E-Authentication Cookbook

Version 1.0.0
July 30, 2004

Executive Summary

This document provides assistance to federal Agencies, Credential Service Providers (CSPs), vendors and other stakeholders who wish to participate in the E-Authentication Initiative. This cookbook contains detailed descriptions for many technical and non-technical procedures, and for software and hardware configurations. In the context of this cookbook, recipes are provided to be a time-saver for those you are responsible for integration with the E-Authentication Initiative. These recipes are designed to answer chronic questions that result from implementing a new and complex architecture required for federated identity management. Recipes are organized in four categories: Processes; Integration; Implementation; and Products and Services.

Table of Contents

1 INTRODUCTION

This document presents specific information for federal agencies, credential service providers, vendors and other stakeholders who wish to participate in the E-Authentication Initiative. It provides 'recipes'--detailed descriptions of technical and non-technical procedures, software and hardware configurations, and the like. These procedures are used to accomplish tasks necessary to implement the E-Authentication Initiative. Building the large community of trust that makes up the E-Authentication Initiative requires the skills of a diverse group of participants; these recipes are annotated with the intended audience, to simplify locating and using the specific recipe needed.

1.1 Purpose

The purpose of this cookbook is to provide detailed procedures for stakeholders implementing E-Authentication.

1.2 Assumptions

Technical staff supporting Agency Applications (AA), and those in organizations that plan to serve as Credential Service Providers (CSPs), should reference this document. For other audiences, like agency program managers or non-technical staff in vendor organizations, there is other documentation and guidance available. Managers will benefit from the guidance available at http://www.cio.gov/eauthentication/library.htm and from two companion E-Authentication Handbooks, one for AAs and one for CSPs.

Readers of this cookbook are assumed to have some familiarity with the E-Authentication Initiative. The reader should understand their role in the Initiative (for example, as an AA or a CSP, or maybe even both). In addition, readers should have knowledge of the high-level E-Authentication architecture, and a clear idea of the role their application or service plays in this architecture.

1.3 Scope

This cookbook provides detailed descriptions of many technical and non-technical-procedures and configurations for AAs, CSPs, and other stakeholders.

This cookbook uses the term "recipe" to denote a detailed description of actions necessary to accomplish a goal. In the context of this cookbook, a recipe is intended to be a time-saver for the E-Authentication implementer. Recipes are designed to answer chronic questions that result from implementing a new, complex architecture required of federated identity management. This document is meant to be a source of information on practices and procedure used in implementing E-Authentication, and will grow and change over time as needs of E-Government initiatives evolve.

This cookbook uses policy and guidance information; found at http://www.cio.gov/eauthentication/library.htm.

1.4 Document Organization

The major portion of the cookbook is recipes pertaining to different aspects of the E-Authentication Initiative. Each has been given a unique identification number, for ease of location and reference. [1] In a printed version of this cookbook, each recipe can be tabbed with its number. Each recipe is also annotated with its intended audience, keywords, categories, and related topics. An index is provided so that an individual can locate recipes of interest. For example, a CSP would use the audience index to find the recipes appropriate to that role.

[1] Note-other indices will be more useful if the document is in electronic format, suitable for indexing and searching (for example, the keyword, audience, and goals characteristics.)

2 E-AUTHENTICATION RECIPES

2.1 E-Authentication Knowledge Base

Cookbook recipes are intended to continuously be identified for addition and update throughout the entire E-Authentication Initiative. Recipes identified for addition or update can be added to the Cookbook via the E-Authentication Knowledge Base lifecycle, through which suggestions are identified, reviewed, created for addition, and approved.

2.2 Recipe Properties

In this Cookbook, recipes are complex and the level of complexity differs among recipes. In order for the user to have an ease of readability, critical factors are identified as Recipe Properties. These properties highlight different factors that the user will need to consider before, during, and after execution of the recipe.

2.2.1 Audiences

Audiences are participants performing various functions or roles who will need these recipes. Certain recipes may be intended for a specific audience, since they will be the primary users of the recipe. These audiences include the following:

- Program Managers
- Other Management
- Contracting Personnel
- Security Officers
- Credential Servicing Assessors (CSAs)
- System Developers/Engineers
- Vendors
- Credential Service Providers (CSPs)
- Agencies

Audiences may also include other groups as needed. The above list should not be considered comprehensive and exclusive of any potential stakeholder.

2.2.2 Summary

Each recipe has a summary. The summary provides an explanation and context for what the reader is trying to accomplish in this recipe.

2.2.3 Keywords

Recipes also have keywords, which are common terms that the reader will find useful as a reference point or sorting mechanism for the recipes.

2.2.4 Categories

Categories are areas or main groupings where the recipes will be sorted in order for users to easily identify recipes that are suitable for them. See section 2.3.1 to see a table with recipes organized by category.

2.2.5 See Also

See Also is a section of each recipe devoted to cross-referencing other documents, subjects, and areas (for example other recipes) that the user might be interested in learning about further.

2.3 RECIPE INDEX

Recipe No.	Recipe Title
R-000001-001	Request and Obtain PKI Server Credentials From the eGovernance CA
R-000002-001	Obtain an Agency Application ID (AAid) from E-Authentication PMO
R-000003-001	Obtain an Credential Service ID (CSid) from E-Authentication PMO
R-000004-001	Browser requirements and E-Authentication
R-000005-001	AA Integration testing with the E-Authentication System
R-000006-001	Redirecting Users to the E-Authentication Portal
R-000007-001	How to Link your Agency Application to Other AAs or Websites
R-000008-001	How to Link your Agency Application with CSs
R-000009-001	Certificate Revocation List Verification & Timelines
R-000010-001	Importing Browser and Server Certificates
R-000011-001	Configuration Guide for setting up HP Select Access for an AA
R-000012-001	Configuration Guide for setting up HP Select Access for a CS
R-000013-001	Configuration Guide for Sun Java System Identity Server for an AA
R-000014-001	Configuration Guide for Sun Java System Identity Server for a CS
R-000015-001	Configuration Guide for Oblix ShareID for an AA
R-000016-001	Configuration Guide for Oblix ShareID for a CS

2.3.1 RECIPES BY CATEGORY

Table continued on next page.

Recipe 01 - Request to Obtain PKI Credentials from the eGovernance CA	
Audience(s): System Developers, Agencies, CSPs, and Other **Categories:** Processes	**Keywords:** PKI, Certificates, GA, eGovernance CA, FPKI **Also See:** Recipe 4
Version 1.0	

Summary:

The E-Authentication Project Management Office (PMO) will be responsible for the issuance of necessary server certificates at assurance levels 1 & 2 via the eGovernance CA (eGCA). These certificates are necessary to satisfy a cryptographic binding between the authentication and transaction requirement, which is available using client certificates over SSL or TLS protocols.

PKI Credentials from the eGCA are only required for AAs and CSs operating at assertion-based assurance levels (1 & 2). These certificates enable an SSL/TLS connection with CSs to transfer the SAML Assertion (or other adopted assertion schemes) securely, thus enabling E-Authentication. Certificates issued specifically by the eGCA are required as part of the architecture to establish the credibility of the claimant as an AA/CS is approved to participate in E-Authentication.

The eGCA is not involved in issuing PKI credentials at certificate-based assurance levels (3 & 4). As a result, Agencies or CSPs operating at assurance levels 3 or 4 should seek their credentials from the Federal Bridge Certificate Authority (FBCA). Contact information for the FBCA can be found at http://www.cio.gov/fbca.

Requirements:

1. In order to request credentials, you must be either an Agency approved for pilot or an approved CSP.

2. To request PKI credentials, please request credential issuance through your assigned E-Authentication Initiative Agency (EIA) Relationship Manager or Credential Manager. Your E-Authentication point of contact will make contact with the FBCA Operation Authority team and issue an authorization letter to begin the credential issuance process.

3. Once the necessary verifications and authorizations are exchanged, the FBCA Operating Authority (OA) team creates and verifies the certificate contents. The certificate(s) will then be sent to the approved technical point of contact at the CSP or Agency via secure, non-electronic means or through the use of digital signatures.

Important References:

The eGCA is operated by the Federal PKI Operating Authority. More information about the FPKI and the Federal Bridge Certificate Authority (FBCA) can be found at the following websites: http://www.cio/gov/fpkipa, and http://www.cio.gov/fbca.

Recipe 02 - Obtaining an Agency Application ID (AAid) from E-Authentication PMO	
Audience(s): AAs, Program Managers, Other Management **Categories:** Processes	**Keywords:** Agency ID, AAID, AA identifier, PMO, Agency Relationship Manager, Agency Application (AA) **Also See:** Recipe 1
	Version 1.0

Summary:

The term AAid is an acronym for Agency Application (AA) Identifier, which is a unique identifier, assigned to each AA-interface within E-Authentication. AA-interfaces are defined as distinct user-interaction services, such as an admin service or a general user service. The AAid plays an important role in the use cases described in the Technical Architecture, which detail the redirection between the Portal, CS, and the AA. Each AA needs to have a unique AAid for global recognition and access by other components of the E-Authentication system.

During the application process to join E-Authentication, each potential Agency is assigned to one of the Agency Relationship Managers at the PMO. This Agency Relationship Manager is responsible for supplying the Agency with the assigned AAid upon approval to pilot. AAid's are assigned to each E-Authentication AA, regardless of assurance level, to provide an application identity mechanism across E-Authentication.

Agencies wishing to obtain an AAid should contact the E-Authentication PMO. Agency applications piloting or otherwise undergoing integration with E-Authentication are assigned to an Agency Relationship Manager, who will be responsible for assigning a unique AAid to each interface.

Requirements:

- Assignment of an Agency Relationship Manager for your Agency by the E-Authentication PMO

Important References:

For more information on the AA process, please reference the following links on the E-Authentication website:

a. Key Contacts: http://www.cio.gov/eauthentication/key_personnel.htm
b. Pilot Funding/Resource Requests: http://www.cio.gov/eauthentication/documents/EApilotFunding.pdf

Recipe 03 - Obtaining an Credential Service ID (CSid) from E-Authentication PMO	
Audience(s): Other Managers, IT Management, CSPs **Categories:** Processes	**Keywords:** Credential Service ID, CSID, CS identifier, Credential Service Application, CAF, Credential Assessment Framework **Also See:** Recipe 1
Version 1.0	

Summary:

The term CSid is an acronym for Credential Service (CS) Identifier. CSids are unique identifiers assigned to each CSP within E-Authentication, and assigned to each CS, regardless of assurance level. This provides a CS-identity mechanism across E-Authentication and is necessary to enable consistency in the federation-based architecture of E-Authentication, in which no central "coordinator" role exists.

During the application process to join E-Authentication, each potential CSP is assigned to one of the Credential Managers at the PMO. This Credential Manager is responsible for supplying the CSP with the assigned CSid upon successful completion of a credential assessment and approval from the PMO.

Requirements:

- Application to be a CSP accepted by the PMO
- Credential Assessment Framework (CAF) review successfully completed by the assessor(s) at the requested assurance level
- E-Authentication Program Manager (PM) has provided approval for the CS in accordance with the CAF.

Important References:

1. For more information on the E-Authentication Engagement Process, please refer to the E-Authentication Handbook for Credential Service Providers.
2. For more information on the CS application process, please reference the following links on the E-Authentication website:
    a. Key Contacts: http://www.cio.gov/eauthentication/key_personnel.htm
    b. CS Application Process: http://www.cio.gov/eauthentication
    c. Credential Assessment Framework & supplementary credential assessment profiles: http://www.cio.gov/eauthentication/library.htm

Please note that evidence of compliance with CAF requirements does not necessarily constitute a complete audit and review of all policies and procedures at a CSP. Rather, this is intended to provide CSPs with the ability to submit records from a recent audit, or even excerpts from policies and procedures proving compliance.

Recipe 04 - Browser Requirements and E-Authentication	
Audience(s): CSPs, Agencies, Program Managers, System Owners, Other Management, and System Developers **Categories:** Products & Services, Integration	**Keywords:** Browser, Web, Browser Requirements, SSL, and Cookie **Also See:** Recipes 2 and 3
	Version 1.0

Summary:

The question of browsers and browser compatibility is often a serious consideration in the design of web applications and systems. In light of these known factors, the E-Authentication Initiative has taken steps to ensure relatively low minimum requirements for user browsers. These requirements should be compatible with all modern and previous generation browsers. These requirements consist of:

a. TLS/SSL Support (128-bit encryption)

b. Session Cookies (Required for single sign-on only)

c. Ability to process a "hint" list and present user-designated PKI credentials (for high-assurance applications)

The E-Authentication Initiative is a strong supporter of standards and compatibility, and does not mandate specific browsers or versions for use with E-Authentication. Support for standards and broad interoperability are a cornerstone of E-Authentication's objective of transparency and interoperability in order to ensure simplicity and foster trust.

While E-Authentication itself has low minimum requirements, it is permissible for CSs and AAs to have additional browser requirements beyond the support of TLS/SSL and Session Cookies. These additional requirements may be necessary to enable certain functions within the CSP or Agency systems. Each CSP or Agency is responsible for delineating any requirements for their services that are more restrictive than the set outlined by the E-Authentication Initiative. The E-Authentication Initiative strongly recommends that all users upgrade their browsers to the latest version and install any and all patches to minimize vulnerabilities associated with unpatched software.

Recipe 05 - AA Integration Testing with the E-Authentication System	
Audience(s): Program Management, System Developers, and System Owners	**Keywords:** AA, Agency Application, Integration Testing, Integration
Categories: Implementation, Integration	**Also See:** Recipes 1, 7, 8, 9, 10
	Version 1.0

Summary:

The success of the E-Authentication Initiative is rooted entirely in interoperability between distinct, unrelated systems to enable credential reuse and facilitate trusted business-to-government, government-to-government, and citizen-to-government electronic interaction. As a result, the Initiative considers the question of interoperability verification very seriously. All prospective components of the E-Authentication architecture, such as adopted scheme COTS, protocol translators, and the Portal, are tested for interoperability to ensure the integrity of the E-Authentication system.

The E-Authentication Initiative also requires interoperability testing with each AA prior to interaction with users. While each component is tested for interoperability, the complexity in product configuration, deployment, and integration are sufficiently high to require testing of the final AA system. Small, seemingly insignificant configuration changes or implementation decisions can result in non-interoperability with the standards adopted by E-Authentication. A final interoperability test ensures that each AA will interact properly with the current production E-Authentication infrastructure, thus ensuring the required minimum level of service to users.

As with all testing, there is the possibility that an AA may not meet all requirements to be approved for production use. The Interoperability lab will provide feedback to the appropriate system owner(s) to assist in the identification of the non-interoperable elements. It should be noted, however, that many AA implementations will involve customization and interaction with legacy or proprietary systems. The Interoperability Lab will not be able to provide step-by-step guidance in each case.

The testing process for an AA will begin with a notification to the assigned Agency Relationship Manager that the system is ready for interoperability testing. The Agency Relationship Manager will coordinate a test with the Agencies primary point of contact and the Interoperability Lab. The E-Authentication Initiative strongly recommends that Agencies communicate any required timelines for participating in E-Authentication. Communication of critical timelines and milestones will enable all participants to better coordinate and assist your agency in meeting those timeframes.

The exact set of test elements will change depending upon the adopted scheme. However the following general concepts will be examined for all schemes:

1. Credential Verification, ex: Trust List Approach, Path Discovery & Validation, SSL/TLS Assertions

2. Credential Service user recognition & mapping to local known user store

3. Compliance with all described functionality and behavior in interface specifications

4. All use cases described in Technical Approach for the Authentication Service Component

5. Proper implementation of assurance level checks, redirections, unexpected input/output
6. Proper construction of redirection URLs
7. Implementation of the "Test" assurance level, accounts as a CS[2]
8. Implementation of the "Test" processing functionality as an AA[3]
9. Interoperability compliance with published E-Authentication standards for scheme(s) in use by the AA

Important References:

For more information on the E-Authentication Interoperability Lab, please refer to the E-Authentication Interoperability Lab Concept of Operations. This document is available online at http://www.cio.gov/eauthentication

[2] See section 2.3 of E-Authentication Interface Specifications for the SAML Artifact Profile

[3] See section 3.2 of E-Authentication Interface Specifications for the SAML Artifact Profile

Recipe 06 - Redirecting Users to the E-Authentication Portal	
Audience(s): System Developers, System Owners, and CSP **Categories:** Implementation, Integration	**Keywords:** Redirect, Unauthenticated, Users, Portal **Also See:** Recipes 1, 6, 8, 9, 10
	Version 1.0

Summary:

Unauthenticated users or users with insufficient credentials will not be provided access to an AA, as this could pose a significant security risk. The E-Authentication Initiative recognizes that unauthenticated users need to be advised of their status in a user friendly way and provided a method for authenticating. This requirement is outlined in the Interface Specifications (section 3.1) and the Technical Approach for the Authentication Service Component.

In summary, users not handed-off via a CS must be redirected to the Portal with the AAid in the query string. The Portal will either request that the user select an appropriate CS or, if the user opted-into single sign-on (SSO), verify the CS-AA assurance levels are sufficient, and proceed accordingly. Users whose SSO CS assurance level is sufficient for the chosen AA will be handed off to the CS. After that hand off occurs, the user will be immediately handed off to the intended AA, per the use case entitled "Starting at the Agency Application". Unauthenticated users, or users bearing credentials of lower assurance than the AAid requires, will be redirected back to the AA after selecting and authenticating at a CS with sufficient assurance level. Together, the E-Authentication Interface Specifications for the SAML Artifact Profile and Technical Approach for the Authentication Service Component fully describe the required AA user-handling functionality.

In addition to following the Interface Specifications regarding unauthenticated users, the E-Authentication Initiative provides several useful suggestions from both public and private sector best practices that will help make the transition to E-Authentication seamless.

These suggestions are meant to supplement the Interface specifications.

1. Unauthenticated users should be presented with a screen advising them that they are not at this time authorized to access the resources, and that the process will follow these general steps:
    a. Redirect to portal
    b. Select authentication system (credential provider)
    c. Authenticate normally
    d. Automatically redirected back to current site

2. Users should also be advised that this application is a part of the E-Authentication Initiative, and can be accessed using credentials from many public and private sources. A link to the E-Authentication Initiative should appear here as well, and open the web page in a separate window.

3. Users should be allowed sufficient time to process this message before the redirect occurs. Ideally, a user-initiated action should be used to trigger the redirect, such as a button labeled "Click Here to Select a Credential" which executes the browser redirect to the portal.
4. Links to a specific CS can be added in compliance with the E-Authentication Interface Specifications
5. The redirect to the portal should be accomplished using the following URL:
    a. http://eauth.firstgov.gov/service/select?AAid=<your_AAid>

The redirection as specified by the interface specifications can be executed via different methods and technologies, such as JavaScript or Active Server Pages (ASP). A simple segment of sample code (in JavaScript) is included below to assist your efforts:

Sample:

```
<SCRIPT LANGUAGE="JavaScript">
<!—
window.location="http://eauth.firstgov.gov/service/select?AAid=<your_AAid>";
// -->
</script>
```

Requirements:

- Creation of the redirect URL as described above and in the Interface Specifications document.

Important References:

For more information on the use cases described above, please see the following documents:

- SAML Artifact Profile as an Adopted Scheme
- Technical Approach for the Authentication Service Component
- E-Authentication Interface Specifications for the SAML Artifact Profile

These documents are available on the E-Authentication website, located at http://www.cio.gov/eauthentication.

Recipe 07 - How to Link Your AA to Other AAs or Websites	
Audience(s): Program Managers, System Owners **Categories:** Implementation, Integration	**Keywords:** Agency ID, AAID, AA identifier, Link **Also See:** Recipes 1, 6, 7, 9, 10
Version 1.0	

Summary:

An important feature of E-Authentication is the ability to enable multi-domain single sign-on between disparate websites of the Federal Government. This is a powerful new capability that complements the federated architecture upon which E-Authentication is based. To support single sign-on, links between E-Authentication enabled sites should be made via the portal. Doing so ensures that appropriate CSs are always used and that single sign-on works for those users who have "opted-in."

There are two methods to create an E-Authentication compatible link to another AA. The E-Authentication architecture does provide the capability to directly hyperlink to another AA as well as hyperlink to another AA via the E-Authentication portal. For example:

Direct Hyperlink - http://www.target_AA.gov
Via Portal - http://eauth.firstgov.gov/service/select?AAid=<target_AAid>>

The first method (direct hyperlink) is the easiest and most familiar. The E-Authentication architecture specifies that the target AA will initiate a handoff (redirect) with the Portal as described in the Interface Specifications for the SAML Artifact Profile.

The second method routes users through the portal. By routing users through the portal, this ensures that users are directed to the proper URL in the case of a change, and that single sign-on is maintained if the user has opted-in.

Both methods are compatible with the single sign-on use case as described in section 3 of the SAML Artifact Profile as an Adopted Scheme document, and in the Interface Specifications for the SAML Artifact Profile.

Requirements:

- Direct hyperlinks to the destination AA are supported in the architecture.
- Links to another AA via the portal must include the AAid of the intended AA's in the querystring to work.

Important References: For more information on constructing an E-Authentication friendly hyperlink from an AA or an external (non-E-Authentication) website, please refer to Appendix A of the Technical Approach for the Authentication Service Component and the E-Authentication Interface Specifications for the SAML Artifact Profile.

Recipe 08 - How to direct users through a specific CS	
Audience(s): Program Managers, System Owners **Categories:** Implementation, Integration	**Keywords:** Agency ID, AAID, AA identifier, CS, Link **Also See:** Recipes 1, 6, 7, 8, 9
	Version 1.0

Summary:

Directing users of your AA to authenticate at a specific CS is compatible and documented with the E-Authentication Architecture. The Initiative has provided guidelines for guidelines in the E-Authentication Interface Specifications for the SAML Artifact Profile and in Appendix A of the Technical Approach for the Authentication Service Component.

Per those documents, handoff to a specific CS via the architecture requires a specially formatted hyperlink, which should generally be formatted according to the following example below:

http://eauth.firstgov.gov/service/select?AAid=<your_AAid>&CSid=<target_CSid>

The above hyperlink routes users through the Portal, which will simply verify that the assurance levels of the AAid and CSid are compatible. If the assurance levels are compatible, the Portal will directly handoff the user to the CS for authentication per the base case, or prompt the user to select a different credential service.

When using links to the portal that specify a CS, it is recommended that the website display a notice to users advising that certain credentials are preferred/required for use with the AA. In addition, it is advisable that the AA system owner maintain close operational contact with the designated CS. Changes in the assurance level of the AA or CS may result in an inability to access the AA using the CSP's credentials. If a very limited number of credential services are properly configured to interact with an AA, assurance level incompatibility can effectively deny access to the AA for users.

Requirements:

- Redirection of the user through the portal
- Inclusion of the intended CS's CSid in the querystring

Important References: For more information on constructing hyperlinks to a CS, please refer to Appendix A of the Technical Approach for the Authentication Service Component.

Recipe 09 - Certificate Revocation List Verification & Timelines	
Audience(s): Program Managers, System Owners, System Developers **Categories:** Processes, Implementation, Integration	**Keywords:** PKI, Certificates, Certificate Revocation, Revocation, CRL, AIA, SIA, CDP, OCSP, FBCA OA, FBCA **Also See:** Recipes 4, 11, 12, 13, 14, 16
	Version 1.0

Summary:

Certificates are issued by certificate authorities (CAs), which are organizations that verify identity. Certificates can be compromised via theft, loss, etc, and to ensure trust each CA provides advice regarding certificates which are no longer valid. The primary method for revoking certificates is via Certificate Revocation Lists. These freely available published documents list all the certificates issued by the specific CA that are no longer valid.

In the E-Authentication model, the eGCA or FBCA issues certificates to specific AAs or CSs. Certificates may also be issued to users who need access to resources deemed assurance levels 3 or 4. Certificate verification is necessary to prevent unauthorized access.

Within the E-Authentication program, two processes have been established for managing certificate revocation. These are Client Security Incidents and Client Routine. Client Security Incidents are revocations that are performed to prevent the compromise of security. Client routine incidents are revocations that are planned as a part of an assurance-level change, AA/CSP startup or shutdown, etc, as can be expected during the normal course of E-Authentication's operations.

For all incidents regardless of classification, the FBCA OA will be notified and after appropriate verification, will revoke the certificate(s) in question and post a new Certificate Revocation List/Certificate Authority Revocation List (CRL/CARL) within 6 hours.

Requirements:

Each participant with E-Authentication is requested to configure the appropriate software within their environment to verify the status of certificates issued by the eGCA and the Federal Bridge CA (FBCA).

Important Notes:

Agencies and CSPs at non-PKI assurance levels are not responsible for implementing the necessary infrastructure to directly accept and verify PKI credentials from users. The E-Authentication Initiative has delegated this task to protocol translators, whose role will be to translate adopted schemes and/or step-down assurance levels as necessary. The only PKI requirement for assurance levels 1 & 2 cover the use and verification of the certificates used to establish secure SSL/TLS communications for communication of the SAML assertion.

Recipe 10 - Importing Browser and Server Certificates

Table of Contents

Version 1.0

1.0 Introduction

A certificate is a digital statement issued by an authority that vouches for the identity of the holder of a private key. A certificate binds a public key to the identity of the person, computer, or service that holds the corresponding private key. Certificates often contain other information related to the public key, such as identity information about the entity that has access to a corresponding private key. Certificates are widely distributed, can be issued by numerous parties, and examined for verification without referring to a centralized database. The issuer of a certificate is attesting to the validity of the relationship using its public key and a private issued certificate.

As discussed in the Technical Approach for the Authentication Service Component document, certificates are needed to enable all agency applications regardless of assurance level. The specific uses for the certificates will differ, however, depending upon the assurance level of the application (high assurance/low assurance).

For assurance levels 1 & 2 using SAML, the certificates are required to provide a secure, trusted link between the AA and the CSP. The certificates serve two purposes – to encrypt (and secure) the identity assertion during transmission, as well as to assert the identities of the servers themselves.

Certificates are required for assurance levels 3 & 4 for PKI identity management of both the user and the AA's web server. Users will present credentials via digital certificates, which will be verified via path discovery and validation to confirm authenticity and validity. In exchange, the AA's web server provides a certificate to reassure the user that the server is indeed the intended server.

For more information regarding certificates and their role in E-Authentication, please visit the E-Authentication website at www.cio.gov/eauthentication.

This configuration guide assumes the following:

a. You are familiar with the role of certificates in the architecture
b. You are likely a systems engineer or consultant with integration experience and a strong understanding of the technical settings which will be changed.
c. You have access (either directly or through another party) to make necessary configuration changes to any required network configurations, if needed.

1.1 View Installed Certificates through Internet Explorer

One of the first steps in this recipe is to review the certificate "store" on the local computer. This is an important step, as it familiarizes you (the user) with the process of accessing, viewing, and updating the certificates on your workstation.

Note: This process is designed for users with Internet Explorer running on a Microsoft Windows platform.

To see imported certificates, open Internet Explorer

- Click on *Tools*
- Then click on *Internet Options*
- Next click on the *Content* tab (see figure 10-1)
- Click on *Certificates* button to view imported certificates (see figure 10-2)

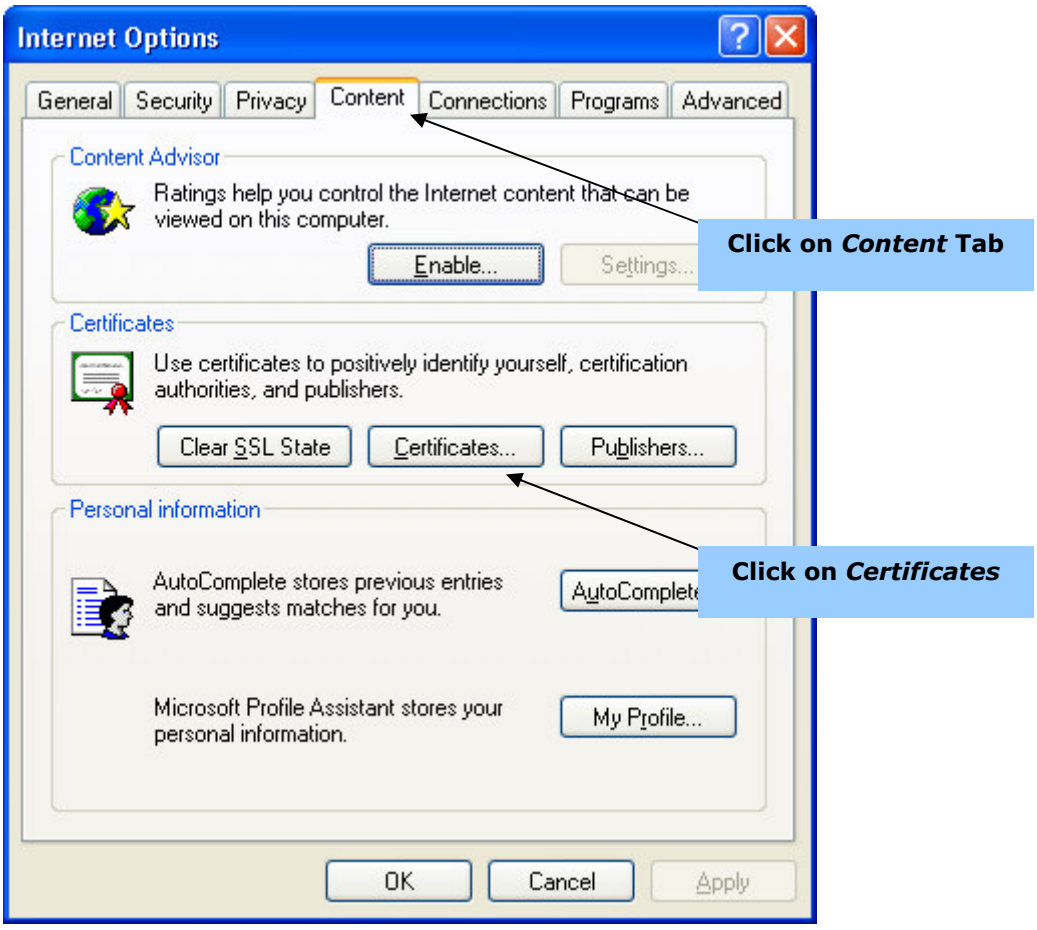


Figure 10-1: Using Internet Options to check certificates

After you click on the *Certificates* button, a window similar to Figure 10-2 will display, revealing the various certificates.

Installed certificates belonging to the current user are visible under the *Personal* tab. You can add more certificates to the Personal category if you are logged in as the Administrator. *Other People* refers to the other users on the computer. See Windows information on associating certificates with specific users.

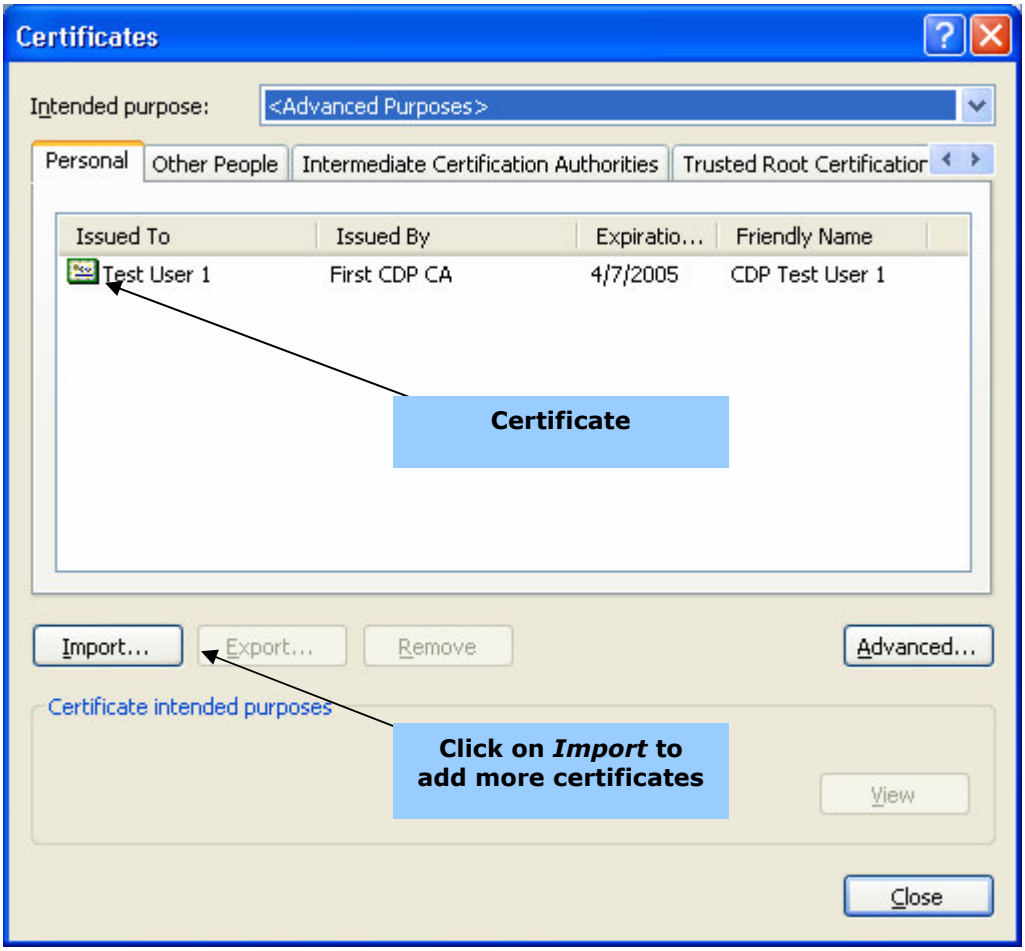


Figure 10-2: List of Certificates

2.0 Importing User Certificates into a browser.

Now that you're familiar with where certificates are stored on your local machine and how to gain access to them, the next step is to actually import your certificate for use with your web browser.

If it's not already open, double click on the Certificate file that you want to import into your browser. The certificate properties will display, as shown in figure 10-4.

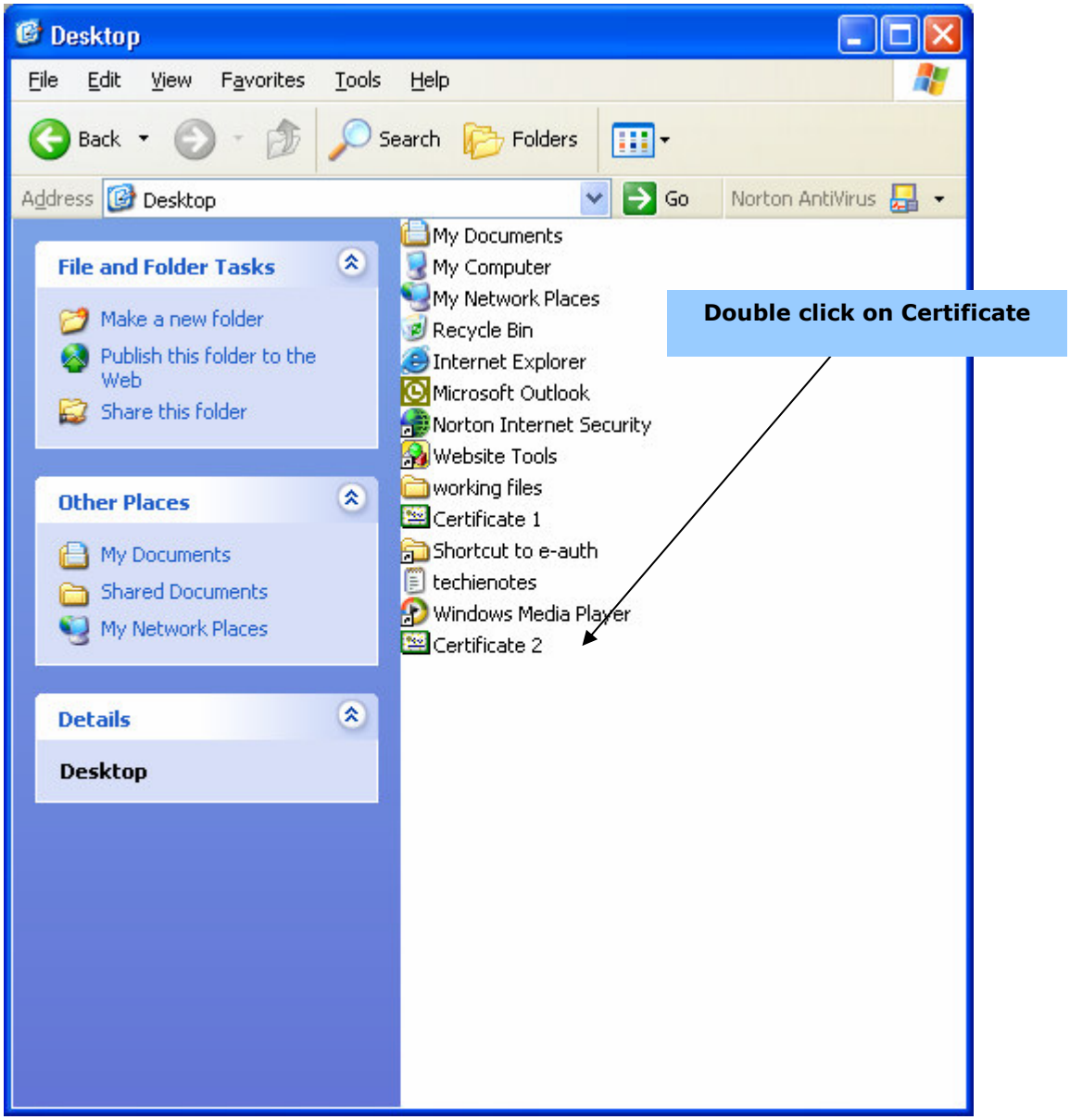


Figure 10-3: Import Certificate

After the Certificate properties window displays, click on the *Install Certificate* button.

