere Application Server verifies the information in the cookie and sets the User Prin

Enterprise Network Deployment with SiteMinder Security Diagram

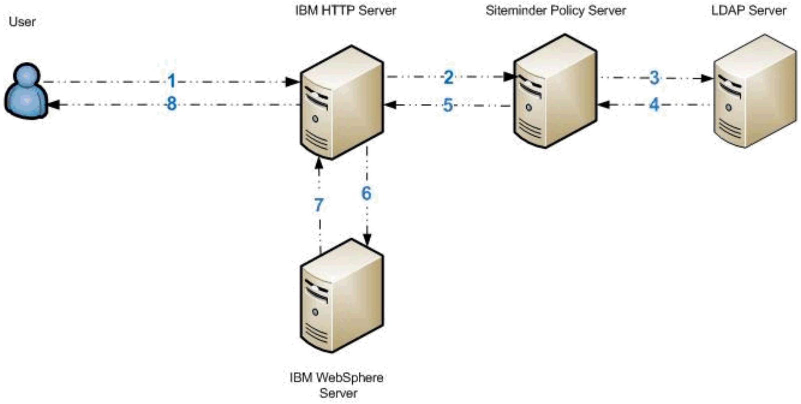
This configuration diagram shows the Lotus Connections architecture with the addition of Computer Associates SiteMinder to protect the entire configuration. In this scenario SiteMinder is connected to the LDAP and has age the webserver SiteMinder intercepts and presents the SiteMinder login page. Once they authenticate SiteMinder adds its SMSESSION cookie to the request and the user is logged onto Lotus Connections via single-sign on.


End User
IBM HTTP Server v7.0.0.11
Siteminder WebAgent
SiteMinder Application Server Agents
SiteMinder Policy Server
IBM WebSphere Application Server ND v7.0.0.11
dmCell01
node01Node
node02Node
Administrator
Deployment Manager
Lotus Connections Shared Data
IBM DB2 v9.7 FP2
IBM Tivoli Directory Server v6.2
IBM Tivoli Directory Integrator V7.0 FP 5

Complex Enterprise Network Deployment Architecture Including Integration

How SiteMinder Integration Works

The following diagram explains how SiteMinder Integration works when used with WebSphere TAI and a Web Agent on the IBM HTTP Server.



The following step numbers correspond to each of the above communications:

1. User access protected resource.

- Siteminder Web Agent on HTTP Server intercepts the request and prompts for Authentication.
- User enters Username and password.

1. Siteminder Web Agent Passes username and password to Siteminder Policy Server.
2. Siteminder Policy Server attempts to Authenticates the user against the LDAP.

- Policy Server uses the User Directory Object Details specified in the Siteminder Administration Console.

1. After successful authentication, the Policy Server Authorizes the user.

- Siteminder checks the users and Groups assigned access in the Policy.
- Siteminder checks the Rules for the Requested methods and urls.
- Siteminder adds SMSESSION cookie to the request.

1. Request is returned to the HTTP Server.

- Siteminder Web Agent on the IBM HTTP Server checks for valid SMSESSION cookie.

1. Request is sent to the WebSphere Server.

- Siteminder ASA Agent on the WebSphere Server checks for valid SMSESSION cookie.
- ASA Agent asserts user details to the WebSphere Server.
- WebSphere performs it's own internal authorization.
- Allows access to the requested resource.

1. Response is returned to the Http Server.
2. Response sent to user with the requested resource.

Enabling Single Sign-On with Computer Associate's SiteMinder

The following section is quite complex, it is therefore recommended to refer to the Lotus Connections 3.0 infocenter along with this guide to get the fullest understanding of how SiteMinder integration with Lotus Connections enablement with Lotus Connections 3.0. For the purposes of this guide the following table represent the values of the various SiteMinder objects required for this configuration.

SiteMinder Objects	HTTP Server connections.example.com	WebSphere Application Server Node 1 node1.example.com	WebSphere Application Server Node 2 node2.example.com
Agent Object	connections_wa	node_TAI	node_TAI
Agent Config Object	connections_wa_conf	node_TAI_conf	node_TAI_conf
Host Config Object	host_connections	host_node1_TAI	host_node2_TAI
Trusted Hostname	connections	node1_TAI	node2_TAI

Important Notes

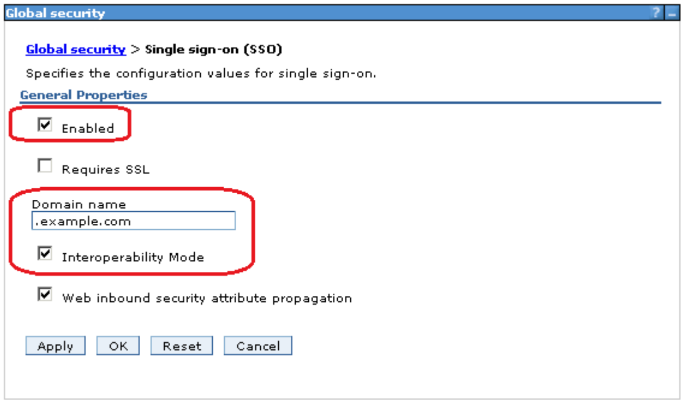
- The connectionsAdmin J2C Authentication Alias that you specified during installation must correspond to a valid account that can authenticate with SiteMinder. It may map to a back-end administrative user account need to update the user ID or credentials for this alias, see the *Changing references to administrative credentials* topic in the Lotus Connections 3.0 InfoCenter.
- For more information about the SiteMinder Policy Server and Web Agent configuration, go to the SiteMinder BookShelf.
- For more information about the SiteMinder Agent for WebSphere, see the SiteMinder Agent for WebSphere Agent Guide (PDF) and CA SiteMinder Agent for WebSphere Agent Release Notes® (PDF).

You need to create SiteMinder Agent and Domain objects with realms, rules, and a policy that is related to IBM HTTP Server and WebSphere Application Server. When a user requests a page that is protected by SiteMinder, authentication. If the user provides valid credentials, the user is authenticated and an SMSESSION cookie is added to the request which is then passed on to the WebSphere Application Server. The SiteMinder Trust Associa Principal that Lotus Connections requires to identify the user.

This task describes a configuration that uses SiteMinder Policy Server 6.0 SP5, SiteMinder ASA 6.0 Agent for WebSphere Application Server (with CR00010 hotfix), and SiteMinder Web Agent v6qmr5-cr035.
To set up SSO using SiteMinder, complete the following steps:

Preparing WebSphere Application Server for SiteMinder

Setup Single Sign-On Domain if not already done so. On the deployment manager navigate to Security -> Global Security -> Web and SIP Security -> Sign Sign-On (SSO). Ensure the following is set:



Specifies the configuration values for single sign-on.

General Properties

☑ Enabled

□ Requires SSL

Domain name: .example.com

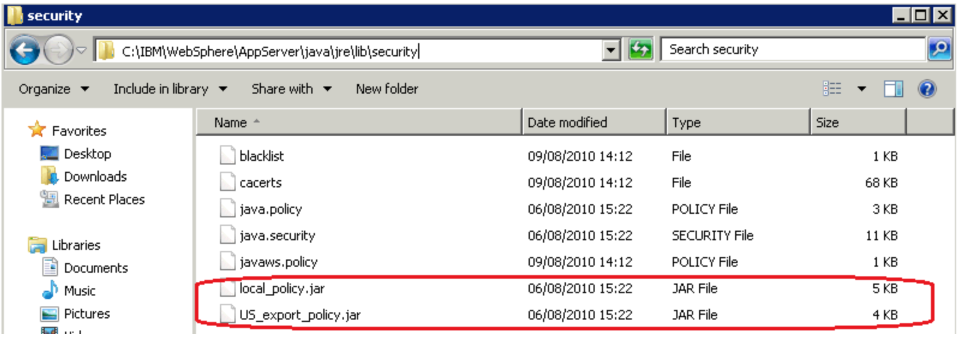
☑ Interoperability Mode

☑ Web inbound security attribute propagation

Next copy the unrestricted JCE policy files to the Application Server and Deployment Manager machines. The unrestricted JCE files can be downloaded from the following web page, note that you will have to login with your /webapp/iwm/web/preLogin.do?source=jcesdk . Once the files are downloaded extract them from the package. The files in question are called :

- US_export_policy.jar
- local_policy.jar.

On the two nodes and deployment manager machine go to the following location and take a backup of the existing files and then copy in the new unrestricted versions to this location. All servers, node agents and deploymen

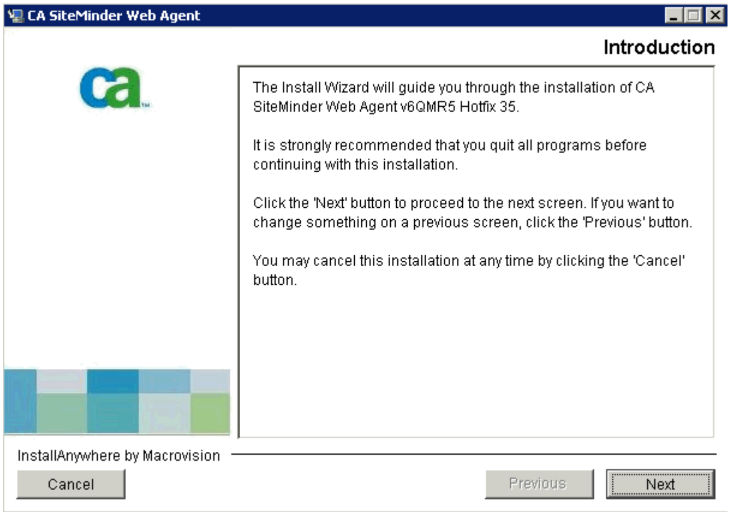


Name	Date modified	Type	Size
blacklist	09/08/2010 14:12	File	1 KB
cacerts	09/08/2010 14:12	File	68 KB
java.policy	06/08/2010 15:22	POLICY File	3 KB
java.security	06/08/2010 15:22	SECURITY File	11 KB
javaws.policy	09/08/2010 14:12	POLICY File	1 KB
local_policy.jar	06/08/2010 15:22	JAR File	5 KB
US_export_policy.jar	06/08/2010 15:22	JAR File	4 KB

Install the Web Agent on IBM HTTP Server

- Download the above version of the Web Agent from the CA website.
- Install the Web Agent. For instructions, go to the SiteMinder BookShelf.
- When you are prompted for the Agent Configuration details, specify the Agent Configuration Object that you created earlier.

