The UK
Access
Management
Federation
FOR EDUCATION AND RESEARCH

Sample Security Configuration for a Shibboleth IdP

Author: Joe Boyle

Contributors: Gemma O'Doherty & Ian Burgess

Version 1.0

24th September 2008

Contents

These guides have been prepared by organisations who participated in the JANET Shibboleth on Windows project. These guides are provided for general information purposes and are not intended to be definitive or exhaustive guides to the configuration, installation and implementation of Shibboleth On Windows.

Document Scope

This document is a low-level technical document which describes and discusses a procedure for securing a Shibboleth IdP.

Implementing and Securing the Shibboleth IdP in C2k

C2k is responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. The process by which the Shibboleth IdP server was implemented and secured in C2k can be summarised as follows:

1. *Networking Tasks*
    a. *Create a DMZ (De-Militarised Zone) for the Shibboleth IdP server*
    b. *Configure firewalls*
2. *Shibboleth Server Tasks*
    a. *Install the base operating system*
    b. *Harden the base operating system*
    c. *Network name resolution*
    d. *Install and configure the Shibboleth IdP software*
3. *Digital Certificates Tasks*
    a. *Request, Install and Configure a Digital Certificate on the Shibboleth IdP server*

Each of these tasks will now be discussed in more detail.

Networking Tasks

In the C2k infrastructure, it is the network configuration and network components that are primarily responsible for ensuring the security of the Shibboleth IdP server. A dedicated DMZ was created to host the Shibboleth IdP server and both the internal and external firewalls were configured to allow the necessary network communications to flow.

Create a DMZ for the Shibboleth IdP Server

There are a number of options for the exact placement of a Shibboleth IdP server within an infrastructure. Figure 1 illustrates one of the most common network zone architectures for a Shibboleth IdP.

Figure 1: Typical Network Zone Architecture for a Shibboleth IdP

In this solution the Shibboleth IdP Server resides in a DMZ. The DMZ is usually connected to a dedicated network interface on an external firewall.

With this network configuration no direct access is allowed from the Internet to the Internal Infrastructure. The external and internal firewalls are configured to support the use of proxies and relays that reside in a DMZ. Rules on the external firewall control the communications that are allowed from the Internet to systems in the DMZ and vice versa. Rules on the internal firewall control the communications that are allowed from the DMZ to the Internal Infrastructure and vice versa.

Configure Firewalls

Table 1 records the rules for the external firewall.

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	External DNS Server	53/UDP	Permit	Allows the Shibboleth IdP to resolve names and IP addresses of systems on the Internet
Shibboleth IdP	*	*	80/TCP	Permit	Allows the Shibboleth IdP to initiate HTTP communications with systems on the Internet
Shibboleth IdP	*	*	443/TCP	Permit	Allows the Shibboleth IdP to initiate HTTPS/Secure Sockets Layer (SSL) communications with systems on the Internet
*	*	Shibboleth IdP	8442/TCP	Permit	Allows systems on the Internet to initiate communications with the browser facing ports of the Shibboleth IdP
*	*	Shibboleth IdP	8443/TCP	Permit	Allows systems on the Internet to initiate communications with the Service Provider facing ports of the Shibboleth IdP

Table 1: Firewall Rules for External Firewall

Table 2 records the rules for the Internal Firewall.

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	AD Domain Controller	88/TCP & 88/UDP	Permit	Allows the Shibboleth IdP to initiate Kerberos communications with the AD Domain Controller
Shibboleth IdP	*	AD Domain Controller	389/TCP	Permit	Allows the Shibboleth IdP to conduct LDAP queries against the AD Domain Controller

Table 2: Firewall Rules for Internal Firewall

Shibboleth Server Tasks

The first task to be performed on the Shibboleth IdP server is the installation of the base operating system. This can be performed in a number of ways – manual, scripted, imaged etc. Irrespective of which method is utilised, the Shibboleth server should be installed with a minimum number of components selected.