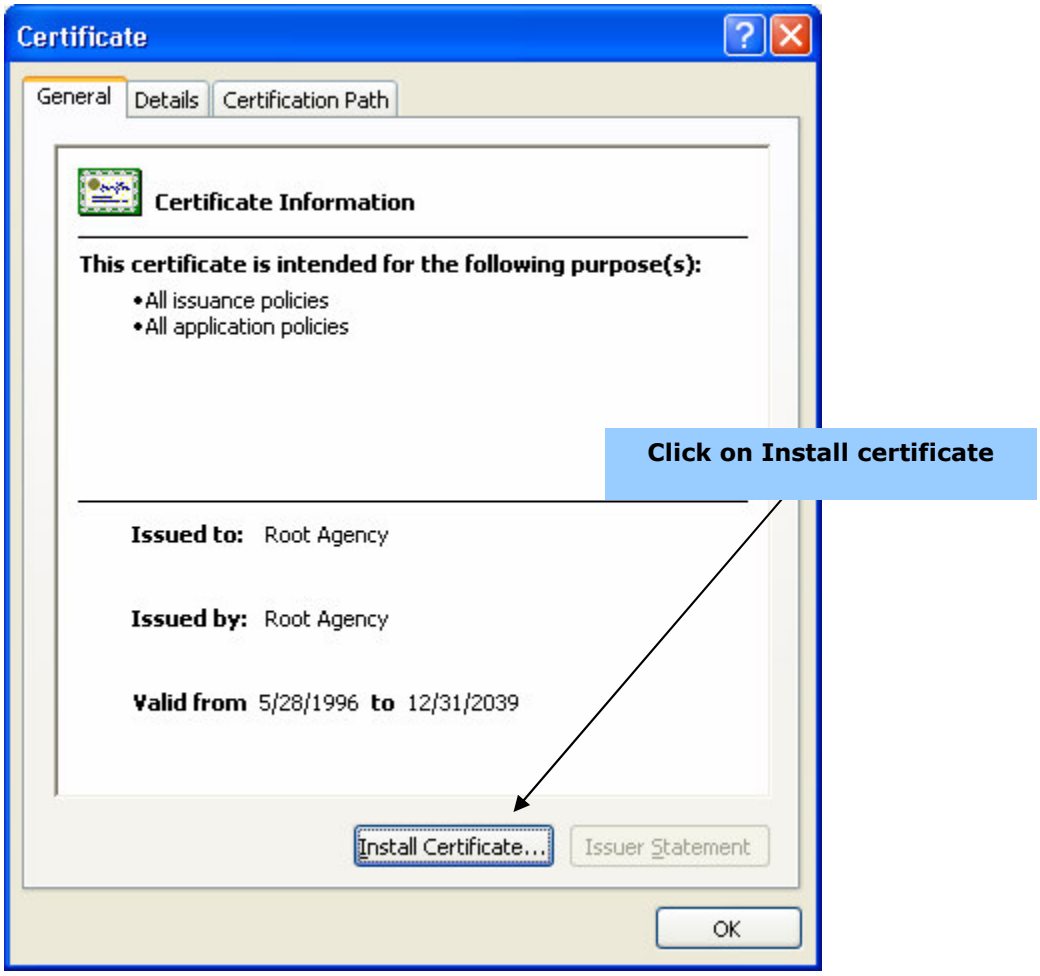


Figure 10-4: Certificate Information

After you click on the *Install Certificate* button, the Certificate Import Wizard will start up, as shown in figure 10-5. This wizard will walk you through the process of importing your certificate.

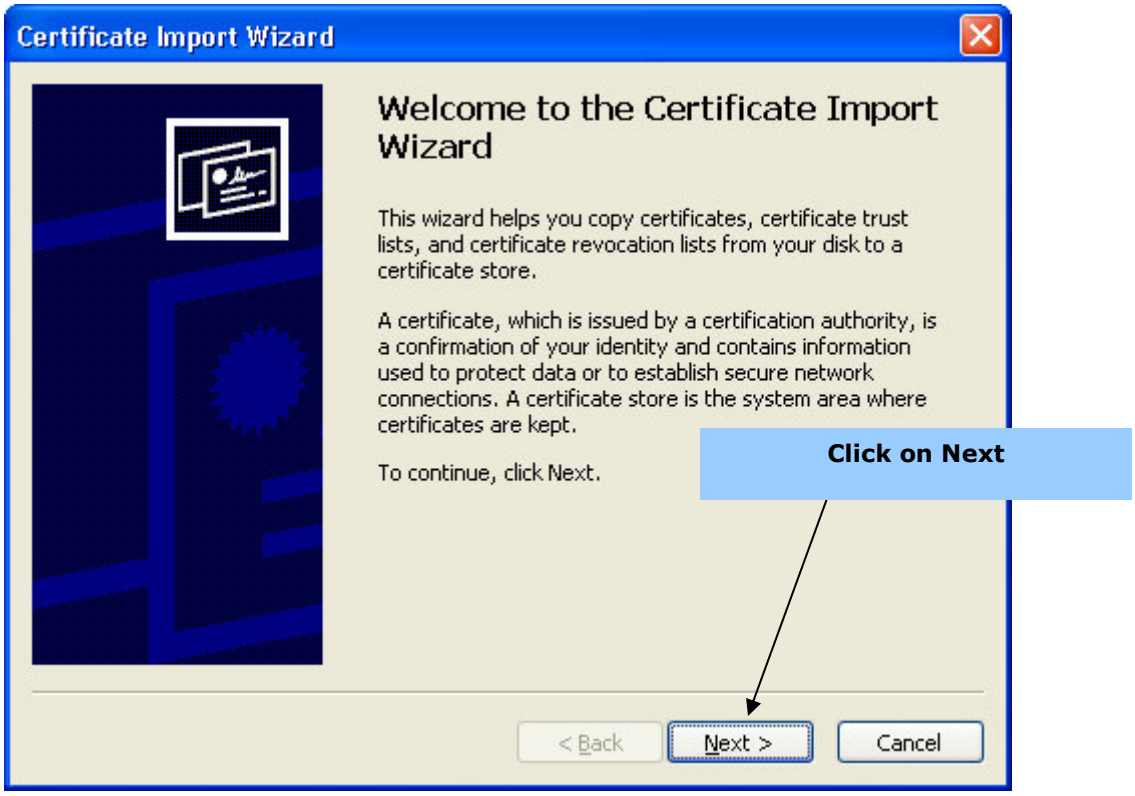


Figure 10-5: Certificate Import Wizard

After the wizard starts, click on *Next*.

When the certificate store options display, allow Windows to automatically select a certificate store. Select *Automatically select the certificate store based on the type of certificate,* and click on *Next*.

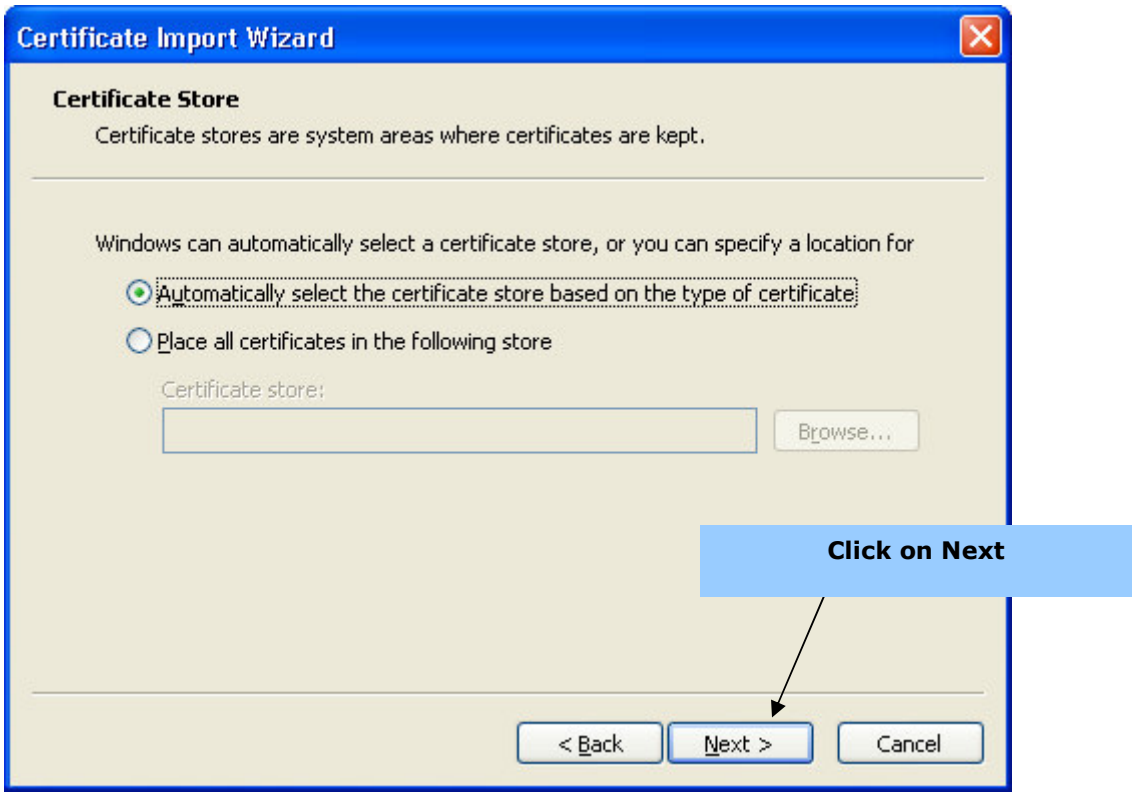


Figure 10-6: Certificate Store

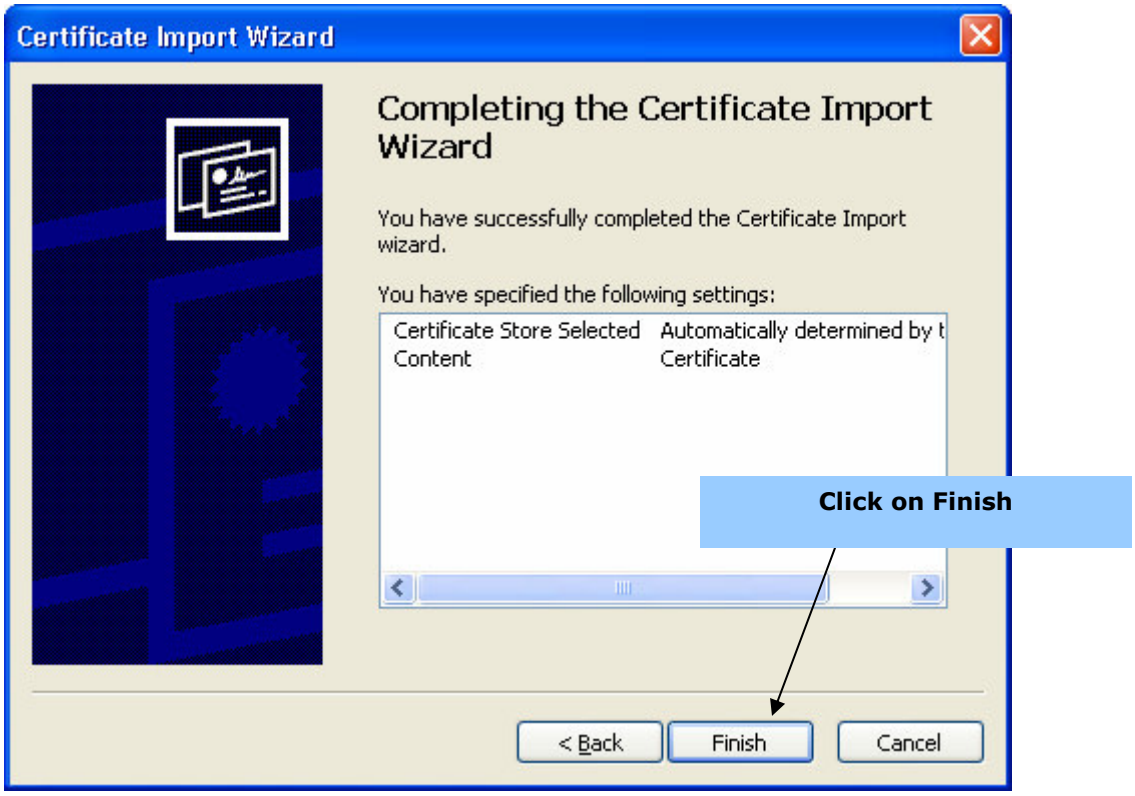


Figure 10-7: Complete the Certificate Import Wizard

Click on *Finish* to complete the import wizard. If the import was successful, a window will display, as shown in figure 10-8.

Figure 10-8: Successful Import

After you click on *OK,* you will be finished importing the user certificate into your browser.

2.1 Importing a PKCS #12 User Certificate

PKCS #12 certificates are a type of certificate that combines both private and public key certificates. This file is protected by a password, which is made by the creator of the PKCS12 file. To import a PKCS12 Certificate into your browser, start by double clicking on the PKCS12 Certificate you want to import, the Import wizard will begin running.

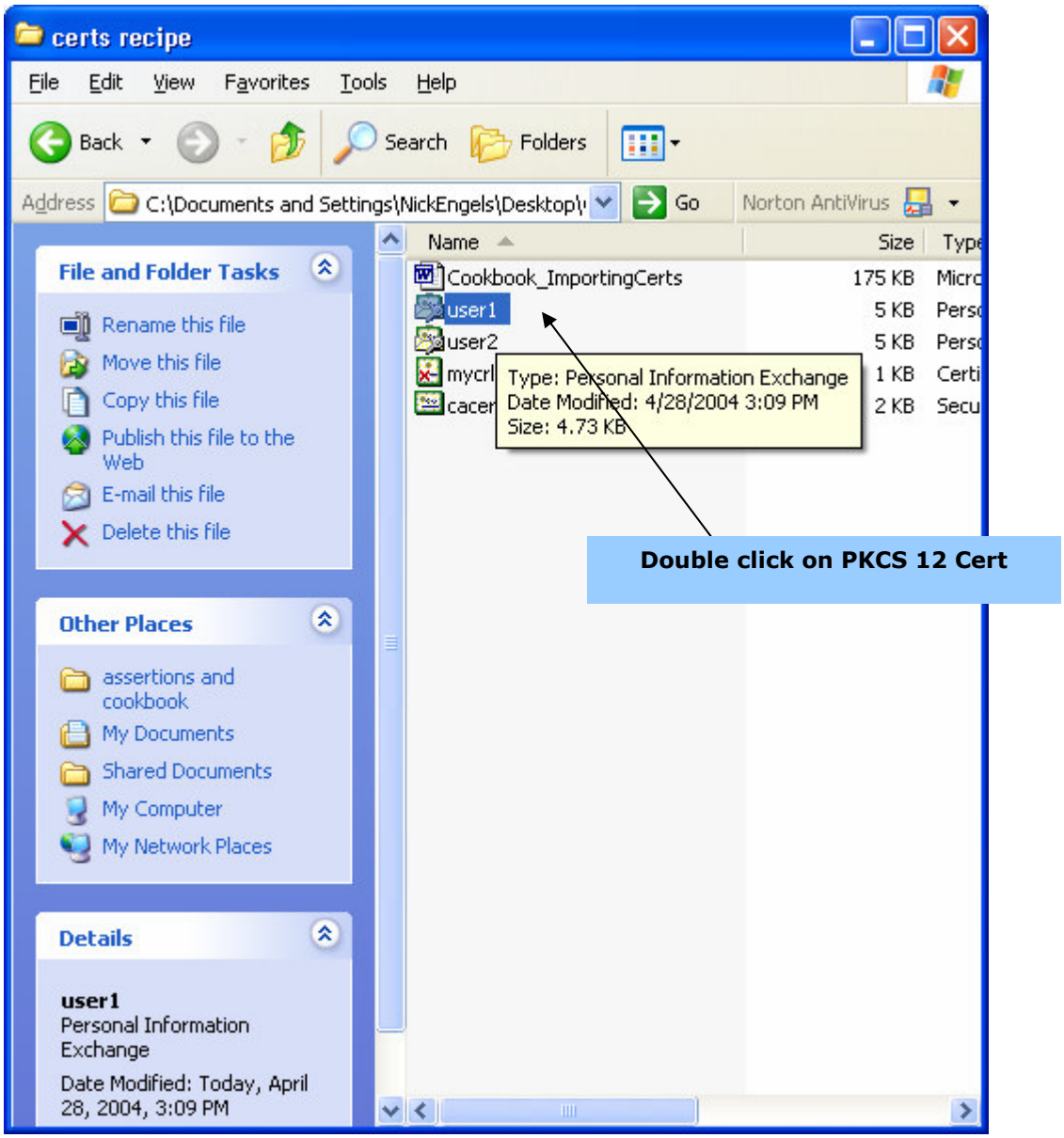


Figure 10-9: Select PKCS12 Certificate

Click *Next* to begin working with the Certificate Import Wizard.

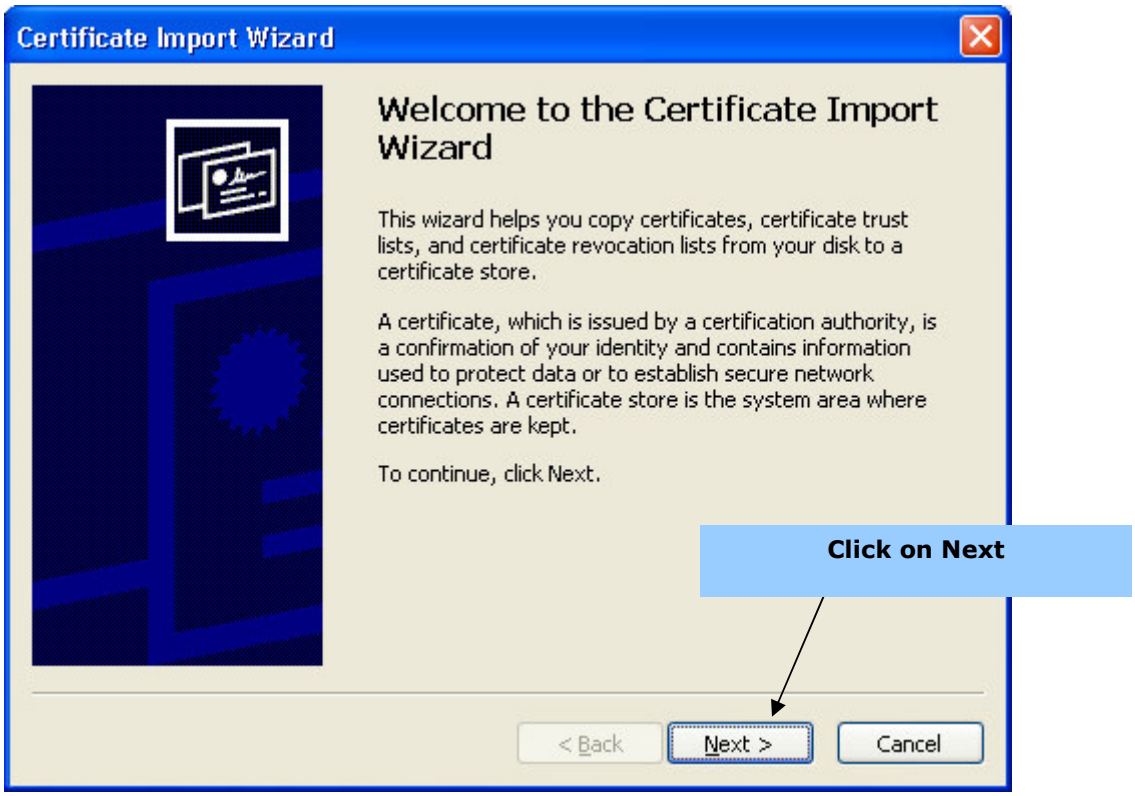


Figure 10-10: Cert Import Wizard

The file you double clicked should already be in the file name box, but if not, click on the *Browse* button and select the certificate file you want to import. After you have selected your PKCS #12 file, click on the *Next* button.

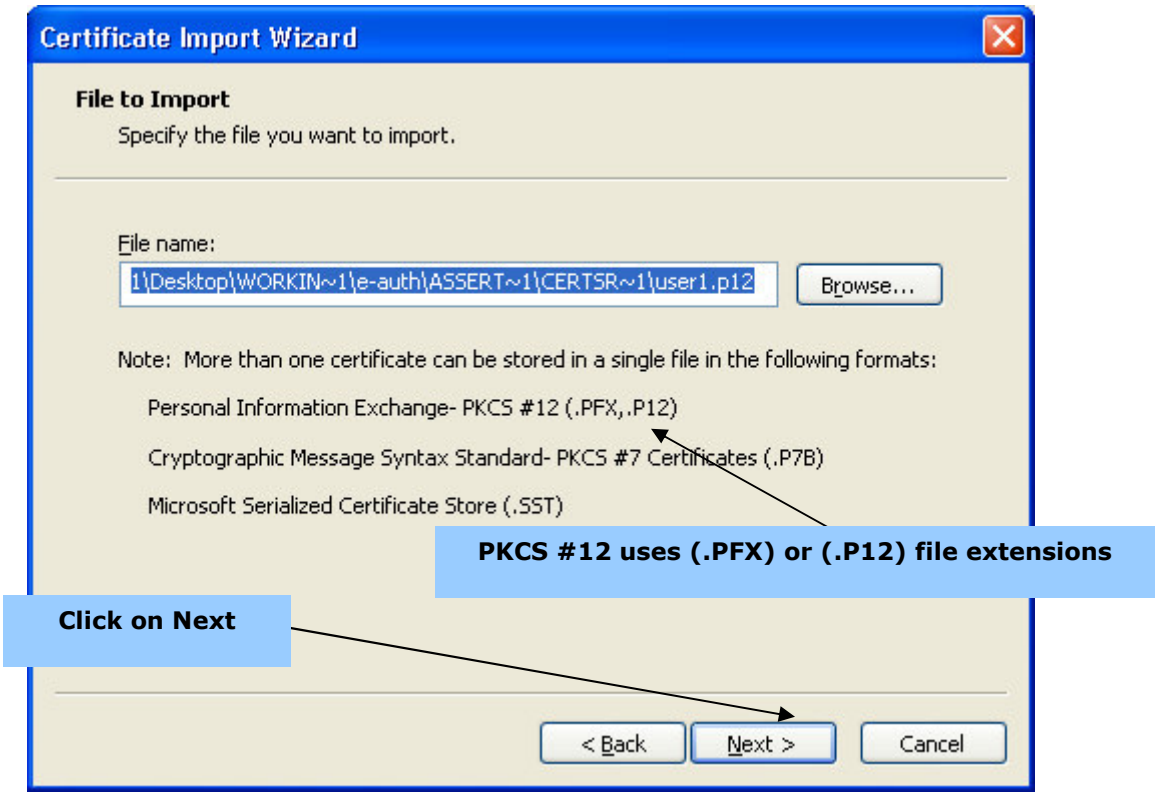


Figure 10-11: Select file to import

To import a PKCS #12 certificate, you must have the password. The password is created when the certificate is made. Enter the password and click on the *Next* button.

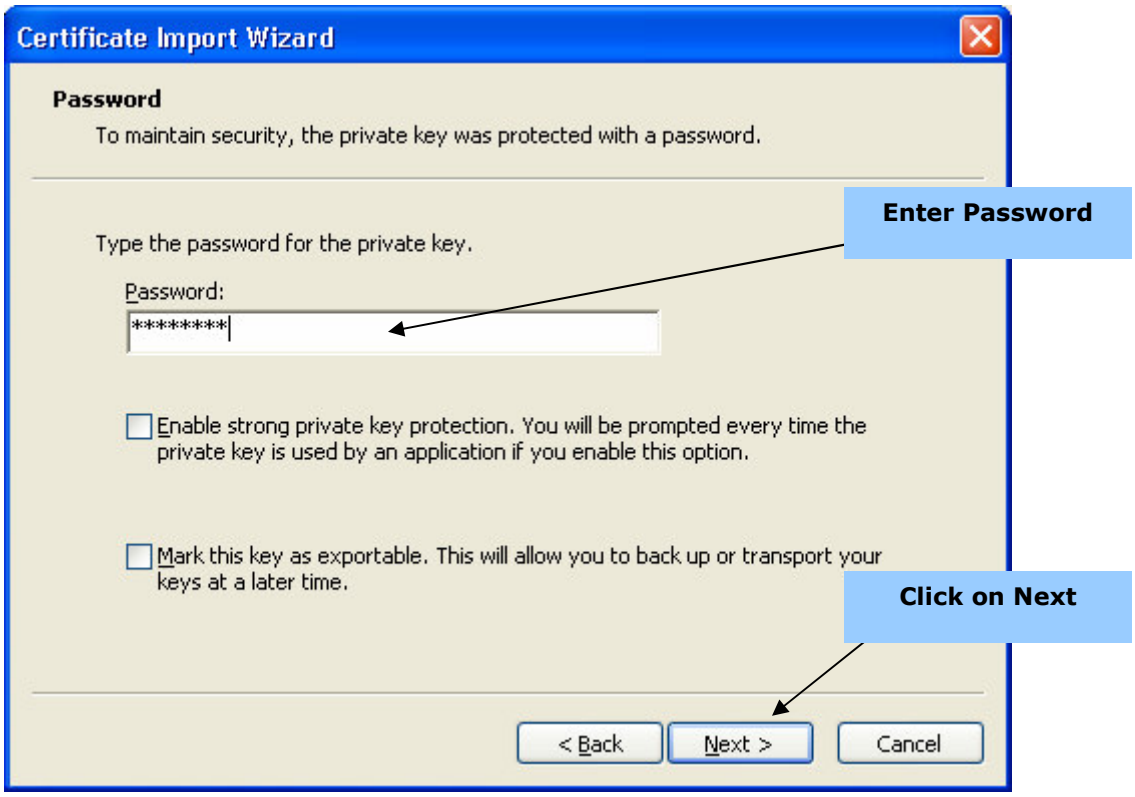


Figure 10-12: Enter Password

After you enter the password, choose to automatically select the certificate store based on the type of certificate. After selecting automatic, as shown in figure 10-13, click on the *Next* button.

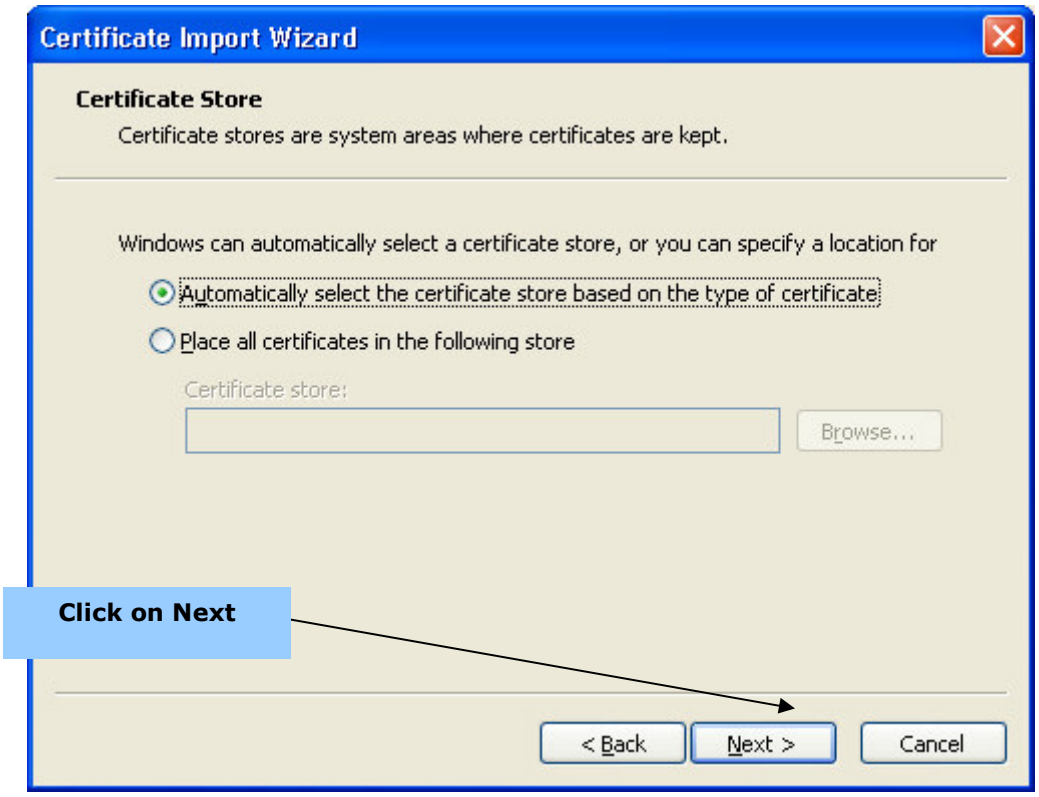


Figure 10-13: Certificate Store

After selecting store settings, click on the *Finish* button, as shown in figure 10-14.

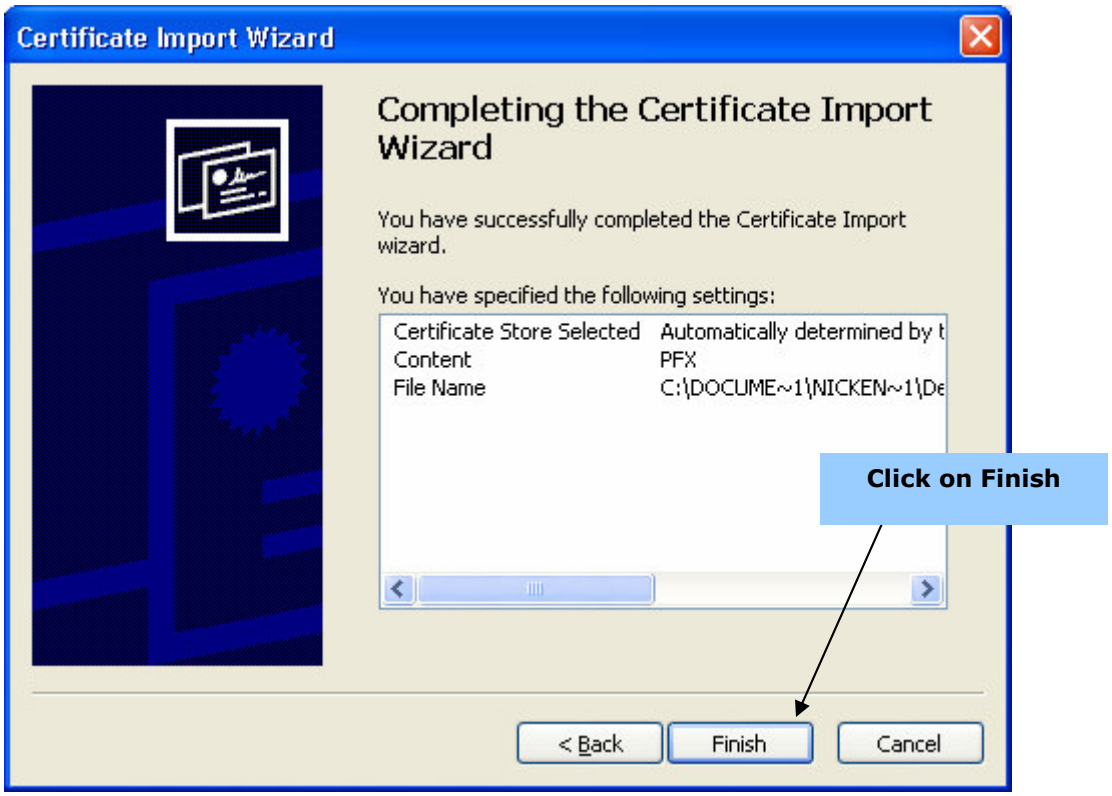


Figure 10-14: Complete the Import Wizard

After you click on the *Finish* button, a window will display asking if you want to add the certificate to the Root Store. The certificate is detailed in this window, as shown in figure 15 below.

Click on **Yes** when the Root Certificate Store window displays.

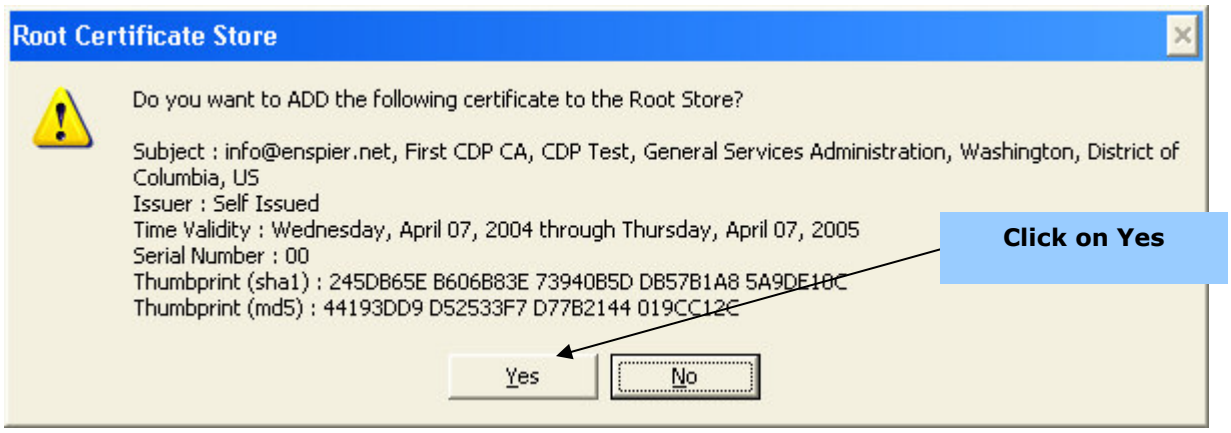


Figure 10-15: Root Certificate Store

If the import wizard worked, and the certificate was imported into your browser, a notification window will display, as shown in figure 10-16.

Figure 10-16: Complete the Import Wizard

3.0 Configure IIS server for SSL with Client Authentication

Before attempting to obtain a Certificate Authority server certificate, use section 3.1 to create a certificate request. Once the request is created, send it to your Agency Relationship Manager and proceed to section 3.2.

3.1 Create a server certificate request

The first step for creating a server certificate request is running Internet Services Manager. Goto:

- Start
- Programs
- Administrative Tools
- Internet Services Manager

After you click on Internet Services Manager, an *Internet Information Services* screen will display, as shown below.

