Web Interface with Active Directory Federation Services
Support Administrator’s Guide

Web Interface with Active Directory Federation Services (ADFS) Support
Citrix Presentation Server™ 4.0 for Windows®
Overview

Web Interface with Active Directory Federation Services (ADFS) Support enables the resource partner of an ADFS deployment to use Presentation Server. Administrators can create ADFS sites to provide users with access to published applications on the resource partner.

Important  ADFS requires secure communications between client, Web server, and federation servers. Web Interface users must use HTTPS/SSL to access the site.

What is Active Directory Federation Services?

Active Directory Federation Services (ADFS) is a feature of Microsoft Windows Server 2003 R2 Enterprise Edition. ADFS provides single-sign on technology to authenticate a user into multiple Web applications in a single session.

ADFS extends the existing Active Directory infrastructures to provide access to resources offered by trusted partners across the Internet. These trusted partners can include external third parties or other departments in your organization.

For two organizations to establish ADFS trust relationships, ADFS must be deployed in both organizations. ADFS trust relationships are explicit, one-way, and nontransitive. In a trust relationship, the party hosting the user accounts is the account partner and the party hosting the applications accessed by users is the resource partner.

Using ADFS requires a federation server on each partner. For additional security, you can locate these federation servers inside the trusted network of each organization and deploy federation server proxies. A federation server proxy relays federation requests from outside the organization to your federation server.
This diagram shows a Web Interface deployment using federation server proxies and a Web Interface server in demilitarized zones (DMZ).

Active Directory Federation Services Terminology

The following table contains basic terms used when describing ADFS.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>account partner</td>
<td>Client organization that wants to use the Web applications from the resource partner. The account partner provides the identities (user accounts).</td>
</tr>
<tr>
<td>federation server</td>
<td>Federation servers host the Federation Service component of ADFS, which controls access to your systems based on identification, authentication, and authorization through the federation trust. Federation servers authenticate requests from trusted partners based on the credentials of the partners. Representations of the credentials are exchanged in the form of security tokens.</td>
</tr>
<tr>
<td>federation server proxy</td>
<td>Federation server proxies host the Federation Service proxy component of ADFS. You can deploy federation server proxies in the demilitarized zone (DMZ) to forward requests to federation servers that are not accessible from the Internet.</td>
</tr>
<tr>
<td>Federation Service</td>
<td>A Windows Server 2003 R2 service that provides security tokens in response to requests.</td>
</tr>
</tbody>
</table>
For more information about ADFS for Windows 2003 R2 and setting up an ADFS environment, see the following documents at www.microsoft.com.

- Overview of Active Directory Federation Services (ADFS) in Windows Server 2003 R2
- Active Directory Federation Services Design Guide
- ADFS Step-by-Step Guide
- Step-by-Step Guide to the Microsoft Management Console

**Citrix Web Interface with Active Directory Federation Services Support Deployment**

The following steps occur when a user on an account partner accesses a published Web application on a resource partner.

- A user opening the Web Interface home page on the resource partner is redirected to the account partner’s authentication page.
- The account partner authenticates the user and sends a security token back to the resource partner.
- ADFS on the resource partner validates the security token, transforms it to a Windows identity (representing a shadow account), and redirects the user to the Web Interface logon page.
- Web Interface displays the application list page for the user.
This diagram shows the steps that occur when a user tries to access an application list.

- The user launches an application by clicking a hyperlink on the page. Web Interface contacts the Citrix XML service to request a launch.

**Note** For applications to be accessible by ADFS users, you must publish the applications on the resource partner’s server for one or more of the shadow accounts.

- The Citrix XML service generates Security Support Provider Interface data and sends it to computers running Presentation Server.
- The server uses the Security Support Provider Interface data to authenticate the user and stores a logon token in Presentation Server for future authentication.
- The server generates a launch ticket to uniquely represent the stored logon token and returns this ticket to the Citrix XML service.
- The Citrix XML service returns the launch ticket to Web Interface.
- Web Interface creates an ICA file containing the launch ticket and sends it to the user’s browser.
- The client on the user’s computer opens the ICA file and attempts an ICA connection to Presentation Server.
- The client sends the launch ticket to computers running Presentation Server.
- The server receives the launch ticket, matches it to the logon token that was generated previously, and uses this logon token to log the user on to the
ICAO session on the server. The ICA session runs under the identity of the shadow account.