Launch the webagent installation wizard, select Next at the below panel:



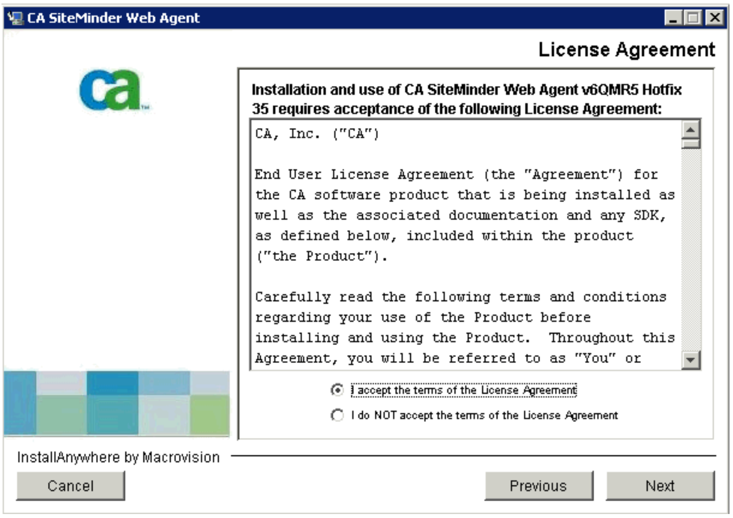
The Install Wizard will guide you through the installation of CA SiteMinder Web Agent v6QMR5 Hotfix 35.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Accept the licence agreement and click next:



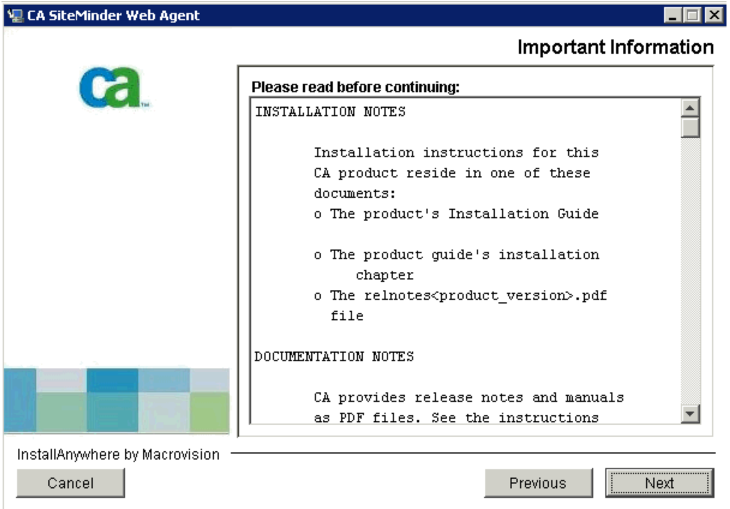
Installation and use of CA SiteMinder Web Agent v6QMR5 Hotfix 35 requires acceptance of the following License Agreement:

```
CA, Inc. ("CA")

End User License Agreement (the "Agreement") for
the CA software product that is being installed as
well as the associated documentation and any SDK,
as defined below, included within the product
("the Product").

Carefully read the following terms and conditions
regarding your use of the Product before
installing and using the Product.  Throughout this
Agreement, you will be referred to as "You" or
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Click next at the information panel below:

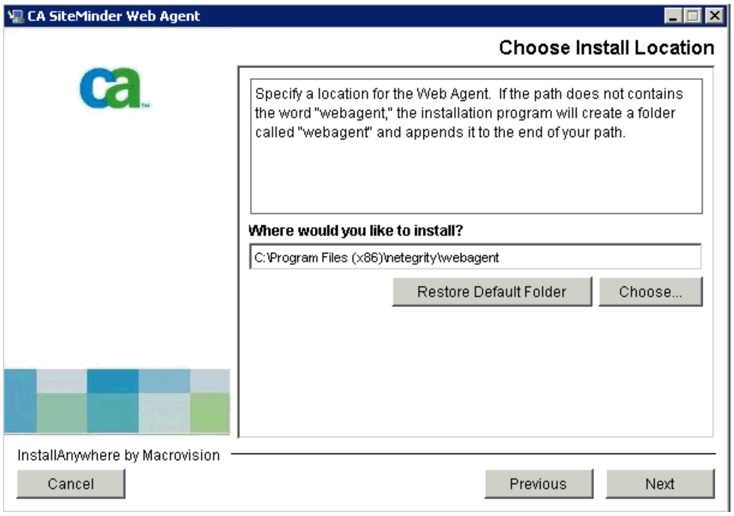


Important Information

Please read before continuing:

```
INSTALLATION NOTES

       Installation instructions for this
       CA product reside in one of these
       documents:
       o The product's Installation Guide

       o The product guide's installation
            chapter
       o The relnotes<product_version>.pdf
         file