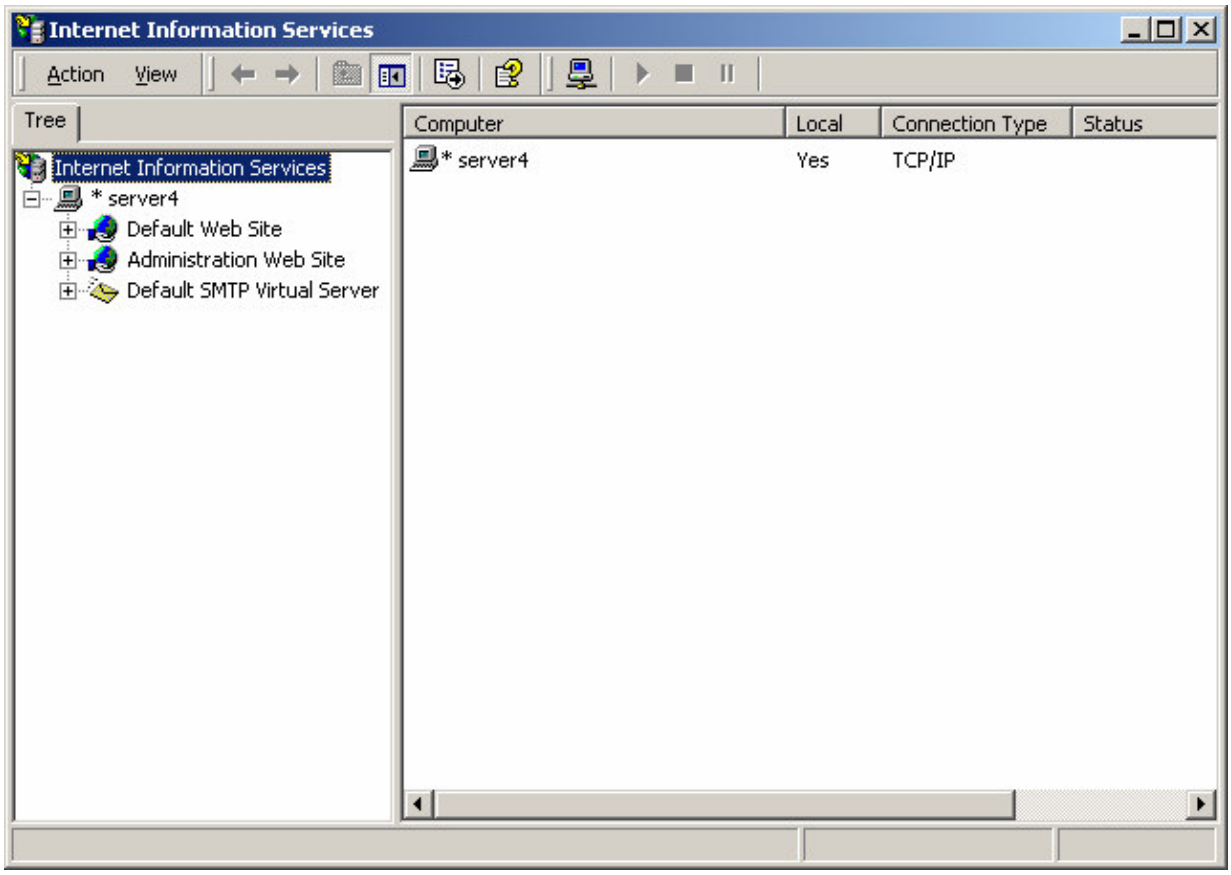


Figure 10-17: Complete the Import Wizard

Choose the Server name and the web site you want to configure by navigating the left pane. Right click on the server you will configure. Ensure that the IIS sever is not running, and click on *Stop* if so.

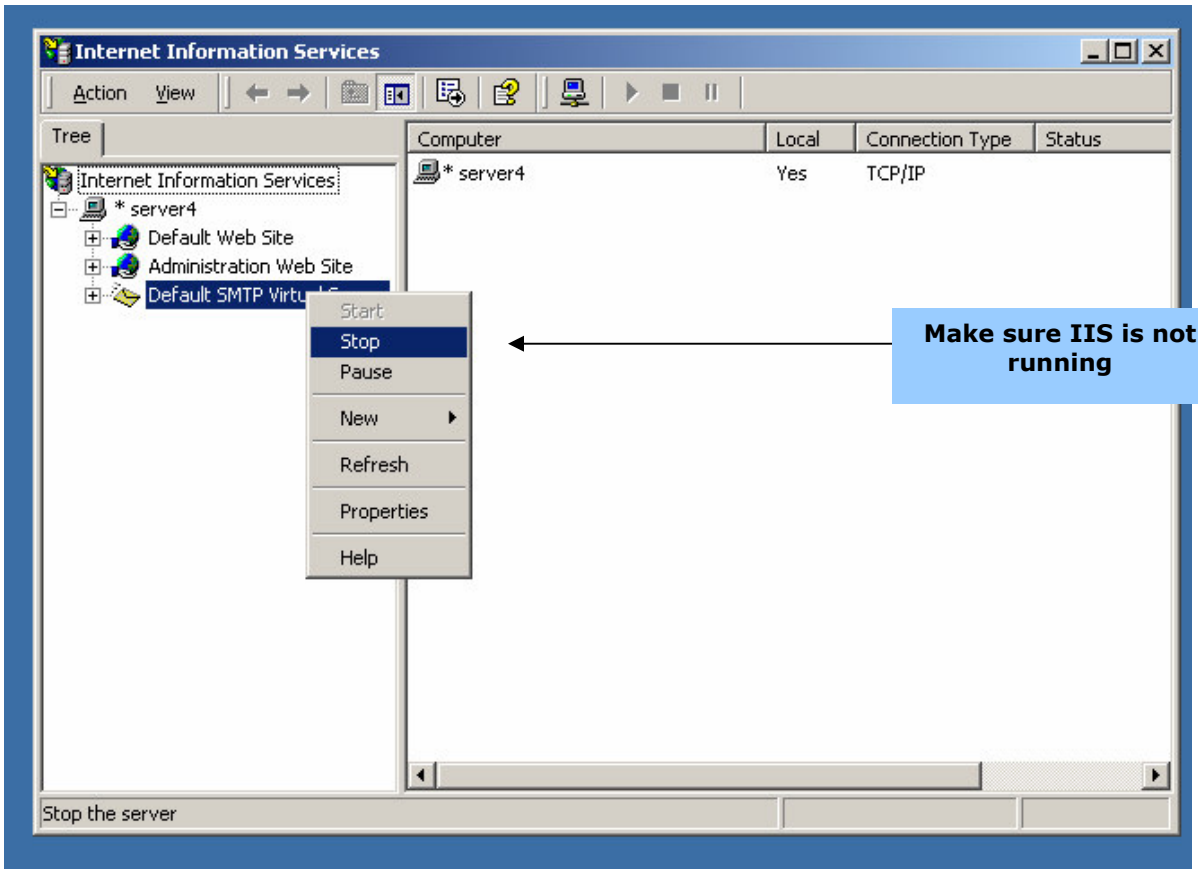


Figure 10-18: Complete the Import Wizard

Right click on the website you want to configure and click on *Properties*. A window with website properties will display, as shown below.

Once the web site properties window displays, click on the *Directory Security* tab.

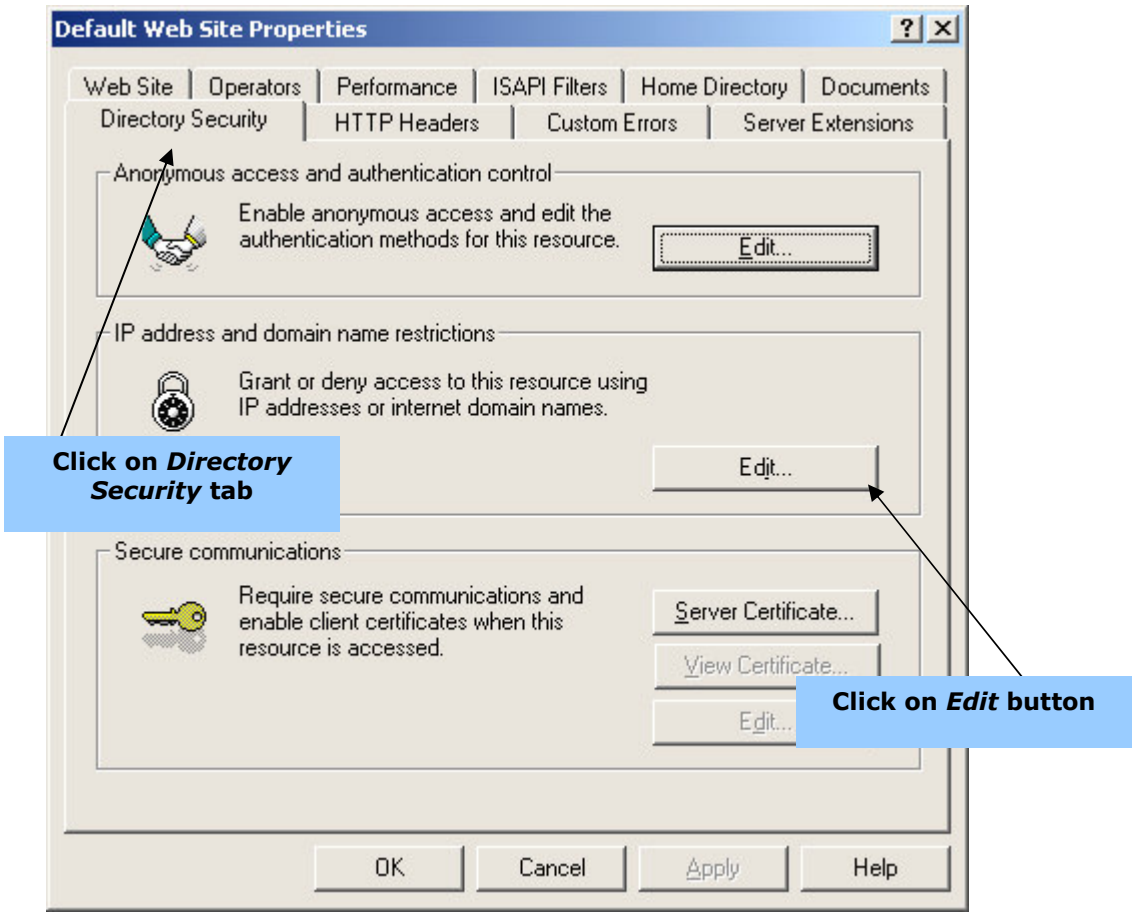


Figure 10-19: Complete the Import Wizard

Once in the *Directory Security* section, click on the *Edit* button.

After you click on the *Edit* button, the window shown below will display.

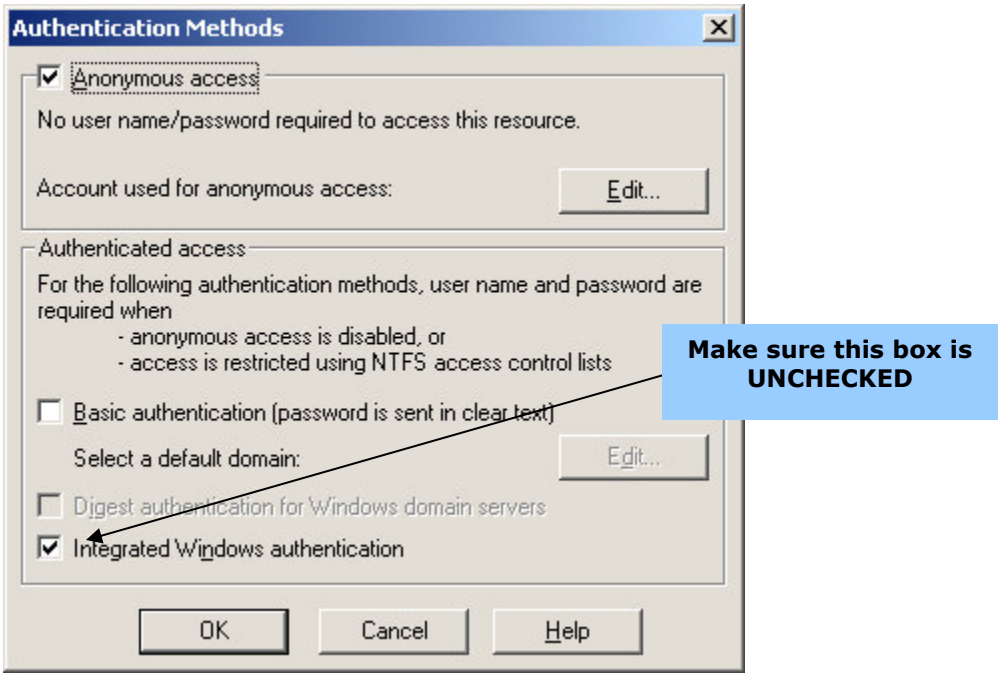


Figure 10-20: Authentication Methods

Clear the *Integrated Windows Authentication* checkbox, then click *OK*. You will be back at the web site properties dialogue box, displayed in figure 10-19, above. Click on *Server Certificate* and the Web Server Wizard will appear, as shown in figure 10-21 below.

Figure 10-21: Web Server Certificate Wizard

The Web Server Certificate Wizard will automate some of the steps for creating server certificate requests. When figure 21 displays click *Next.*

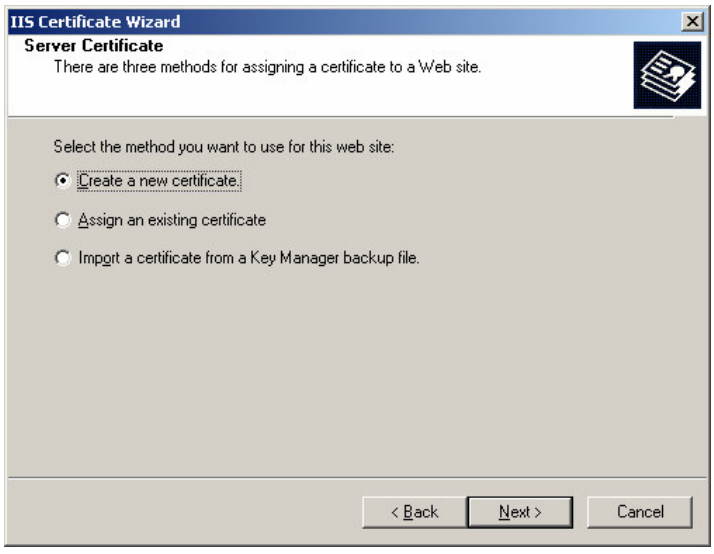


Figure 10-22: Web Server Certificate Wizard

There are three methods for assigning a certificate to a Web site. Make sure you select *Create a new certificate* and then hit the *Next* button.

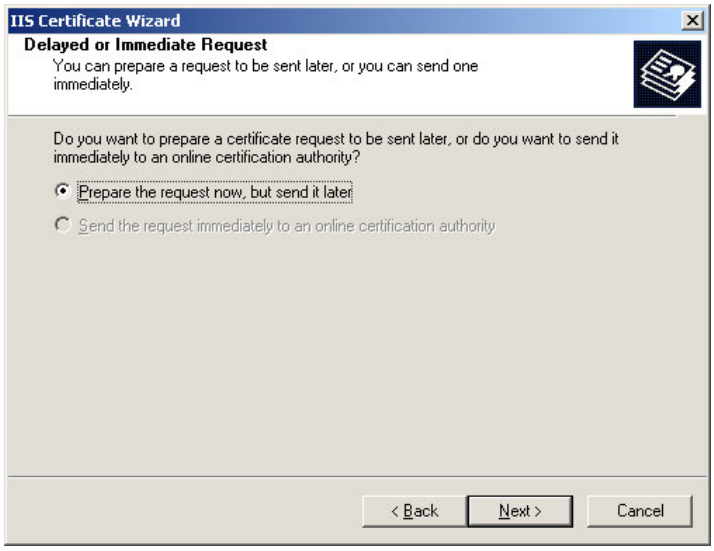


Figure 10-23: Delayed or Immediate Request

Select *Prepare the request now, but send it later* and then click on the *Next* button. The Name and Security Settings window will display.

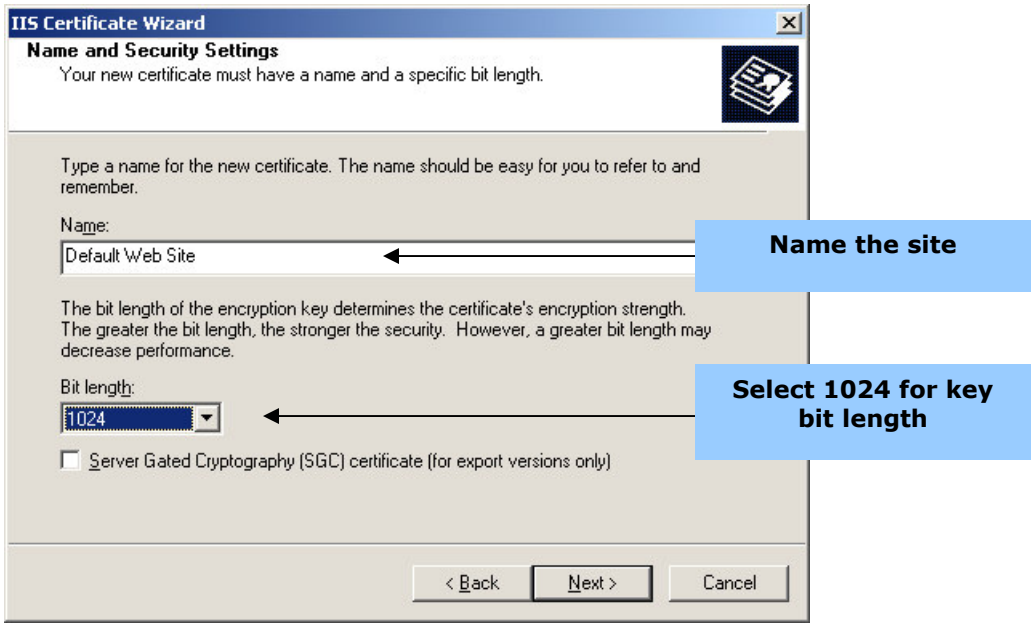


Figure 10-24: Name and Security Settings

Choose an easy to remember name for the website for which you want to create the certificate. Select a bit length of 1024, then click on the *Next* button.

Your certificate must include information about your organization that makes it easier to distinguish it from similar organizations. Select or type your organization's name and your organizational unit or department, then click *Next*.

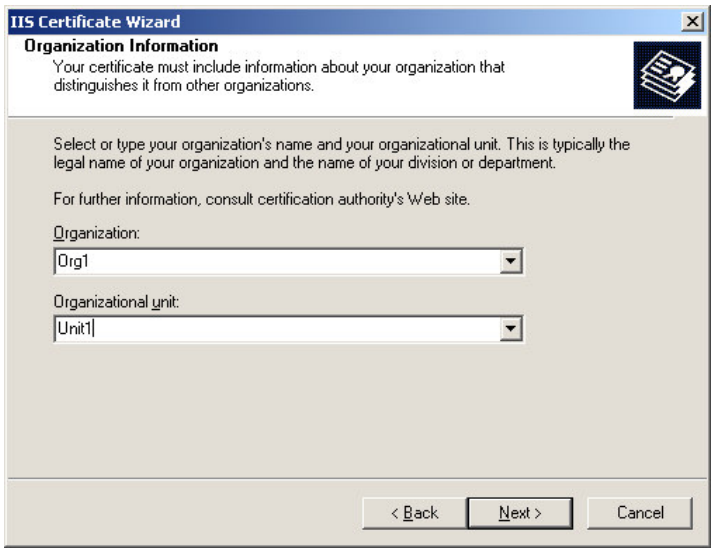


Figure 10-25: Organization Information

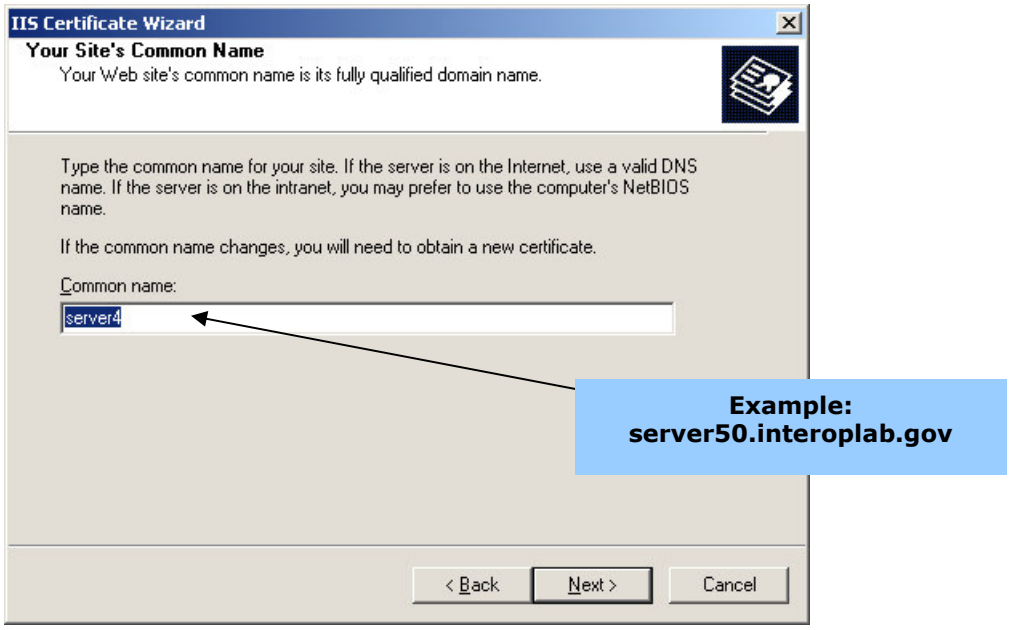


Figure 10-26: Your Site's Common Name

Select a common name, but ensure that this is the full DNS name of the server.
Click on *Next* after you choose a name. **Example: server50.interoplab.gov**

Fill out information about your location, then click on *Next*.

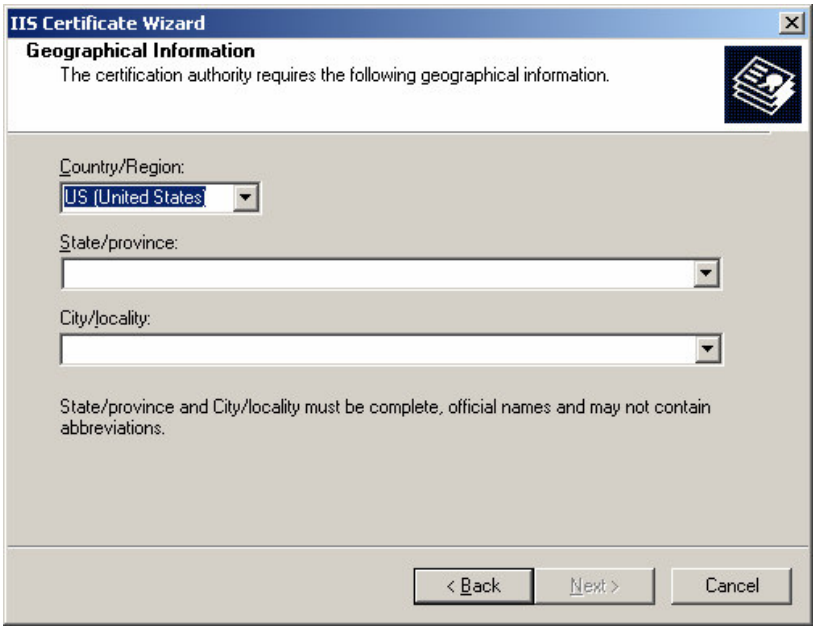


Figure 10-27: Geographic Information

After you enter your geographic information, you will be prompted to enter a filename for the certificate request. Choose a name or browse to find the most desirable location to store this file.

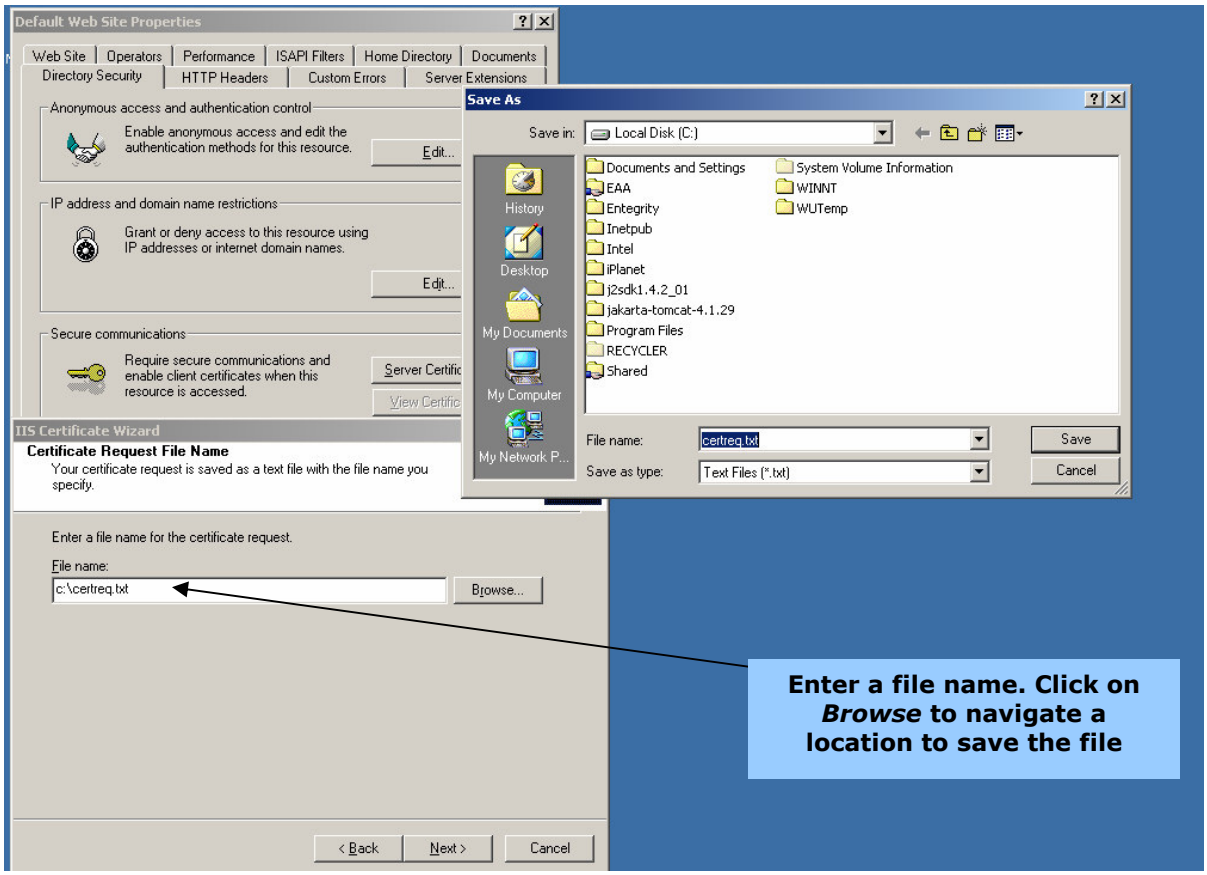


Figure 10-28: Certificate Request File Name

After you name the file and location, you will have an opportunity to review the information you entered. To change something, click on the *Back* button, otherwise click on *Next*.

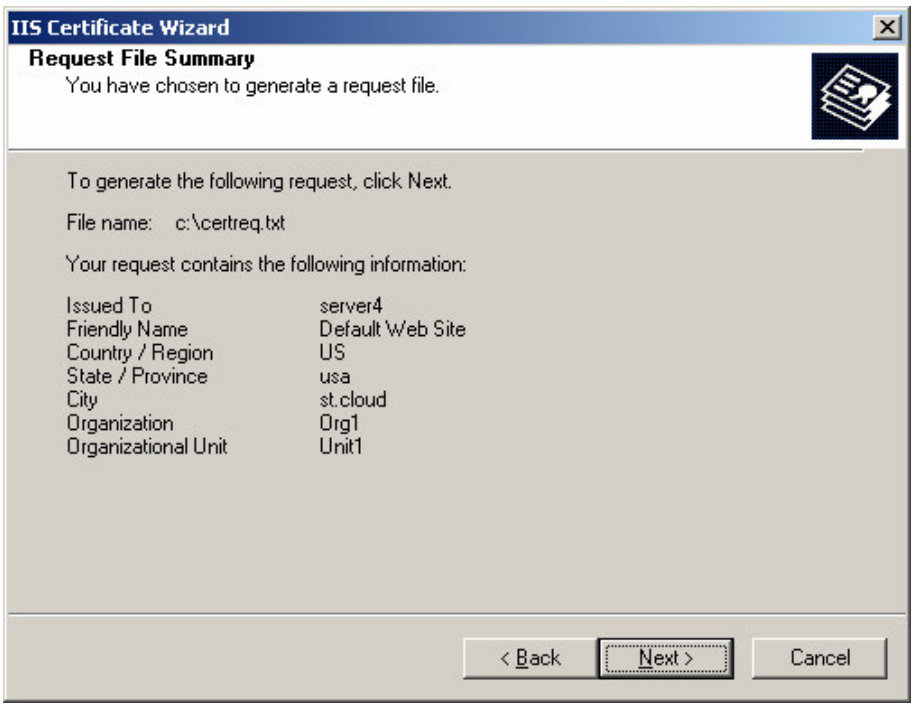


Figure 10-29: Request File Summary

When you are satisfied with the information you entered, click on *Finish* to exit the certificate wizard.

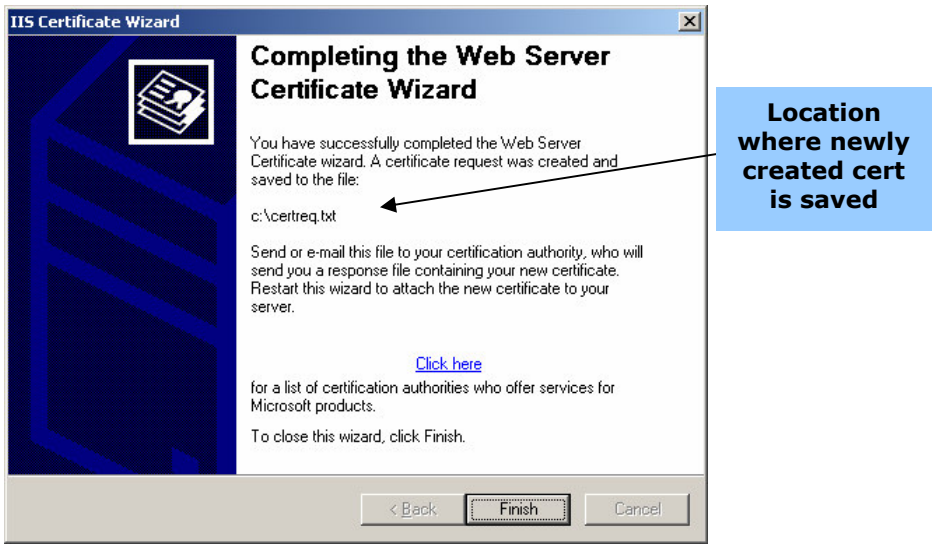


Figure 10-30: Finish the Cert Wizard

3.2 Import server certificate into IIS

Before you can begin section 3.2, send the certificate request created in 3.1 to your CA. Save the certificate returned by the CA in an appropriately named file, for example, **c:\cert1.cer**

After you have the certificate returned by the CA, you will import a server certificate into IIS by running Internet Services Manager. Goto:

- Start
- Programs
- Administrative Tools
- Internet Services Manager

After you click on Internet Services Manager, an *Internet Information Services* screen will display, as shown below.

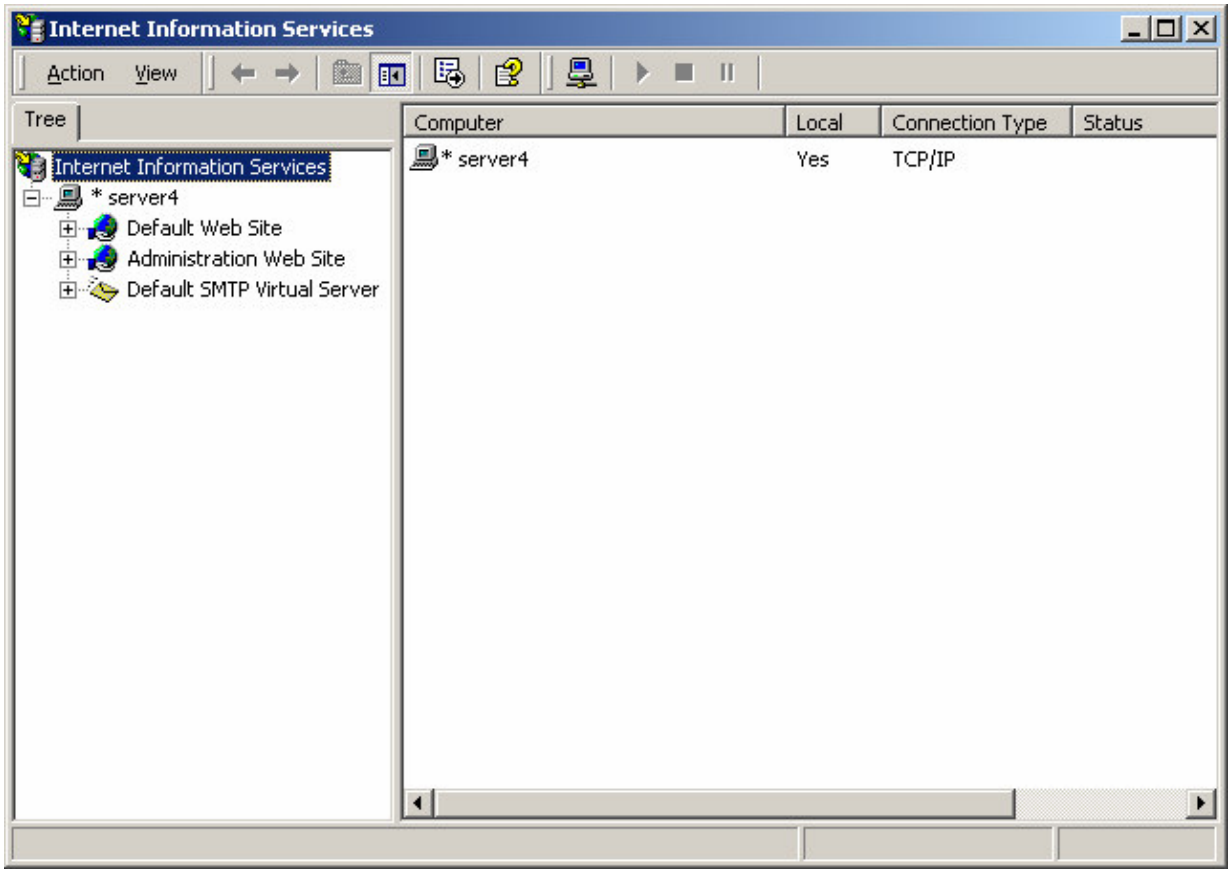


Figure 10-31: Complete the Import Wizard

Choose the Server name and the web site you want to configure by navigating the left pane. Right click on the server you will configure. Ensure that the IIS sever is not running, and click on *Stop* if so.

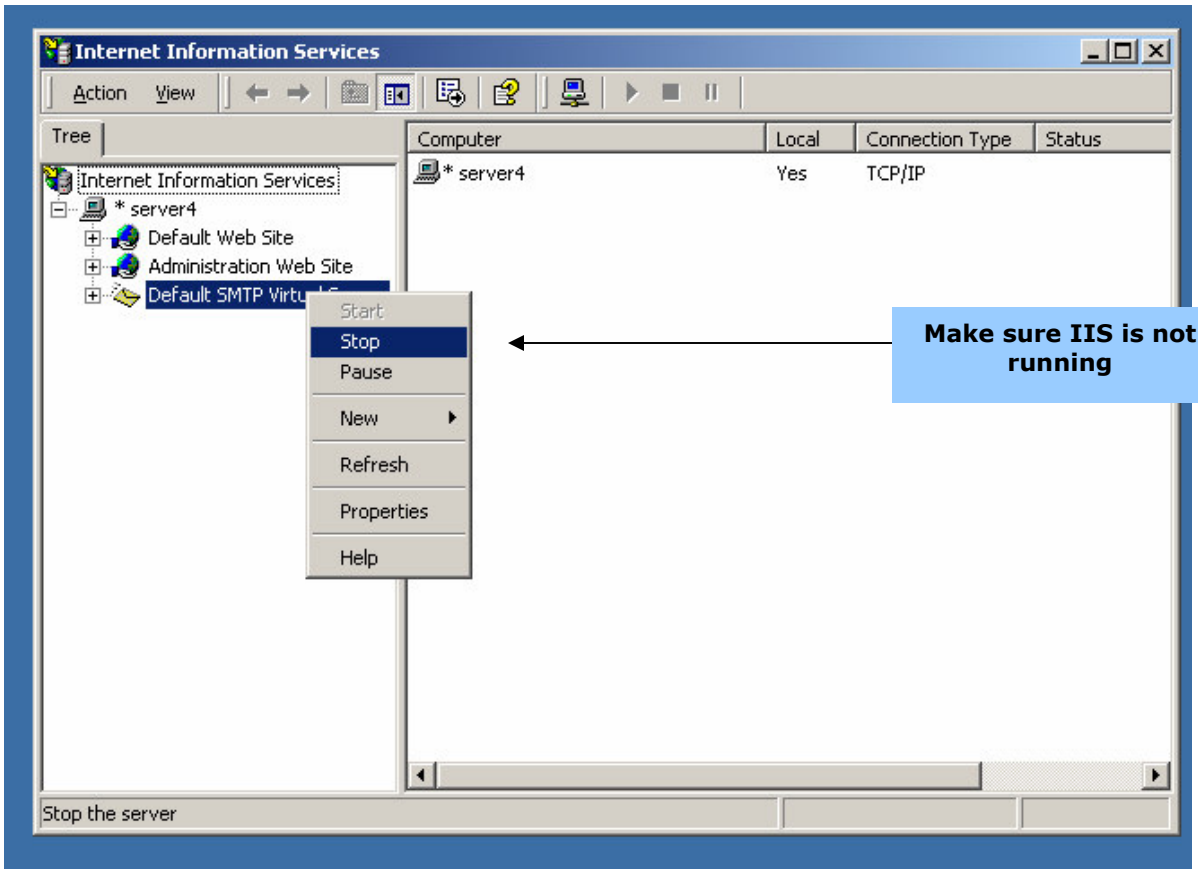


Figure 10-32: Complete the Import Wizard

Right click on the website you want to configure and click on *Properties*. A window with website properties will display, as shown below.