Shibboleth Server Hardening

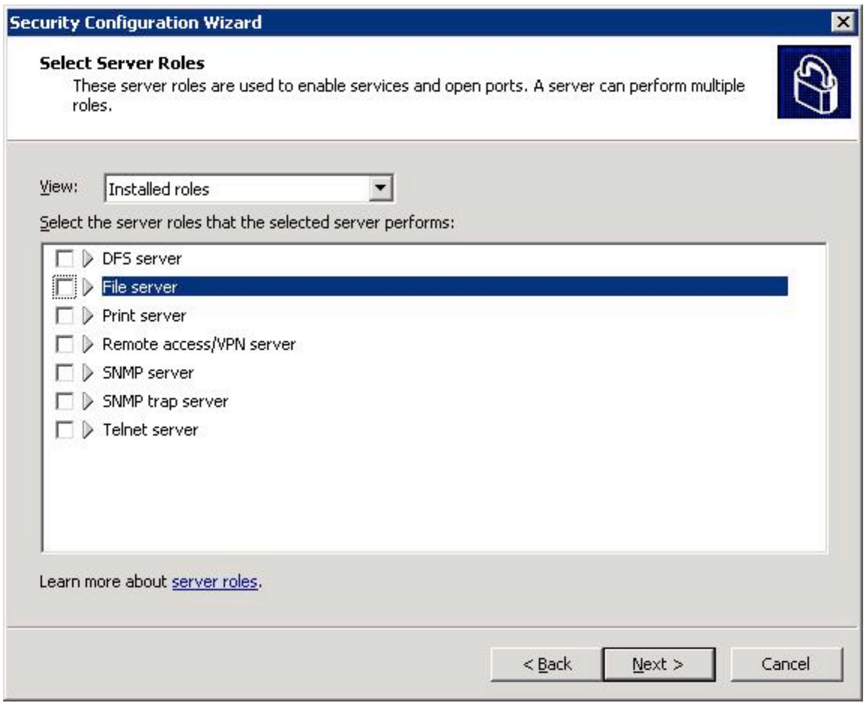
The Shibboleth server is a web facing server and for this reason the security hardening applied to this server is in accordance with Microsoft Best Practice in relation to securing a web server. Although the Shibboleth IdP does not run the Microsoft IIS server, the Windows 2003 Operating System security hardening implementation in the Web Security Guide Best Practices is still the most appropriate baseline security implementation.

In Windows Server 2003 SP1, Microsoft released the Security Configuration Wizard (SCW). The SCW provides a flexible, step-by-step process to reduce the attack surface on servers that run Windows Server 2003 with SP1. It quickly and accurately determines the minimum functionality that is required for the roles that specific servers must fulfil. It can create, test, troubleshoot and deploy security policies that disable all non-essential functionality. Finally it also provides the ability to roll back security policies.

The SCW is used to accomplish the following tasks on the Shibboleth IdP Server:

- *Determine which services must be active, which services need to run when required, and which services can be disabled.*
- *Reduce the protocol exposure to the server message block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Lightweight Directory Access Protocol (LDAP).*
- *Create useful Audit policies that capture the events of interest.*

The Shibboleth IdP server is not performing any of the standard based roles that a Windows server might do. For example, it is not a Domain Controller or a Certificate Server or File & Print Server. For this reason all roles are deselected.



Security Configuration Wizard

Select Server Roles

These server roles are used to enable services and open ports. A server can perform multiple roles.

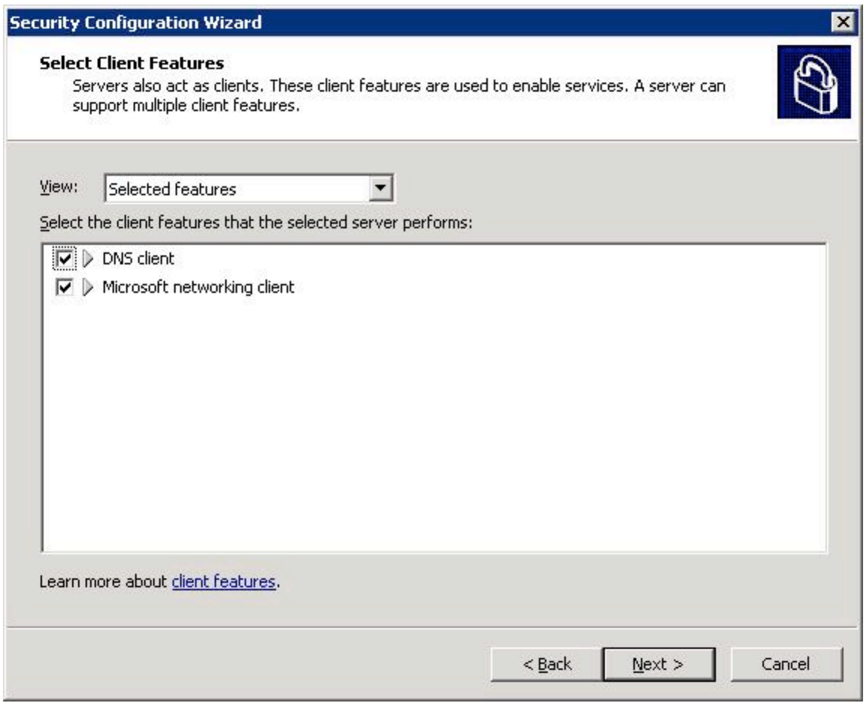
View: Installed roles

Select the server roles that the selected server performs:

- □ DFS server
- □ File server
- □ Print server
- □ Remote access/VPN server
- □ SNMP server
- □ SNMP trap server
- □ Telnet server

Learn more about server roles.

The "DNS Client" & "Microsoft networking client" options are selected.



Security Configuration Wizard

Select Client Features

Servers also act as clients. These client features are used to enable services. A server can support multiple client features.