This diagram shows the steps that occur when the user clicks a link on the application list.

**Note** When the user logs off from Web Interface, a message appears instructing the user to close the browser. This forces a logoff from the ADFS session. The user cannot log back on to Web Interface until the browser is closed.

**Software Requirements**

These items are required for ADFS functionality with Citrix Presentation Server and Web Interface.

- Citrix Presentation Server 4.0 with Hotfix Rollup Pack 2
- Web Interface with ADFS support
- Microsoft Visual J# .NET 1.1 redistributable package
- These items should be installed and configured before going any further in this document:
  - Microsoft Windows Server 2003 R2 Enterprise Edition for federation and Web servers
  - Microsoft Active Directory Federation Services (ADFS) on the resource and account partners
Planning Active Directory Federation Services Sites

Before you create an ADFS site, you must consider the following notes and restrictions. Disregarding any of them can cause failure.

- Synchronize the clocks on the account partner federation server and the resource partner federation server to within five minutes of each other. If not, the security tokens generated by the account partner might not be accepted by the resource partner because the tokens seem to have expired. To avoid this problem, both organizations should synchronize their servers with the same Internet time server. Refer to “Setting up the Relationships between Domains” on page 13.

- Use sitemgr.exe to create a site, specifying the XML service computer as a computer name without domain (for example, cpsserver1), rather than a fully qualified domain name (for example, cpsserver1.mydomain.com) or an IP address. Refer to “Setting up the Relationships between Domains” on page 13.

- The resource federation and Web servers must be able to access the Certificate Authority’s Certificate Revocation Lists (CRLs). ADFS might fail if the servers cannot ensure that a certificate was not revoked. Refer to “Setting up the Relationships between Domains” on page 13.

- When installing Citrix Presentation Server 4.0, ensure that the XML service is set to share its port with IIS and that IIS is configured to support HTTPS. Refer to “Installing Citrix Presentation Server and the ADFS Hotfix” on page 23.

- When configuring your site as an ADFS application, make sure you use HTTPS and the fully qualified domain name (FQDN) of your Web server, including the final forward slash; for example, https://wi.treyresearch.net/Citrix/PresentationServer/. Refer to “Configuring Your Site as an ADFS Application” on page 25.

- Only the Citrix Presentation Server Client for 32-bit Windows is supported for use with ADFS. You cannot use the embedded Remote Desktop Protocol (RDP) client to launch applications.
Because of an ADFS/Java issue, the Citrix Presentation Server Client for Java is not supported with ADFS when used through Internet Explorer. However, the Client for Java works correctly when used through other supported browsers; for example, Netscape.

- Ensure that all servers within your deployment are trusted for delegation. For more information, see “Configuring Delegation for the Computers Running Web Interface and Citrix Presentation Server” on page 15.

- Set up shadow accounts in the resource partner domain for each external user who can authenticate to the Web Interface through ADFS. For more information, see “Setting up Shadow Accounts” on page 21.

- Set up a trust relationship between the server running the Web Interface and any other servers in the farm running the Citrix XML service that the Web Interface contacts. For more information see the Web Interface Administrator’s Guide.
Installation and Configuration

This guide does not document how to install ADFS. You should have a working ADFS installation, with external account users able to access ADFS-enabled Web applications in a resource partner.

Note Install Web Interface with ADFS support on a clean computer. You cannot upgrade a Web Interface Version 4.x installation to Web Interface with ADFS support nor install Web Interface with ADFS support alongside any other version.

Installation and Configuration Task List

Complete the following tasks in this order. Each step is described in detail in this document.

• “Setting up the Relationships between Domains”
• “Configuring Delegation for the Computers Running Web Interface and Citrix Presentation Server”
• “Setting up Shadow Accounts”
• “Installing Citrix Presentation Server and the ADFS Hotfix”
• “Configuring Your Site as an ADFS Application”
• “Configuring Your Site as an ADFS Application”
• “Testing Your Deployment”
Setting up the Relationships between Domains

The deployment documented in this section consists of two domains (in their own forests), one for the account partner and one for the resource partner.