Once the web site properties window displays, click on the *Directory Security* tab.

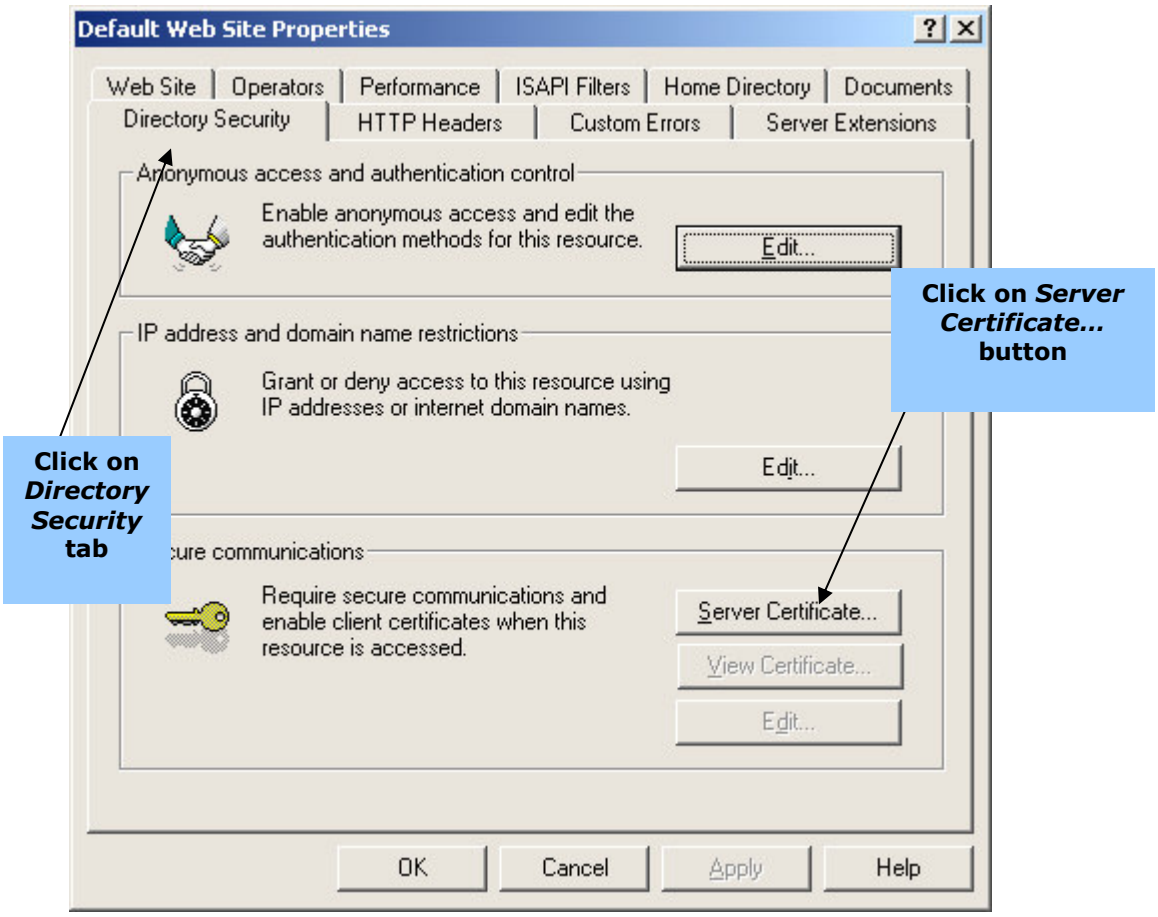


Figure 10-33: Complete the Import Wizard

Once in the *Directory Security* section, click on the *Server Certificate* button. The Web Server wizard will appear, click *Next* and follow the steps below.

- Select *Process the pending request and install the certificate,* then click *Next.*
- Enter path name of the file containing the certification authority's response, click *Open.*
- Click *Next.*
- Click Finish.
- Click *Edit* in the *Secure Communications* section.
- Click *Require secure channel SSL,* click *require 128-bit encryption.*
- Click *Require client certificates,* and then click *OK.*
- After you click *OK,* click on Web site tab. The SSL port has been changed to 443.
- For inheritance overrides, click *OK*
- Click *OK*
- Stop and then start IIS

Recipe 11 - Configuration Guide for Setting up HP as an Agency Application (AA)

Table of Contents

Version 1.0

1.0 Setup

1.1 Terms and Introduction

The SAML Artifact profile is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML, to use this Sun application as a Credential Service or as an Agency application. The Oblix setup screens are the same, whether setting up an AA or a CS. In section 2, each type of setup is outlined separately. After reviewing the terms, configure your scheme to handle SAML, starting at the main page shown in Figure 11-1.

Term	Definition
Agency Application (AA)	An online government service, provided by an agency, which requires a user to be authenticated.
Credential Service (CS)	A service, provided by a CSP, that electronically validates identity or a transaction.
Credential Service Provider (CSP)	An organization that offers one or more Credential Services (CS). If a CS offers more than one type of credential then each one is considered a separate CS.
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations for the Initiative.

1.2 Using the setup tool

To open the setup tool, go to the HP directory under the Program Files folder; click on the Setup Tool.

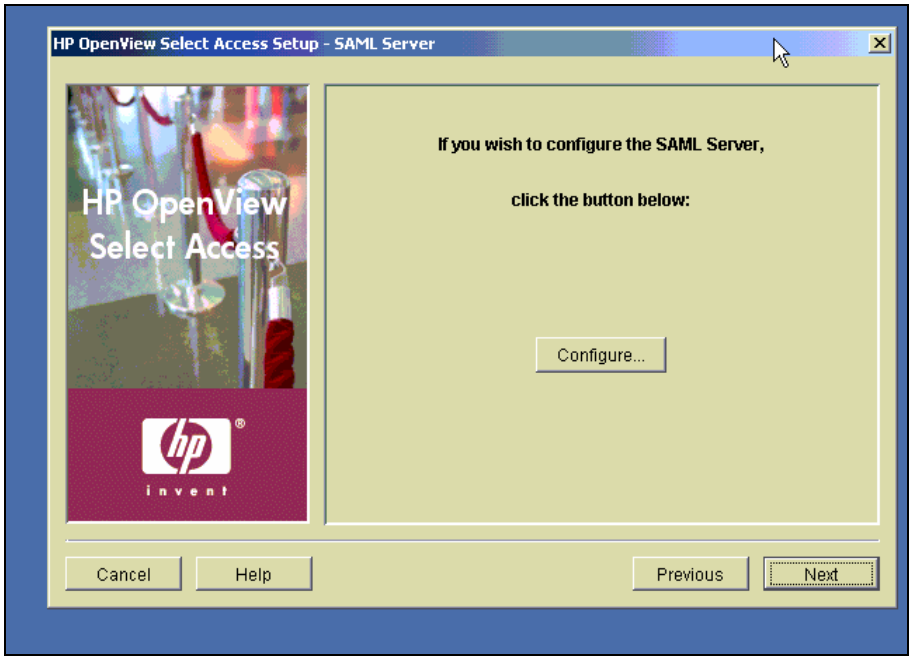


Figure 11-1: Start Setup Tool

Use the setup tool to configure a SAML server. The setup program is the same whether you are setting up a CS or an AA. After the initial setup, do not attempt to use the setup tool again. Instead, use SAML partner properties (See section 2.0 for details) to access properties.

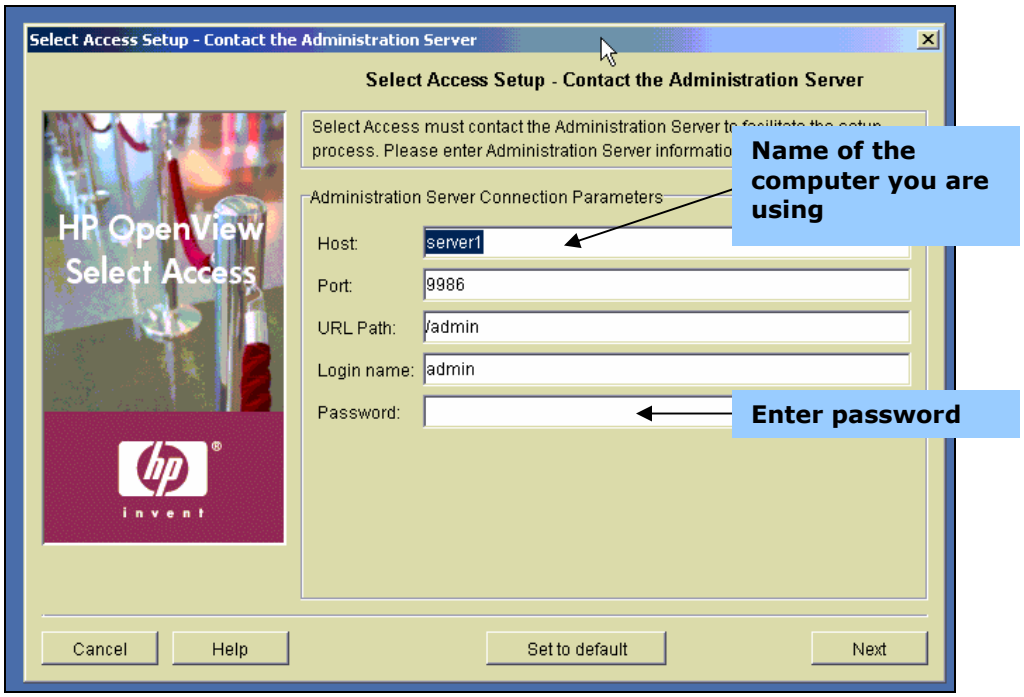


Figure 11-2: Select Access Setup

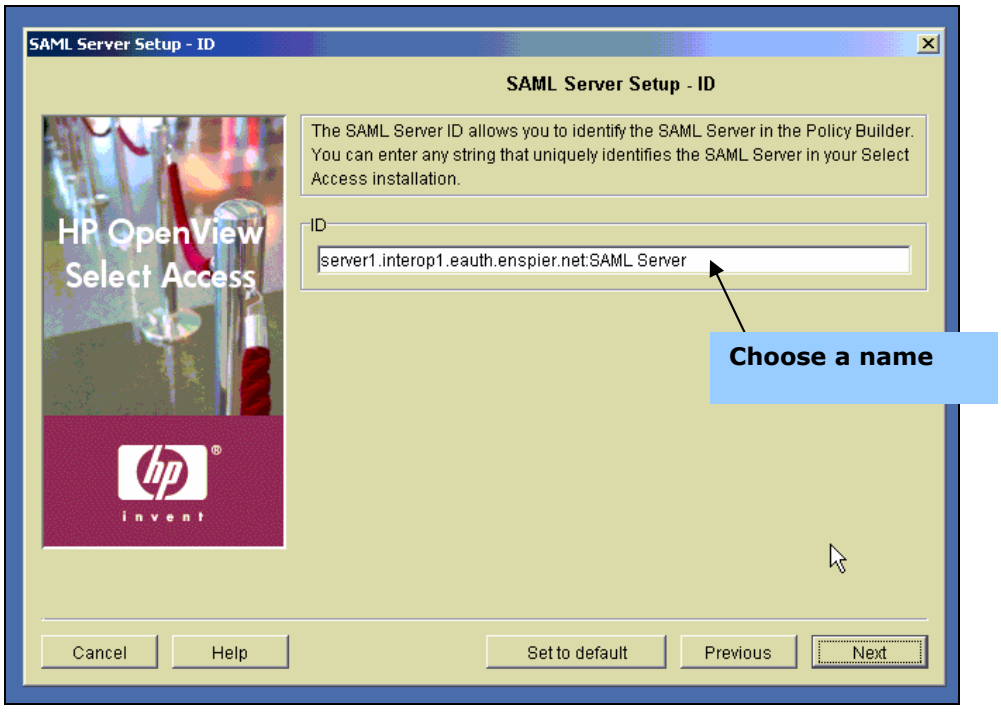


Figure 11-3: Define SAML Server ID

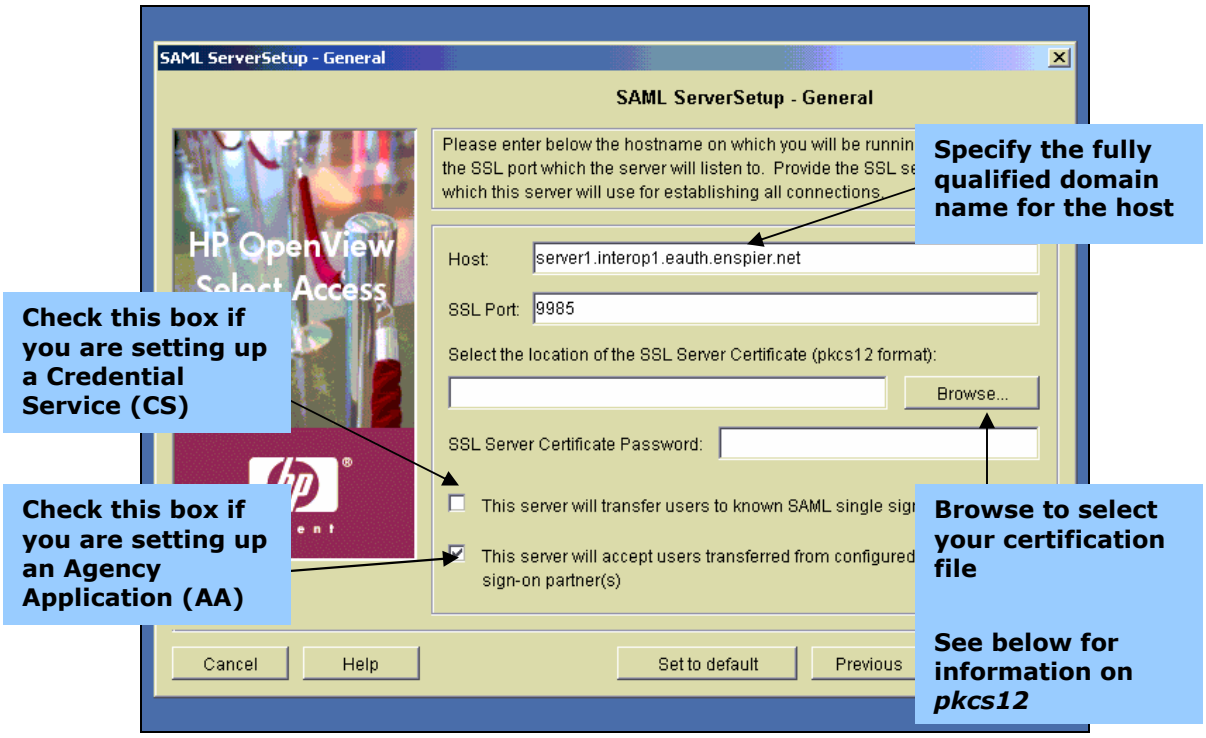


Figure 11-4: General Server Setup

PKCS12 files combine private and public key certificates. This file is protected by a password, which you will provide when you create your PKCS12 file.

2.0 Authenticating Users from a Credential Service

As an AA that seeks to authenticate users utilizing a certain CS, you must create an authentication server that HP will use to authenticate users. Before you can add a CS, you must create a new group to store user credentials. HP uses a policy matrix to create groups. The following pages will help you use policy matrix, opening a door to HP's user directory.

2.1 Use policy builder to add a group of users from a Credential Service (CS) to your AA

First open Policy Builder; go to the Program files folder and open the HP directory. Click on the open view folder, then click on SelectAccess, then click on Policy Builder.

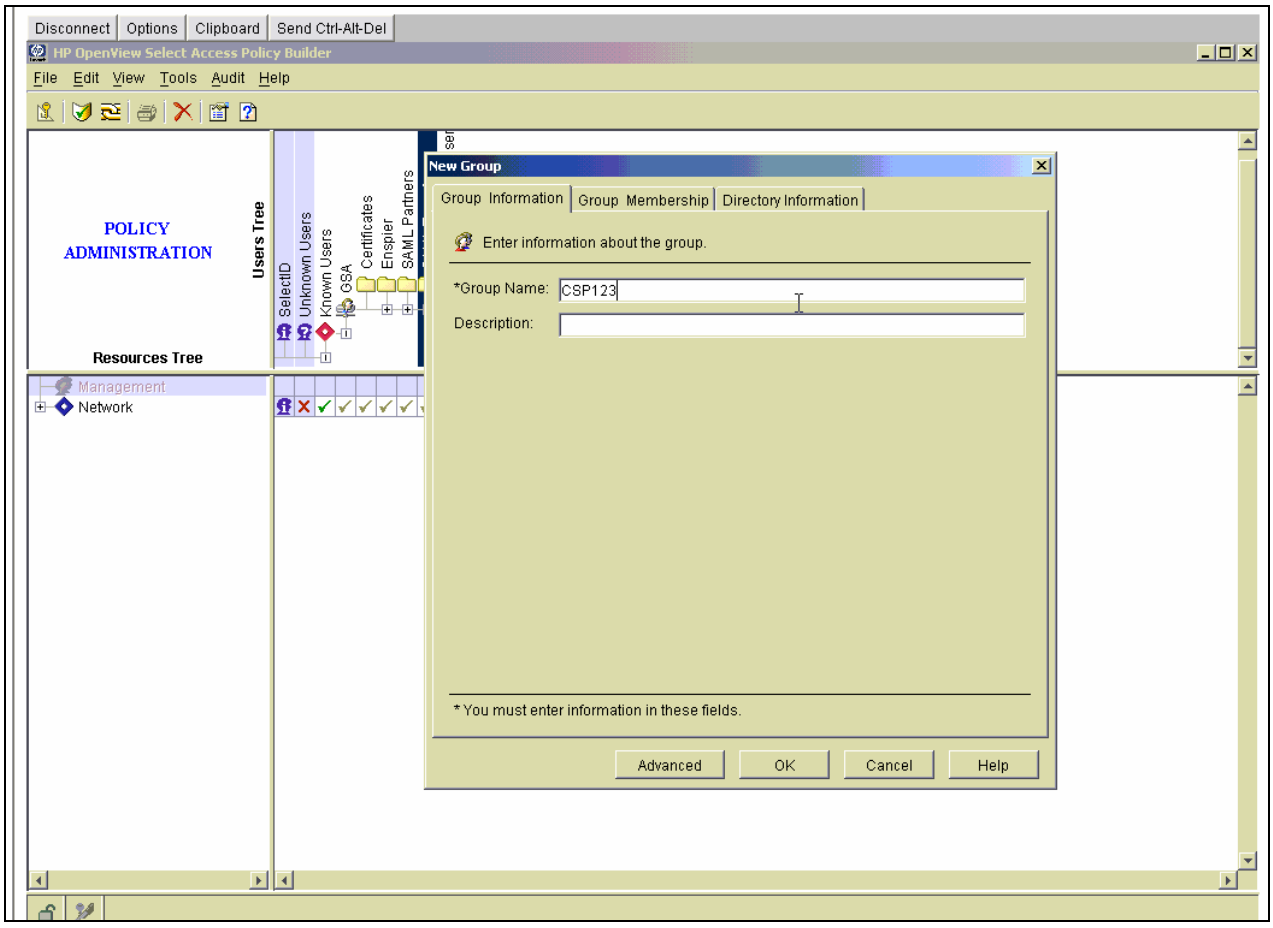


Figure 11-5: Create new CS group

Right click on the folder where you want to store your new group file. Create a new group inside of your known users, where people from you CS will be stored.

2.2 Use Policy Builder to Modify SAML Configuration

After establishing an authentication server, you must configure the SAML partnership for a CS within the authentication server. Use Policy Builder to modify SAML component configuration. To open, go to the Program files folder and open the HP directory. Click on the open view folder, then click on SelectAccess, then click on Policy Builder.

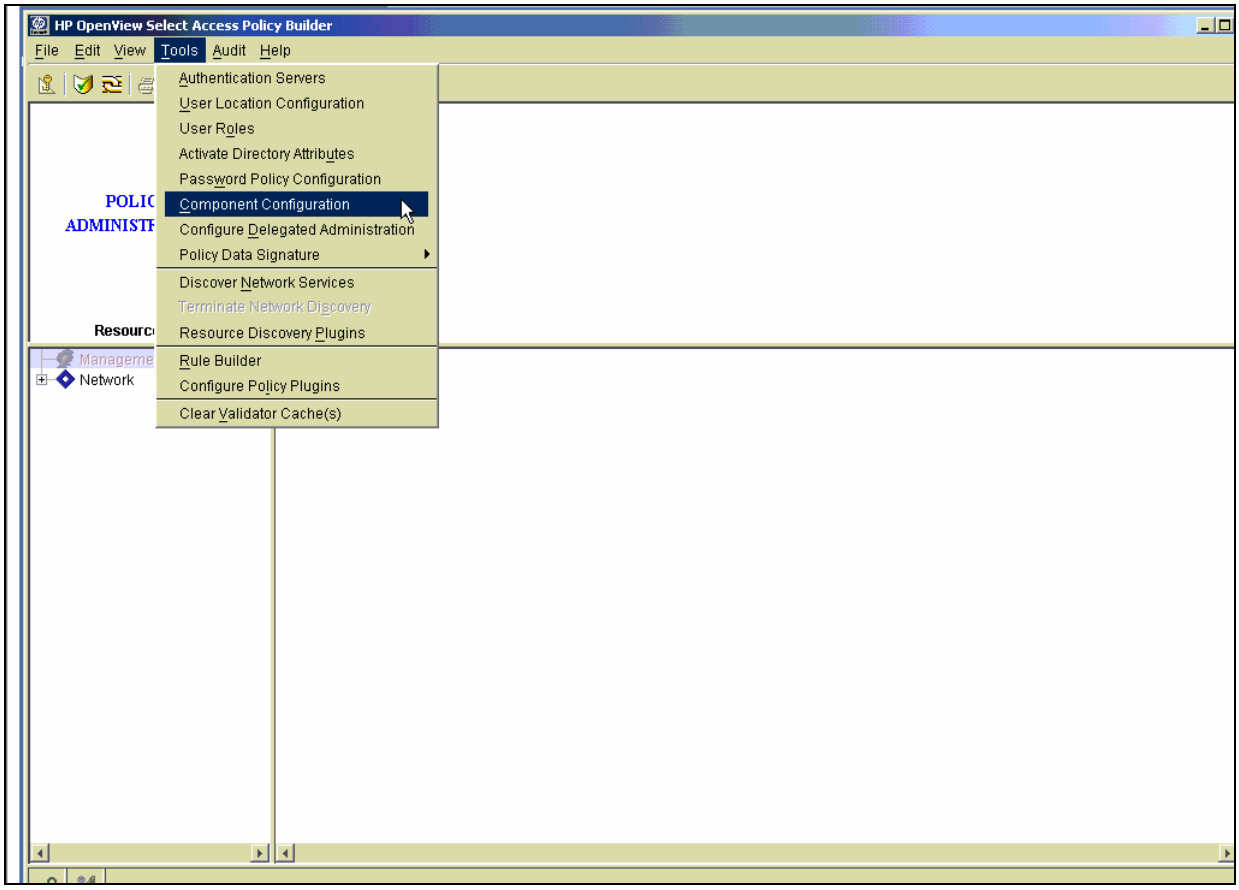


Figure 11-6: Working with Policy Builder

Click on Tools, the select *Component Configuration.* A component configuration window will open, as shown in Figure 11-7 below.

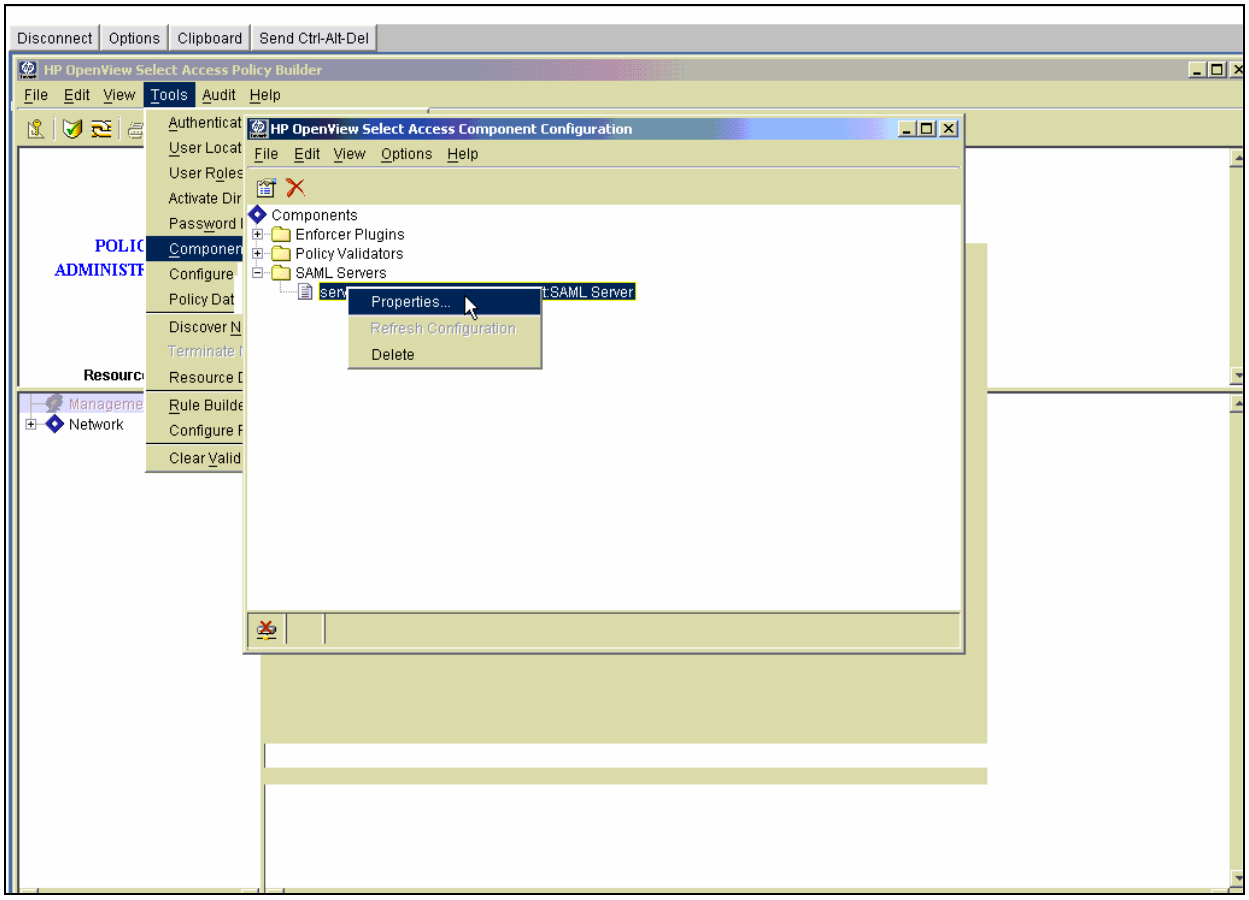


Figure 11-7: Navigating to Component Configuration

To view assertion properties, right click on a SAML server file, choose *Properties*. A window for assertion properties, as shown in Figure 11-8, will open.

2.3 Add a SAML Authentication Server

From the *HP OpenView Select Access Component Configuration* window, open the properties.

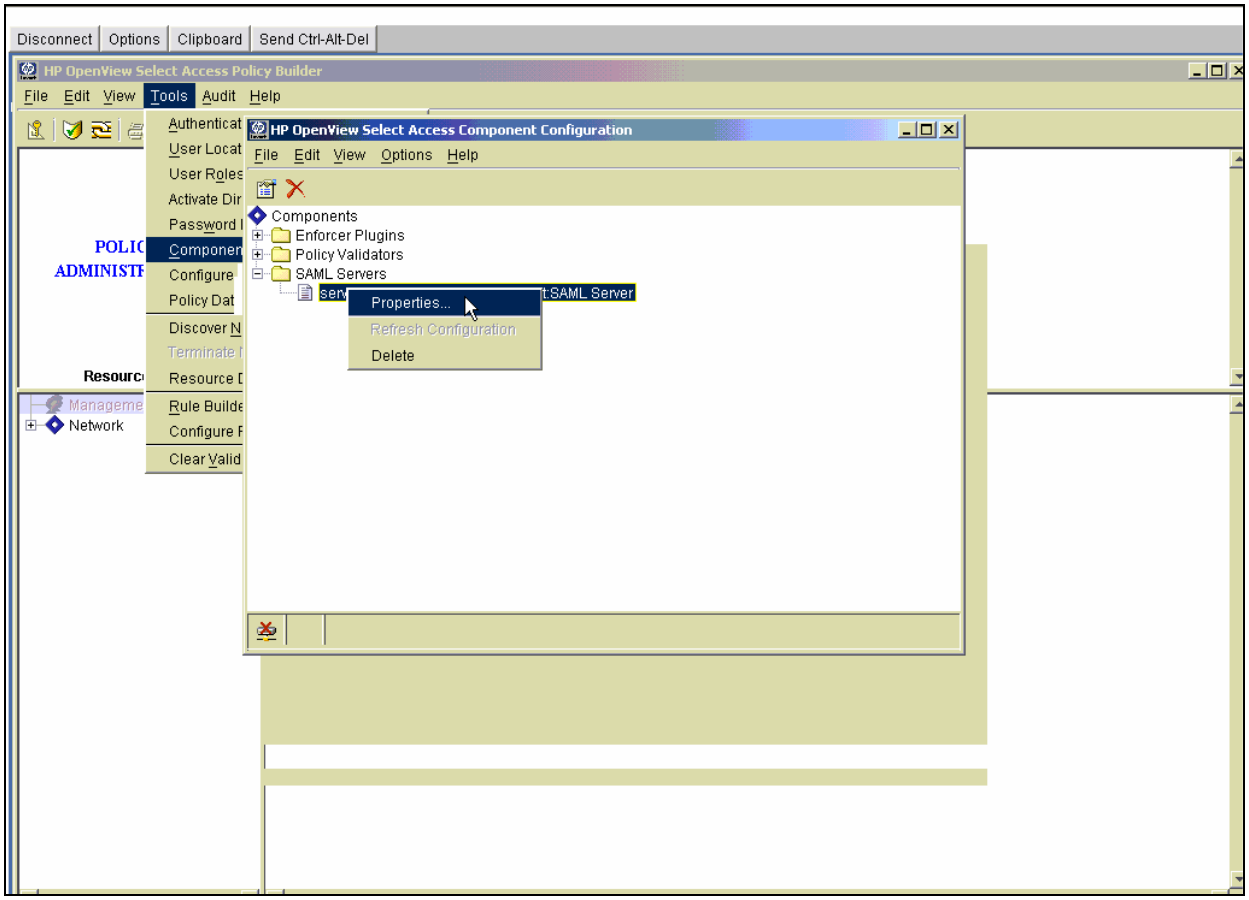


Figure 11-8: Navigate to Properties

After you click on *Properties*, the window shown in Figure 9 will open.