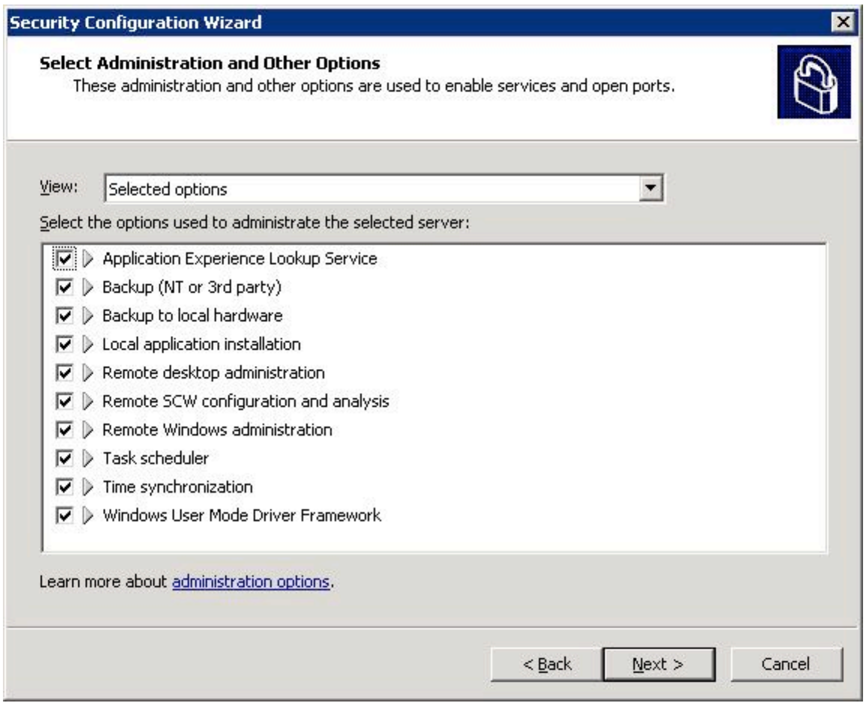
View: Selected features

Select the client features that the selected server performs:

- ☑ DNS client
- ☑ Microsoft networking client

Learn more about client features.

In this example ten features have been selected; however there is scope to dramatically reduce this number depending on decisions yet to be made on managing the Shibboleth IdP server.


Security Configuration Wizard

Select Administration and Other Options

These administration and other options are used to enable services and open ports.

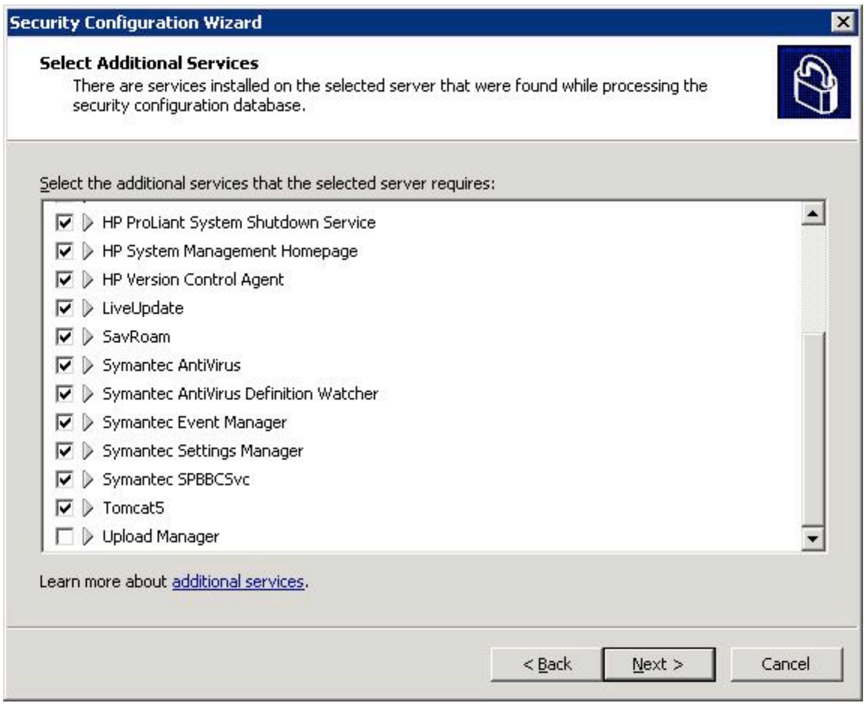
View: Selected options

Select the options used to administrate the selected server:

- ☑ Application Experience Lookup Service
- ☑ Backup (NT or 3rd party)
- ☑ Backup to local hardware
- ☑ Local application installation
- ☑ Remote desktop administration
- ☑ Remote SCW configuration and analysis
- ☑ Remote Windows administration
- ☑ Task scheduler
- ☑ Time synchronization
- ☑ Windows User Mode Driver Framework

Learn more about administration options.

Next, a list of additional services that are required to support the server is presented. This will include hardware-specific services, anti-virus and patch management software etc. The list also includes the Tomcat5 web server which is a core part of the Shibboleth IdP software.