To set up the relationships between domains

1. Ensure you have the following components:

<table>
<thead>
<tr>
<th>Account Partner</th>
<th>Resource Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain controller</td>
<td>Domain controller</td>
</tr>
<tr>
<td>Federation server*</td>
<td>Federation server*</td>
</tr>
<tr>
<td>Client devices</td>
<td>Web server*</td>
</tr>
<tr>
<td></td>
<td>One or more servers in a farm running Presentation Server</td>
</tr>
</tbody>
</table>

Components marked with an asterisk (*) must be on computers running Windows 2003 R2 and have the **Active Directory Federation Services** component installed.

2. Obtain separate server certificates for the Web server and both federation servers.
   - Certificates must be signed by a trusted entity called a Certificate Authority (CA).
   - The server certificate identifies a specific computer, so you must know the fully qualified domain name (FQDN) of each server; for example, cpsserver1.mydomain.com.
   - Install the Web server certificate into Internet Information Services (IIS) to enable the IIS default Web site for SSL traffic.
   - Install federation server certificates using the Certificate Microsoft Management Console (MMC) snap-in. See the *Step-by-Step Guide to the Microsoft Management Console* at www.microsoft.com for more information.

3. To ensure the resource partner’s federation server trusts the account partner’s federation server, install the account partner’s federation server root certificate into the Trusted Certification Authorities area of the resource partner’s federation server.
4. To ensure the Web server trusts the resource partner’s federation server, install the resource partner’s federation server root certificate into the Trusted Certification Authorities area of the Web server.

**Important** The resource federation and Web servers must be able to access the CA’s Certificate Revocation Lists (CRLs). The resource federation server must have access to the account partner Certificate Authority and the Web server must have access to the resource partner Certificate Authority. ADFS might fail if the servers cannot ensure that a certificate has not been revoked.

5. On the resource partner federation server, open the MMC Active Directory Federation Services snap-in. In the left pane, select **Federation Service > Trust Policy > Partner Organizations > Account Partners**, and then select the account partner name.

6. From the **Action** menu, click **Properties**.

7. From the **Resource Accounts** tab, select **Resource accounts exist for all users** and click **OK**.

*Resource accounts exist for all users is enabled on the Resource Accounts tab*
8. Using the same Internet time server, synchronize the clocks on the account partner federation server and the resource partner federation server to within five minutes of each other. If not, the security tokens generated by the account partner may not be accepted by the resource partner because the tokens appear to have expired.

The resource and account partners can be in different time zones, but they must be correctly synchronized. For example, the account partner is in New York and is set to 4:00 p.m. Eastern Standard Time (EST). The resource partner in California has to be set to within 12:55 to 1:05 p.m. Pacific Standard Time (PST). (There is a three-hour difference between EST and PST zones.)

Configuring Delegation for the Computers Running Web Interface and Citrix Presentation Server

You must ensure that all servers within your deployment are trusted for delegation. To do this, you must complete the following tasks. Procedures for each task are included in this section.

- Ensure the resource partner domain’s functional level is correct
- Trust the server running the Web Interface for delegation
- Trust the server running the XML service for delegation
- Determine which resources are accessible from the server running Presentation Server

**Important** To complete the procedures in this step, log on as an administrator to the resource partner domain controller, and then use the MMC Active Directory Users and Computers snap-in.

**To ensure the resource partner domain is at the Windows Server 2003 functional level**

**Note** To raise the domain level, all domain controllers in the domain must be running Windows Server 2003.

1. From the MMC Active Directory Users and Computers snap-in, select the domain name.
2. From the Action menu, click Properties.

3. If the domain is not at the Windows Server 2003 functional level, select the domain name and select Raise domain functional level.

To trust the server running the Web Interface for delegation

1. In the MMC Active Directory Users and Computers snap-in View menu, enable Advanced Features.

2. In the Computers folder under the domain name, select the server running the Web Interface.

3. From the Action menu, click Properties.

4. From the Delegation tab, click Trust this computer for delegation to specified services only and Use any authentication protocol, and then click Add.

5. From the Add Services screen, click Users or Computers.

6. From the Select Users or Computers screen, type the name of the server running the XML service in the Enter the object names to select text box, and then click OK.

7. Select the http service type from the list and then click OK.
8. From the Delegation tab, verify the http service type for the server running Presentation Server appears in the Services to which this account can present delegated credentials list, and then click OK.

On the Delegation tab, the http service type for the server running Citrix Presentation Server appears.