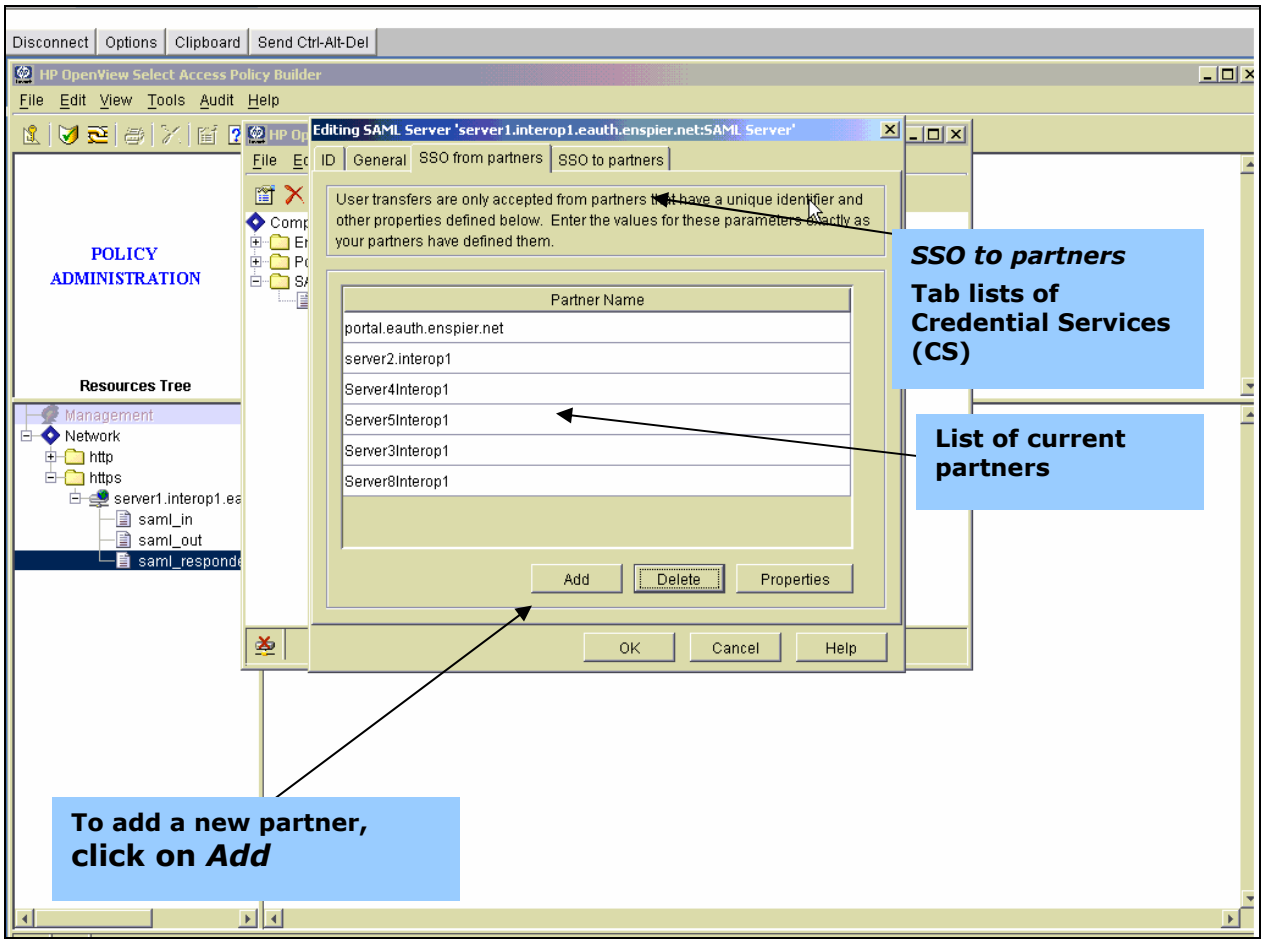


Figure 11-9: Editing the SAML server

After you click on *Add (See Figure 11-10)*, the *New SAML Authentication Server* window will display. Enter a name, then click on *Next.*

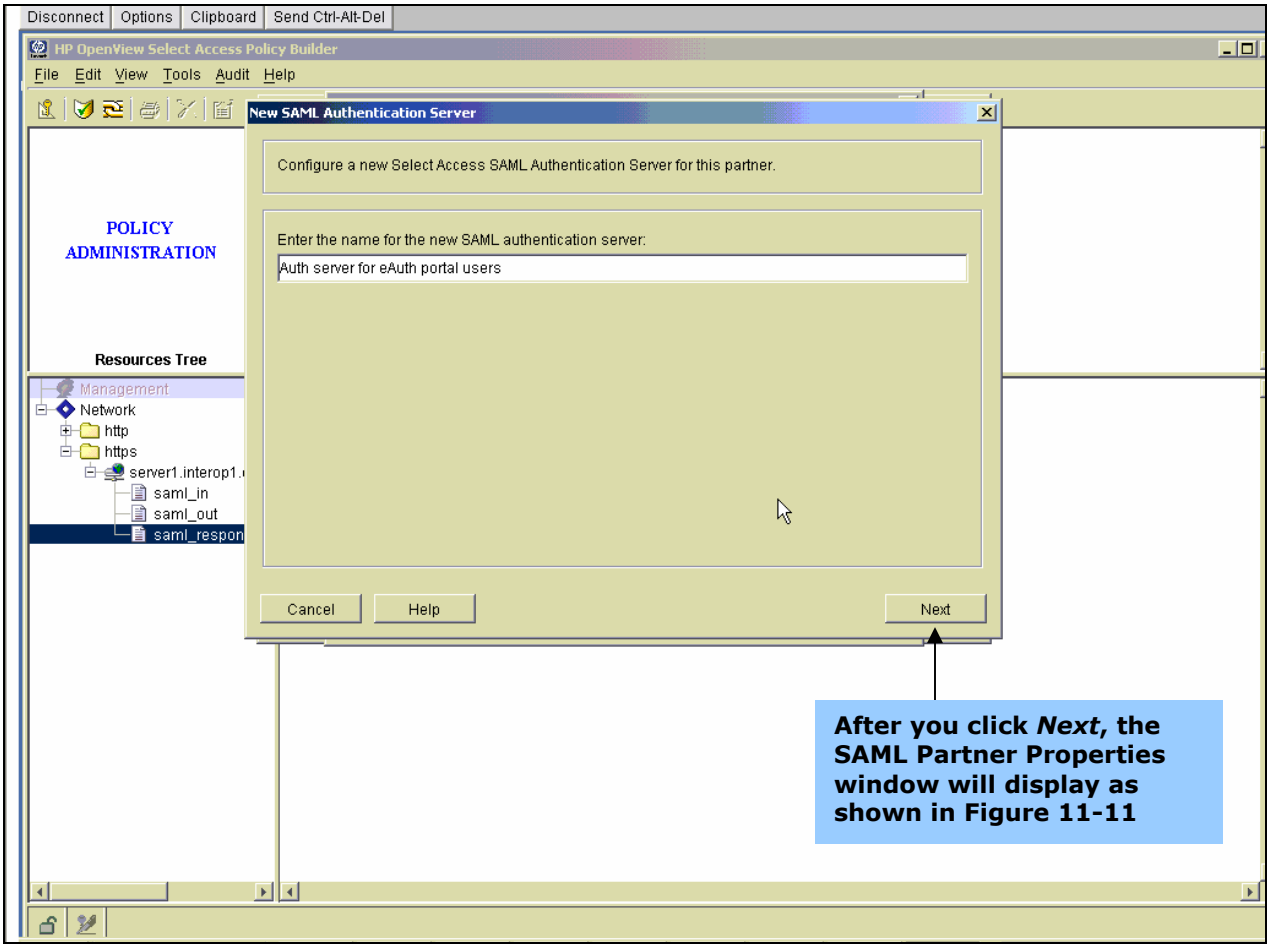


Figure 11-10: Naming new SAML authentication server

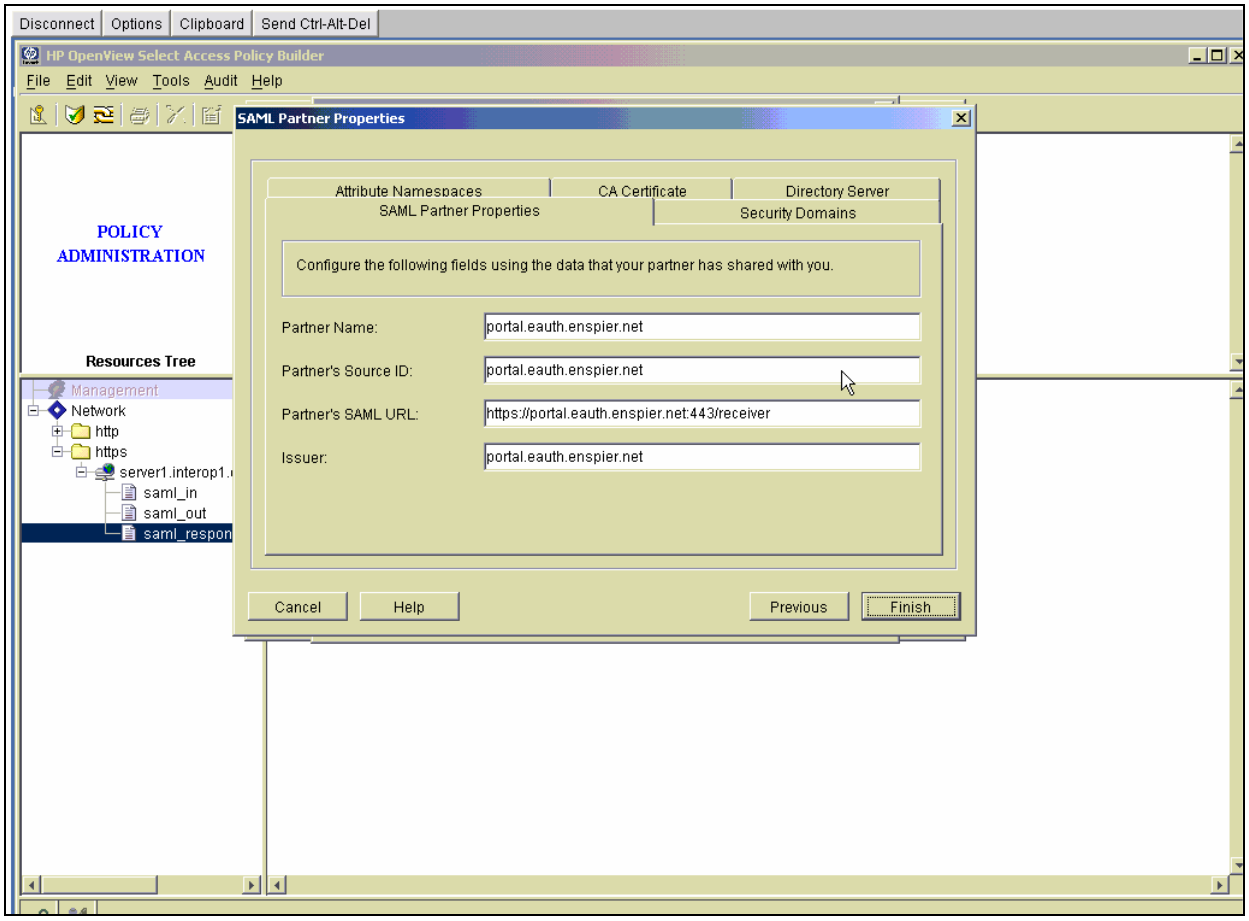


Figure 11-11: SAML partner properties tab

Fill in the partner name. Partner source ID can be obtained from the CS.

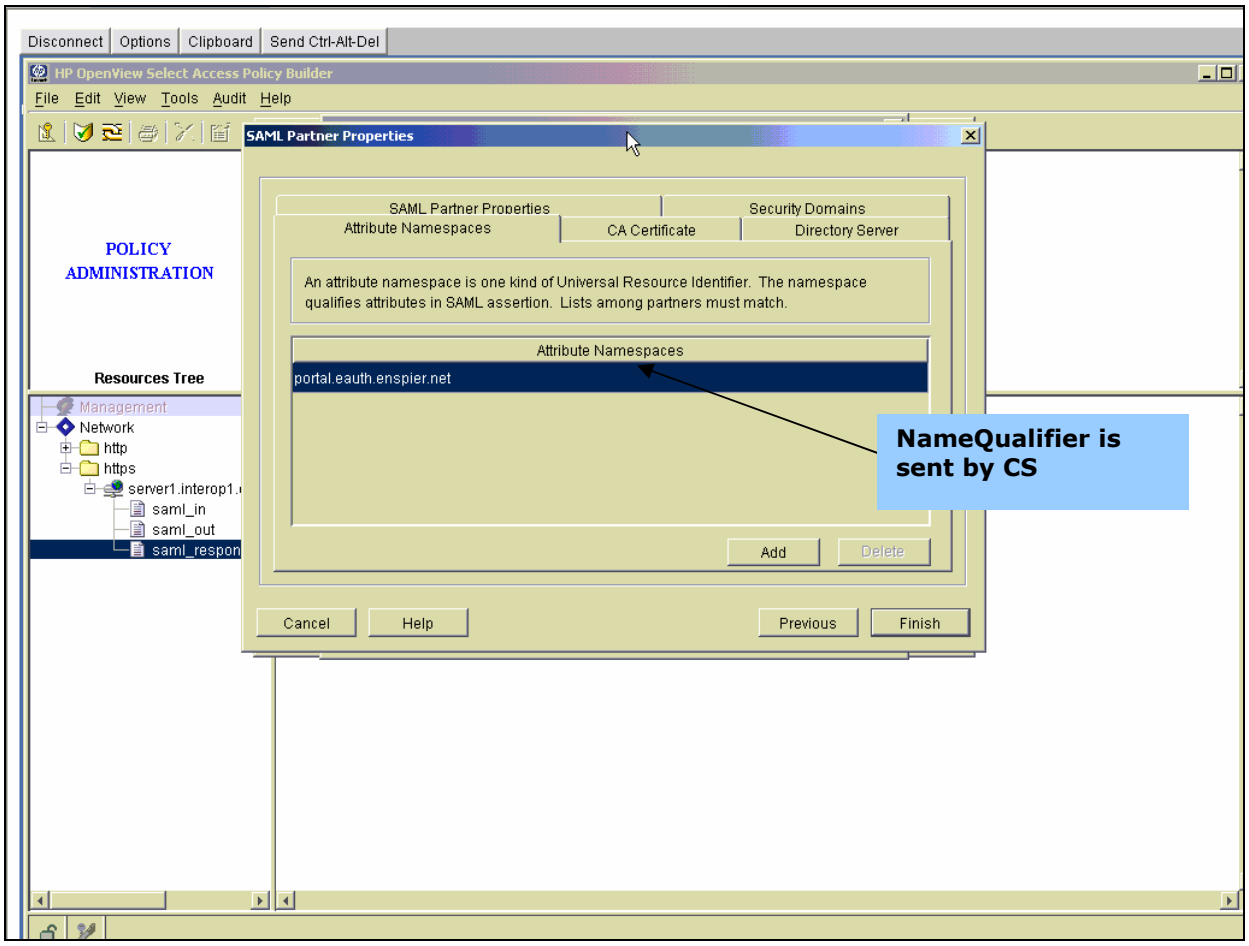


Figure 11-12: Attribute namespace tab

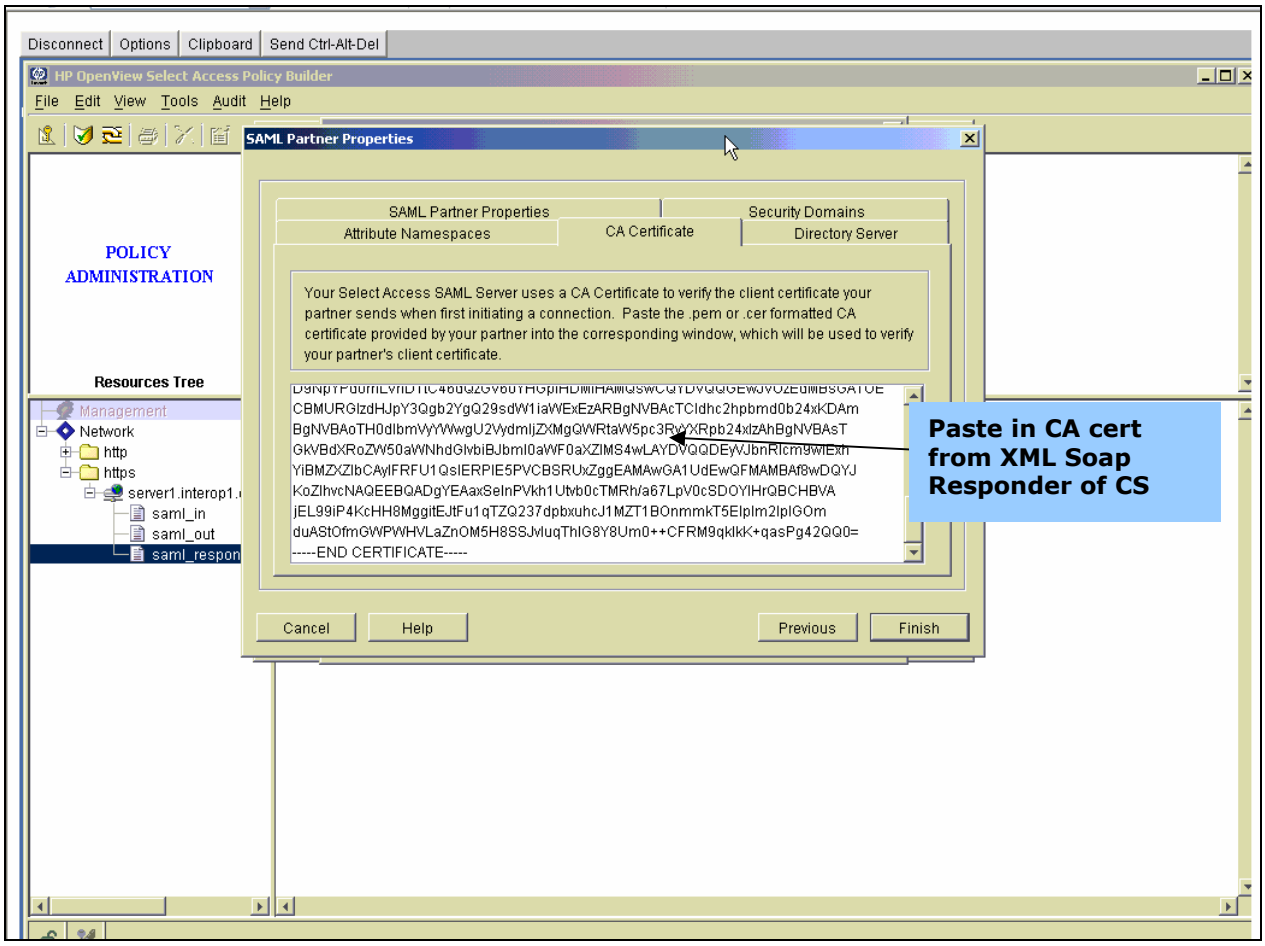


Figure 11-13: CA Certificate tab

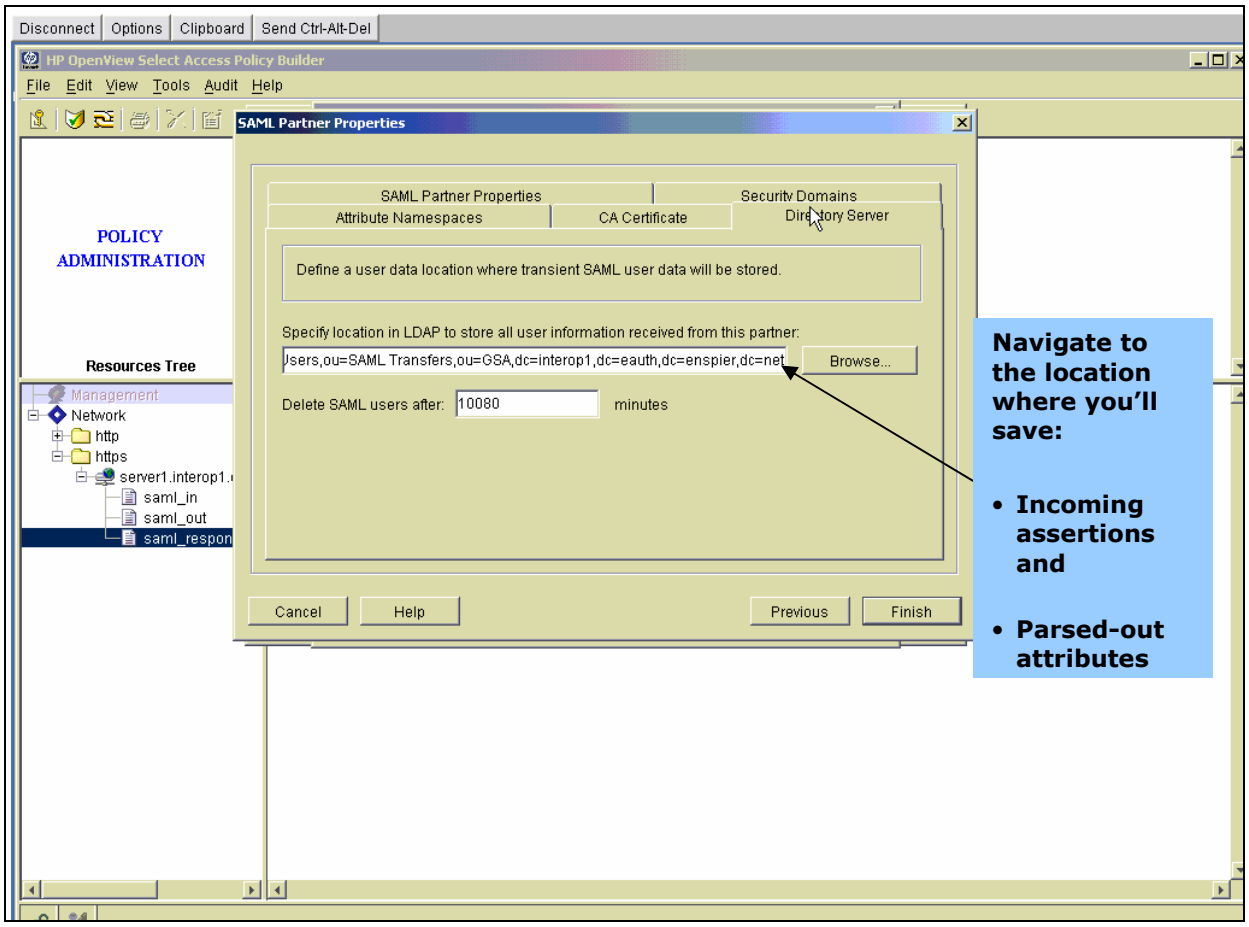


Figure 11-14: Directory server tab

Click on *Finish* when you are done inspecting and editing these tabs.

2.4 Enable the Authentication Server

Modify Select ID properties in order to allocate the desired resources in the resource tree. Use Policy Builder to enable the authentication server. To open, go to the Program files folder and open the HP directory. Click on the open view folder, then click on SelectAccess, then click on Policy Builder.

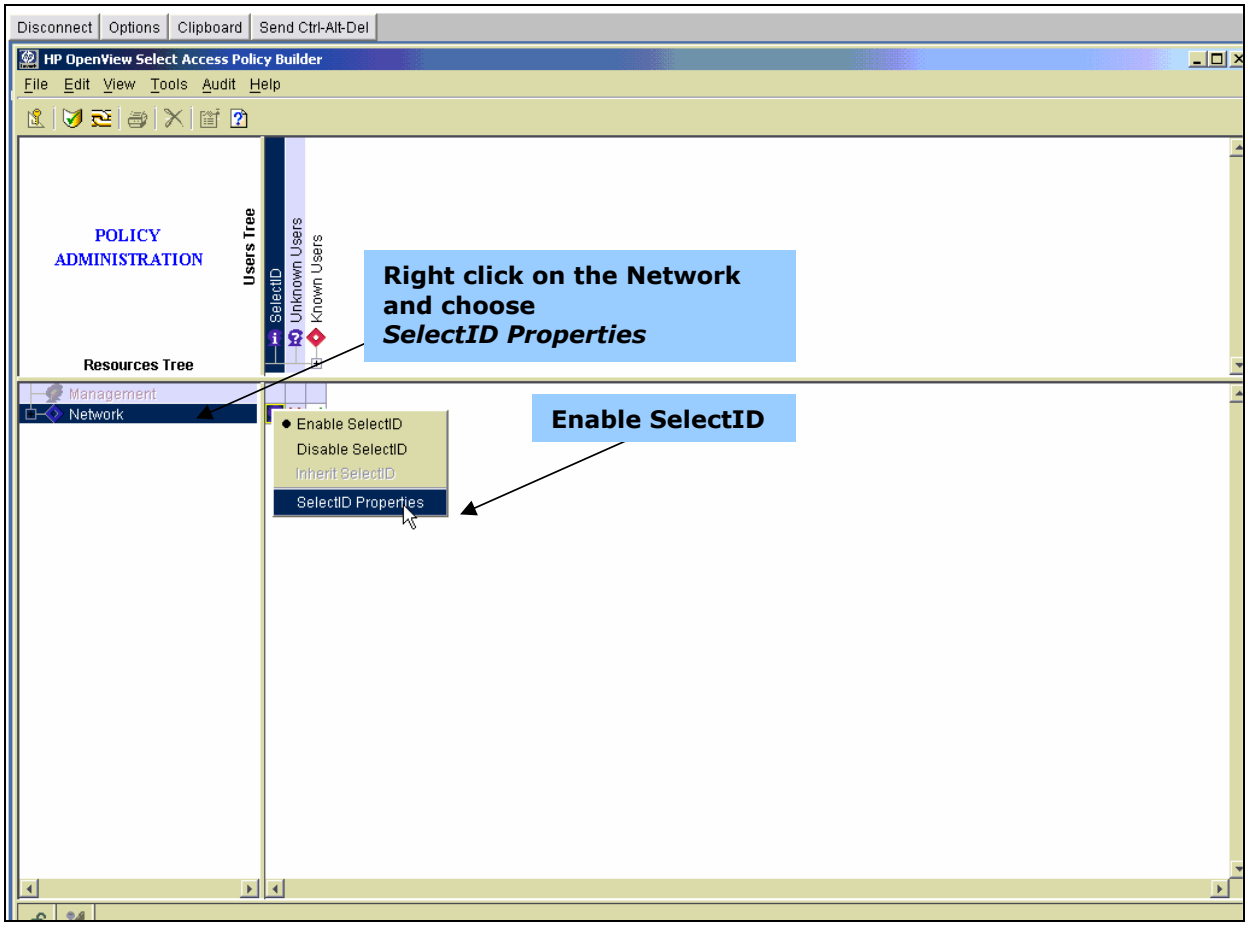


Figure 11-15: Open SelectID Properties

After you choose *SelectID Properties*, the *Authentication Properties* window will open, as shown in Figure 11-16. Use SelectID properties to allow users from this CS access to resources within the resource tree.

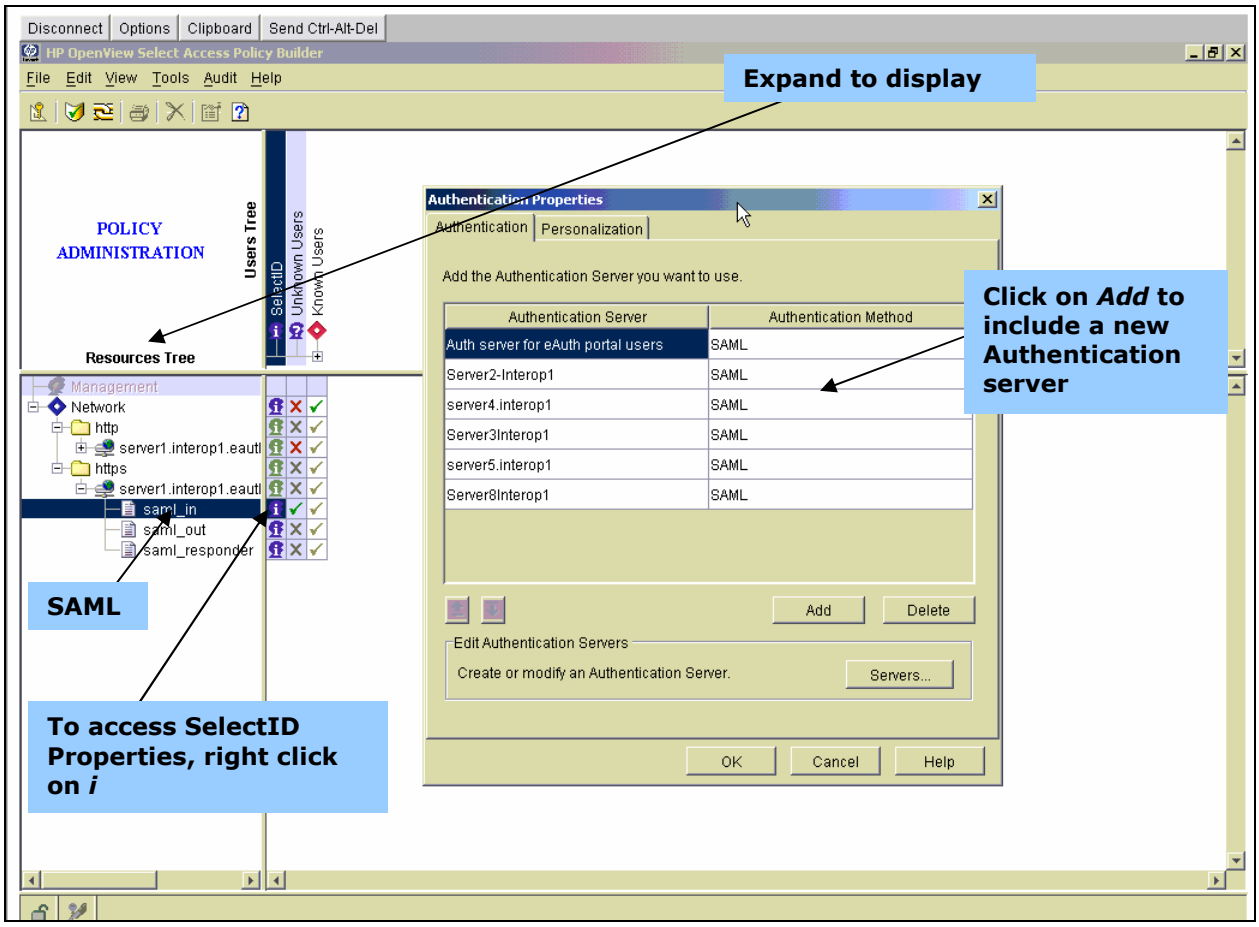


Figure 11-16: Authentication Properties

Recipe 12 - Cookbook for Setting up HP Select Access as a Credential Service (CS)

Table of Contents:

Version 1.0

1.0 Setup

1.1 Terms and Introduction

The SAML Artifact profile is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML and to use this HP application as a Credential Service. Remember that the HP setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML, starting at the main page shown in Figure 12-1.

Term	Definition
Agency Application (AA)	An online government service, provided by an agency, which requires a user to be authenticated.
Credential Service (CS)	A service, provided by a CSP, that electronically validates identity or a transaction.
Credential Service Provider (CSP	An organization that offers one or more Credential Services (CS). If a CS offers more than one type of credential then each type is considered a separate CS.
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations for the Initiative.

1.2 Using the Setup tool

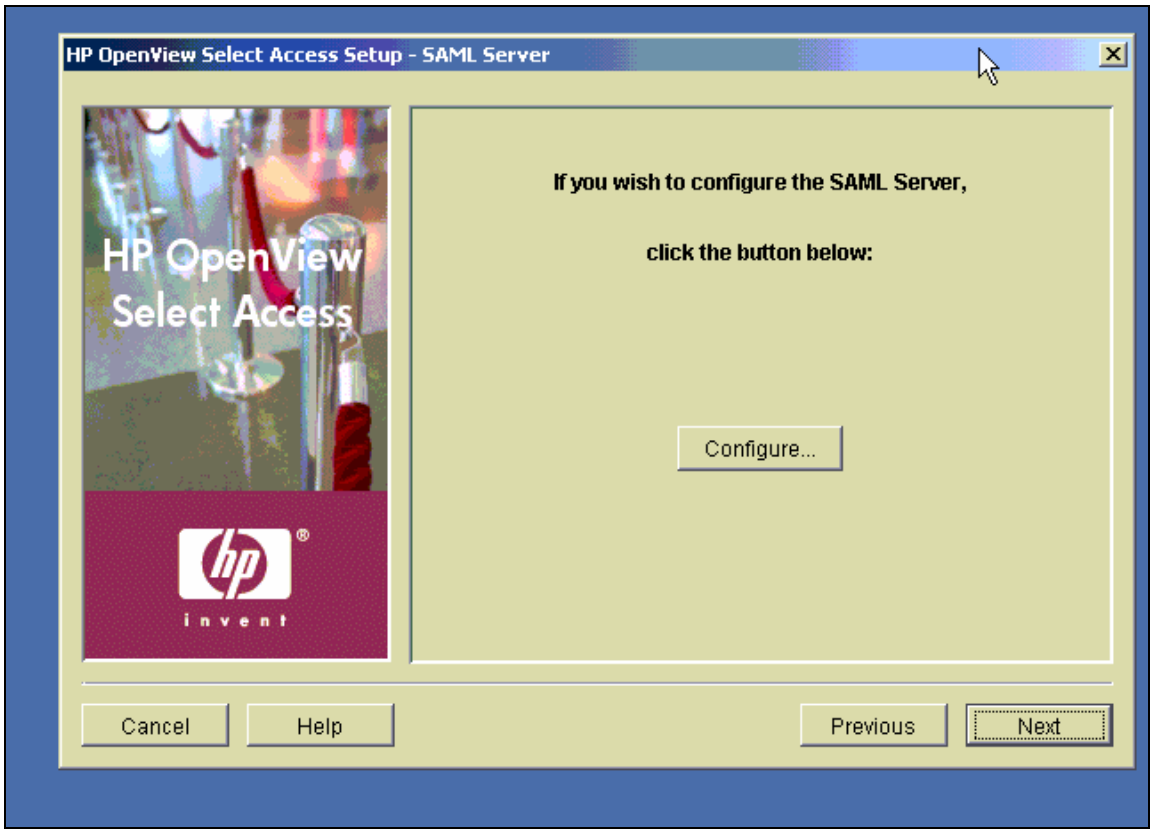


Figure 12-1: Start Setup Tool

Use the setup tool to configure a SAML server. Accessing the set up program is the same whether you are setting up a CS or an AA. After the initial setup, do not attempt to use the setup tool again. Instead, use SAML partner properties to access properties.

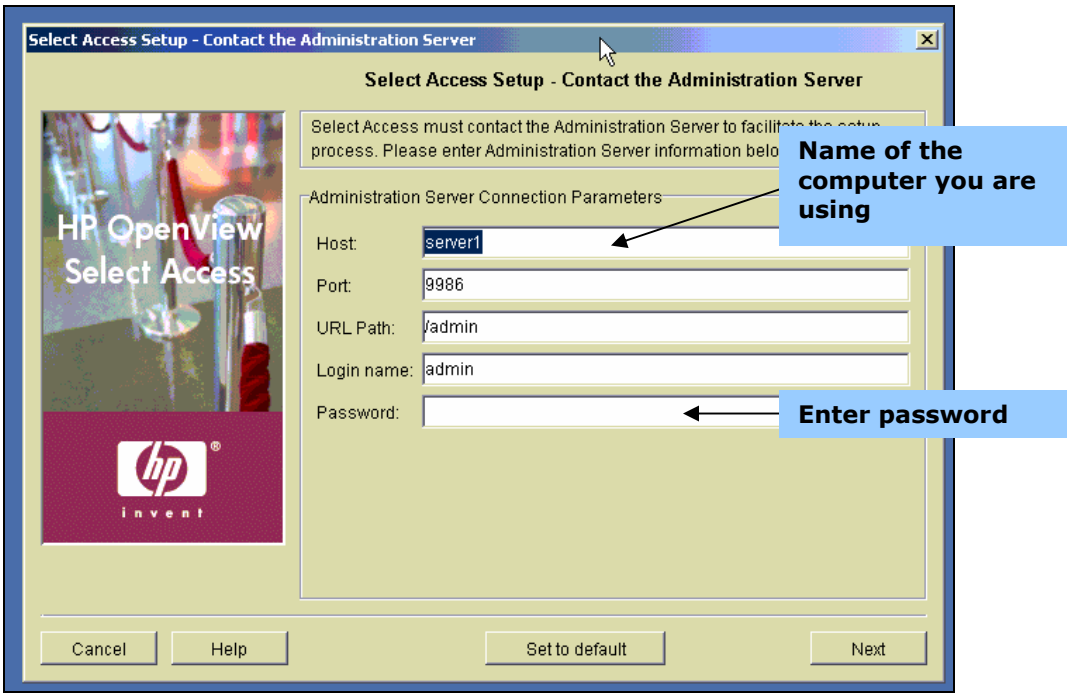


Figure 12-2: Select Access Setup

Figure 12-3: Define SAML Server ID

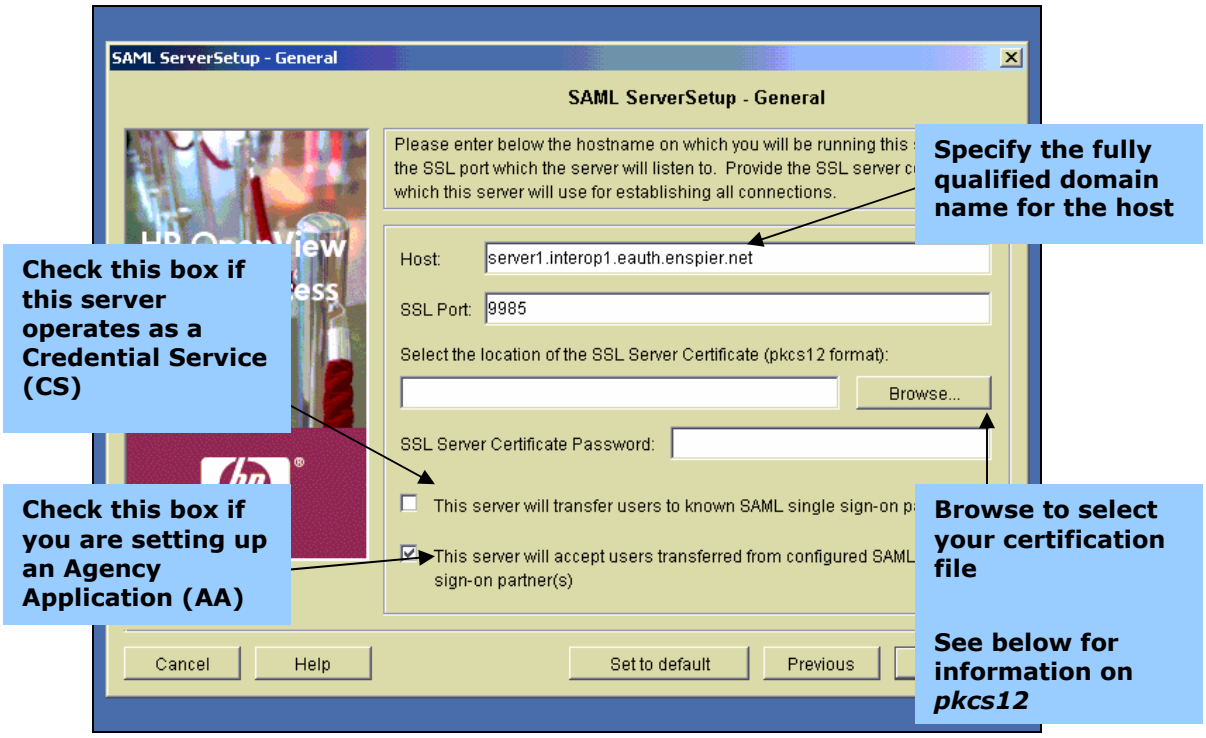


Figure 12-4: General Server Setup

PKCS12 files combine private and public key certificates. This file is protected by a password, which you will provide when you create your PKCS12 file.