Security Configuration Wizard

Select Additional Services

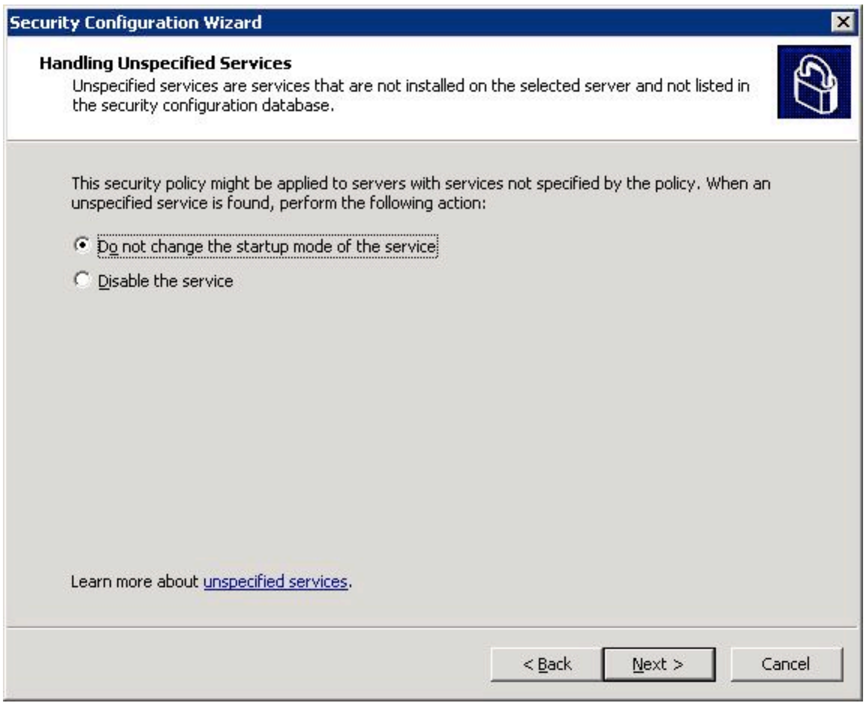
There are services installed on the selected server that were found while processing the security configuration database.

Select the additional services that the selected server requires:

- ☑ HP ProLiant System Shutdown Service
- ☑ HP System Management Homepage
- ☑ HP Version Control Agent
- ☑ LiveUpdate
- ☑ SavRoam
- ☑ Symantec AntiVirus
- ☑ Symantec AntiVirus Definition Watcher
- ☑ Symantec Event Manager
- ☑ Symantec Settings Manager
- ☑ Symantec SPBBCSvc
- ☑ Tomcat5
- ☐ Upload Manager

Learn more about additional services.

Next, a decision must be made on how to handle Unspecified Services. In this example, the wizard is set to "Do not change the start-up mode of the unspecified service".



Security Configuration Wizard

Handling Unspecified Services

Unspecified services are services that are not installed on the selected server and not listed in the security configuration database.

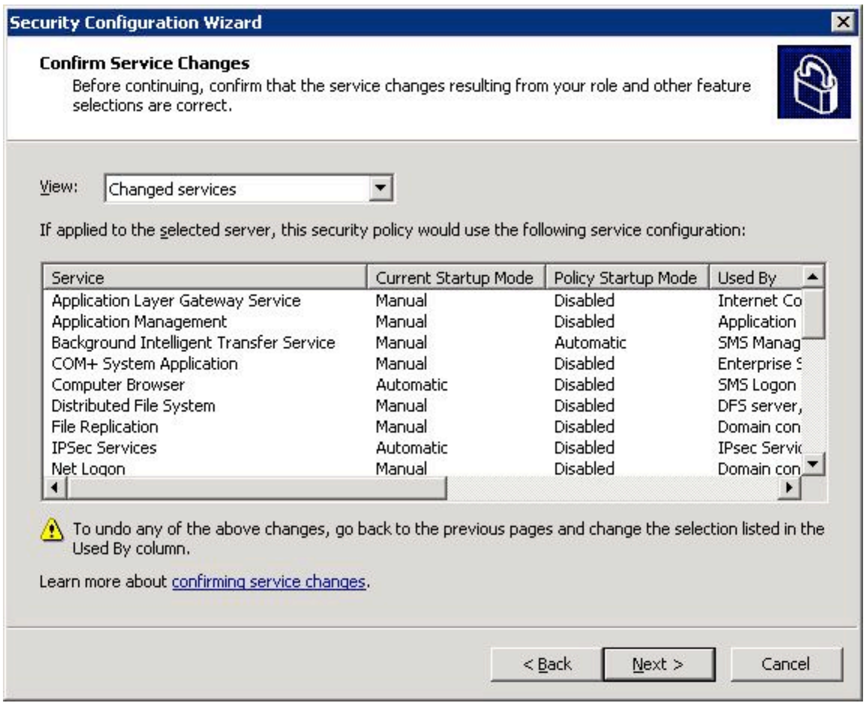
This security policy might be applied to servers with services not specified by the policy. When an unspecified service is found, perform the following action:

● Do not change the startup mode of the service

○ Disable the service

Learn more about unspecified services.

The wizard then provides the option to review the resulting security policy of the settings which have been chosen. This illustrates how the SCW will disable services and re-define the startup mode of services.



Security Configuration Wizard

Confirm Service Changes

Before continuing, confirm that the service changes resulting from your role and other feature selections are correct.