Note Repeat the process for each server in the farm running the XML service that the Web Interface is configured to contact.

To trust the server running the XML service for delegation

1. In the Computers folder under the MMC Active Directory Users and Computers snap-in, select the name of the server running the XML service that the Web Interface is configured to contact.

2. From the Action menu, click Properties.

3. From the Delegation tab, click Trust this computer for delegation to specified services only and Use Kerberos only, and then click Add.

4. From the Add Services screen, click Users or Computers.

5. From the Select Users or Computers screen, type the name of the server running the XML service in the Enter the object names to select text box, and then click OK.
6. Select the **HOST** service type from the list and then click **OK**.
7. On the **Delegation** tab, verify the **HOST** service type for the server running the XML Service appears in the **Services to which this account can present delegated credentials** list, and then click **OK**.

![Image of Delegation tab]

*On the Delegation tab, verify the HOST service type appears for the XML service*

8. For a multiserver farm, repeat Steps 3 to 7 for each server running Presentation Server.

**Note** Repeat the process for each server in the farm running the XML service that the Web Interface is configured to contact.

**To determine which resources are accessible from the server running Presentation Server**

1. In the Computers folder under the MMC Active Directory Users and Computers snap-in, select the name of the server running Presentation Server.
2. From the **Action** menu, click **Properties**.
3. From the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use Kerberos only**, and then click **Add**.
4. From the **Add Services** screen, click **Users or Computers**.
5. From the **Select Users or Computers** screen, type the name of the resource partner domain controller in the **Enter the object names to select** text box, and then click **OK**.

6. From the list, select the **cifs** and **ldap** service types for the resource partner domain controller and click **OK**.

   **Note** The **cifs** service type applies to network shares. Add the cifs service to the list for any computers on which users can access network shares.

   If two choices appear for the **ldap** service, select the one that matches the FQDN of your domain controller.

7. From the **Delegation** tab, verify the **cifs** and **ldap** services for the resource partner domain controller appear in the **Services to which this account can present delegated credentials** list, and then click **OK**.

   **Note** If you are using multiserver farms, repeat the procedure for each server running Presentation Server.
Configuring Servers for Constrained Delegation
For security reasons, you must configure all servers running Presentation Server for constrained delegation. To provide users with access to resources on those servers you must add the relevant services to the Services list using the MMC Active Directory Users and Computers snap-in. For example, to enable users to authenticate to a Web server on host foo, add the http service for server foo; to enable users to authenticate to a SQL server on host bar, add the MSSQLSvc service for server bar.

For more detailed information, see the Service Principal Names and Delegation whitepaper (CTX110784) in the Citrix Knowledge Center.

Configuring a Time Limit for Access to Resources
By default, ADFS users have access to resources on a network for 15 minutes. You can increase this time limit by modifying the following registry entry on the server running the XML service:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\S4UTicketLifetime
This value specifies the number of minutes users have access to resources for after a session starts.

The domain security policy governs the maximum value you can set for the S4ULifetime parameter. If you specify a value for the S4UTicketLifetime parameter that is greater than the value specified at domain level, the domain level setting takes precedence.

To configure a time limit for access to resources at domain level
1. Log on to the domain controller as a domain administrator.
2. From the Start Menu, click All Programs > Administrative Tools > Domain Security Policy.
3. In the console tree, expand Account Policies.
4. Select Kerberos Policy.
5. In the details pane, click Maximum lifetime for a service ticket.
6. From the Action menu, click Properties.

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.
7. Enter a value (in minutes) in the **Ticket expires in:** box. Click **OK**.

8. Close the **Domain Security Policy** dialog box.

If you do not want to configure a time limit for access to resources, select **Use any authentication protocol** when determining which resources are accessible from the server running Presentation Server. If you select this option, any value specified for the S4UTicketLifetime parameter is ignored.

For more information, see Microsoft’s Web site at http://support.microsoft.com/.

**Setting up Shadow Accounts**

To launch applications, Presentation Server requires that users accessing Web Interface through ADFS possess real Windows accounts. Therefore, you must manually create a shadow account in the resource partner domain for each external user that authenticates to the Web Interface through ADFS (even if users are set up in Groups). You cannot disable shadow accounts.

**Note**  If you have a large number of users in the account partner domain that will access applications in the resource partner domain, you can use a third-party account-provisioning product to enable rapid creation of user shadow accounts in Active Directory.