2.0 Policy Builder

2.1 Using Policy Matrix to modify SAML component configuration

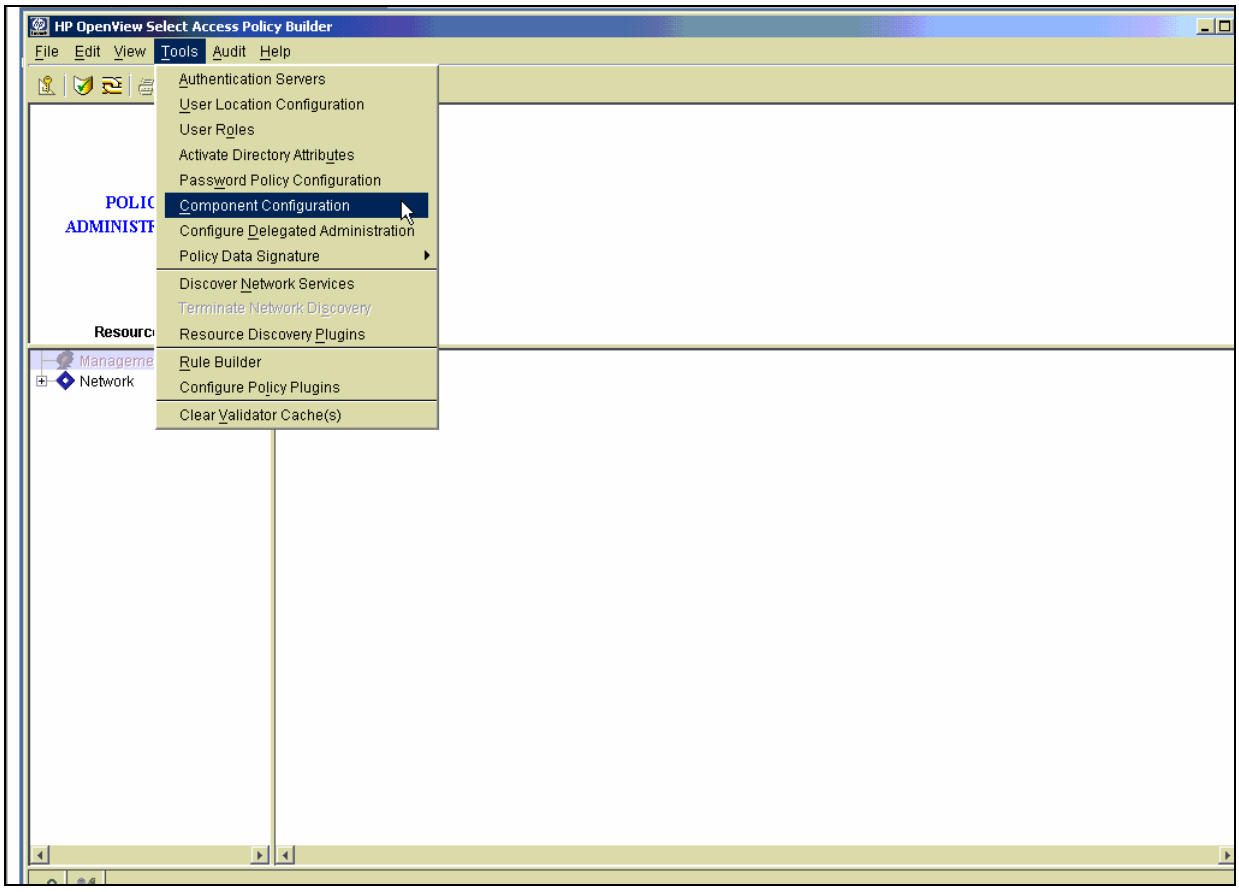


Figure 12-5: Working with Policy Builder

Click on Tools, the select *Component Configuration.* A component configuration window will open, as shown in Figure 12-6 below.

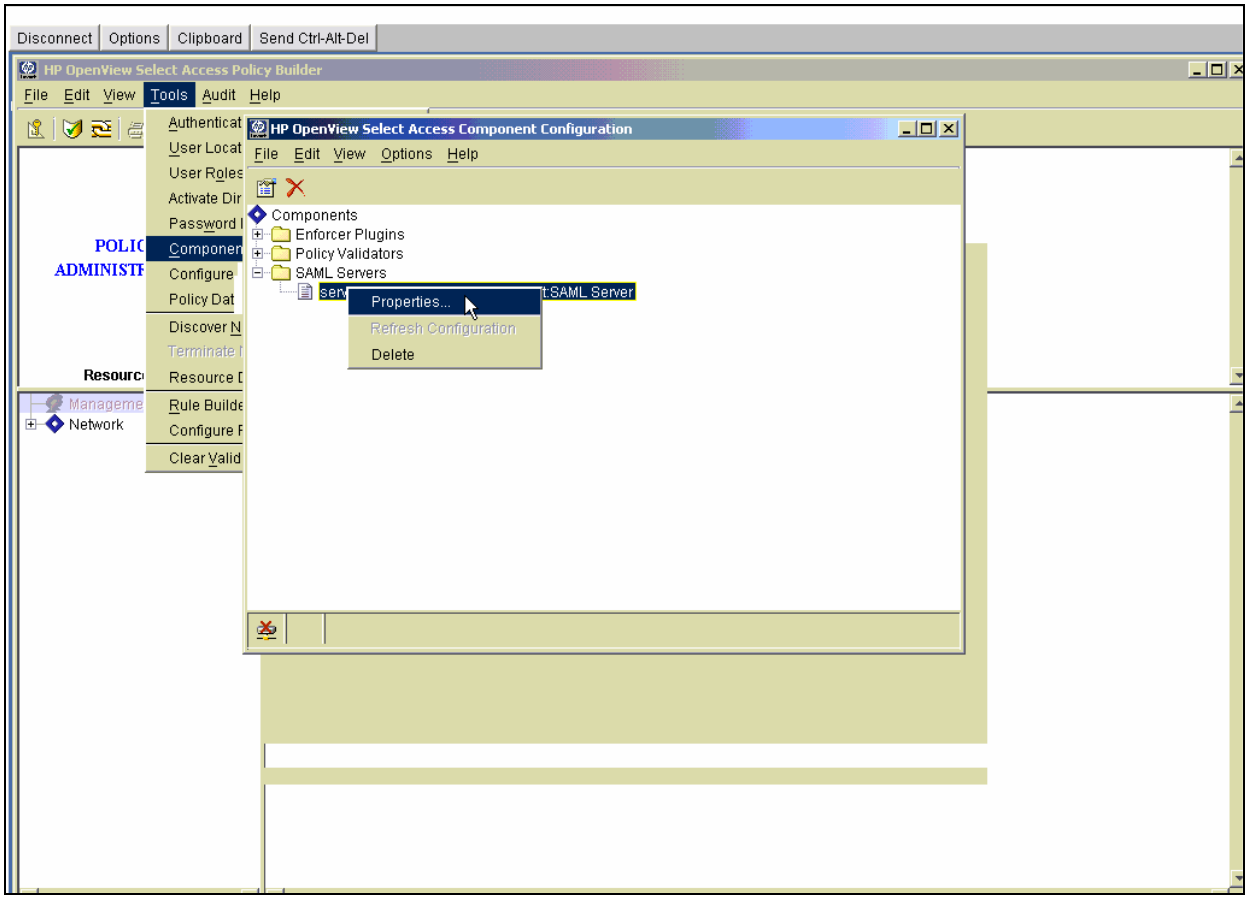


Figure 12-6: Navigating to Component Configuration

To view assertion properties, right click on a SAML server file, choose *Properties*. A window for assertion properties, as shown in Figure 12-7, will open.

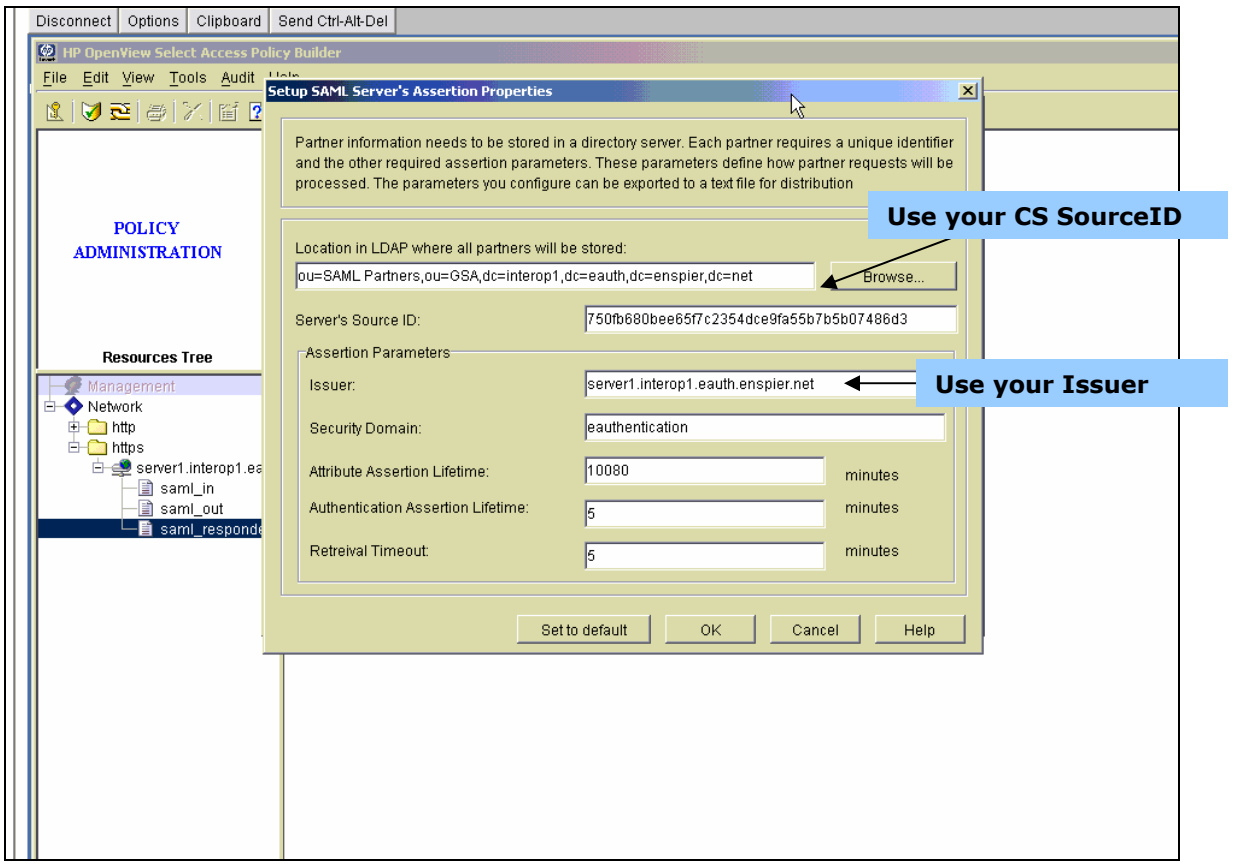


Figure 12-7: **Configure AA Assertion Properties**

2.2 Adding an AA

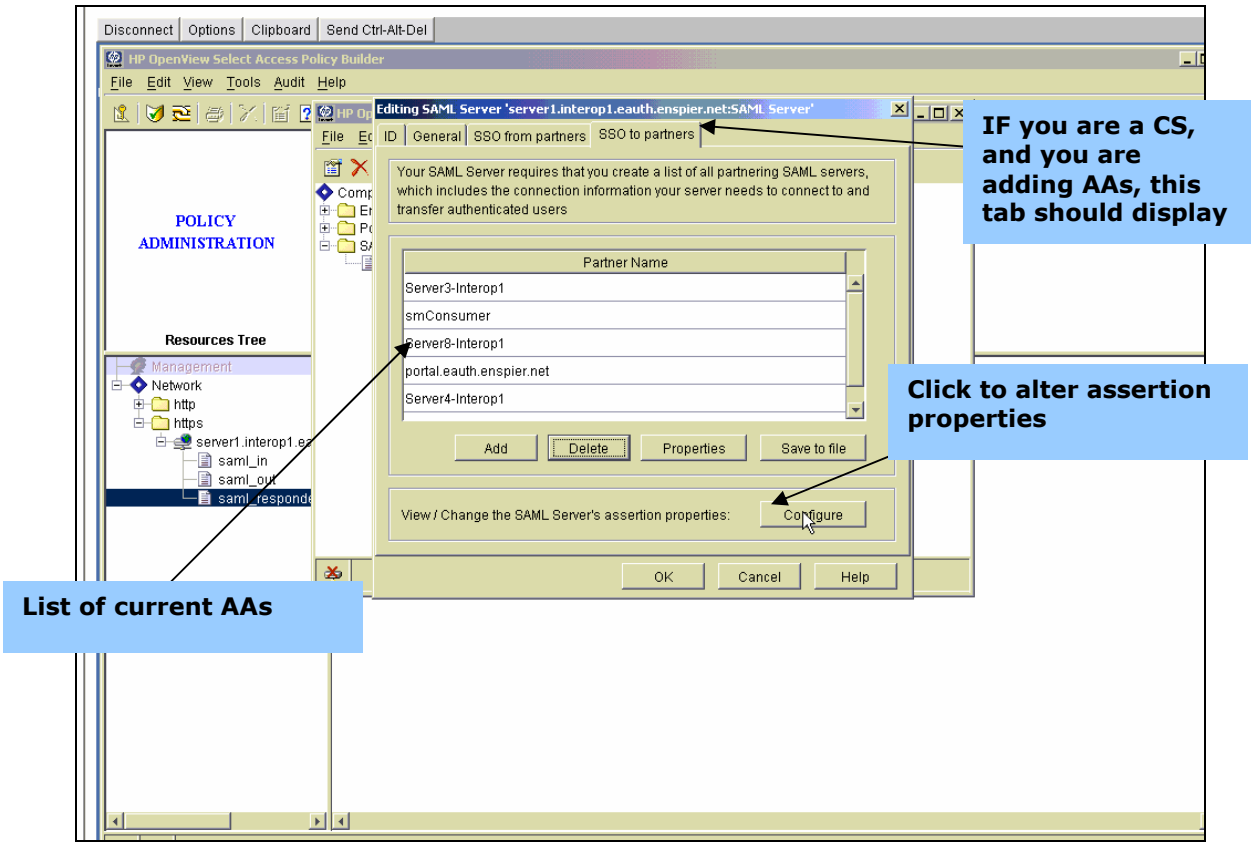


Figure 12-8: Starting point for modifying and adding new AAs

If you click on Configure, the *Setup SAML Server's Assertion Properties* window will display, as shown in Figure 12-9. This information is also found in the setup tool, but it is best to configure through the steps defined in section 2.5.

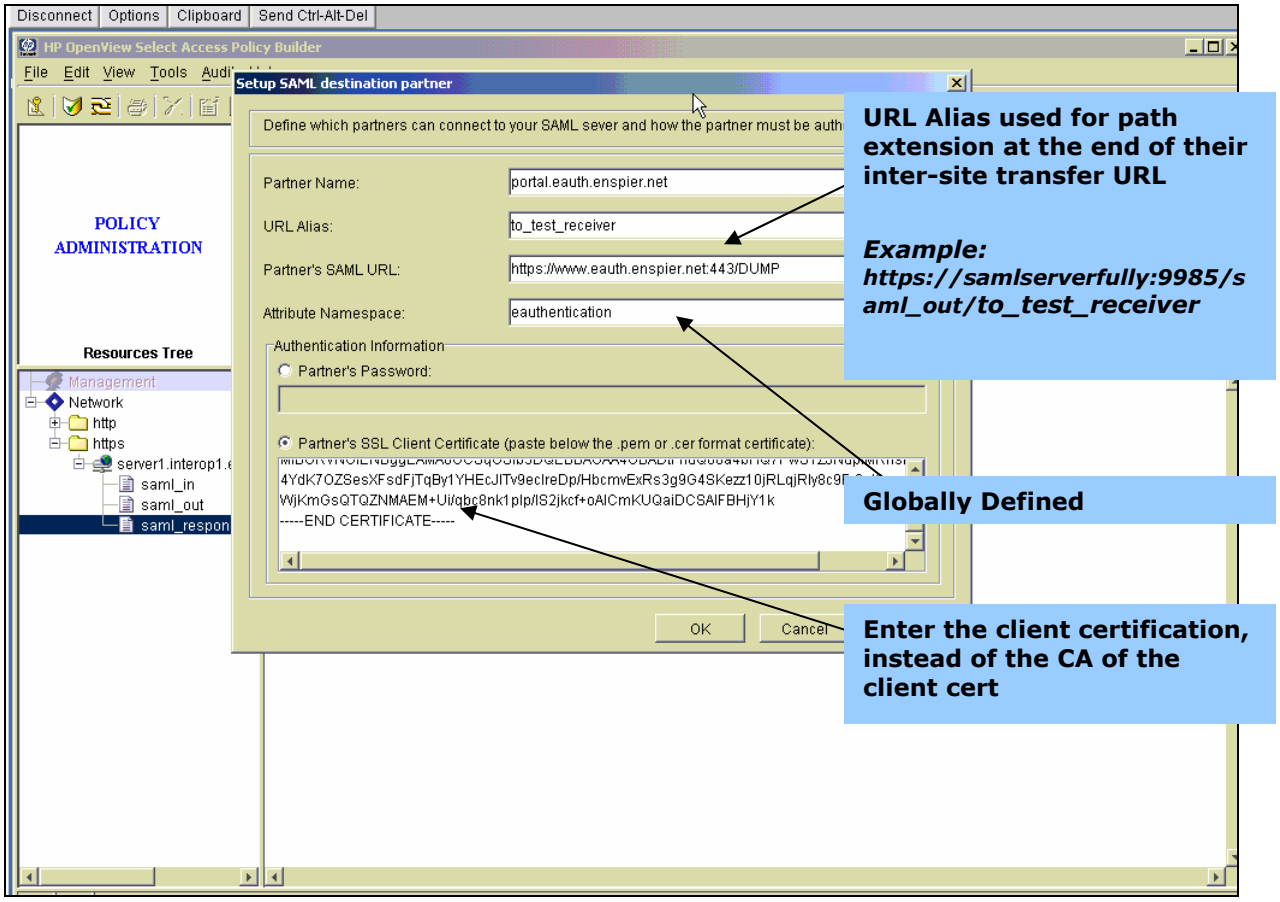


Figure 12-9: **Configure AA Assertion Properties**

After you click on the *Add* button, see figure 12-10, the *Setup SAML destination partner* window will display. Enter your *Name*, *URL Alias*, etc., and then click on *OK* to finish and save settings.

2.3 Adding SAML Assertion Attribute

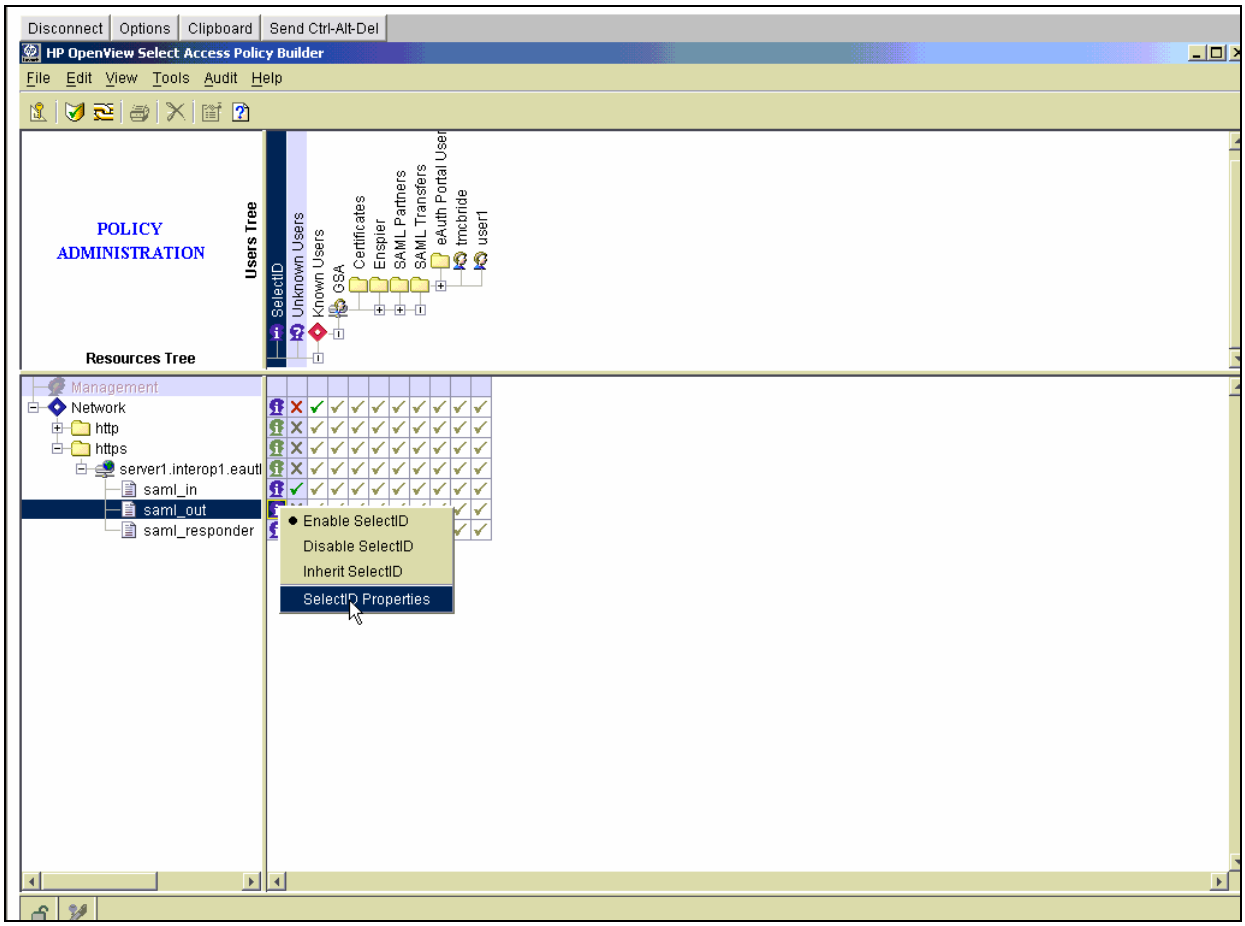


Figure 12-10: **Configure AA Assertion Properties**

Right click on the ***i*** next to the SAML file you want to work with. Choose *SelectID Properties.* The window shown in figure 12-11 will display, click on the *Personalization* tab when the window finishes loading.

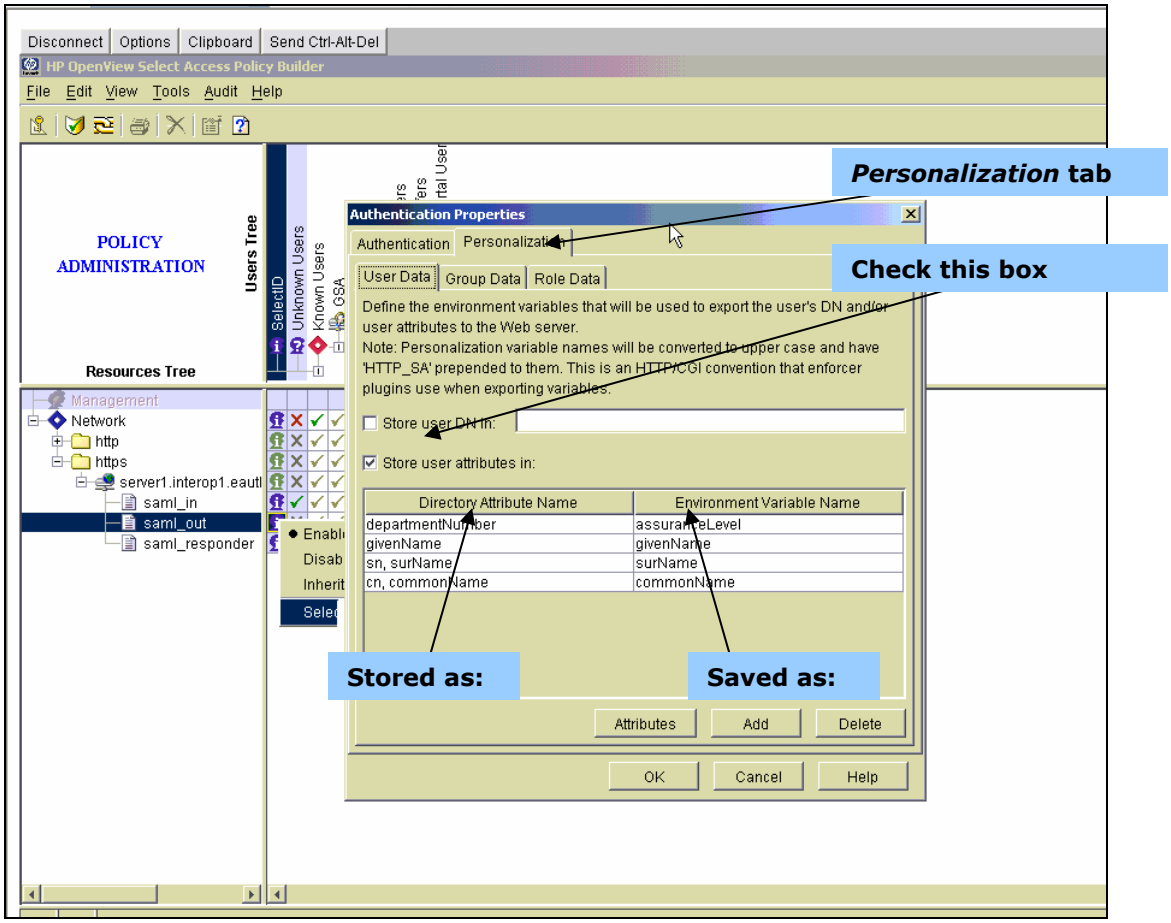


Figure 12-11: Personalization tab

Recipe 13 - Configuration Guide for Sun Java System Identity Server for an AA and CS

Table of Contents

Version 1.0

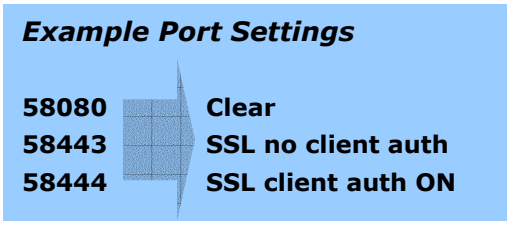
1.0 Setup

1.1 Terms and Introduction

The SAML Artifact profile is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML, to use this Sun application as a Credential Service or as an Agency application. The Sun setup screens are the same, whether setting up an AA or a CS. In section 2, each type of setup is outlined separately. After reviewing the terms, configure your scheme to handle SAML, starting at the main page shown in Figure 13-1.

1.2 Web Server SSL setup

To setup your web server, first enable SSL on the web server that will be running Sun Java System Identity server. Make sure client auth is on. Other than enabling SSL on the web server, you must create a port requiring client certifications.



2.0 SAML Server Configuration

To begin SAML server configuration, you will be logging on to the Sun Java System Identity Server Administration. To access the Sun Java System Identity Server Administration Console, go to:

http://is.fqdn.com:58080/amconsole

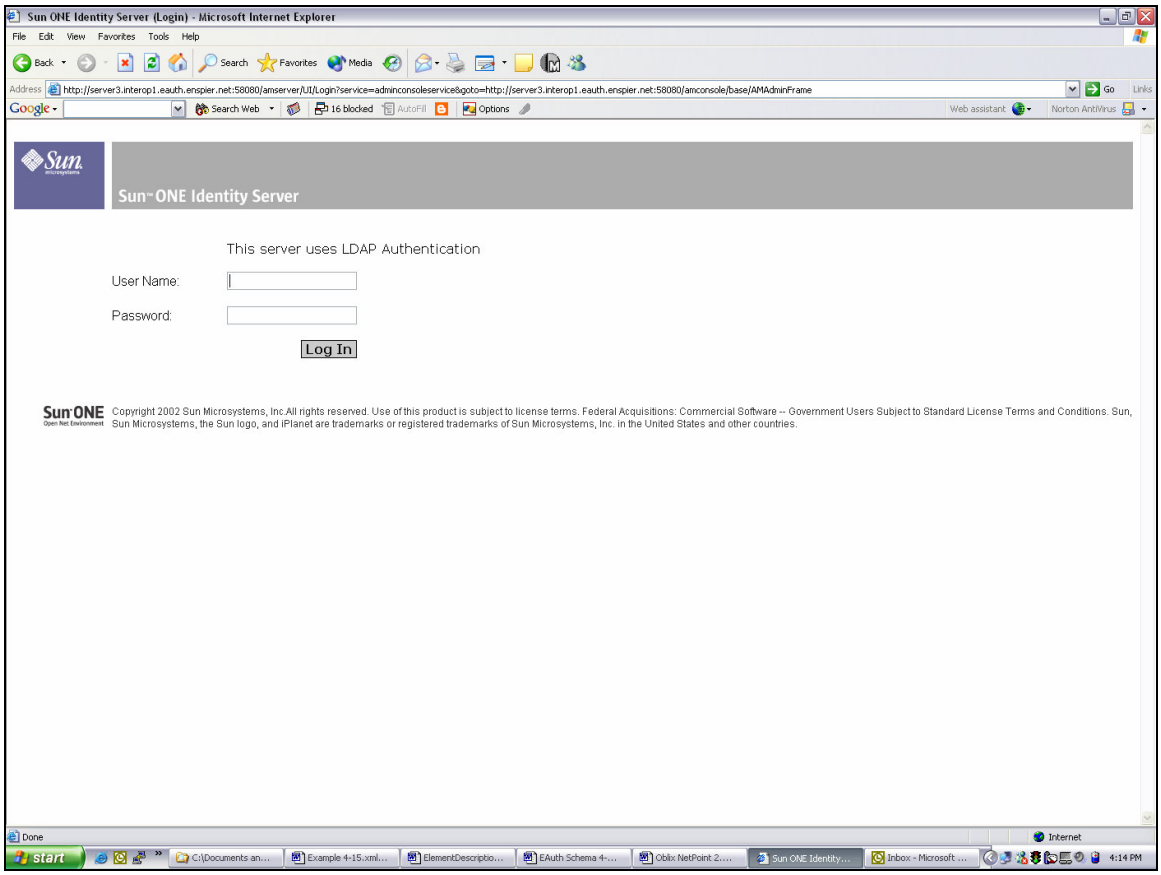


Figure 13-1: Security Settings

After you Log In, a screen similar to Figure 13-2 will display.

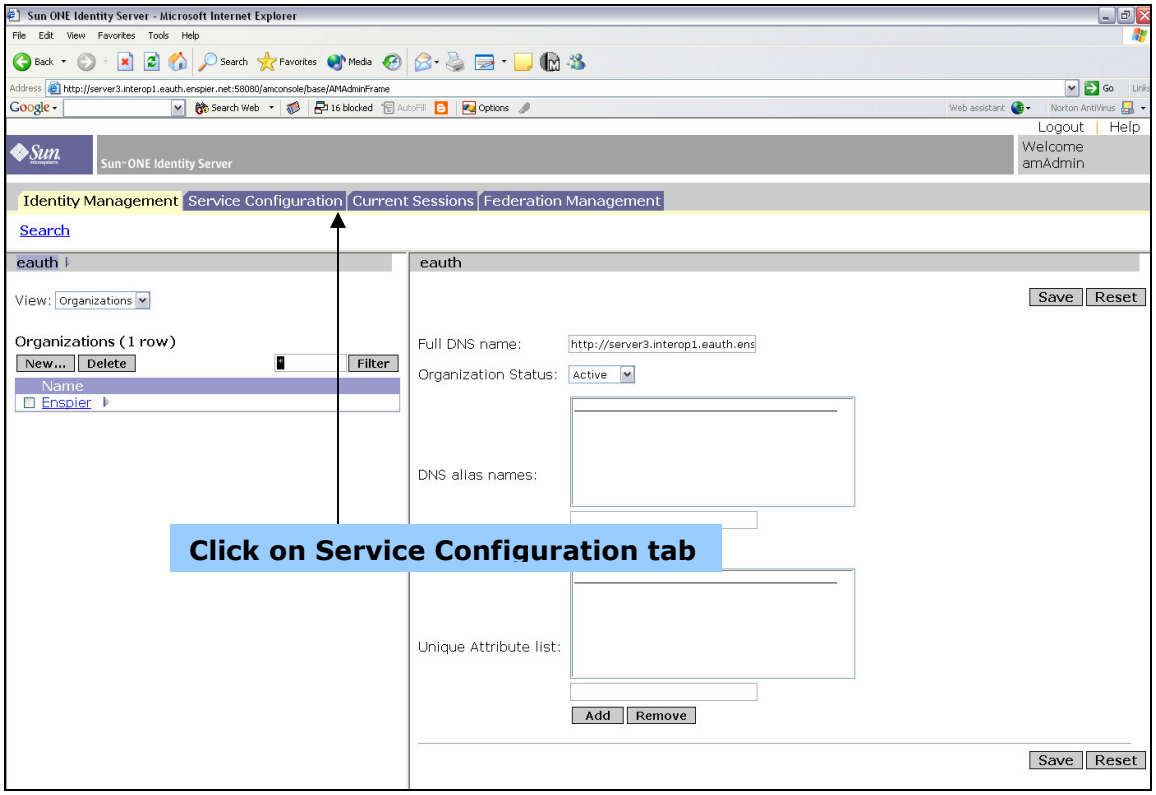


Figure 13-2: Identity Management Page

First, Click on *Service Configuration* tab.

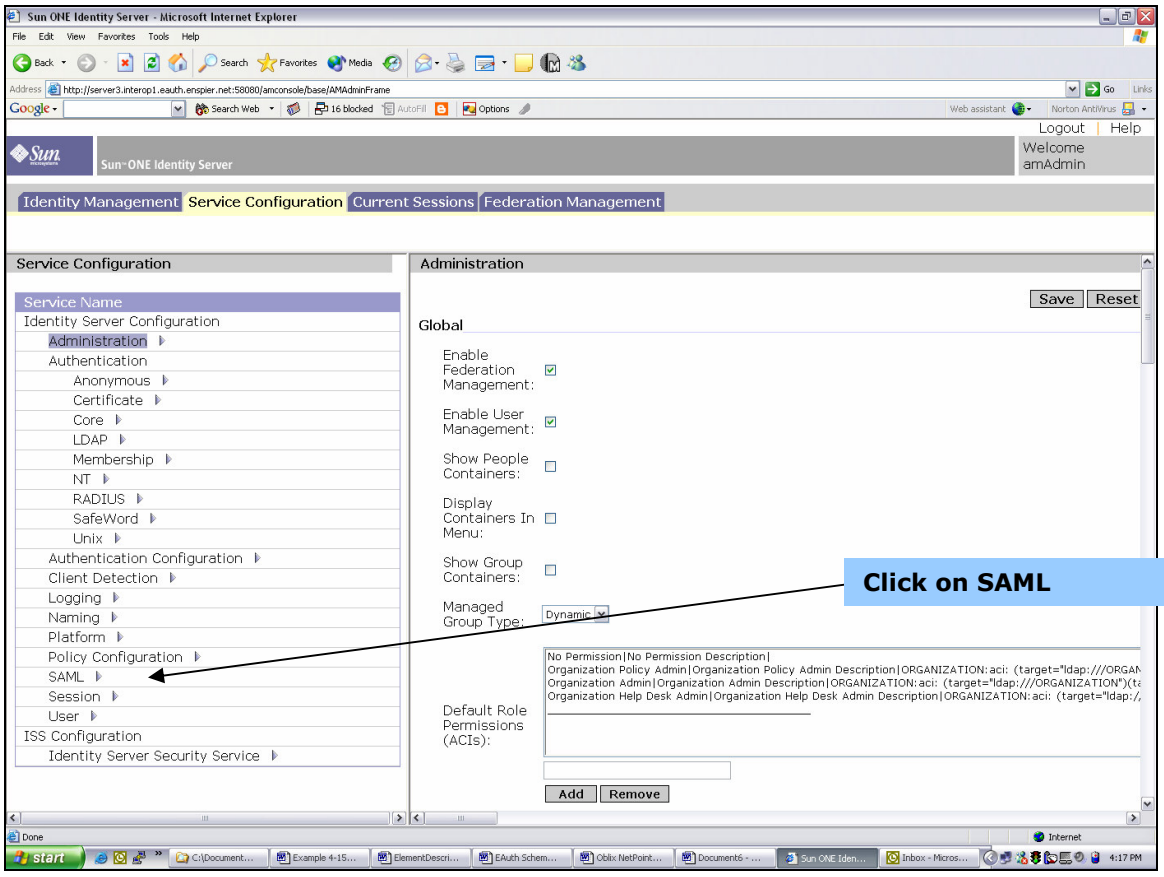


Figure 13-3: Admin Page

Then click the arrow next to *SAML* (under *Service Name*), and a window similar to figure 13-4 will display.