View: Changed services

If applied to the selected server, this security policy would use the following service configuration:

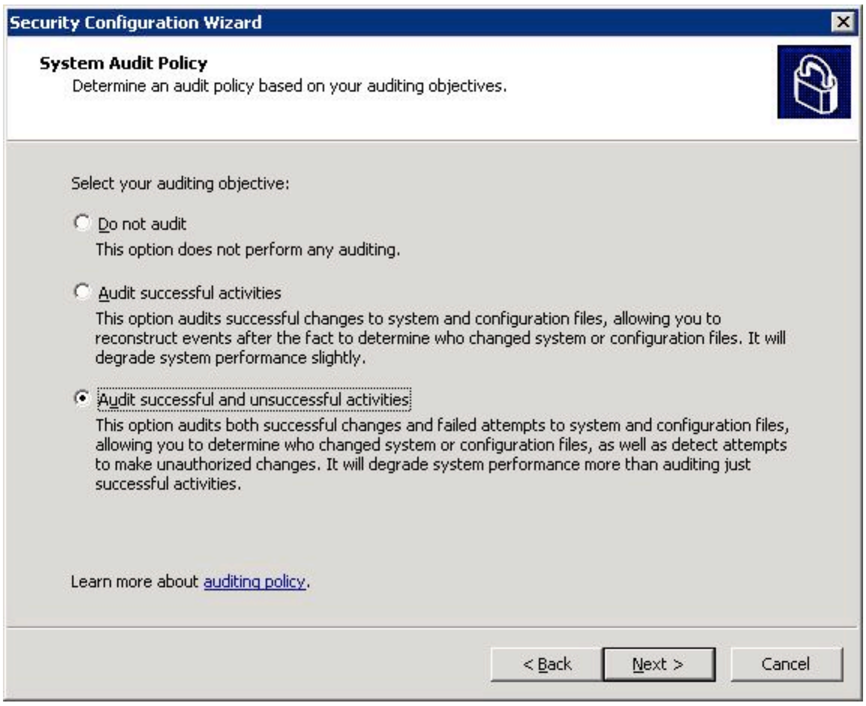
Service	Current Startup Mode	Policy Startup Mode	Used By
Application Layer Gateway Service	Manual	Disabled	Internet Co
Application Management	Manual	Disabled	Application
Background Intelligent Transfer Service	Manual	Automatic	SMS Manag
COM+ System Application	Manual	Disabled	Enterprise S
Computer Browser	Automatic	Disabled	SMS Logon
Distributed File System	Manual	Disabled	DFS server,
File Replication	Manual	Disabled	Domain con
IPSec Services	Automatic	Disabled	IPsec Servic
Net Logon	Manual	Disabled	Domain con

To undo any of the above changes, go back to the previous pages and change the selection listed in the Used By column.

Learn more about confirming service changes.

Defining the Audit Policy

When defining the audit policy the "Audit Successful and Unsuccessful activities" option is selected.



Security Configuration Wizard

System Audit Policy

Determine an audit policy based on your auditing objectives.

Select your auditing objective:

○ Do not audit

This option does not perform any auditing.

○ Audit successful activities

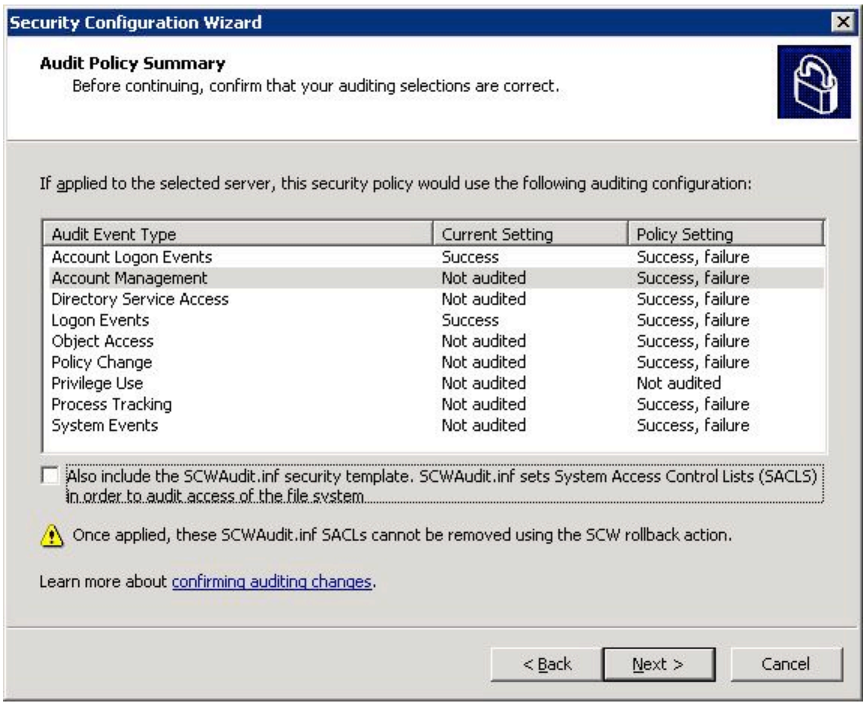
This option audits successful changes to system and configuration files, allowing you to reconstruct events after the fact to determine who changed system or configuration files. It will degrade system performance slightly.