To create shadow accounts, complete the following tasks as an administrator on the domain controller for the resource partner domain. Procedures for each task are included in this section.

- Add user principal name (UPN) suffixes for all external *account partners*
- Define the shadow account user

**To add UPN suffixes**

1. Open the MMC Active Directory Domains and Trusts snap-in.
2. In the left pane, select **Active Directory Domains and Trusts**.
3. From the **Action** menu, click **Properties**.
4. Add a UPN suffix for each external *account partner*. For example, if the Active Directory domain of the account partner is adatum.com, add adatum.com as the UPN suffix.
5. Click **OK**.
To define the shadow account user

1. Open the MMC Active Directory Users and Computers snap-in.
2. In the left pane, select the domain name.
3. From the Action menu, click Users > New user. Type the user’s first name, initials, and last name in the corresponding text boxes.
4. In the User logon name text box, type the account name. Make sure this name matches the name on the account partner.
5. From the drop-down list, choose the external UPN suffix, and then click Next.

![Image of user creation window]

Complete the text boxes to define a new shadow account

6. In the Password and Confirm password text boxes, type a password that meets your password policy. This password is never used because the user authenticates through ADFS.
7. Clear the User must change password at next logon check box.
8. Select the User cannot change password and Password never expires check boxes.

Note  Presentation Server automatically checks the expiration status of user passwords no matter how users log on. The shadow account password here is never used, but it is still checked by Presentation Server. So selecting the Password never expires option ensures that Presentation Server does not fail when this unused password expires.
9. Click Next, and then click Finish.

Installing Citrix Presentation Server and the ADFS Hotfix

For Web Interface with ADFS support to work, you must install Citrix Presentation Server 4.0 and Hotfix Rollup Pack 2.

To install Citrix Presentation Server and the ADFS hotfix

1. Log on as an administrator to the server or servers that will run Citrix Presentation Server in the resource partner.

2. Install Citrix Presentation Server 4.0. Ensure that the XML service is set to share its port with IIS. See the Citrix Presentation Server Administrator’s Guide, Version 4.0 for installation details.


4. Open the Citrix Presentation Server Console on the computers hosting the Citrix XML service.

5. In the left pane, select Servers, and then select the particular server.

6. From the Action menu, select Properties.

7. Click XML Service, enable Trust requests sent to the XML Service, and then click OK.

8. Publish one or more applications that can be accessed by your users.

**Note** You can administer all of the servers in a farm using a single console. Select each server (they are listed under the Servers node) and update its properties.

**Note** Users will launch the applications using one of the previously-created shadow accounts. Because the shadow accounts belong to the resource partner domain, you can make applications accessible to everyone by publishing to Domain Users.
Installing Web Interface with Active Directory Federation Services Support and Creating a Site

Web Interface with ADFS support provides users with access to Citrix Presentation Server 4.0 published applications through a standard Web browser. It enables you to use ADFS technology. You cannot install Web Interface with ADFS support in addition to Web Interface 4.0.

Important After you install Web Interface, you must make the Web Interface available to your users. To do this, create and configure sites. Create the Web Interface site with local configuration, using the sitemgr.exe site management tool on a command line. sitemgr.exe creates the WebInterface.conf configuration text file. Manually edit this file when configuration changes are needed.

To install the Web Interface with ADFS support and create a site

1. Log on as an administrator to the resource partner’s server running Web Interface.
2. Install the Microsoft Visual J# .NET 1.1 redistributable package from the Support directory on the installation CD for Citrix Presentation Server 4.0.
3. Install Web Interface with ADFS support.
4. From a command-line, change to the directory where you just installed Web Interface; for example, C:\Program Files\Citrix\Web Interface\4.0.
5. Create a new site using the site management tool. To display the command syntax, type sitemgr -h.

This command-line example,

Sitemgr -c "WIDest=1:/Citrix/PresentationServer,Config=Local,XMLService=cpserver1:80"
Does the following:

- Creates a site at Citrix/PresentationServer on IIS site 1 (the default Web site).
- Creates a local configuration file (WebInterface.conf) that you can edit manually. Centralized configuration is not supported.
- Points to cpsserver1 on port 80 as its Citrix XML service.