DOCUMENTATION NOTES

       CA provides release notes and manuals
       as PDF files. See the instructions
```

Select a path to install the webagent to and click next to continue



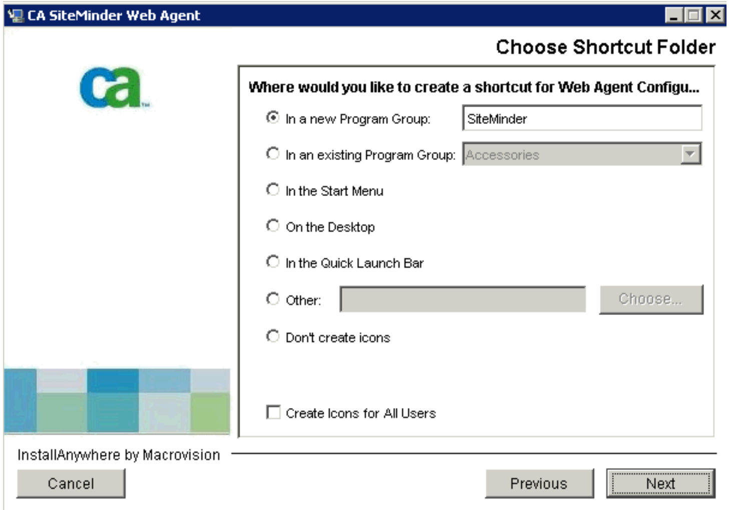
Choose Install Location

Specify a location for the Web Agent. If the path does not contains the word "webagent," the installation program will create a folder called "webagent" and appends it to the end of your path.

Where would you like to install?

C:\Program Files (x86)\netegrity\webagent

Select if you wish a new group to be created in your start menu:



Choose Shortcut Folder

Where would you like to create a shortcut for Web Agent Configu...

● In a new Program Group: SiteMinder

○ In an existing Program Group: Accessories

○ In the Start Menu

○ On the Desktop

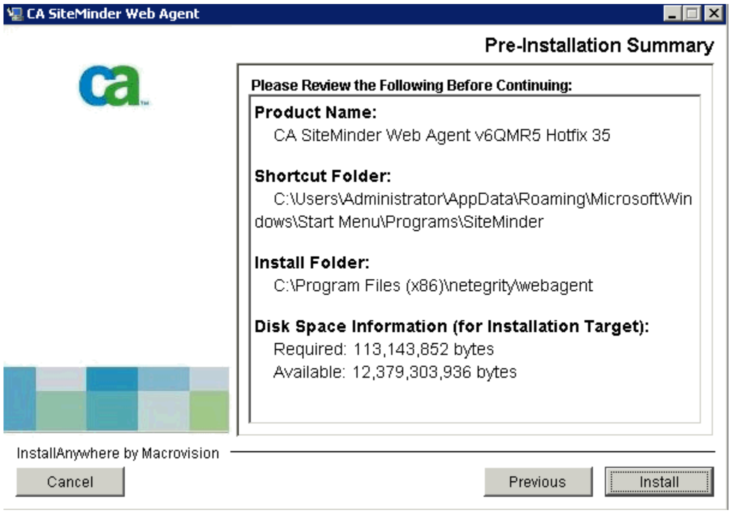
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

□ Create Icons for All Users

Click Install to begin the Web Agent installation.



Pre-Installation Summary

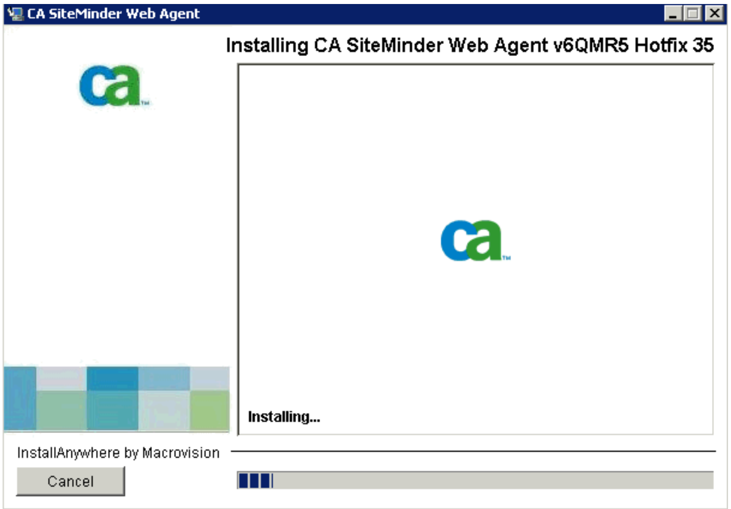
Please Review the Following Before Continuing:

Product Name:
CA SiteMinder Web Agent v6QMR5 Hotfix 35

Shortcut Folder:
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\SiteMinder

Install Folder:
C:\Program Files (x86)\netegrity\webagent

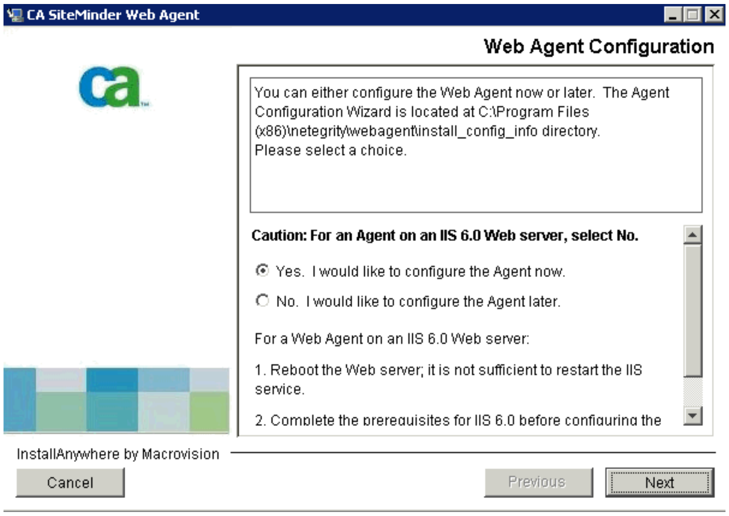
Disk Space Information (for Installation Target):
Required: 113,143,852 bytes
Available: 12,379,303,936 bytes



Installing CA SiteMinder Web Agent v6QMR5 Hotfix 35

Installing...

Select Yes to configure the web agent now.



Web Agent Configuration

You can either configure the Web Agent now or later. The Agent Configuration Wizard is located at C:\Program Files (x86)\netegrity\webagent\install_config_info directory.
Please select a choice.

Caution: For an Agent on an IIS 6.0 Web server, select No.

● Yes. I would like to configure the Agent now.

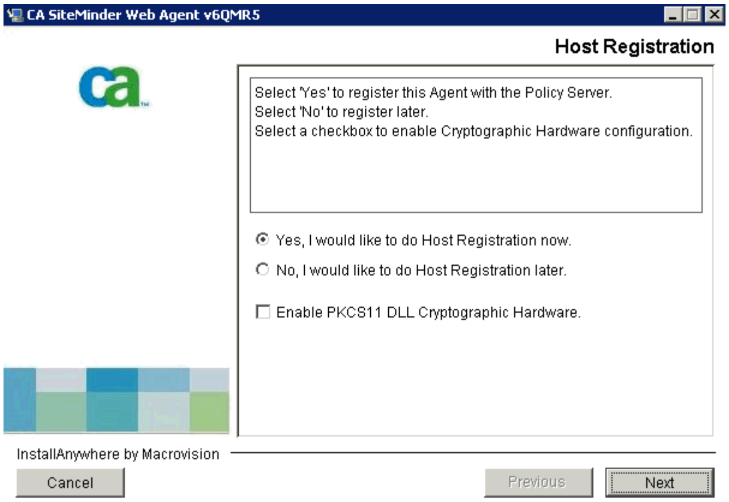
○ No. I would like to configure the Agent later.

For a Web Agent on an IIS 6.0 Web server:

1. Reboot the Web server; it is not sufficient to restart the IIS service.

2. Complete the prerequisites for IIS 6.0 before configuring the

Select Yes to do host registration now :

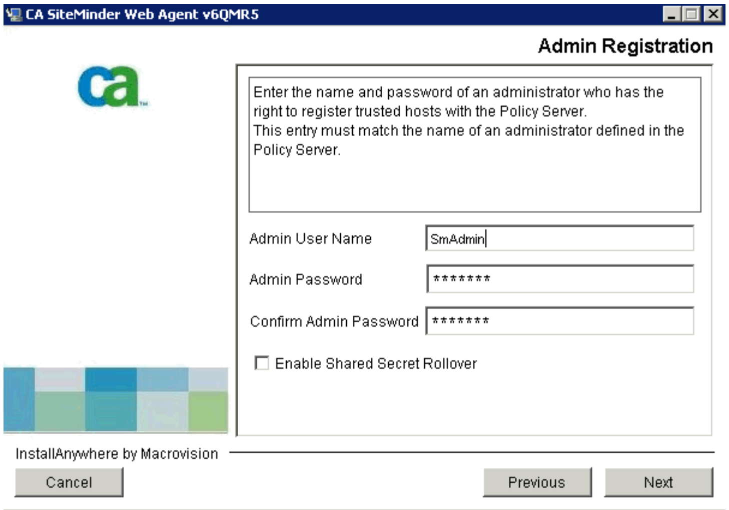

CA SiteMinder Web Agent v6QMR5
Host Registration
InstallAnywhere by Macrovision
Cancel
Previous
Next

Select 'Yes' to register this Agent with the Policy Server.
Select 'No' to register later.
Select a checkbox to enable Cryptographic Hardware configuration.

● Yes, I would like to do Host Registration now.
○ No, I would like to do Host Registration later.

□ Enable PKCS11 DLL Cryptographic Hardware.

Input the username and password of the SiteMinder administrator and click next:


CA SiteMinder Web Agent v6QMR5
Admin Registration
InstallAnywhere by Macrovision
Cancel
Previous
Next

Enter the name and password of an administrator who has the right to register trusted hosts with the Policy Server.
This entry must match the name of an administrator defined in the Policy Server.

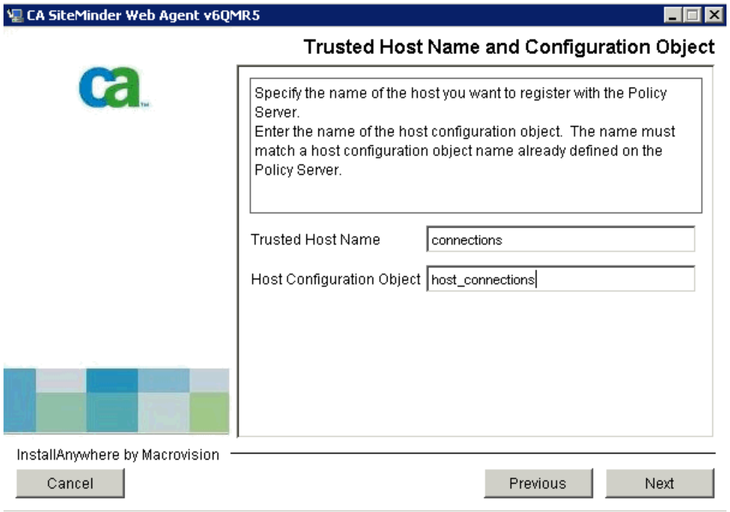
Admin User Name: SmAdmin

Admin Password: *******

Confirm Admin Password: *******

□ Enable Shared Secret Rollover

Input the Trusted Host Name and Host Configuration Object, remember these values are taken from the table at the start of this section and are assumed to already exist before completing this task.

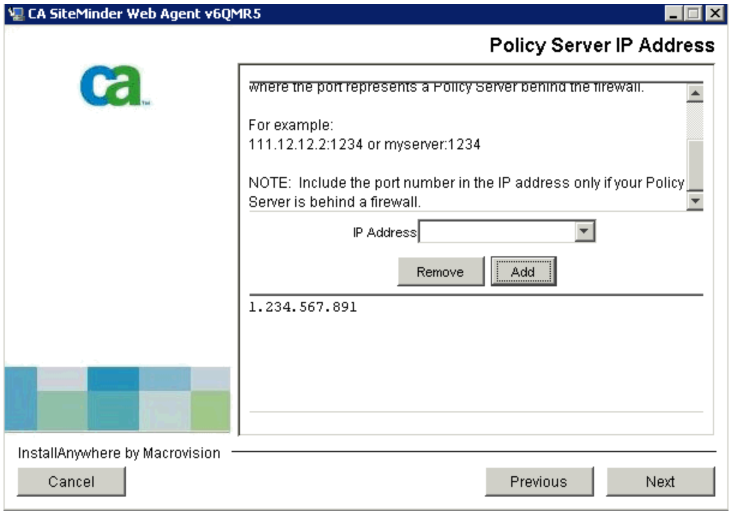

CA SiteMinder Web Agent v6QMR5
Trusted Host Name and Configuration Object
InstallAnywhere by Macrovision
Cancel
Previous
Next

Specify the name of the host you want to register with the Policy Server.
Enter the name of the host configuration object. The name must match a host configuration object name already defined on the Policy Server.

Trusted Host Name: connections

Host Configuration Object: host_connections

Add the IP address of the SiteMinder server:


CA SiteMinder Web Agent v6QMR5
Policy Server IP Address
InstallAnywhere by Macrovision
Remove
Add
Cancel
Previous
Next

where the port represents a Policy Server behind the firewall.

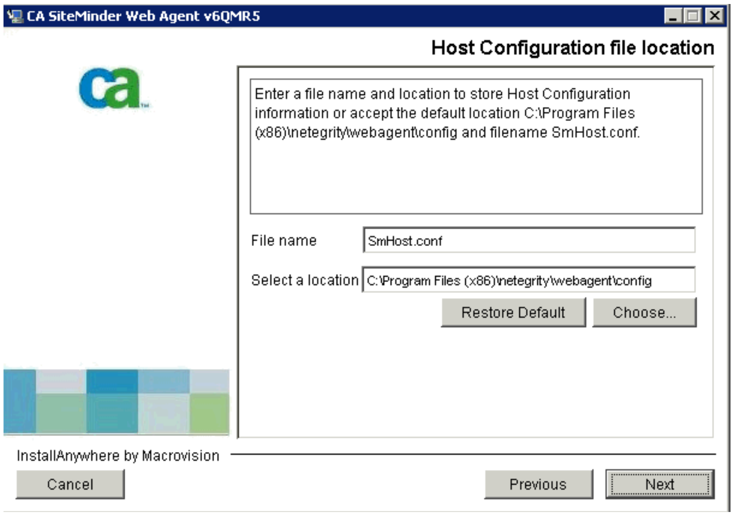
For example:
111.12.12.2:1234 or myserver:1234

NOTE: Include the port number in the IP address only if your Policy Server is behind a firewall.

IP Address

1.234.567.891

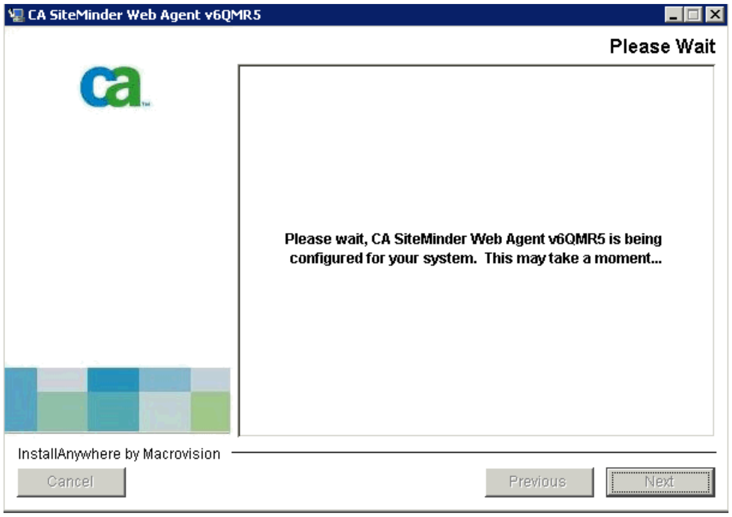
Properties for the SmHost.conf, select next to continue:


CA SiteMinder Web Agent v6QMR5
Host Configuration file location
InstallAnywhere by Macrovision
Restore Default
Choose...
Cancel
Previous
Next

Enter a file name and location to store Host Configuration information or accept the default location C:\Program Files (x86)\netegrity\webagent\config and filename SmHost.conf.

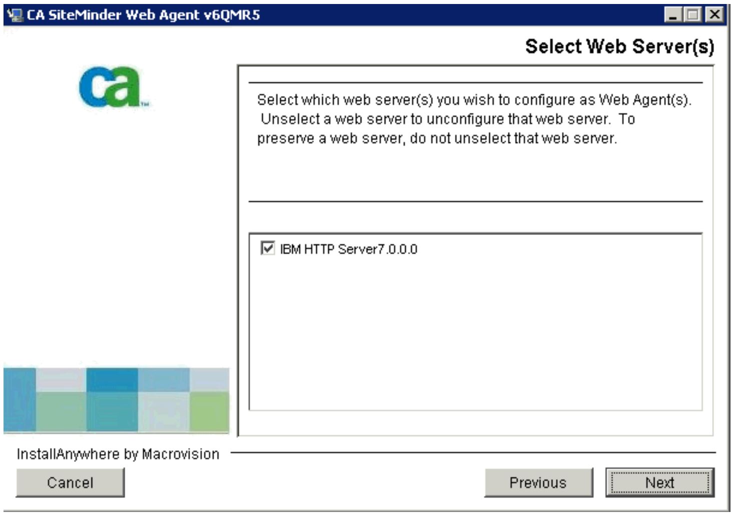
File name: SmHost.conf

Select a location: C:\Program Files (x86)\netegrity\webagent\config


CA SiteMinder Web Agent v6QMR5
Please Wait
InstallAnywhere by Macrovision
Cancel
Previous
Next

Please wait, CA SiteMinder Web Agent v6QMR5 is being configured for your system. This may take a moment...

Register the IBM HTTP Server with SiteMinder, click next. See troubleshooting steps for SiteMinder if no options appear on this screen.


CA SiteMinder Web Agent v6QMR5

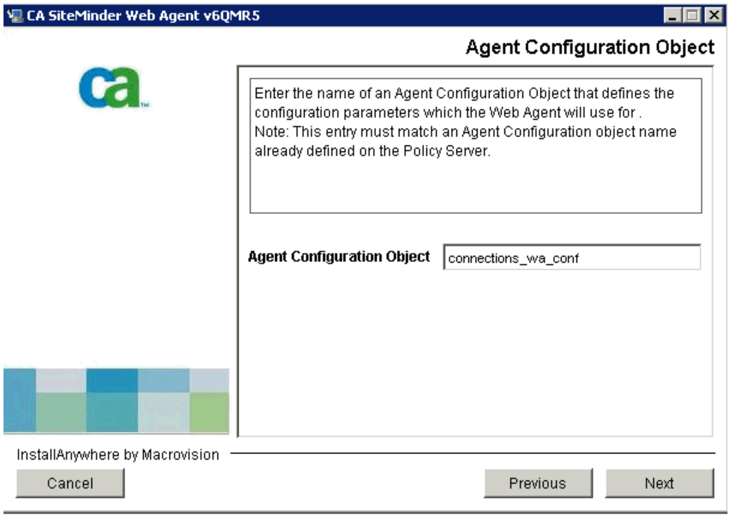
Select Web Server(s)

Select which web server(s) you wish to configure as Web Agent(s). Unselect a web server to unconfigure that web server. To preserve a web server, do not unselect that web server.

☑ IBM HTTP Server7.0.0.0

InstallAnywhere by Macrovision

Input the agent configuration object name :


CA SiteMinder Web Agent v6QMR5

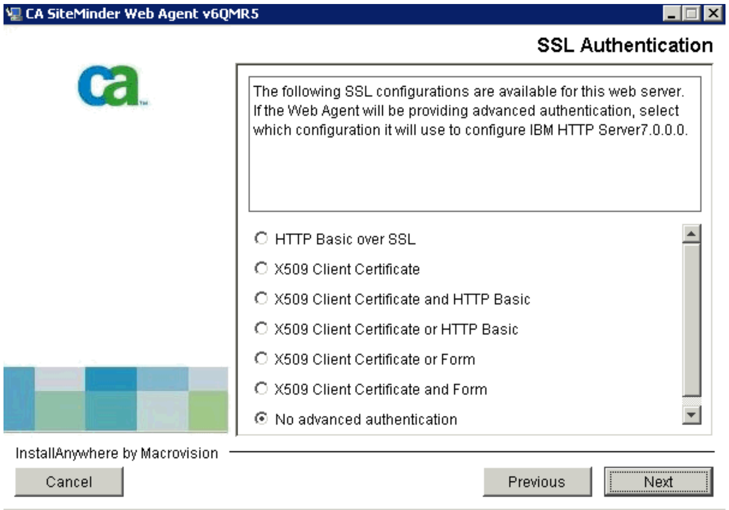
Agent Configuration Object

Enter the name of an Agent Configuration Object that defines the configuration parameters which the Web Agent will use for .
Note: This entry must match an Agent Configuration object name already defined on the Policy Server.

Agent Configuration Object connections_wa_conf

InstallAnywhere by Macrovision

Select the advanced authentication to use depending on your requirements click Next.


CA SiteMinder Web Agent v6QMR5

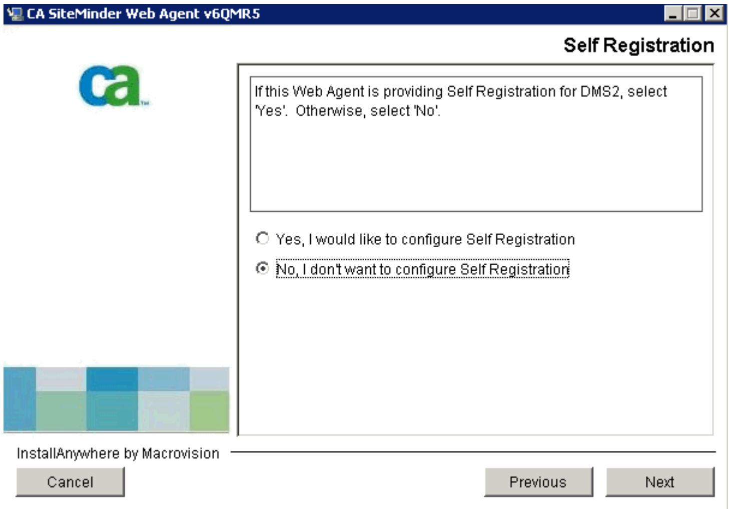
SSL Authentication

The following SSL configurations are available for this web server. If the Web Agent will be providing advanced authentication, select which configuration it will use to configure IBM HTTP Server7.0.0.0.

○ HTTP Basic over SSL
○ X509 Client Certificate
○ X509 Client Certificate and HTTP Basic
○ X509 Client Certificate or HTTP Basic
○ X509 Client Certificate or Form
○ X509 Client Certificate and Form
● No advanced authentication

InstallAnywhere by Macrovision

At the following panel click No, I don't want to configure Self Registration and click next.



CA SiteMinder Web Agent v6QMR5

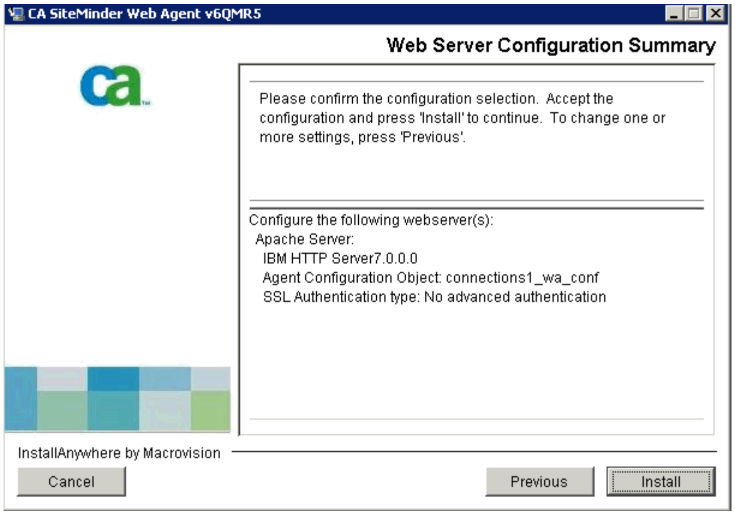
Self Registration

If this Web Agent is providing Self Registration for DMS2, select 'Yes'. Otherwise, select 'No'.

○ Yes, I would like to configure Self Registration

● No, I don't want to configure Self Registration

Review the web agent configuration options and click Install.



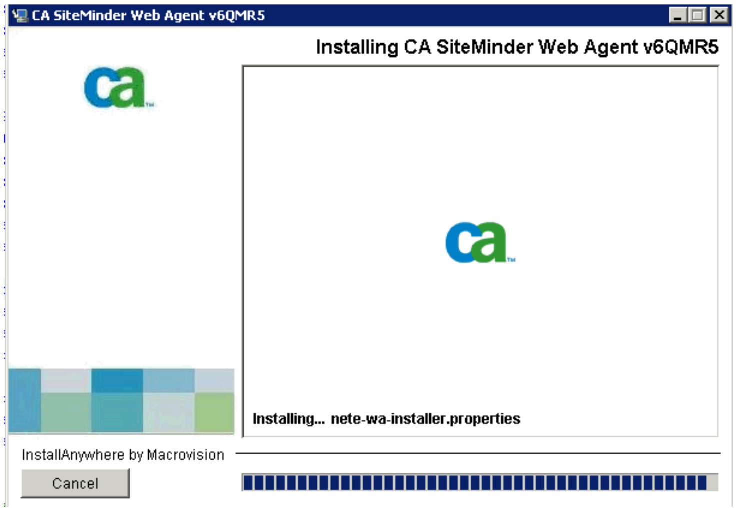
CA SiteMinder Web Agent v6QMR5

Web Server Configuration Summary

Please confirm the configuration selection. Accept the configuration and press 'Install' to continue. To change one or more settings, press 'Previous'.