● Audit successful and unsuccessful activities

This option audits both successful changes and failed attempts to system and configuration files, allowing you to determine who changed system or configuration files, as well as detect attempts to make unauthorized changes. It will degrade system performance more than auditing just successful activities.

Learn more about auditing policy.

An Audit Policy Summary is presented, prior to confirmation that the selections are correct.



Security Configuration Wizard

Audit Policy Summary

Before continuing, confirm that your auditing selections are correct.

If applied to the selected server, this security policy would use the following auditing configuration:

Audit Event Type	Current Setting	Policy Setting
Account Logon Events	Success	Success, failure
Account Management	Not audited	Success, failure
Directory Service Access	Not audited	Success, failure
Logon Events	Success	Success, failure
Object Access	Not audited	Success, failure
Policy Change	Not audited	Success, failure
Privilege Use	Not audited	Not audited
Process Tracking	Not audited	Success, failure
System Events	Not audited	Success, failure

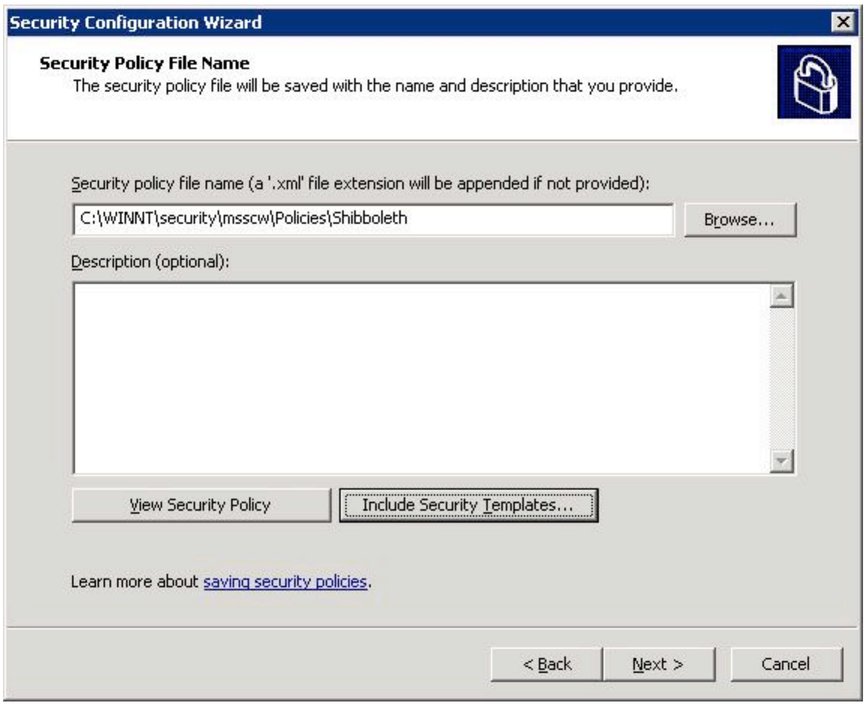
□ Also include the SCWAudit.inf security template. SCWAudit.inf sets System Access Control Lists (SACLS) in order to audit access of the file system.

⚠ Once applied, these SCWAudit.inf SACLs cannot be removed using the SCW rollback action.

Learn more about confirming auditing changes.

The Security Policy is saved to a file and stored under the following directory path:

```
C:\Winnt\Security\msscw\policies\shibboleth.xml
```



Security Configuration Wizard
Security Policy File Name
The security policy file will be saved with the name and description that you provide.
Browse...
View Security Policy
Include Security Templates...
< Back
Next >
Cancel

Security policy file name (a '.xml' file extension will be appended if not provided):
C:\WINNT\security\msscw\Policies\Shibboleth

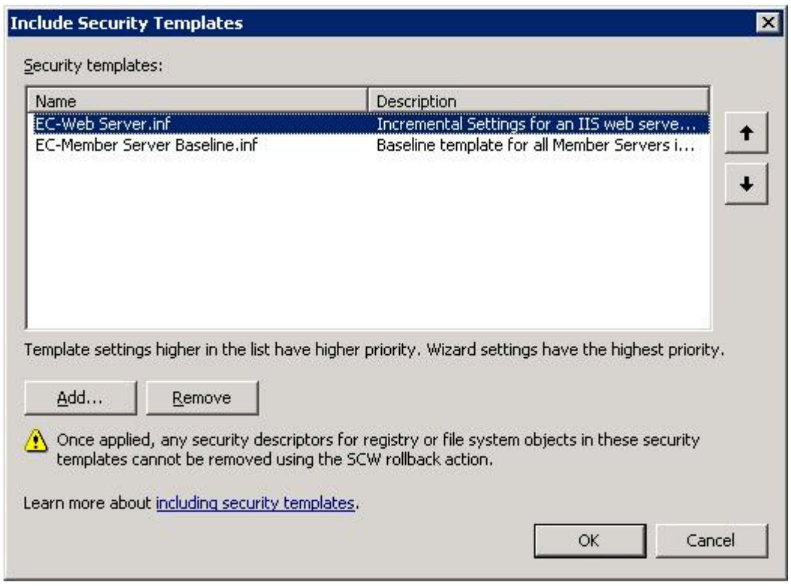
Description (optional):

Learn more about saving security policies.