**Important**  Specify the computer running the XML service as a computer name without domain (for example, cpsserver1), rather than an FQDN (for example, cpsserver1.mydomain.com) or an IP address.

6. Select the site name (in the example it is PresentationServer).
7. From the **Action** menu, select **Properties**.
8. On the **ASP.NET** tab, ensure that the version is set to 1.1.x and not 2.0.x.

### Configuring Your Site as an ADFS Application

You must configure your newly created site as an ADFS application so the federation server recognizes it.

**To configure your site as an ADFS application**

1. Open the MMC Active Directory Federation Services snap-in on the resource partner federation server. In the left pane, select **Federation Service >Trust Policy > My Organization > Applications**.
2. From the **Action** menu, select **New > Applications**.
3. Select **Windows NT token based application**, and then click **Next**.
4. In the application name text box, type **Citrix Web Interface**.
5. Type the URL of your Web Interface site, and then click **Next**.

**Important**  Make sure you use HTTPS and the FQDN of your Web server, including the final forward slash; for example, `https://wi.treyresearch.net/Citrix/PresentationServer/`.

6. Depending on how you configured ADFS (which is usually PKI), select **Public Key Infrastructure** or **Domain Service Account**, and then click **Next**.
7. Select User Principal Name (UPN) and click Next.
8. Make sure Enable this application is checked and click Next.
9. Click Finish.

**Note** You do not have to configure the site on the Web server. The site management tool configures all the appropriate ADFS settings in IIS.

## Testing Your Deployment

After configuring your site as an ADFS application, test your deployment to ensure everything is working correctly between the account partner and the resource partner.

**To test the Web Interface ADFS deployment**

1. Log on to your client computer on the account partner.
2. Open a Web browser and type the FQDN URL of the Web Interface site that you previously created.
   The Web Interface application list page appears.

**Note** If you did not configure ADFS for integrated authentication, you may be prompted to enter your credentials or insert a smart card.

3. If you did not install the Citrix Presentation Server Client, do so now. For more information, see the *Clients for Windows Administrator’s Guide.*

**Note** The Client for Java or Remote Desktop Connection software are not supported on ADFS integrated sites.

4. Click an application to launch it.
Index

A
account partner 5–6
Active Directory Federation Services, see ADFS
ADFS 9
hotfix 23
installation the hotfix 23
overview 5
setting up the hotfix 23

C
Citrix Presentation Server 7
ADFS 7
deployment 7
installation 23
setting up 23
configuration 12
delegation for servers running Web Interface and
Presentation Server 15
WebInterface.conf 24–25
configuring
constrained delegation 20
constrained delegation 20
configuring 20
creating Web Interface site 24

D
delegation
servers running Web Interface and Presentation
Server 15
deployment
Citrix Presentation Server 7
Web Interface 6
Web Interface with ADFS support 7
documentation, Microsoft 7
domains
correct functional level 15
setting up relationships between 13

F
federation
server 6
server proxy 6
service 6
service proxy 7
functional level for resource partner domain 15

I
important considerations
Client for Java 11
Remote Desktop Protocol (RDP) 10
installation 12
ADFS hotfix 23
Citrix Presentation Server 23
Web Interface 24

J
Java, Client 11

L
local configuration
Web Interface site 24

M
Microsoft
Active Directory Federation Services (ADFS) 9
documentation 7
Visual J# .NET 1.1 redistributable package 9, 24
Windows Server 2003 R2 9

O
overview
ADFS 5
P
partners
  account 5–6
  resource 5, 7
proxies
  federation server 6
  federation service 7

R
references, documentation 7
Remote Desktop Protocol (RDP) 10
requirements
  software 9
resource partner 5, 7

S
servers
  delegation 15
  federation 6
  synchronize clocks 10
  synchronizing clocks 15
service
  federation 6
setting up
  ADFS hotfix 23
  Citrix Presentation Server 23
  domain relationships 13
shadow accounts 7
site creation 24
sitemgr.exe, creating a site 24
software requirements 9
synchronize server clocks 10
synchronizing
  server clocks 15

T
time limit 20

V
Visual J# .NET 1.1 redistributable package 9, 24

W
Web Interface
  ADFS support 7
  deployment 6–7
  installation 24
  site, local configuration 24
WebInterface.conf 24–25
Windows Server 2003 R2 9

X
XML service 10, 25