```
Configure the following webserver(s):
 Apache Server:
  IBM HTTP Server7.0.0.0
  Agent Configuration Object: connections1_wa_conf
  SSL Authentication type: No advanced authentication
```

InstallAnywhere by Macrovision
Cancel
Previous
Install



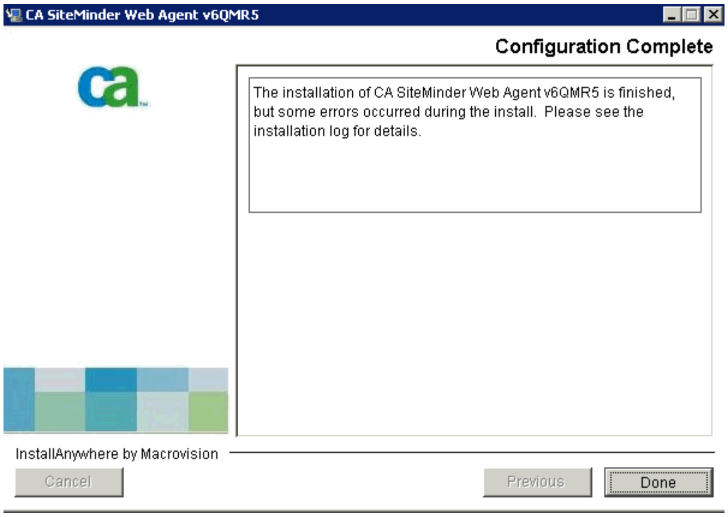
CA SiteMinder Web Agent v6QMR5

Installing CA SiteMinder Web Agent v6QMR5

Installing... nete-wa-installer.properties

InstallAnywhere by Macrovision
Cancel

Review any errors which occur, in this case they are benign but it is important to check SiteMinder logs when completing this step. Click Done to end the wizard.


CA SiteMinder Web Agent v6QMR5

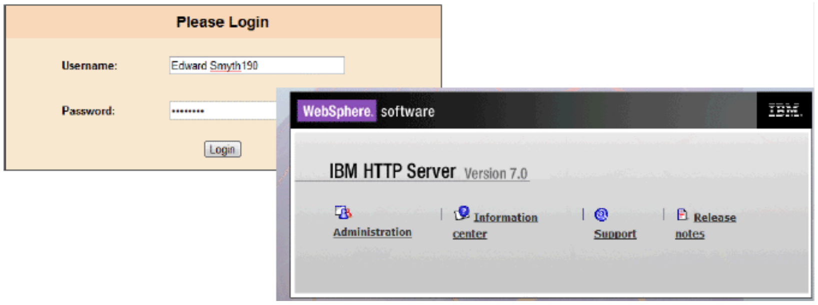
Configuration Complete

The installation of CA SiteMinder Web Agent v6QMR5 is finished, but some errors occurred during the install. Please see the installation log for details.

In this case the installation log at C:\Program Files\netegrity\webagent\install_config_info\CA_SiteMinder_Web_Agent_v6QMR5_InstallLog.log reports the following, there are no fatal errors so we are safe to proceed:

```
Installation: Successful with errors.



273 Successes

0 Warnings

11 NonFatalErrors

0 FatalErrors
```

After configuring the webagent as above. Find the WebAgent.conf in the HTTPServer/conf directory. Open this file and edit it so EnableWebAgent=YES. Now restart your HTTP Server. When attempting to access the HTTP HTTP Server Splash Screen. This indicates that SiteMinder is set up correctly with the WebAgent.


Please Login

Username: Edward Smyth190

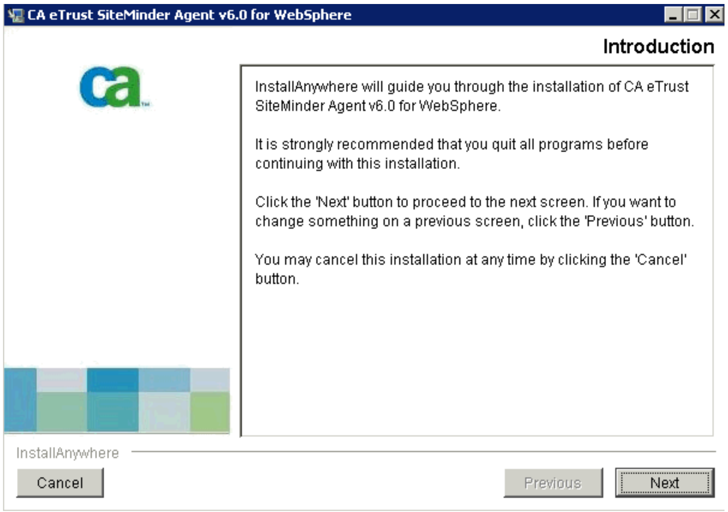
Password: ••••••••

Install the Application Server Agent

Install the Application Server Agent on your both nodes - node1.example.com and node2.example.com

- Download the above version of the Application Server Agent from the CA website.
- Install the Application Server Agent on each node in your Lotus Connections deployment. For instructions, see the SiteMinder Agent for WebSphere Agent Guide.
- When you are prompted for the Agent Configuration details, specify the Agent Configuration Object that you created earlier.

Launch the installer for the application server agent click next to continue:


CA eTrust SiteMinder Agent v6.0 for WebSphere

Introduction

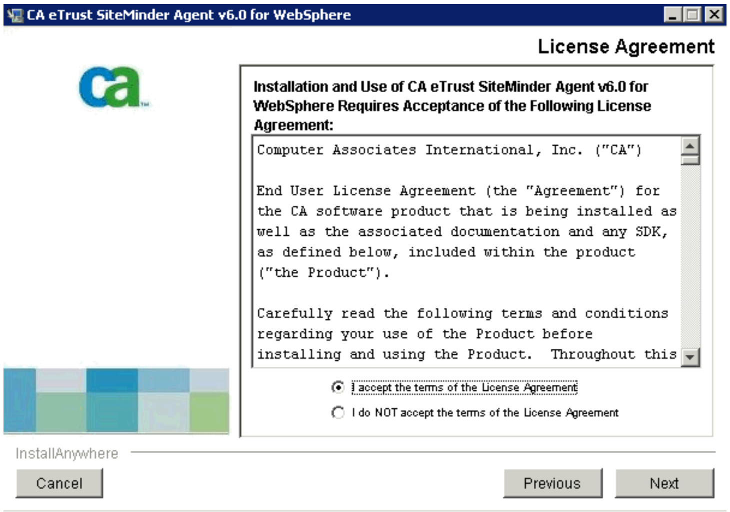
InstallAnywhere will guide you through the installation of CA eTrust SiteMinder Agent v6.0 for WebSphere.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Accept the licence agreement, click next to continue:


CA eTrust SiteMinder Agent v6.0 for WebSphere

License Agreement

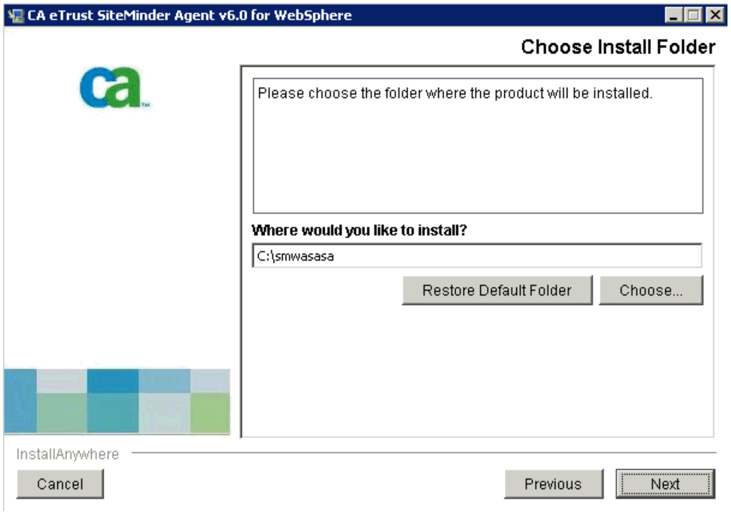
Installation and Use of CA eTrust SiteMinder Agent v6.0 for WebSphere Requires Acceptance of the Following License Agreement:

```
Computer Associates International, Inc. ("CA")

End User License Agreement (the "Agreement") for
the CA software product that is being installed as
well as the associated documentation and any SDK,
as defined below, included within the product
("the Product").

Carefully read the following terms and conditions
regarding your use of the Product before
installing and using the Product.  Throughout this
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Choose a installation location and click next to continue


CA eTrust SiteMinder Agent v6.0 for WebSphere

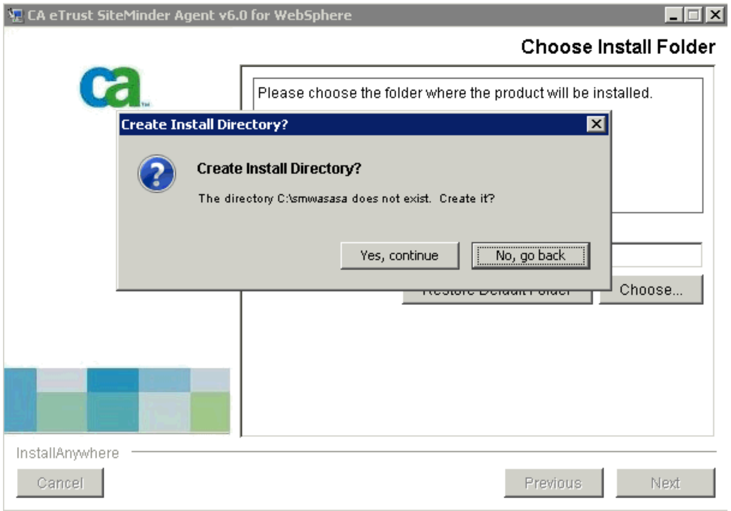
Choose Install Folder

Please choose the folder where the product will be installed.

Where would you like to install?