Security Templates

The Security Configuration Wizard can also integrate Microsoft template security files that are designed for servers that perform specific roles.

A web server template "EC-Web Server.inf" is associated with the Shibboleth IdP Server. Additionally, a member server template file "EC-Member Server Baseline.inf" is included to tie down more general operating system issues.



Security templates:

Name	Description
EC-Web Server.inf	Incremental Settings for an IIS web serve...
EC-Member Server Baseline.inf	Baseline template for all Member Servers i...

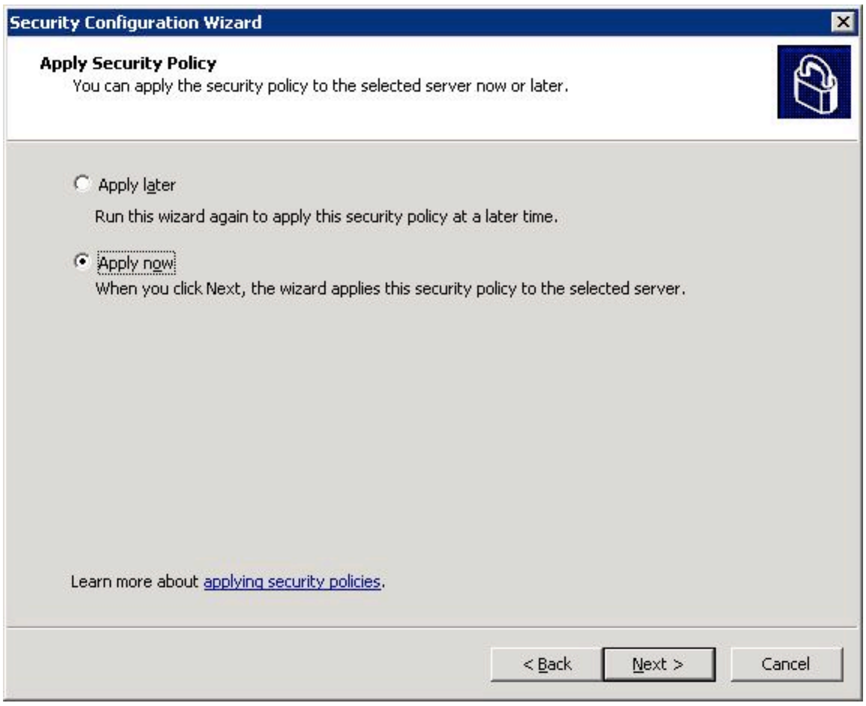
Template settings higher in the list have higher priority. Wizard settings have the highest priority.

⚠ Once applied, any security descriptors for registry or file system objects in these security templates cannot be removed using the SCW rollback action.

Learn more about including security templates.

The template files are stored in C:\Winnt\Security.

Finally you have the option to apply the security policy now or wait until later.



Security Configuration Wizard

Apply Security Policy

You can apply the security policy to the selected server now or later.

○ Apply later

Run this wizard again to apply this security policy at a later time.

● Apply now

When you click Next, the wizard applies this security policy to the selected server.

Learn more about applying security policies.

The advantage of using the SCW is that it allows you to roll back the policy changes from a single point of reference. It also allows you to generate an xml report that specifies in detail what security features are configured. To illustrate how extensive this is the reports runs to 30 pages for the Shibboleth server configuration.

Security Patch Management & Anti-Virus Protection

The Shibboleth IdP Server should also be configured with a patch management client to ensure that the latest Microsoft Security patches are always installing and running on the Server. The server should also use anti-virus software to protect against viruses and other security risks.

Network Name Resolution

Network name resolution must now be configured so that the Shibboleth IdP Server can identify and locate systems on the Internet and the Internal Infrastructure.

DNS is configured so that the Shibboleth IdP Server resolves names from an external DNS server. The external DNS server could be one operated by an ISP, or alternatively it could be a dedicated external DNS server owned and operated by an internal IT group.

In the case of C2k an added complexity is the use of the same DNS namespace (i.e. “c2ktest.net”) on both the Internal Infrastructure and the Internet. This configuration is often referred to as “split-brain DNS”. Figure 2 illustrates where the different zones in a split-brain DNS configuration would be hosted.

Figure 2: The Scope of DNS zones in a split-brain configuration

Also, the DNS records stored in the internal and external zones will differ greatly:

- *Internal DNZ zones contain entries for all internal systems e.g. file servers, workstations etc.*
- *External DNZ zones contain entries for all external systems e.g. web servers, Shibboleth servers etc.*

This setup presents a problem for the Shibboleth IdP Server because it needs to resolve names of systems on the Internet and resolve the name of a Domain Controller on the Internal Infrastructure. The Shibboleth IdP Server is setup to query an external DNS server which will know nothing about a Domain Controller in the Internal Infrastructure. A simple solution is to modify the "%windir%\System32\drivers\etc\hosts" file and add an entry for the Domain Controller which we want to locate e.g.

```
10.10.5.5   DC01.ACME.COM
```

Install and Configure the Shibboleth IdP Software

For detailed information on how to install and configure the Shibboleth IdP software please refer to the following document: "Integrating a Shibboleth IdP with Microsoft Active Directory".