When configuring Sun, either as an AA or a CS, you will spend most of your time working with the screen displayed in figure 13-4.

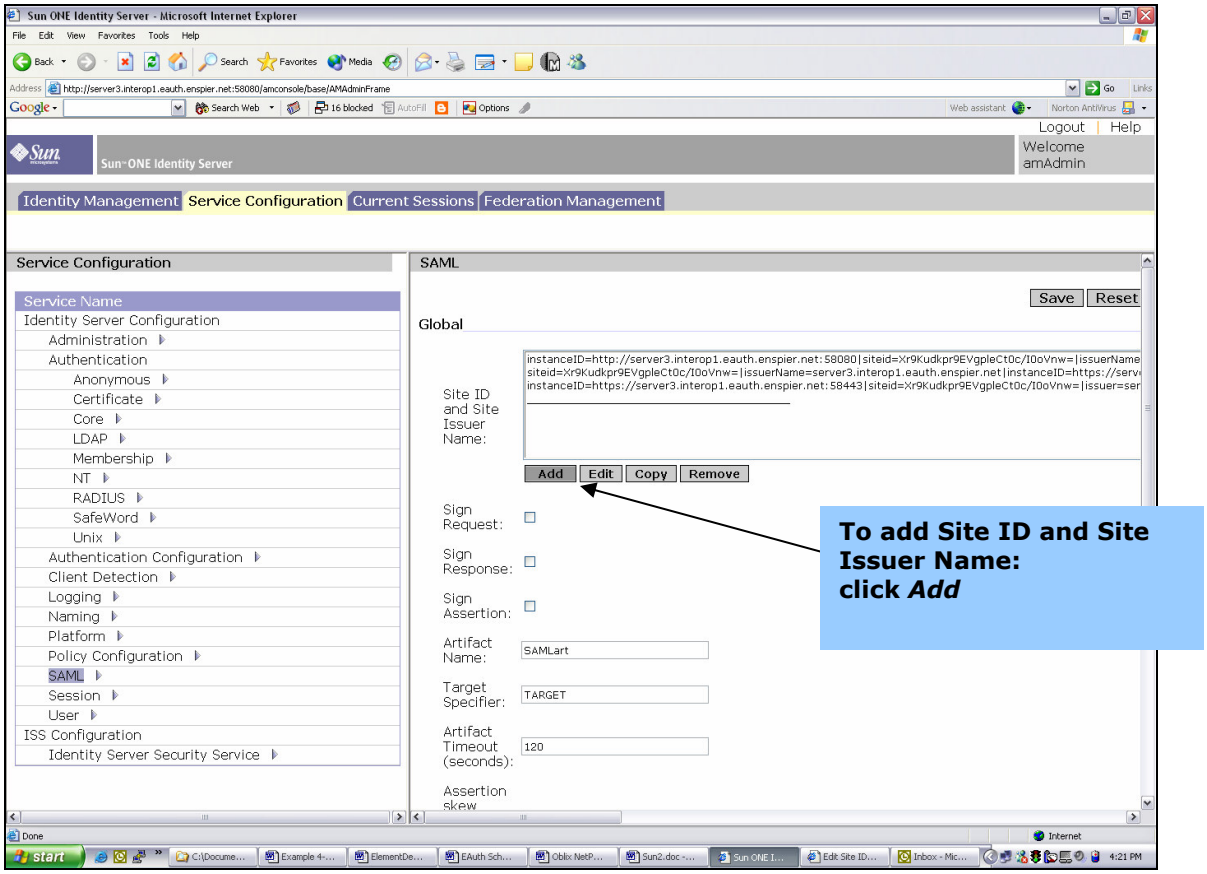


Figure 13-4: Identity Server Console

Click the *Add* button to include a new Site ID and Site Issuer Name. After you click Add, a window similar to figure 13-5 will display.

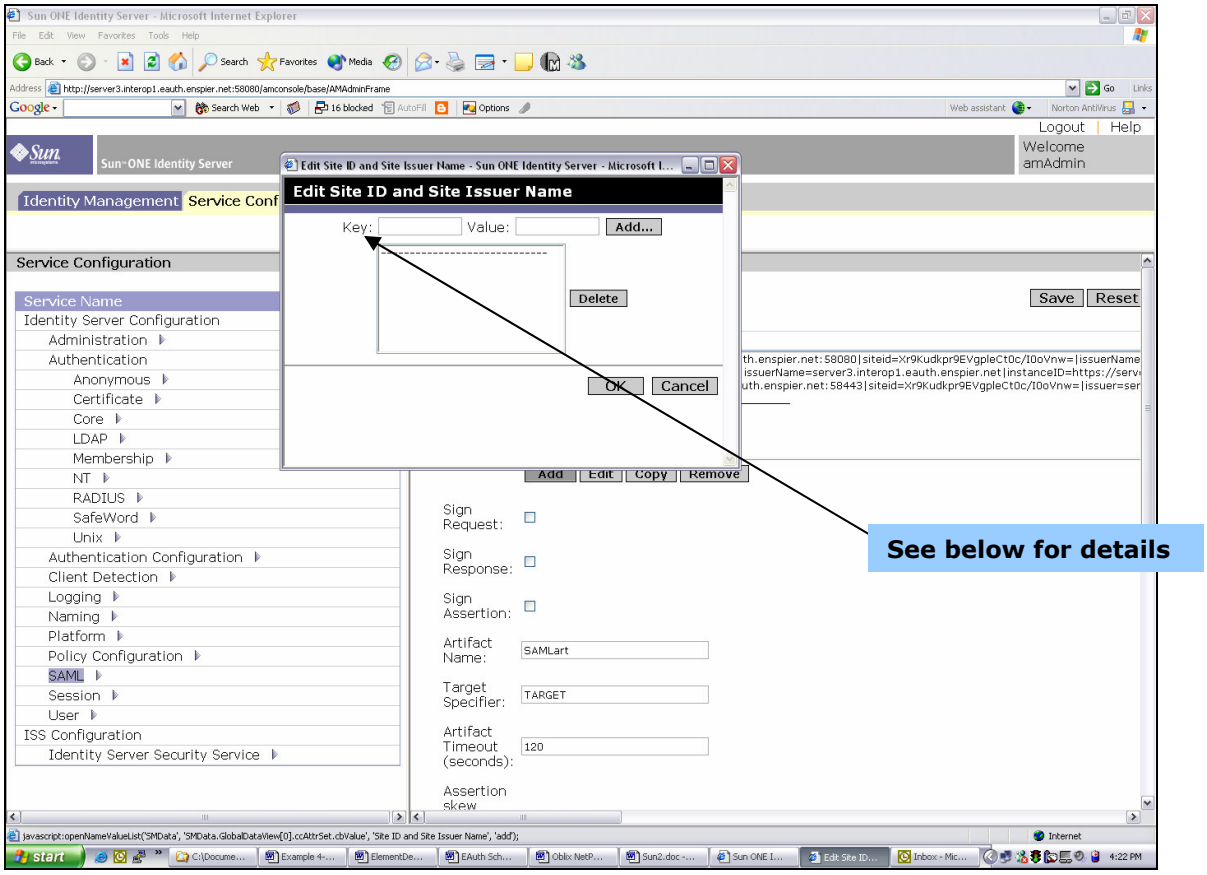


Figure 13-5: Edit Site ID Site Issuer Name

Duplicate the pre-existing Site ID and Site Issuer Name name/value pairs changing only instanceID to reflect the https protocol and the port number. There should be 3 entries in the Site ID and Site Issuer Name section. One for the http port, one for https not requiring a client certificate, and one for https requiring a client certificate.

For example:
instanceID=http://is.fqdn.com:58080
instanceID=https://is.fqdn.com:58443
instanceID=https://is.fqdn.com:58444

Next, scroll to the bottom of the page to the “Trusted Partner Sites” section. Click add and this pops up: Fill in different name/value pairs depending on your role (AA or CS).

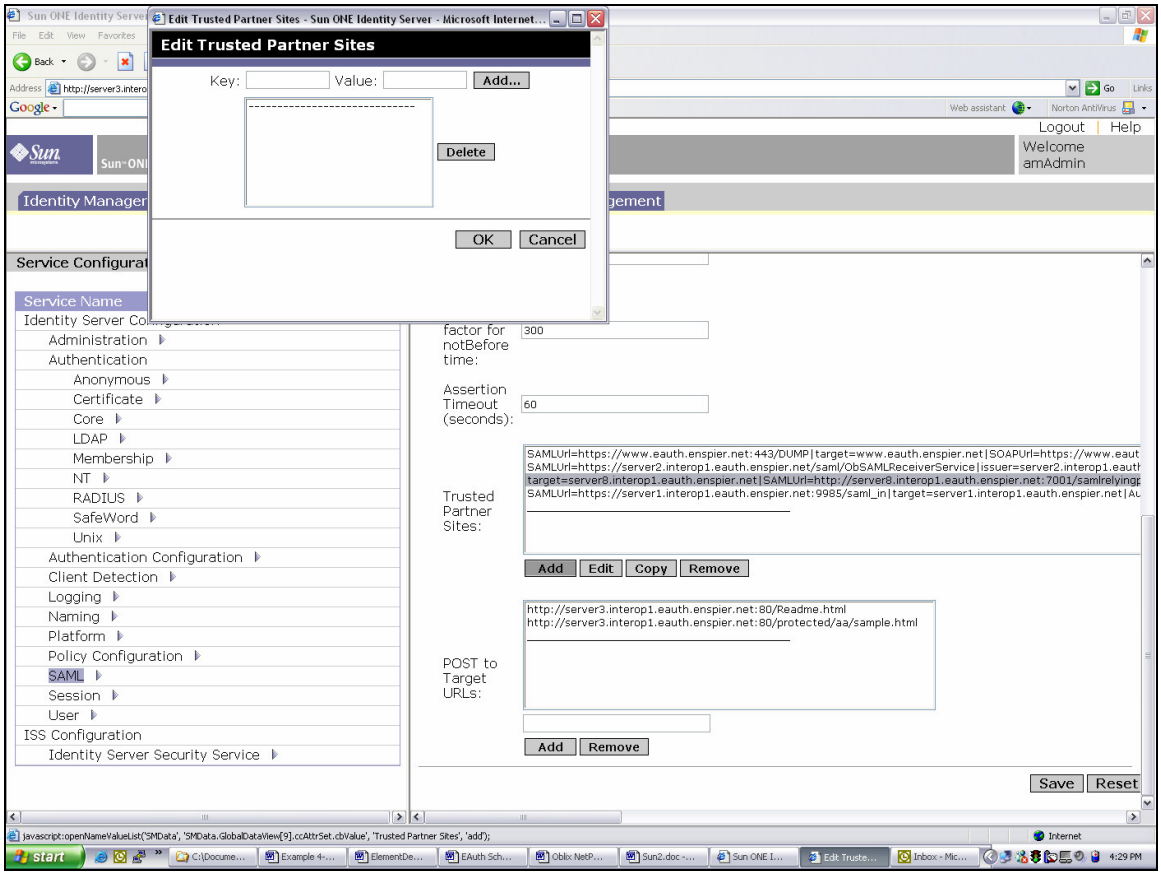


Figure 13-6: Edit trusted partner sites

3.0 Partner Configuration

To add either a CS or an AA, you'll be adding a new line to the Trusted Partner Sites list. You will need to obtain a SourceID for the partner you are adding. Click and select a line under the T*rusted Partner Sites* and then click on *Edit*.

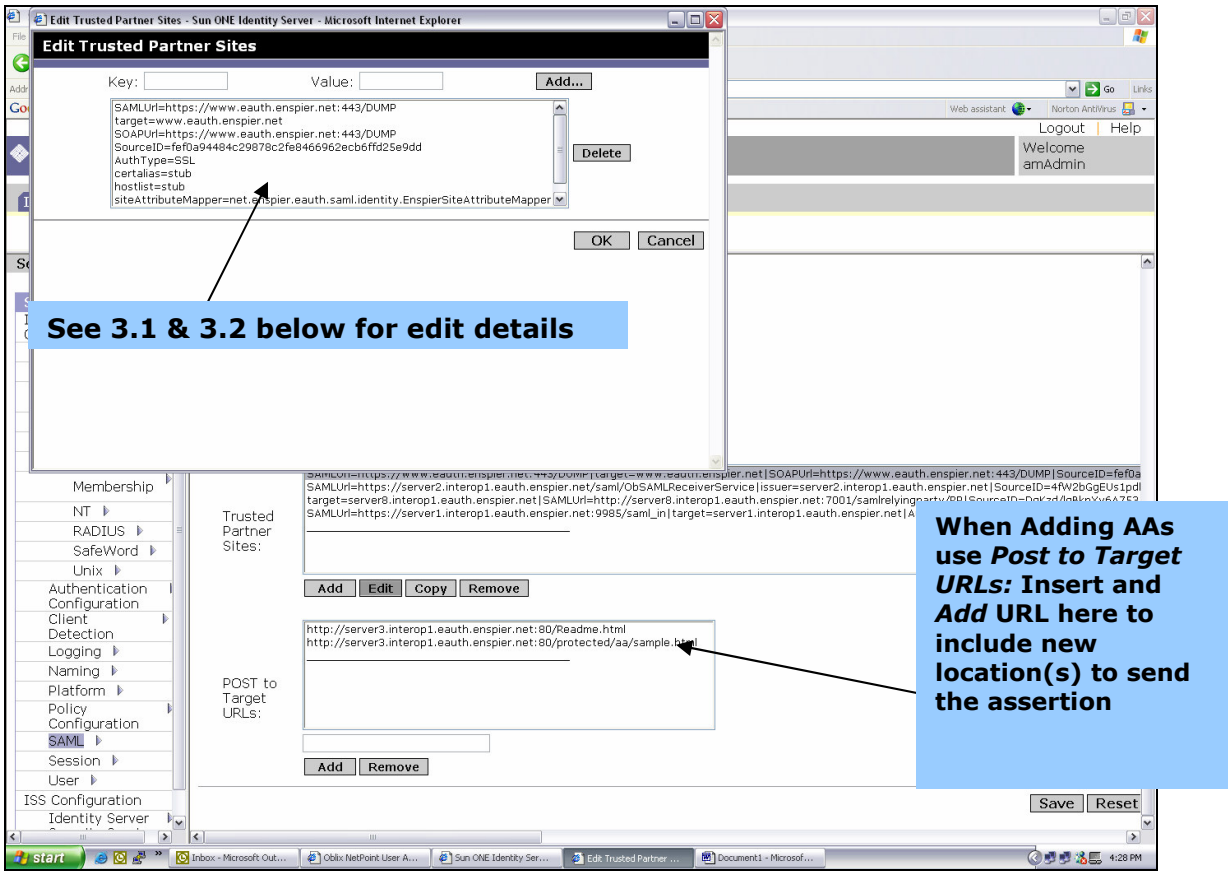


Figure 13-7: Edit trusted partners window

3.1 Adding AAs

To add an AA, you must be set up as a CS. Change the following when adding new entry for *Trusted Partner Sites* list:

- Target = fq domain name of partner site
- AuthType = SSL

- Hostlist = cert alias or name (certificate in certificate)
- Site AttributeMapper = java plugin store class to send attribute
- SAML URL = URL of partners artifact receiver

3.2 Add a new CS

You must be setup as an AA to add a new CS. Edit the list that appears next to the words *Trusted Partner Sites.* Click *Add* when you finish your edits.

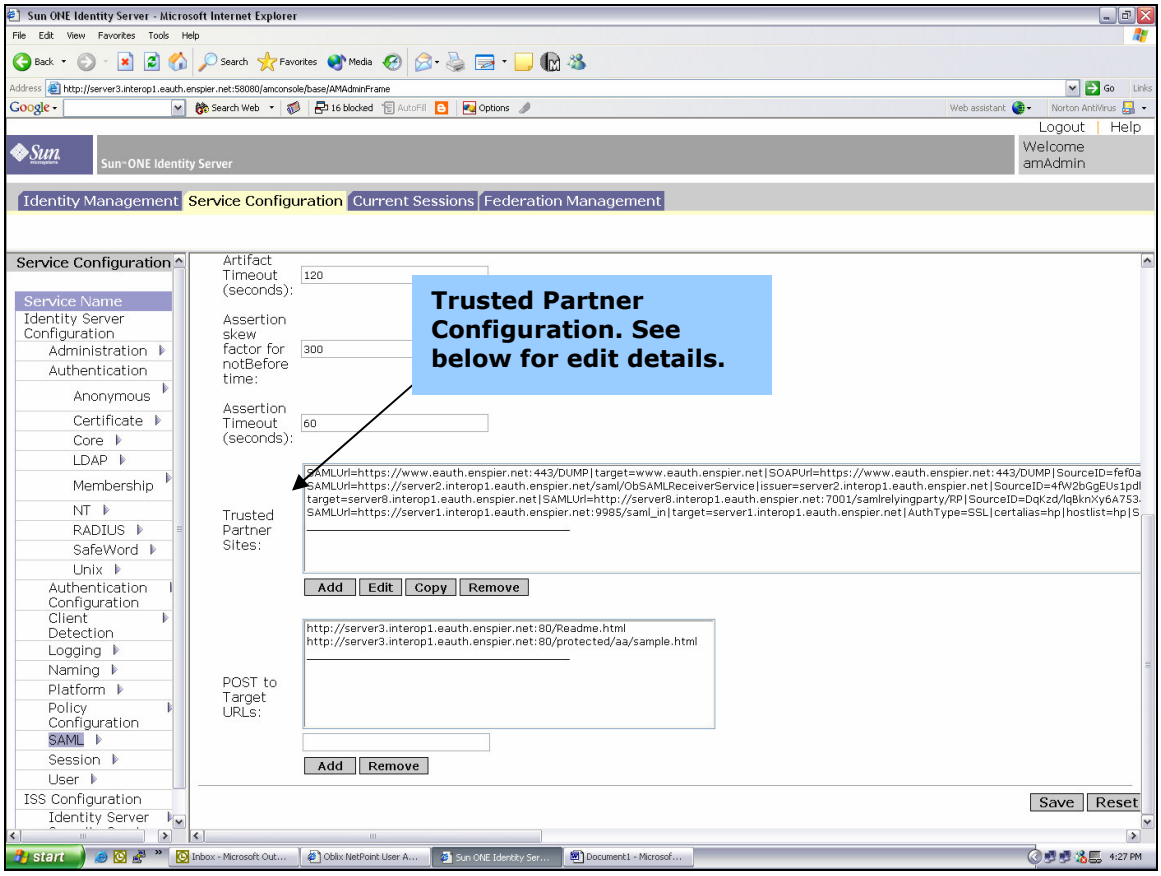


Figure 13-8: Edit Trusted Partner Sites List

To add a CS you must be setup as an AA. Select a line next to *Trusted Partner Sites*, and click on *Edit.* Change the criteria below, and click on *Add.*

- SOAP URL= URL of SAML responder
- AuthType = SSL

- AttributeMapper = java plugin to read attributes from the assertion
- Action Mapper = java plugin to do tings based on the assertion

3.2.1 Set Up a Certificate Store

See Solaris and Windows 2000 examples in figure 13-9 for setting up the certificate store.

Example 1: Solaris

---
setenv LD_LIBRARY_PATH /opt/SUNWam/servers/bin/https/lib (assuming install dir is /opt, change it if not to what the install dir is)
cd /opt/SUNWam/servers/bin/https/admin/bin
./certutil -A -n greed -t P -d /opt/SUNWam/servers/alias -P https-arth.red.iplanet.com-arth- -f /opt/SUNWam/config/.wtpass - i infile

where -d is the com.iplanet.am.admin.cli.certdb.dir parameter from /opt/SUNWam/lib/AMConfig.properties
-P is the com.iplanet.am.admin.cli.certdb.prefix parameter from /opt/SUNWam/lib/AMConfig.properties
-f is the com.iplanet.am.admin.cli.certdb.passfile parameter from /opt/SUNWam/lib/AMConfig.properties
-i is the client certificate of B (greed).

Example 2: Windows2000

---
assuming product is installed in c:\sunone\sunoneis directory
go to c:\sunone\sunoneis\servers\bin\https\admin\bin
certutil -A -n greed -t P -d c:\sunone\sunoneis\servers\alias -P -P https-arth.red.iplanet.com-arth- -f \sunone\sunoneis\config\.wtpass -i infile

where -d is the com.iplanet.am.admin.cli.certdb.dir parameter from c:\sunone\sunoneis\\lib\AMConfig.properties
-P is the com.iplanet.am.admin.cli.certdb.prefix parameter from c:\sunone\sunoneis\\lib\AMConfig.properties
-f is the com.iplanet.am.admin.cli.certdb.passfile parameter from c:\sunone\sunoneis\\lib\AMConfig.properties
-i is the client certificate of B (greed).

Figure 13-9: Example Certificate Setup

Recipe 14 - Configuration Guide for Oblix ShareID for an AA and CS

Table of Contents:

Version 1.0

1.0 Setup

1.1 Terms and Introduction

The SAML Artifact profile is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML, to use Oblix as a Credential Service or as an Agency application. The Oblix setup screens are the same, whether setting up an AA or a CS. In section 2, each type of setup is outlined separately. After reviewing the terms, configure your scheme to handle SAML, starting at the main page shown in Figure 14-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires a user to be authenticated.
Credential Service (CS)	A service of a Credential Service Provider (CSP) that provides credentials to subscribers for use in electronic transactions. If a CS offers more than one type of credential then each one is considered a separate CS.
Project Management Office (PMO)	The PMO is the organization that handles EAuthentication program management, administration, and operations for the Initiative.

To get started, type in the URL and click on *Access Manager.*

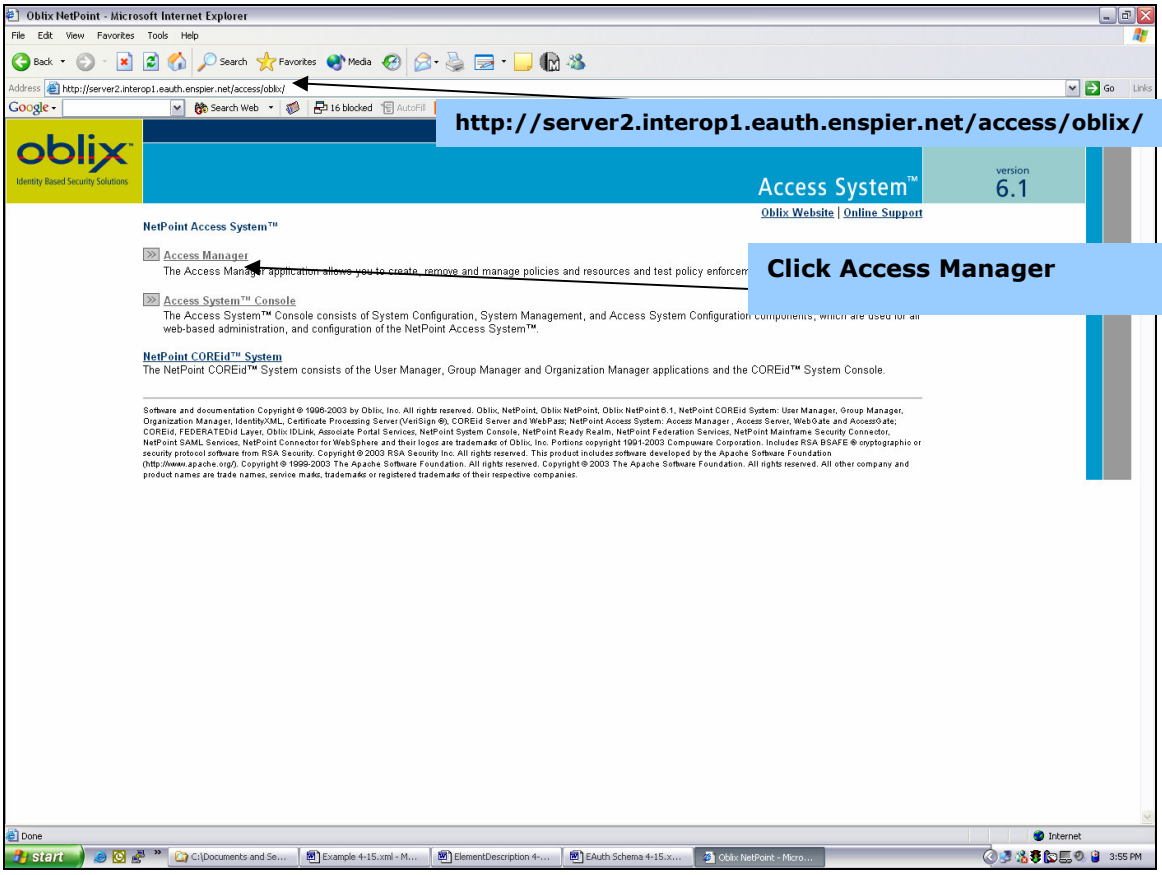


Figure 14-1: Access System

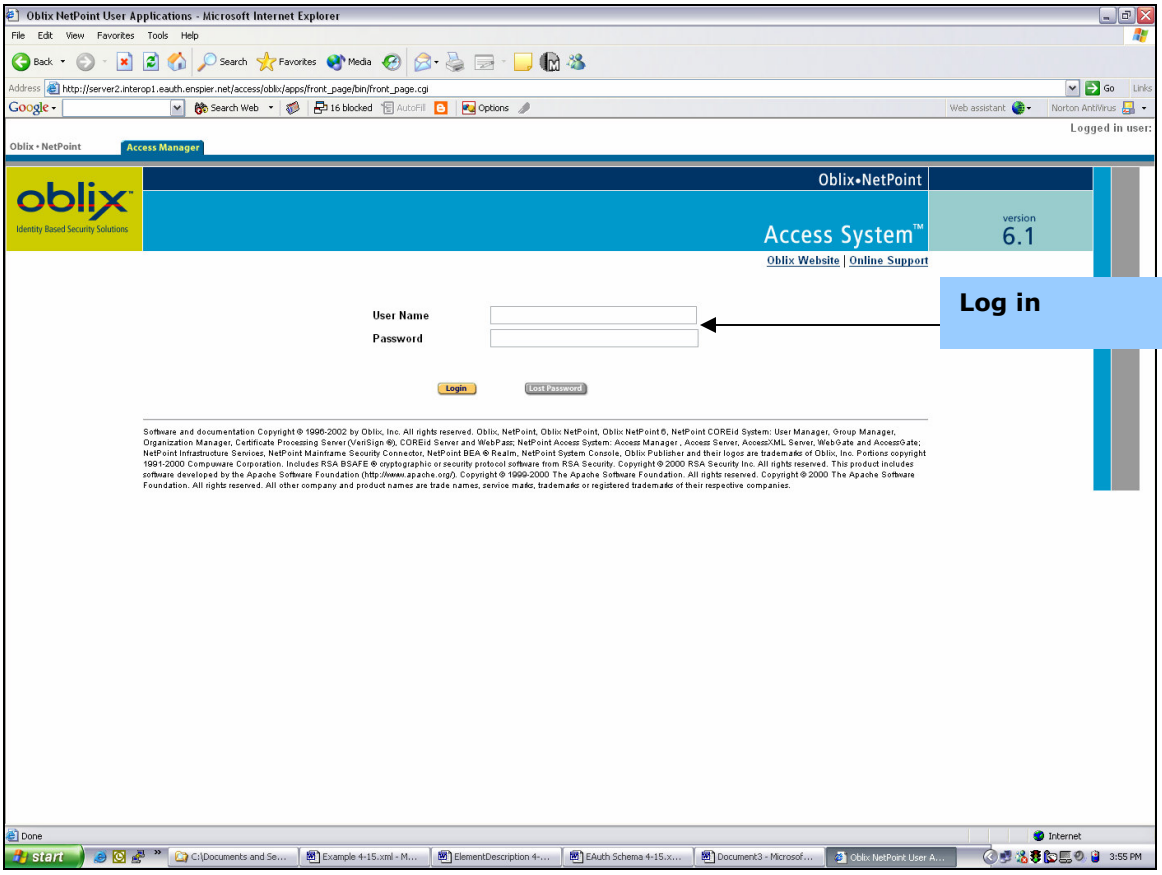


Figure 14-2: Log In

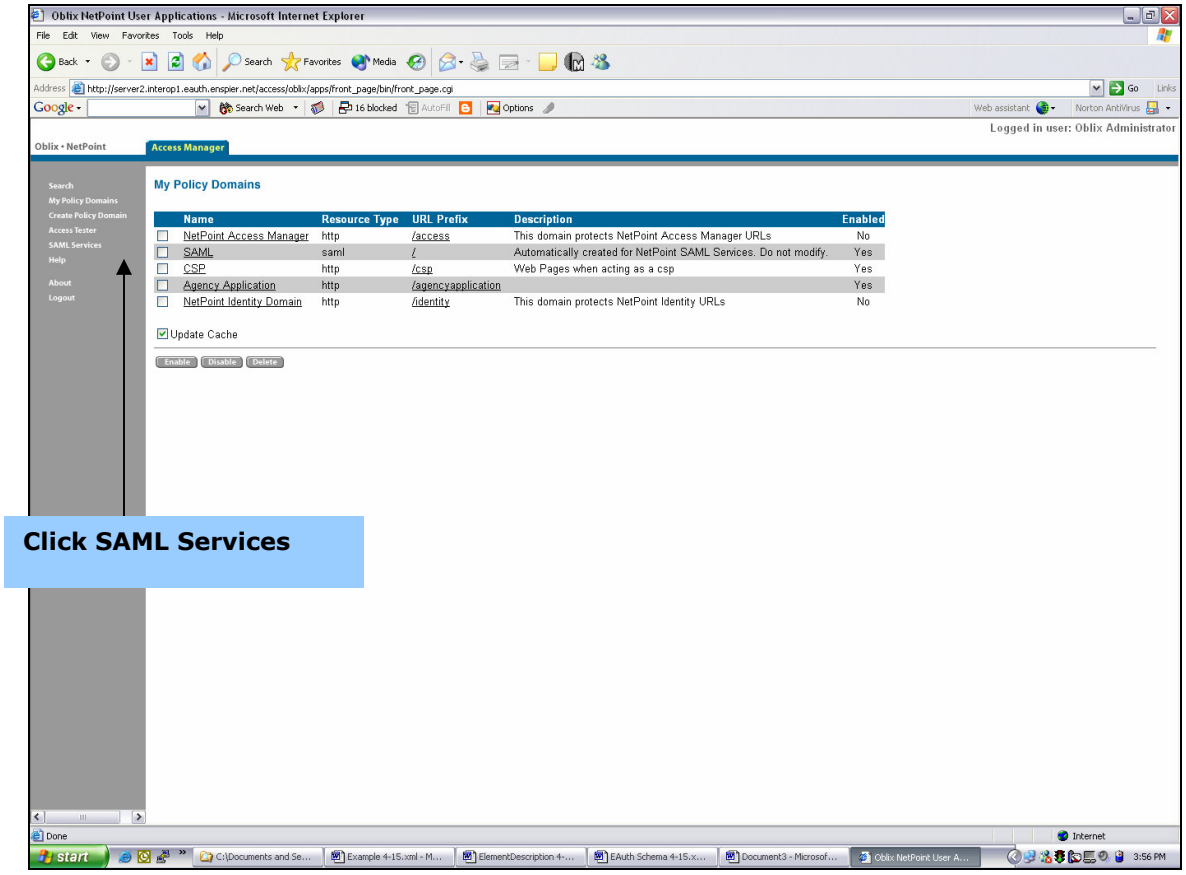


Figure 14-3: My Policy Domains

You are shown the default *My Policy Domains* screen. Click *SAML Services* on the left navigation menu.

1.2 SAML Properties

Modify your assertion properties to match the screen in figures 14-4 and 14-5 below.

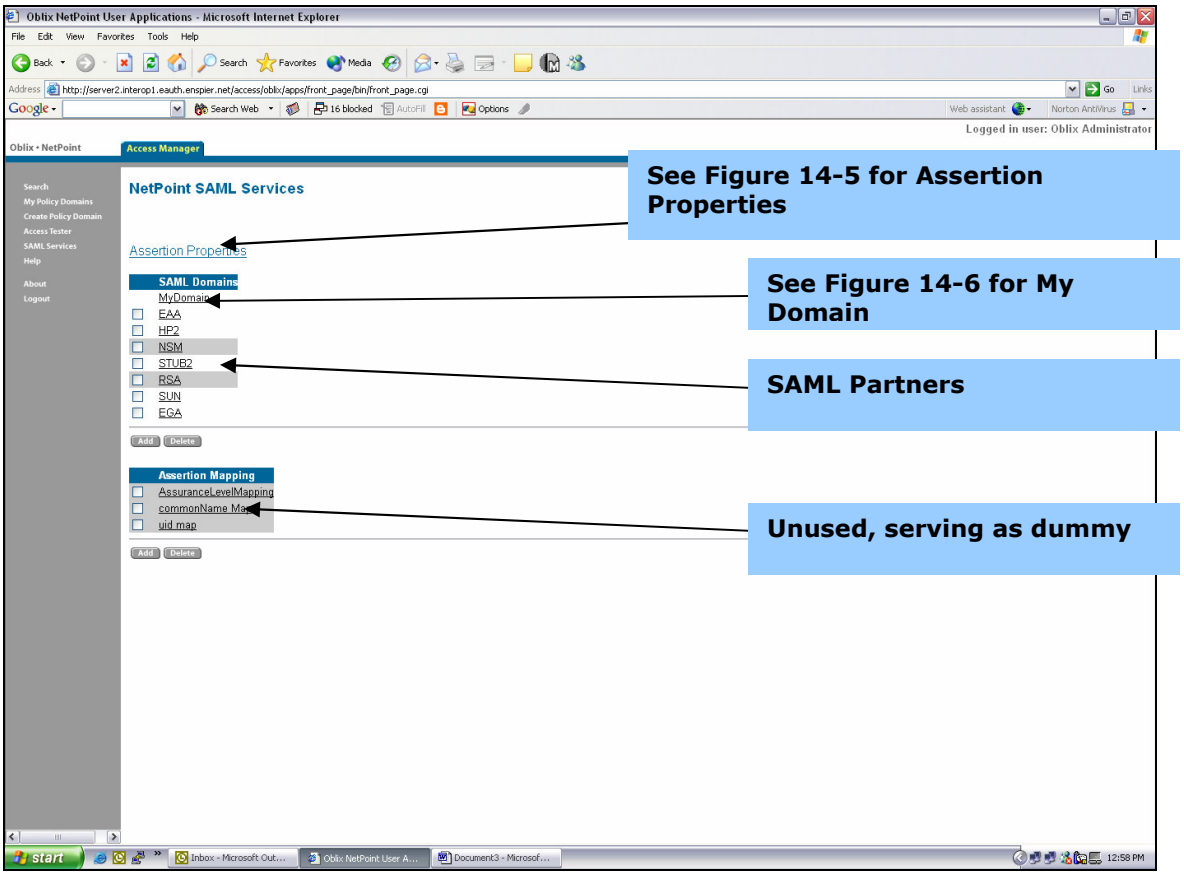


Figure 14-4: SAML Services

To add either an AA or CS click *Add* under SAML Domains. To view assertion properties, click on the Oblix Assertion Properties link and a window shown in figure 4 will display.