C:\smwasasa

Select Yes, Continue :


CA eTrust SiteMinder Agent v6.0 for WebSphere

Choose Install Folder

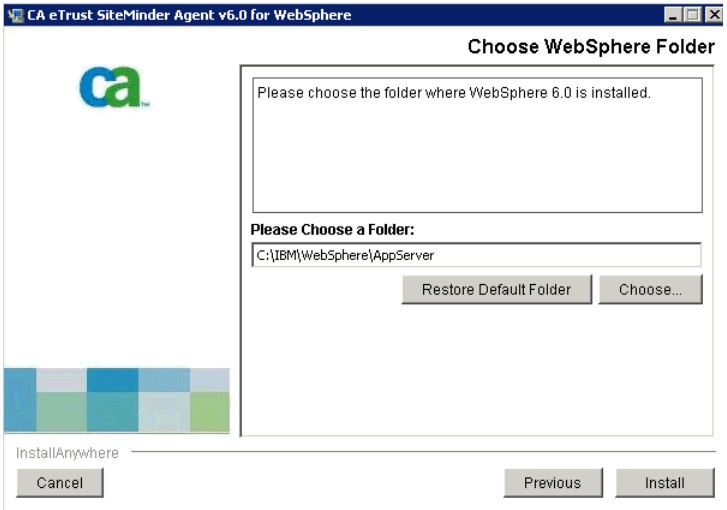
Please choose the folder where the product will be installed.

Create Install Directory?

Create Install Directory?

The directory C:\smwasasa does not exist. Create it?

Specify where WebSphere is installed:


CA eTrust SiteMinder Agent v6.0 for WebSphere

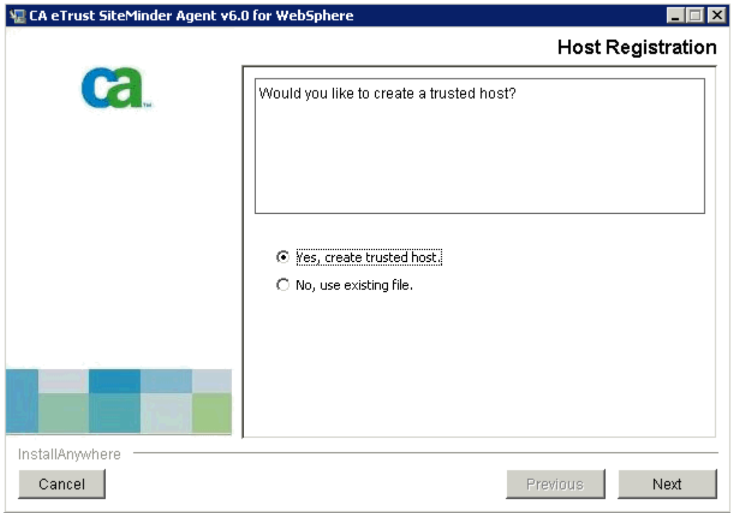
Choose WebSphere Folder

Please choose the folder where WebSphere 6.0 is installed.

Please Choose a Folder:

C:\IBM\WebSphere\AppServer

Select Yes, create a trusted host:


CA eTrust SiteMinder Agent v6.0 for WebSphere

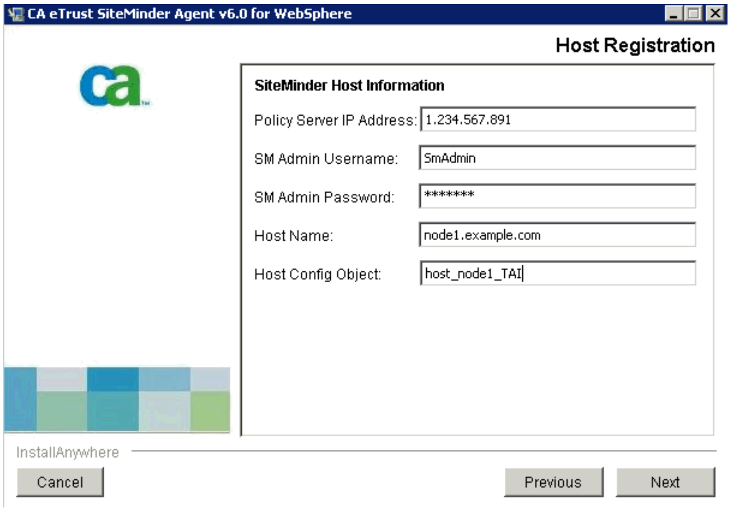
Host Registration

Would you like to create a trusted host?

● Yes, create trusted host.

○ No, use existing file.

Enter the information of the SiteMinder server, click Next to continue:


CA eTrust SiteMinder Agent v6.0 for WebSphere

Host Registration

SiteMinder Host Information

Policy Server IP Address: 1.234.567.891

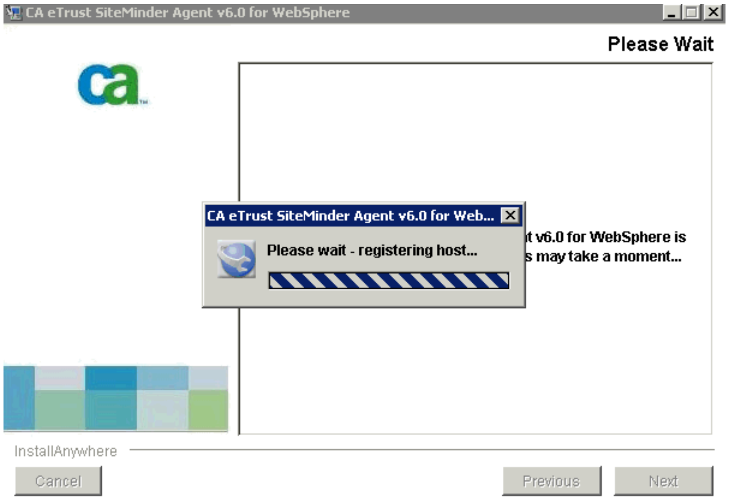
SM Admin Username: SmAdmin

SM Admin Password: *******

Host Name: node1.example.com

Host Config Object: host_node1_TAI

Allow the wizard time to register the host :


CA eTrust SiteMinder Agent v6.0 for WebSphere

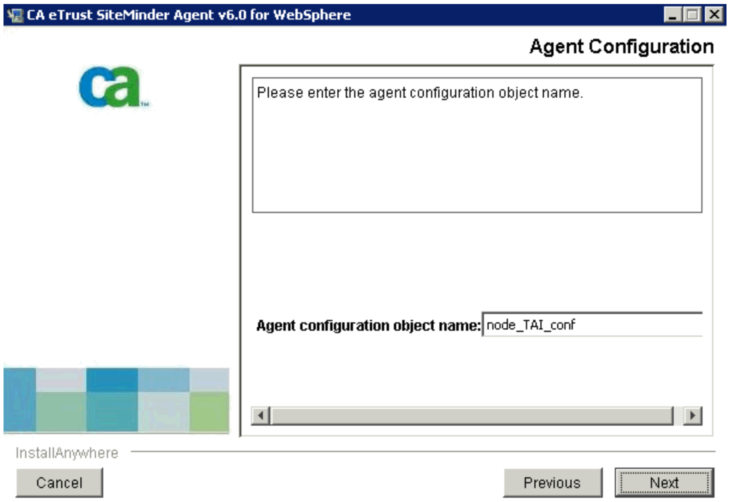
Please Wait

CA eTrust SiteMinder Agent v6.0 for Web...

Please wait - registering host...

t v6.0 for WebSphere is
s may take a moment...

Enter the agent configuration object name and click next :

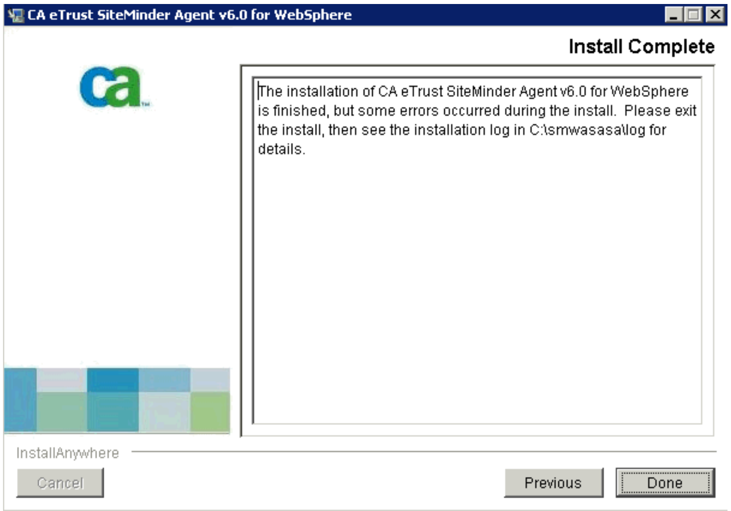

CA eTrust SiteMinder Agent v6.0 for WebSphere

Agent Configuration

Please enter the agent configuration object name.

Agent configuration object name: node_TAI_conf

Review any errors messages in the installation log. In this case there are benign errors. Click Done to exit the wizard.



The installation of CA eTrust SiteMinder Agent v6.0 for WebSphere is finished, but some errors occurred during the install. Please exit the install, then see the installation log in C:\smwasasa\log for details.

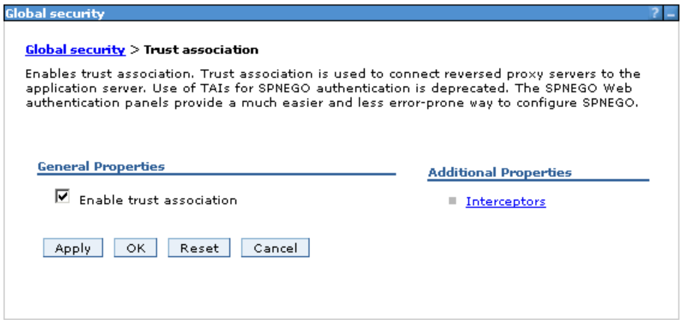
In this case the installation log at C:\smwasasa\log\CA_eTrust_SiteMinder_Agent_v6.0_for_WebSphere_InstallLog.log reports the following, again there are no fatal errors so we are safe to proceed :

```
Summary

-------


Installation: Successfulwith errors.


96 Successes

0 Warnings

1 NonFatalErrors

0 FatalErrors
```

Actions on WebSphere Application Server post Agent Installation

When the Application Server Agent is configured ensure to copy smagent.properties from the agent installation directory - smwasasa\conf to AppServer\profiles\AppSrv01\properties

Configure Trust Association Interceptor on WebSphere Application Server. From the deployment manager administrative console for WebSphere Application Server, click Security > Global security -> Web and SIP security, c



Global security

Global security > Trust association

Enables trust association. Trust association is used to connect reversed proxy servers to the application server. Use of TAIs for SPNEGO authentication is deprecated. The SPNEGO Web authentication panels provide a much easier and less error-prone way to configure SPNEGO.