Digital Certificate Tasks

An X.509 digital certificate is required to secure the network communications that take place between your Shibboleth IdP and other systems in the UK Federation. The digital certificate must be one of the X.509 digital certificate products recognised by the federation. As of September 2008, these are:

- GlobalSign OrganizationSSL certificates
- JANET Server Certificate Service (JANET SCS) certificates
- TERENA Server Certificate Service (TERENA SCS) certificates
- Thawte SSL web server certificates
- UK e-Science CA host certificates
- VeriSign Secure Site certificates

More information on the process of getting a certificate can found at: http://www.ukfederation.org.uk/content/Documents/GetCertificate

In the C2k environment, the digital certificate for Shibboleth was purchased from VeriSign. The remainder of this section discusses the process which C2k used to complete the installation.

Pre-Requisites

A Shibboleth IdP is a system which must be locatable on the Internet. It therefore requires a fully-qualified name e.g. shibboleth.acme.com.

In the C2k environment there are a number of separate infrastructures e.g.:

- Production
- Pre-Production
- Development & Test

Within this section we discuss the process of linking the "Development & Test" infrastructure into the UK Federation. The Pre-Production and Production environments will be brought into the UK Federation in later stages of the Shibboleth project.

For the C2k Development and Test infrastructure it was decided that the Shibboleth IdP server would be known on the Internet as "shibboleth.c2ktest.net".

The domain name "c2ktest.net" was registered by C2k.

An externally contactable IP Address (85.31.137.110) was then bound to the newly registered "c2ktest.net" domain and an alias record created for "**shibboleth.c2ktest.net**". VeriSign requires this information to be publicly available via a DNS registration host before it can verify the requesting party.

Shibboleth Server Certificate Setup

The C2k environment uses a Java based certificate, generated by the keytool utility. The certificate is then signed by VeriSign, which provides the follow security features:

- *Encryption of sensitive information during online transactions*
- *Authenticated information about the certificate owner*
- *Verifies the identity of the certificate owner when it is issued*

A Java keystore is created using the keytool utility and is stored in a secure directory on the Shibboleth server:

```
C:\Program Files\Internet2\Idp\Etc
```

Certificate Request

A Certificate Signing Request (CSR) is then generated against the Java keystore and is submitted to VeriSign via their web site. The information provided in the CSR must meet a specific format and must be verifiable by VeriSign before it will sign the CSR submitted. Once verification has been completed VeriSign emails the signed certificate to a registered contact. The returned signed Certificate is chained with the VeriSign Intermediate Certificate.

```
C:\Program Files\Internet2\CaptiveJava\bin\keytool -certreq -keyalg RSA -
alias Shibboleth -file "c:\Program Files\Internet2\Idp\Etc\certreqc2k.csr"
-keystore "c:\Program Files\Internet2\Idp\Etc\C2k.jks
```

Importing the VeriSign Intermediate Certificate

The VeriSign Intermediate CA certificate is imported into the Java keystore with the Keytool utility:

```
C:\Program Files\Internet2\CaptiveJava\bin>keytool -import -alias
intermediateCA -keystore "c:\Program Files\Internet2\Idp\Etc\C2k.jks" -
trustcacerts -file "c:\Program Files\Internet2\Idp\Etc\VeriSignInterCA.crt"

Enter keystore password: *************

Certificate was added to keystore
```

Note*: there is no requirement to import the VeriSign Root certificate because this is already present on all browsers.*

Importing the Shibboleth Certificate

The signed Shibboleth certificate is imported into the Java keystore with the Keytool utility:

```
C:\Program Files\Internet2\CaptiveJava\bin>keytool -import -alias
Shibboleth -keystore "c:\Program Files\Internet2\Idp\Etc\C2k.jks" -
trustcacerts -file "c:\Program Files\Internet2\Idp\Etc\c2kcert.cer"

Enter keystore password: *************

Certificate reply was installed in keystore
```

Configure Shibboleth to use the new Certificate

Shibboleth must now be configured to use the new certificate. The resultant configuration secures communication traffic between users' Internet browsers and the Shibboleth server.

The server.xml file is modified in order to facilitate this:

```
C:\Program Files\Internet2\CaptiveTomcat5.5\conf\server.xml
```

Two lines are added to the file:

```
keystoreFile="C:\Program Files\Internet2\\Idp\etc\c2k.jks"

keystorePass="password"
```

The keystoreFile parameter provides the path to the keystore where the signed certificate can be located. The keystorePass parameter provides the keystore password.

These modifications bind the Shibboleth certificate to port 8442. This is the port that the Shibboleth IdP uses to respond to IdP traffic via a web browser. Any communication taking place between a browser and the Shibboleth server will do so via secure SSL encryption with a certificate that VeriSign has verified issued to C2k.

Disclaimer

This guide is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.