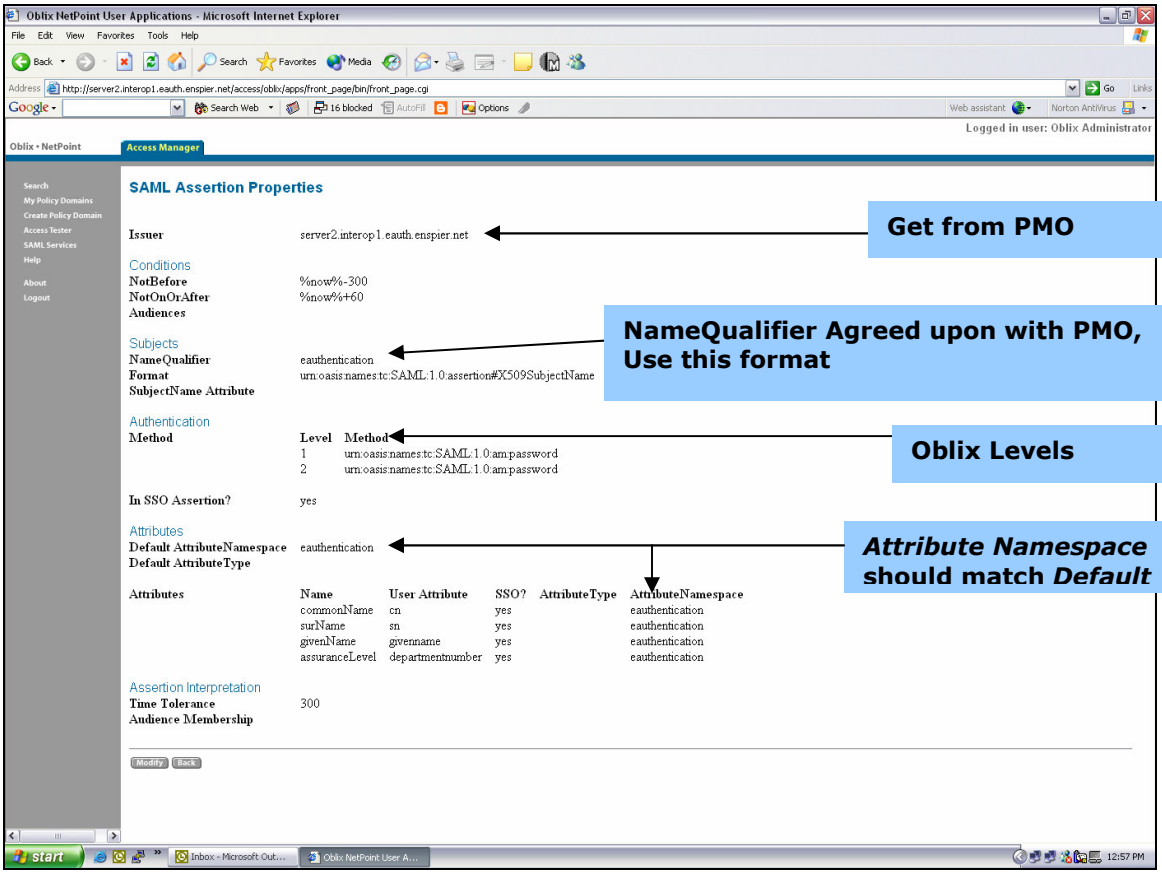


Figure 14-5: SAML Assertion Properties

The *Attributes* portion of the screen above is the attributes in the assertion. Make sure the attributes match the default settings agreed upon with the PMO.

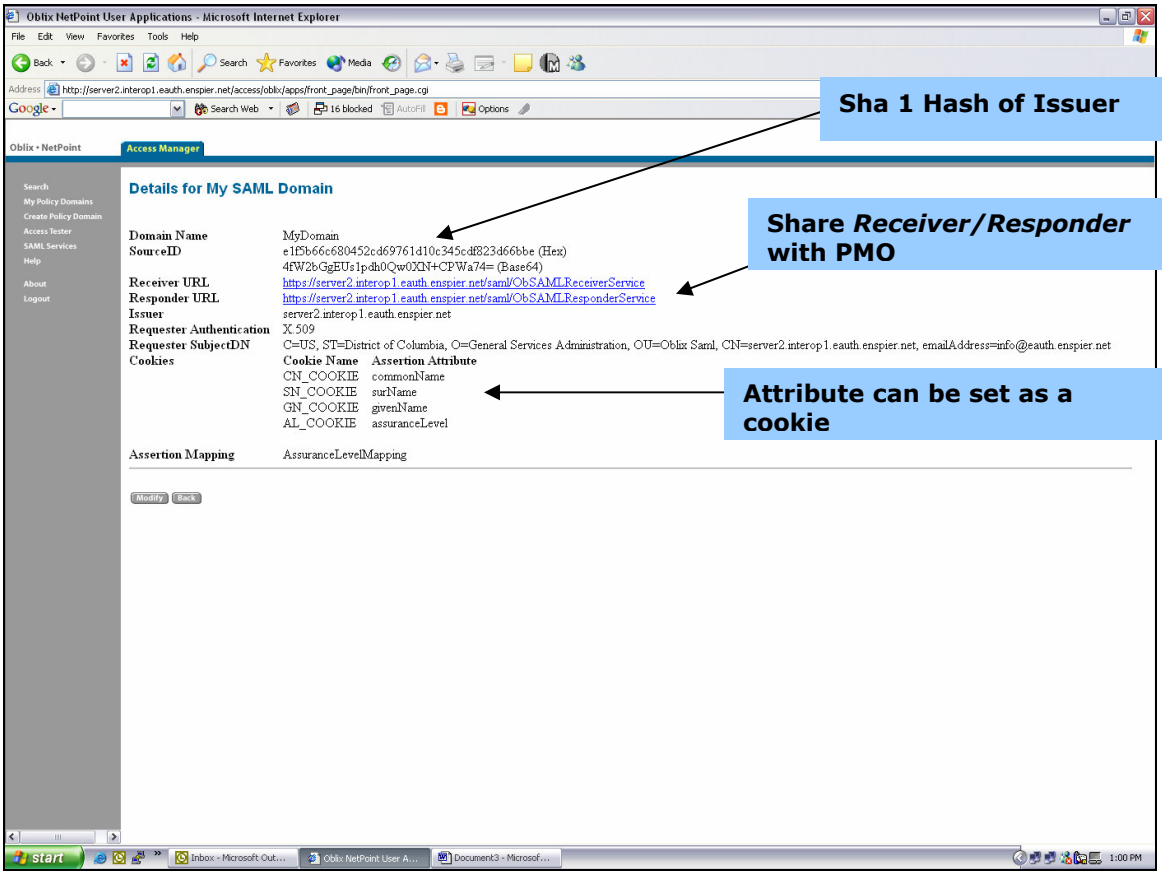


Figure 14-6: Details for My SAML Domain - A

2.0 Partner Configuration

Whether setting up Oblix as a CS or an AA, the same setup screens are used. Placeholders or "dummy" values will be exercised from time to time, depending on the phase and type of setup.

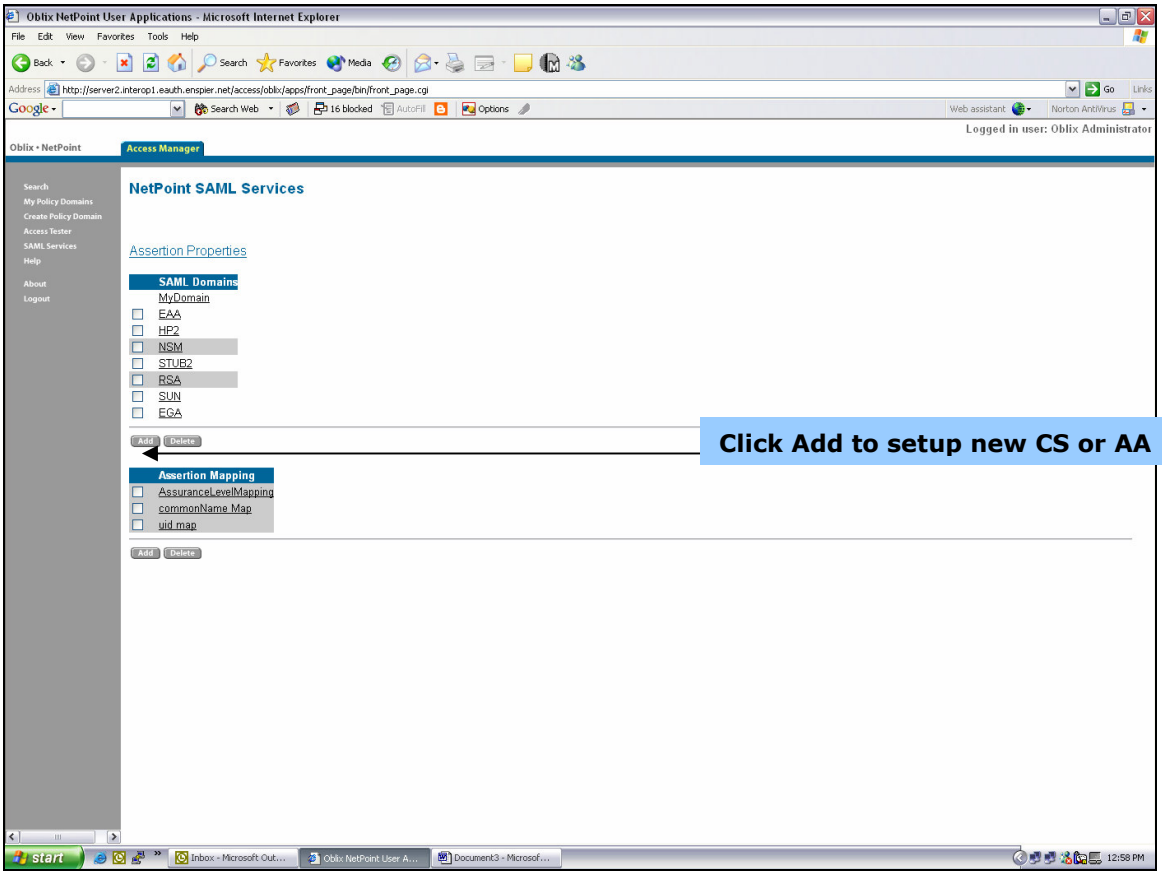


Figure 14-7: Add new CS or AA

After you click *Add,* a screen as shown in figure 14-8 will show up.

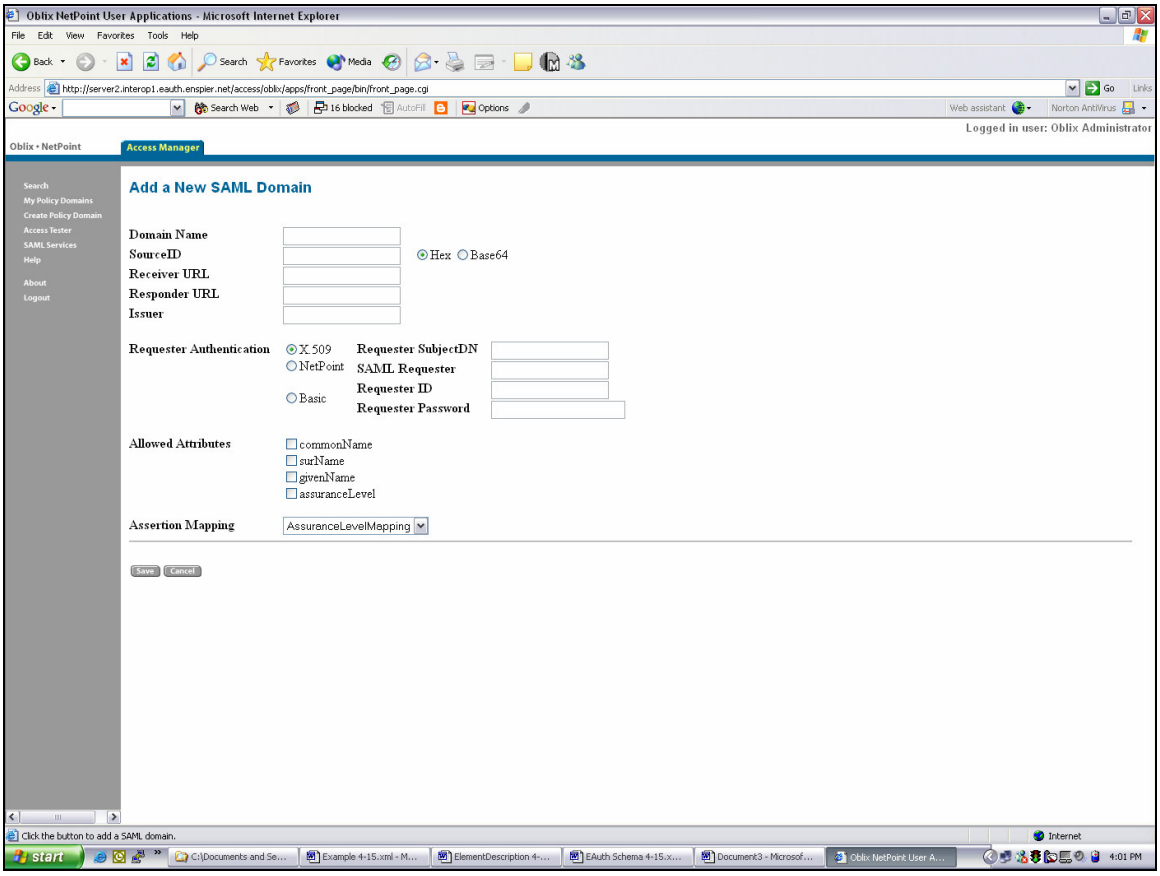


Figure 14-8: New SAML Domain

Add a Domain. This is used by the Inter-site Transfer Service to identity the SAML site the user would like to visit. An example Inter-site Transfer URL for NetPoint looks like:

https://netpoint.fqdn.com/saml/ObSAMLTransferService?DOMAIN=foo&TARGET=http://partner.fqdn.com/resource/to/visit

Please see sections 2.1 and 2.2 to view the settings for setting up a CS versus an AA.

2.1 Adding Agency Applications (AAs)

If you are adding AAs, then you are setup as a CS. Note the details in the following two figures. After clicking on *My Domain* at the top of the screen shown in figure 14-6, the screen below will display.

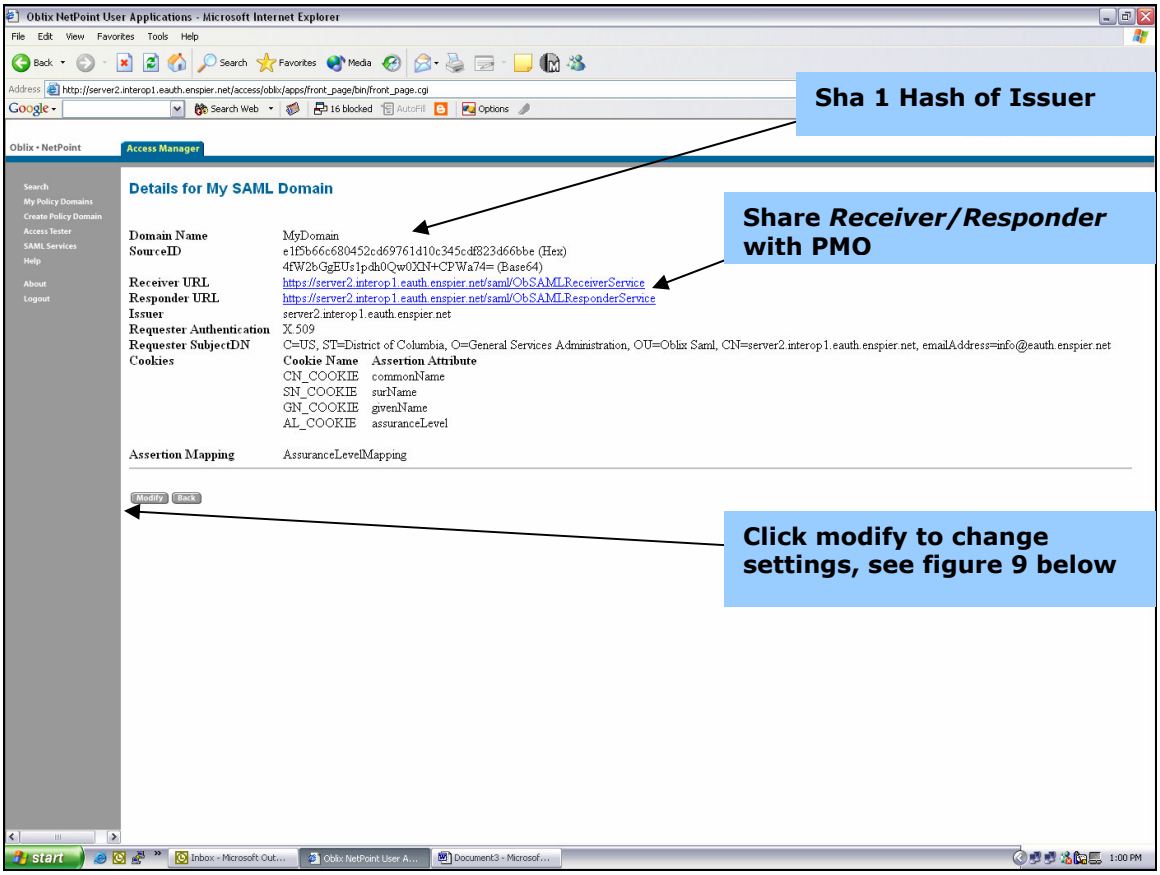


Figure 14-9: Details for My SAML Domain

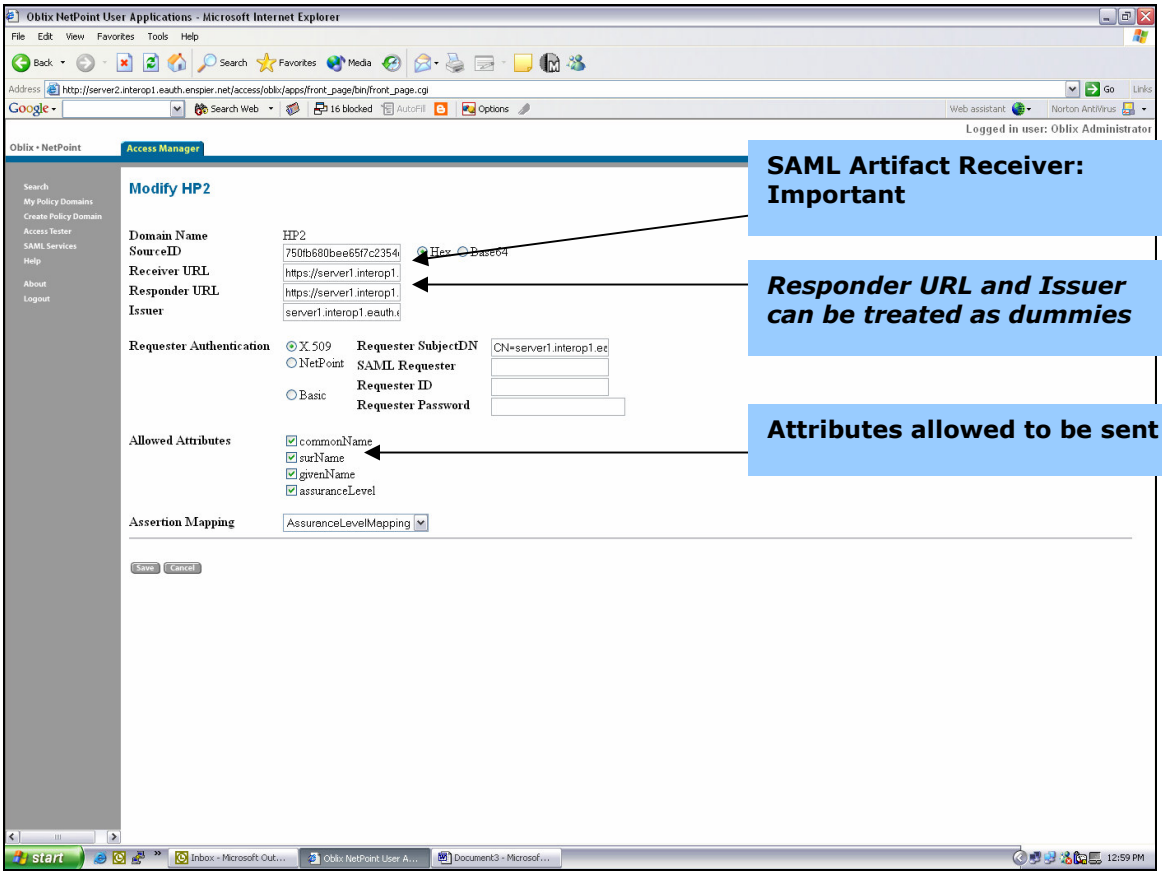


Figure 14-10: Modify HP2

2.2 Adding Credential Services (CS)

If you are adding a CS, then you are setup as an AA. Note the details in the following figures.

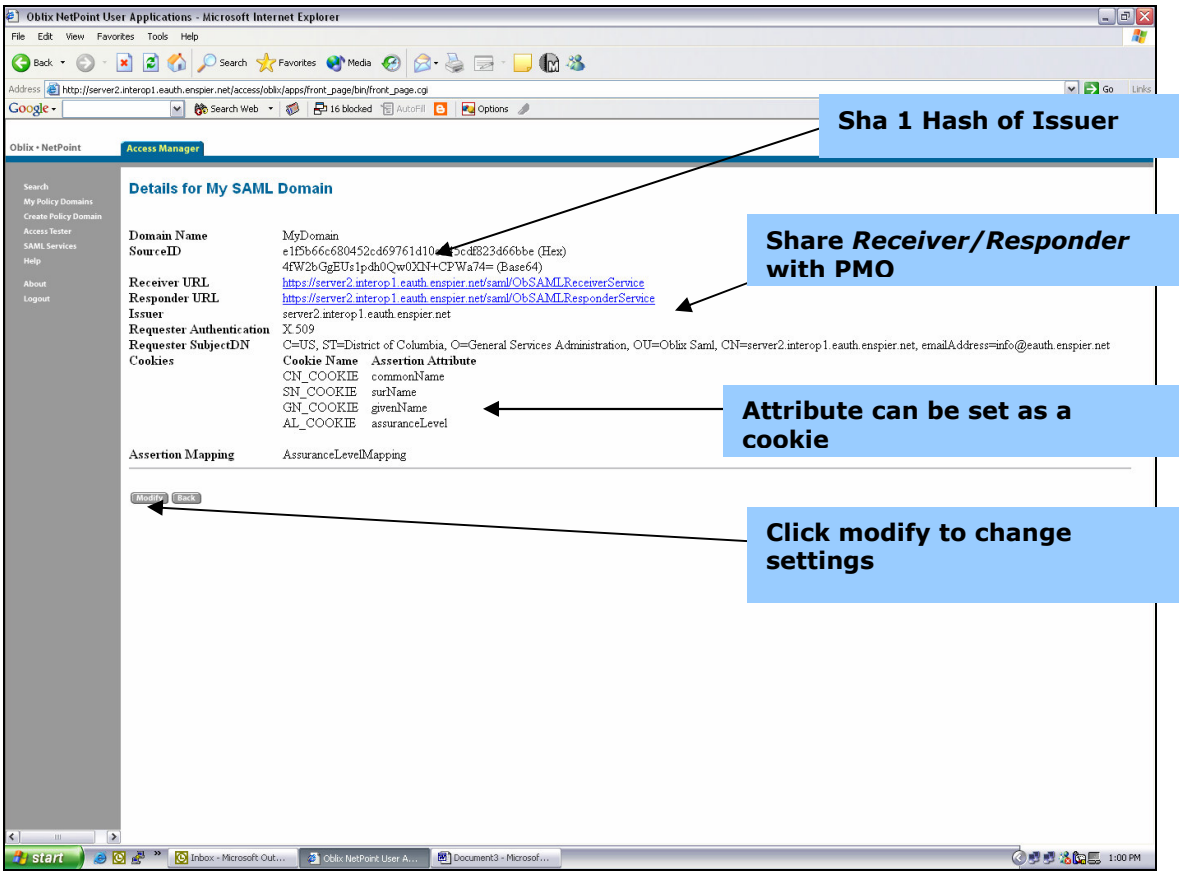


Figure 14-11: Details for My SAML Domain – CS Setup

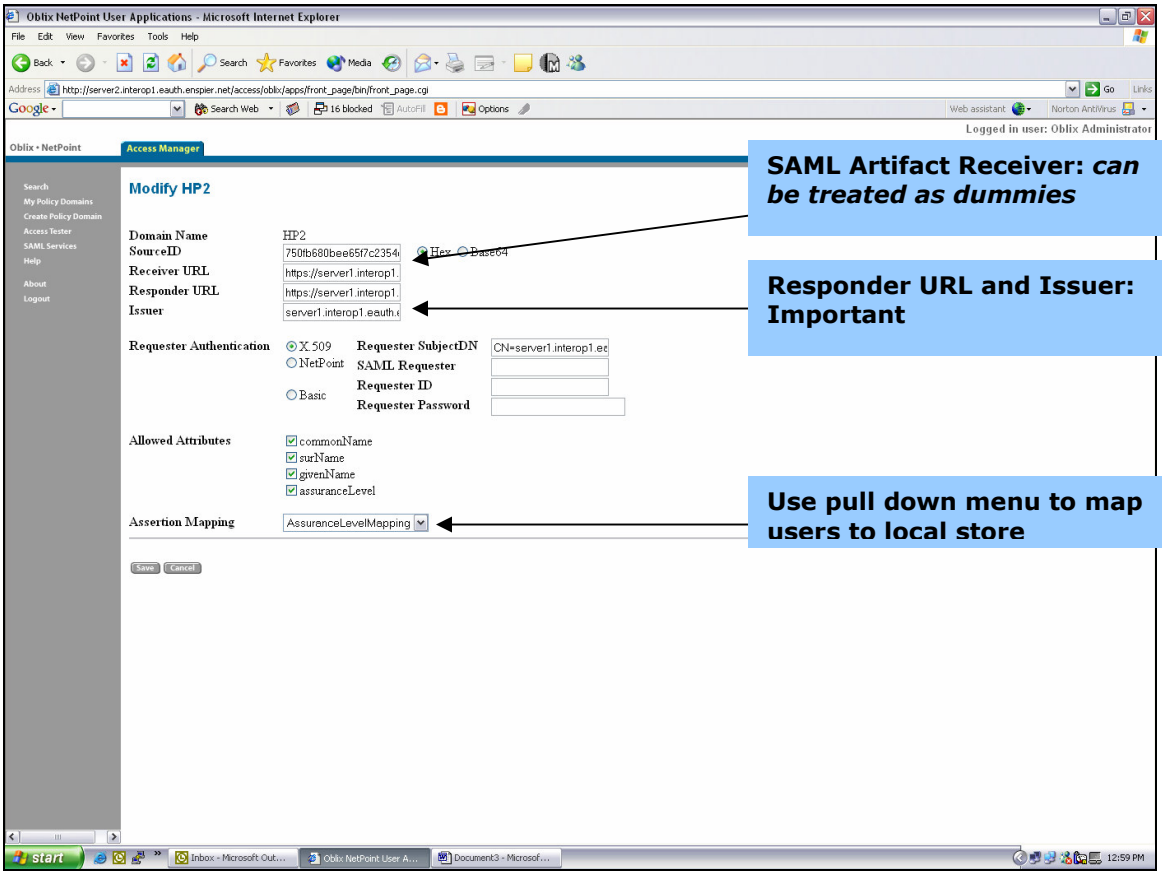


Figure 14-12: Modify HP2 – CS Setup

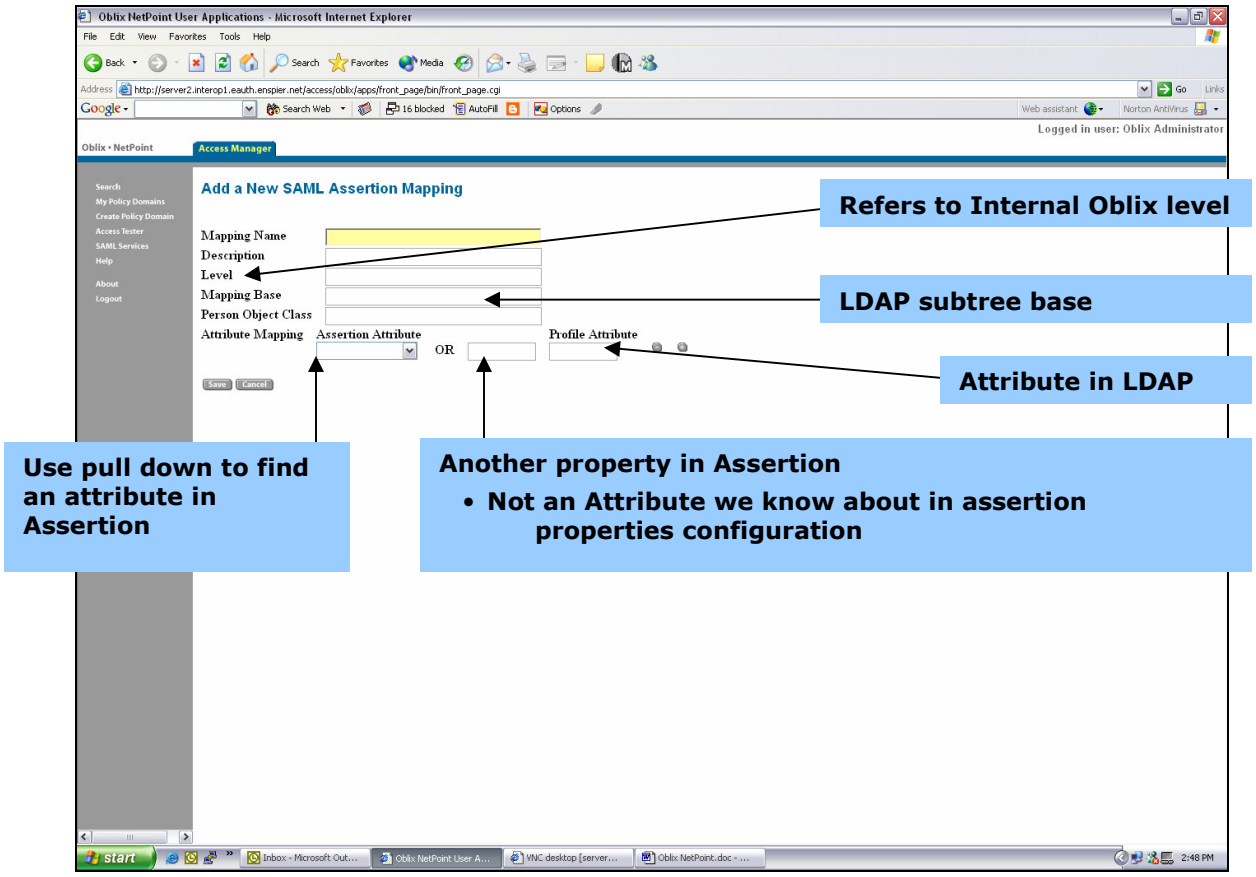


Figure 14-13: SAML Assertion Mapping

2.3 Create a keystore

- **Create** a Java keystore with data from the CA and the command:
  keytool –genkey –keyalg RSA –alias *mykey* –keystore *keystore_filename* –keysize 1024 (enter the same password for the keystore as the private key)

  - Import the certificate of the CA that will issue this CS's certificate with:
  keytool –import –trustcacerts –alias *some_alias* –file *ca_filename* –keystore *keystore_filename*

  - If operating at level 1 import the certificate of the level 1 CA (see above)

  Create a certificate sign request keytool –certreq –alias *mykey* –file *csr_file*

  - Have the CA sign your request and install it with:

  keytool –import –alias *mykey* –file *signed_certificate*

- **Create** C:\NetPoint\NetPointSAML\NetPointSAML.properties *(windows)*
  [optional – recommend for non-production]

  Log=c:/NetPoint/NetPointSAML/oblix/logs/saml.log *(actual log path)*

  LogLevel=High

  Keystore=C:/NetPoint/NetPointSAML/oblix/lib/keystore *(actual path to keystore above)*

  KeystorePassword=*password for keystore AND private key*

APPENDIX A DEFINITIONS

Term	Description
Agency Application (AA)	An online system provided by a government agency that requires a user to be authenticated.
Agency Application Provider	An organization that offers one or more Agency Applications (AAs).
Agency Session	The period of time the AA will trust a user before they are handed off to the CS for re-authentication. AAs do not have access to Authentication Session information; they must maintain their own session with a user and decide how long a user remains authenticated once they have started their transaction.
Application for Assessment	A package submitted by CSPs who wish to make a CS available for use in the Initiative.
Assessment Package	A package submitted by CSPs who have been accepted for assessment. The package contains evidence of compliance with all applicable criteria.
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication.
Authentication Session	The period of time that a user remains trusted after the user authenticates. A CS typically does not require a user to re-authenticate for every page they request; they continue to be trusted for some period of time after each authentication. The allowed period between re-authentication is referred to as the Authentication Session.
Browser Session	The period of time the End Users browser is open. The browser session begins when the user opens their browser and ends when it is closed. All session cookies are terminated when the Browser Session ends.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	Digital documents used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property such as his or her current network address. Note that this guidance distinguishes between credentials, and tokens (see below) while other documents may lump tokens with credentials.

Term	Description
Credential Assessment Profile (CAP)	A list of related criteria used to assess the Assurance Level of a Credential Service. The E-Authentication Initiative has several CAPs.
Credential Service (CS)	A service of a Credential Service Provider (CSP) that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more Credential Services (CSs).
E-Authentication Portal	A website that helps users locate the CSs and AAs they need to complete their transactions. The Portal also maintains information about CSs and AAs referred to as metadata, which includes technical interface data as well as descriptive information.
Electronic Credential Provider (ECP)	An organization that offers one or more Credential Services (CSs). This is also referred to as a CSP.
End Users	Any citizen, government employee, contractor, or business who uses an AA. One of the principle goals of E-Authentication is to make the End User experience as simple as possible by improving the availability and ease of use of credentials.
PKE	Public Key-enabled
PKI	Public Key Infrastructure
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations for the Initiative.
Token	Something that the claimant possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the token includes a userid and password that ensures token uniqueness within a credential domain.
Trust List	The list of authorized CSs and their associated assurance levels.

APPENDIX B ACRONYMS AND ABBREVIATIONS

Acronym	Description
AA	Agency Application
CA	Certification Authority
CAF	Credential Assessment Framework
CAG	Credential Assessment Guidelines
CAP	Credential Assessment Profile
COTS	Commercial off the Shelf
CONOPS	Concept of Operations
CRL	Certificate Revocation List
CS	Credential Service
CSP	Credential Service Provider
DPV	Delegated Path Validation
DSP	Directory System Protocol
E-Auth	E-Authentication
EAP	Electronic Authentication Partnership
E-RA	E-Authentication Risk and Requirements Analysis
GSA	General Services Administration
LDAP	Lightweight Directory Access Protocol
PII	Personally Identifiable Information
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PMO	Program Management Office
PVM	Path Validation Module
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
SSO	Single Sign On
TLS	Transport Layer Security
URI	Uniform Resource Identifier

APPENDIX C REFERENCES

Guidance Document	Description	Web URL
OMB M-04-04: E-Authentication Guidance for Federal Agencies, [GSA03]	Policy guidance that defines four levels of authentication (levels 1 to 4) in terms of the consequences of the false positive authentication, and misuse of credentials.	http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
NIST Special Publication 800-63 DRAFT Recommendation for Electronic Authentication NOVEMBER 2003	Technical guidance to agencies implementing electronic authentication.	http://csrc.nist.gov/publications/drafts/draft-sp800-63.pdf
Technical Approach for the Authentication Service Component	Provides a description of the Authentication Service Component Technical Approach for the E-Authentication Initiative.	http://cio.gov/eauthentication/library.htm
E-Authentication Interim Credential Assessment Framework (CAF)	Describes the interim framework used by the PMO to assess CSPs for use by the E-Authentication service.	http://cio.gov/eauthentication/library.htm
E-Authentication Interim Credential Assessment Guidance (CAG)	Guidance concerning assessments performed under the CAF; assessors will use this document to ensure assessments are performed consistently and adhere to appropriate policies and standards.	http://cio.gov/eauthentication/library.htm

Guidance Document	Description	Web URL
E-Authentication Risk and Requirements Assessment (E-RA)	The E-RA is a risk-based technique to elicit authentication requirements for electronic transactions. Its purpose is to guide users in selecting an appropriate level of authentication to resist threats to their data, users, and organizations that could result from unauthorized use of system transactions.	http://cio.gov/eauthentication/library.htm
E-Authentication Interoperability Testing Procedures for SAML 1.0	Procedures and scenarios for interoperability and conformance testing for the SAML 1.0 artifact.	http://cio.gov/eauthentication/library.htm
SAML Artifact Profile as an Adopted Scheme for E-Authentication	The SAML Artifact Profile is one of the adopted schemes within the E-Authentication architectural framework.	http://cio.gov/eauthentication/library.htm
E-Authentication Interface Specifications for the SAML Artifact Profile	Provides the interface specifications for the SAML Artifact Profile for use with the E-Authentication Initiative.	http://cio.gov/eauthentication/library.htm