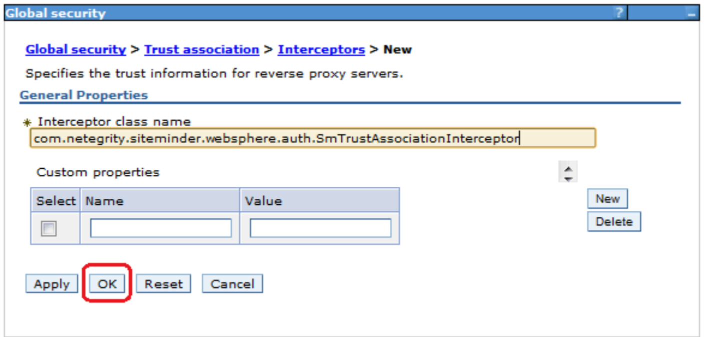
General Properties

☑ Enable trust association

Additional Properties

- Interceptors

Next Click Interceptors, Click the new button and add an interceptor with the following name (com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor). Click OK and save the change.



Global security

Global security > Trust association > Interceptors > New

Specifies the trust information for reverse proxy servers.

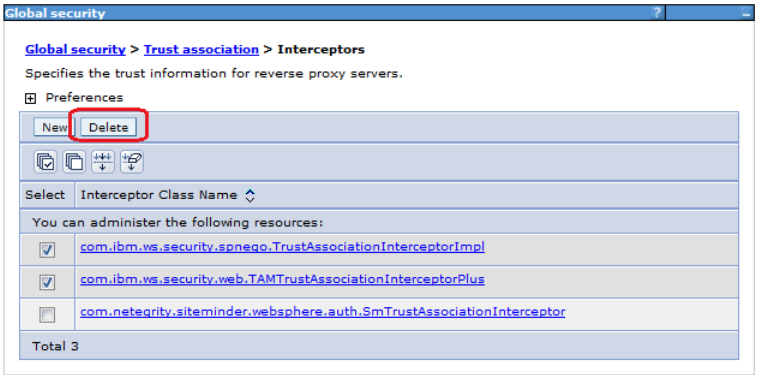
General Properties

* Interceptor class name
com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor

Custom properties

Select	Name	Value
□		

It is OK to delete any unused interceptors - in this case the interceptor we added is the only one required for SiteMinder enablement. Leaving these other interceptors inplace will not cause any issues but will results in error r
and save this change.



Global security

Global security > Trust association > Interceptors

Specifies the trust information for reverse proxy servers.

⊞ Preferences

Select	Interceptor Class Name
You can administer the following resources:	
☑	com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl
☑	com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus
□	com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor
Total 3	

Actions on HTTP Server post Agent Installation

Create rewrite rules to remap Atom API requests and to redirect URLs when users log out of Lotus Connections. Open the IBM HTTP Server httpd.conf configuration file. The file is stored in the C:\IBM\HTTPServer\conf dire
httpd.conf below shows these rules implemented in both the HTTP and HTTPS sections of this file. The rules added are shown in bold, your httpd.conf should reflect the below when this step is completed. In this extract the
they will be redirected back to the page at home.example.com, which may be a corporate homepage for example. When this change is made save and close the httpd.conf file. Restart the IBM HTTP Server.

```
RewriteEngine on

RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)

RewriteCond %{QUERY_STRING} !=logoutExitPage=http://home.example.com

RewriteRule /(.*)/ibm_security_logout(.*)  /homepage/web/ibm_security_logout?logoutExitPage=http://home.example.com [noescape,L,R]
```

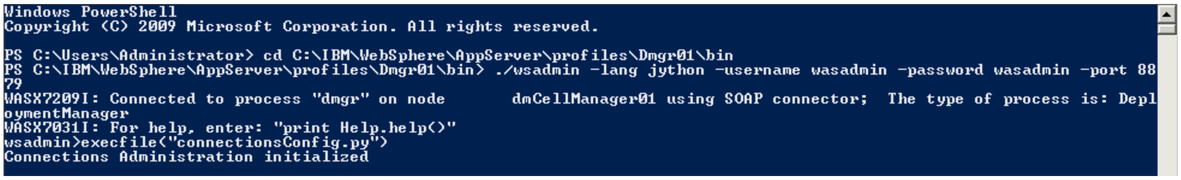
```
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/api/(.*) /blogs/roller-ui/rendering/api/$1/api/$2 [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/tags/atom(.*) /blogs/roller-ui/rendering/feed/$1/tags/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/entries/atom(.*) /blogs/roller-ui/rendering/feed/$1/entries/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/comments/atom(.*) /blogs/roller-ui/rendering/feed/$1/comments/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/blogs/atom(.*) /blogs/roller-ui/rendering/feed/$1/blogs/atom/ [R,L]

#Connections Config for SSL
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName connections.example.com
SSLEnable

RewriteEngine on
```

```
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)

RewriteCond %{QUERY_STRING} !=logoutExitPage=http://home.example.com

RewriteRule /(.*)/ibm_security_logout(.*)  /homepage/web/ibm_security_logout?logoutExitPage=http://home.example.com [noescape,L,R]



RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)

RewriteRule ^/blogs/(.*)/api/(.*) /blogs/roller-ui/rendering/api/$1/api/$2 [R,L]

RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)

RewriteRule ^/blogs/(.*)/feed/tags/atom(.*) /blogs/roller-ui/rendering/feed/$1/tags/atom/ [R,L]

RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)

RewriteRule ^/blogs/(.*)/feed/entries/atom(.*) /blogs/roller-ui/rendering/feed/$1/entries/atom/ [R,L]

RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)

RewriteRule ^/blogs/(.*)/feed/comments/atom(.*) /blogs/roller-ui/rendering/feed/$1/comments/atom/ [R,L]

RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)

RewriteRule ^/blogs/(.*)/feed/blogs/atom(.*) /blogs/roller-ui/rendering/feed/$1/blogs/atom/ [R,L]



</VirtualHost>

</IfModule>

SSLDisable
```

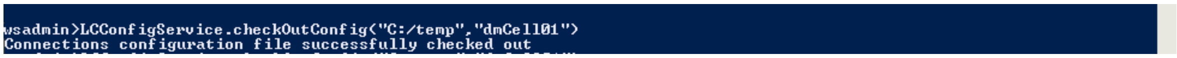
Configure Lotus Connections Custom Authenticator for SiteMinder

The customAuthenticator element in the LotusConnections-config.xml file defines some key parameters of your single sign-on (SSO) solution. The configuration settings that you can specify in this XML element only affect ba customAuthenticator element can differ, depending on the SSO solution that you have implemented. Most attributes are optional, but some might be mandatory in the context of your SSO solution. For more information, see th topic.

Add a SiteMinder authenticator property to the Lotus Connections configuration by editing the LotusConnections-config.xml file. Start the wsadmin client and check out the Lotus Connections configuration file.



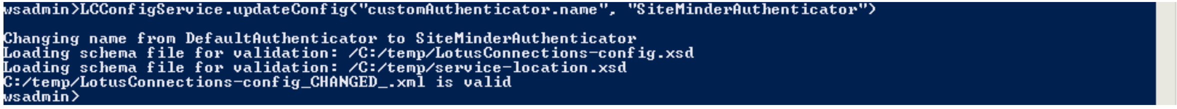
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin
PS C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin> ./wsadmin -lang jython -username wasadmin -password wasadmin -port 88
79
WASX7209I: Connected to process "dmgr" on node       dmCellManager01 using SOAP connector;  The type of process is: Depl
oymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("connectionsConfig.py")
Connections Administration initialized
```



```
wsadmin>LCConfigService.checkOutConfig("C:/temp","dmCell01")
Connections configuration file successfully checked out
```

Update the custom authenticator values by running the following commands:

Configure the custom authenticator to support server-to-server authentication for SiteMinder:



```
wsadmin>LCConfigService.updateConfig("customAuthenticator.name", "SiteMinderAuthenticator")

Changing name from DefaultAuthenticator to SiteMinderAuthenticator
Loading schema file for validation: /C:/temp/LotusConnections-config.xsd
Loading schema file for validation: /C:/temp/service-location.xsd
C:/temp/LotusConnections-config_CHANGED_.xml is valid
wsadmin>
```

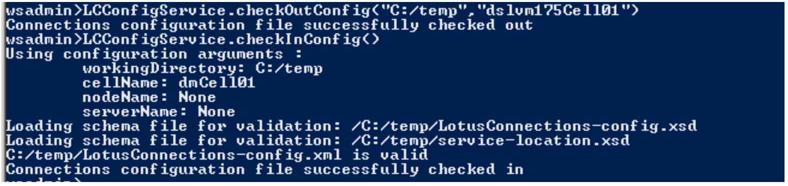
Set the value of the custom.authenticator.cookieTimeout parameter to be equal to or less than the maximum timeout and idle timeout values already configured. To do this you must open the LotusConnections-config.xml fron of this file. Specify the timeout value in minutes. In this case 60 minutes is the specified timeout value.

Note:when your production environment is ready, set the AllowSelfSignedCerts property to false. In a similar fashion to adding CookieTimout this must be done manually on the checked out LotusConnections-config.xml befo

The below is a snippet of the content of the XML as it should look when updated with the aforementioned values:

```
<customAuthenticator name="SiteMinderAuthenticator" >

     <attribute key="AllowSelfSignedCerts" value="true" />

       <attribute key="CookieTimeout" value="60" />

</customAuthenticator>
```

Check the LotusConnections-config.xml file back in by running the following command:



```
wsadmin>LCConfigService.checkOutConfig("C:/temp","dslvm175Cell01")
Connections configuration file successfully checked out
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
        workingDirectory: C:/temp
        cellName: dmCell01
        nodeName: None
        serverName: None
Loading schema file for validation: /C:/temp/LotusConnections-config.xsd
Loading schema file for validation: /C:/temp/service-location.xsd
C:/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
```

Update the reauthenticate property in the files-config.xml file. When this property is set to false, and when a Lotus Connections application detects a session timeout, users must log in again through the SSO authentication n

1. Login to the wsadmin client.
2. Execute the following command to load files administration - execfile("filesAdmin.py")
3. Execute the following command to check out the files configuration file - FilesConfigService.checkOutConfig("*C:/temp*","dmCell01")
4. Update the reauthenticate property by running the following command - FilesConfigService.updateConfig("security.reauthenticateAndSaveSupported", "false")
5. Check the files-config.xml file in by running the following command - FilesConfigService.checkInConfig()

Enabling and Disabling SiteMinder on the Configuration

If there is need to enable or disable SiteMinder at any point do the following :

1. Edit the WebAgent.conf on the HTTP Server machine (HTTPServer/conf/WebAgent.conf) and set "EnableWebAgent=NO". Restart the IBM HTTP Server.
2. Change the custom authenticator back to the default authenticator in the LotusConnections-config.xml.
3. Edit smwasasa/conf/AsaAgent-assertion.conf on both nodes and set "EnableWebAgent=NO".
4. Resynchronise nodes and restart Lotus Connections 3.0.

Repeat this process to enable SiteMinder and instead set EnableWebAgent=YES where we set it to NO before. You must also re-enable the custom authenticator in the LotusConnections-config.xml and restart the deployme

When SiteMinder is enabled the following message should appear in the SystemOut.log for all Lotus Connections application servers to indicate SiteMinder has loaded correctly with the config:

```
[10/11/10 12:45:23:225 EDT] 00000000 TrustAssociat A   SECJ0121I: Trust Association Init class com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor loa
```

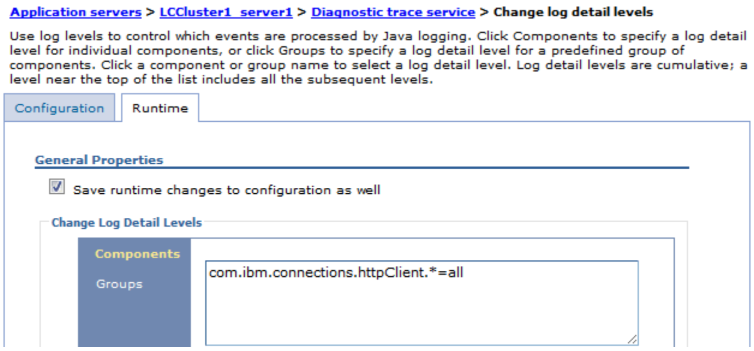
Troubleshooting SiteMinder Issues

The following section outlines how to gather trace and log information from the servers for troubleshooting purposes. There is also a common issue outlined with a solution and a brief overview of the key SiteMinder configura SiteMinder agents.

Enabling Trace

Most errors encountered in this environment are typically interservice issues - communication errors between the back-end servers often due to authorization issues caused by the introduction of SiteMinder to the configurati

```
com.ibm.connections.httpClient.*=all
```



Application servers > LCCluster1_server1 > Diagnostic trace service > Change log detail levels

Use log levels to control which events are processed by Java logging. Click Components to specify a log detail level for individual components, or click Groups to specify a log detail level for a predefined group of components. Click a component or group name to select a log detail level. Log detail levels are cumulative; a level near the top of the list includes all the subsequent levels.

General Properties

☑ Save runtime changes to configuration as well

Change Log Detail Levels

com.ibm.connections.httpClient.*=all

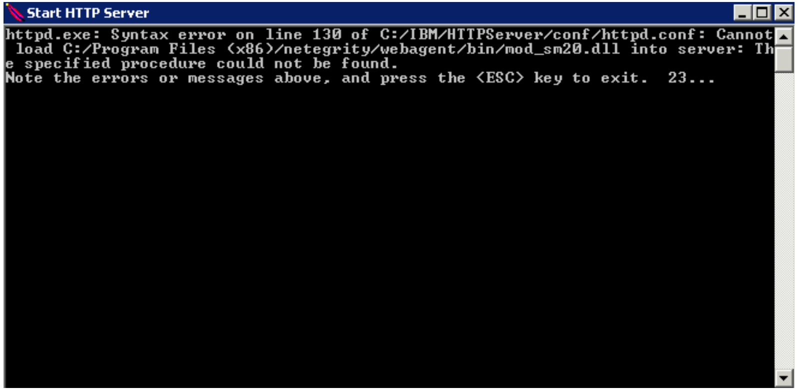
Log Files to Help Diagnose Issues

To get complete overview of any issues on the system with SiteMinder enabled the following log files should be consulted:

- **Lotus Connections Server Log Files**
- SystemOut.log
- trace.log (if applicable)
- **SiteMinder Log Files (On Nodes...)**
- smwasasa/log/smasa.log
- smwasasa/log/sm_tai.log
- **SiteMinder Log Files (On web server...)**
- nnetegrity/webagent/log/wa.log
- netegrity/webagent/log/wa_trace.log
- **SiteMinder Server Log Files**
- Consult the SiteMinder documentation to uncover what traces and logs can be enabled / referenced on the SiteMinder server side.

Common Issue - HTTP Server does not Start with SiteMinder Enabled

The following error message occurs when attempting to start the HTTP Server.



```
httpd.exe: Syntax error on line 130 of C:/IBM/HTTPServer/conf/httpd.conf: Cannot
 load C:/Program Files (x86)/netegrity/webagent/bin/mod_sm20.dll into server: Th
e specified procedure could not be found.
Note the errors or messages above, and press the <ESC> key to exit.  23...
```

Open the httpd.conf on the webserver and comment out the line containing mod_sm20.dll below.

```
#LoadModule sm_module "C:/Program Files (x86)/netegrity/webagent/bin/mod_sm20.dll"
```

Now add the below line ending with sm22.dll in its place to load the correct module for SiteMinder Web Agent to work as expected.

```
LoadModule sm_module "C:/Program Files (x86)/netegrity/webagent/bin/mod_sm22.dll"
```

SiteMinder Configuration Files created by Web Agent and TAI/ASA

Here is a sample of the key configuration files on the nodes which are correctly configured. Note the relationship between all of the files below. Changes to these files require a restart to the web server in case of web agent a

WebAgent.conf

WebAgent.conf is found in /conf/WebAgent.conf and refers to the AgentConfigObject and SmHost.conf (which contains the policy server connection details). Also note the EnableWebAgent parameter.

```

# WebAgent.conf - configuration file for SiteMinder Web Agent

# Web Agent Version = 6QMR5, Build = 852, Update = 0


#agentname="<AgentName>, <IPAddress>"

HostConfigFile="/opt/netegrity/webagent/config/SmHost.conf"

AgentConfigObject="connections_wa_conf"

EnableWebAgent="YES"

ServerPath="/opt/IBM/HTTPServer/conf"

localconfigfile="/opt/IBM/HTTPServer7/conf/LocalConfig.conf"

LoadPlugin="/opt/netegrity/webagent/bin/libHttpPlugin.so"

#LoadPlugin="/opt/netegrity/webagent/bin/libAffiliate10Plugin.so"

#LoadPlugin="/opt/netegrity/webagent/bin/libSAMLAffiliatePlugin.so"

#LoadPlugin="/opt/netegrity/webagent/bin/libeTSSOPlugin.so"

#LoadPlugin="/opt/netegrity/webagent/bin/libIntroscopePlugin.so"
```

```
LogFile="YES"
LogFileName="/opt/netegrity/webagent/log/wa56.log"
LogAppend="NO"
TraceFile="YES"
TraceFileName="/opt/netegrity/webagent/log/wa56_trace.log"
TraceAppend="NO"
TraceConfigFile="/opt/netegrity/webagent/config/webagenttrace.conf"
```

SmHost.conf

SmHost.conf is found at /bin/SmHost.conf, refers to the policy server by IP address. It also contains the hostname and hostconfigobject reference.

```

# Host Registration File - SmHost.conf
#
# This file contains bootstrap information required by
# the SiteMinder Agent API to connect to Policy Servers
# at startup.  Be sure the IP addresses and ports below
# identify valid listening Policy Servers.  Please do not
# hand edit the encrypted SharedSecret entry.

hostname="node1.example.com"
hostconfigobject="host_node_TAI"
policyserver="9.162.138.40,44441,44442,44443"
```

```
requesttimeout="60"

sharedsecret="{RC2}jEJuWUWx0sCpKF6D4mUIkWxLBjAHFvKW0ArU/khAqlmTRFziYgglFlRRppcPGaQJhJzjRTzC1VdS70um1Le/+mzTeGEpFOtTwurkmSJy2DCECGD0BAGDGTvsezeisbR

sharedsecrettime="1277806946"
```

AsaAgent-assertion.conf

AsaAgent-assertion.conf, found at /conf/AsaAgent-assertion.conf, contains an EnableWebAgent flag as well as references SmHost.conf and holding the value of the agent configuration object

```
#######################################################

## SiteMinder IBM WebSphere Application Server Agent

#######################################################

EnableWebAgent="YES"

HostConfigFile="/opt/smwasasa/bin/SmHost.conf"

AgentConfigObject="node_TAI_conf"
```

smagent.properties

SmAgent.properties, found at /conf/smagent.properties, is created when the ASA is registered. It contains the location of the AsaAgent-assertion.conf and is copied to /profiles/AppSrv01/properties on both nodes during the S

```
################################################################

# SiteMinder Generic Application Server Agent Properties File

################################################################

logfilename="/opt/smwasasa/log/smasa.log"

loglevel="4"

logappend="NO"
```

```
logfile="YES"

logconsole="NO"

smazconf="/opt/smwasasa/conf/AsaAgent-az.conf"

smauthconf="/opt/smwasasa/conf/AsaAgent-auth.conf"

smassertionconf="/opt/smwasasa/conf/AsaAgent-assertion.conf"
```

About the Author

Colm O'Brien is a member of the Lotus Connections System Verification Test (SVT) team and works in the area of product deployment and reliability testing. Colm has worked extensively in the area of SiteMinder Single Sig

Article information

Category:	Deployments			
Tags:	3, deploying, 3_deployment, scenarios, test_infrastructure, siteminder, single sign on, sso, security			
This Version:	Version 9	June 21, 2011	12:36:03 PM	by Amanda J Bauman

Attachments (0)

Versions (9)