

# Lesson 18: Implementing Active Directory Federation Services

MOAC 70-412: Configuring Advanced  
Windows Server 2012 Services

# Overview

- Objective 6.1 – Implement Active Directory Federation Services.
  - Manage AD FS certificates
  - Implement claims-based authentication including relying party trusts
  - Configure Claims Provider Trust rules
  - Configure attribute stores including Active Directory Lightweight Directory Services (AD LDS)
  - Configure AD FS proxy
  - Integrate with cloud services

# Understanding Active Directory Federation Services

Lesson 18: Implementing Active Directory  
Federation Services

# Active Directory Federation Services

- The **Active Directory Federation Services (AD FS)** role allows administrators to configure **Single Sign-On (SSO)** for web-based applications across a single organization or multiple organizations without requiring users to remember multiple usernames and passwords.
- This enables you to configure Internet-facing business-to-business (B2B) applications between organizations.

# Active Directory Federation Services

- AD FS-enabled applications are claims based, which allows a much more scalable authentication model for Internet-facing applications.
- AD FS is an identity access solution that allows any browser-based clients to access a website with a single login to one or more protected Internet-facing applications, even when the user accounts and applications are on different networks and exist within different organizations via a federated trust relationship.

# Active Directory Federation Services

- An AD FS configuration consists of two types of organizations:
  - **Resource organizations:** Own the resources or data that are accessible from the AD FS-enabled application, similar to a trusting domain in a traditional Windows trust relationship.
  - **Account organizations:** Contain the user accounts that access the resources controlled by resource organizations.
- AD FS can be used within a single organization—the single organization is the resource organization and the account organization.

# Federated Trust Relationship

- To establish an identity federation partnership, both partners agree to create a ***federated trust relationship***.
- Each partner defines what resources are accessible to the other organization and how access to those resources is enabled.
- User identities and their associated credentials are stored, owned, and managed by the organization where the user is located.

# AD FS Components

- AD FS uses the following components:
  - **Federation server:** The server that issues, manages, and validates requests involving identity claims. A federation server is needed in each participating forest.
  - **Federation server proxy:** An optional component that is usually deployed in a perimeter network such as DMZ that can receive externally and forward the packets to the internal federation server.
  - **Claim:** A statement made by a trusted entity about an object such as a user that includes key information identifying the user.
  - **Claim rules:** Rules that determine what makes up a valid claim and how claims are processed by the federation servers.



# AD FS Components

- **Attribute store:** A database, such as AD DS, that is used to look up claim values.
- **Claims provider:** The server that issues claims and authenticates users.
- **Relying party:** The application or web services that accepts claims from the claims provider. The relying party server must have the Microsoft Windows Identity Foundation installed, or use the AD FS 1.0 claims-aware agent.
- **Claims provider trust:** Configuration data that specifies which client may request claims from a claims provider and subsequently submit them to a relying party.
- **Relying party trust:** Configuration data that is used to provide claims about a user or client to a relying party.

# Implementing AD FS

...

Lesson 18: Implementing Active Directory  
Federation Services

# Implementing AD FS

- Before implementing AD FS, you need to plan your implementation.
- You should also create a test environment so that you can foresee any potential problems.

# Implementing AD FS

- First, make sure that the client and servers can communicate with the necessary computers:
  - The client must be able to communicate with the web application, the resource federation server (or federation server proxy), and the account federation server (or federation proxy) using HTTPS.
  - If using federation server proxy, you must be able to communicate with the federation servers in the same organization using HTTPS.
  - The internal clients must be able to communicate with the organization's federation servers.
  - The client federation server must be able to communicate with the client domain controllers for authentication.

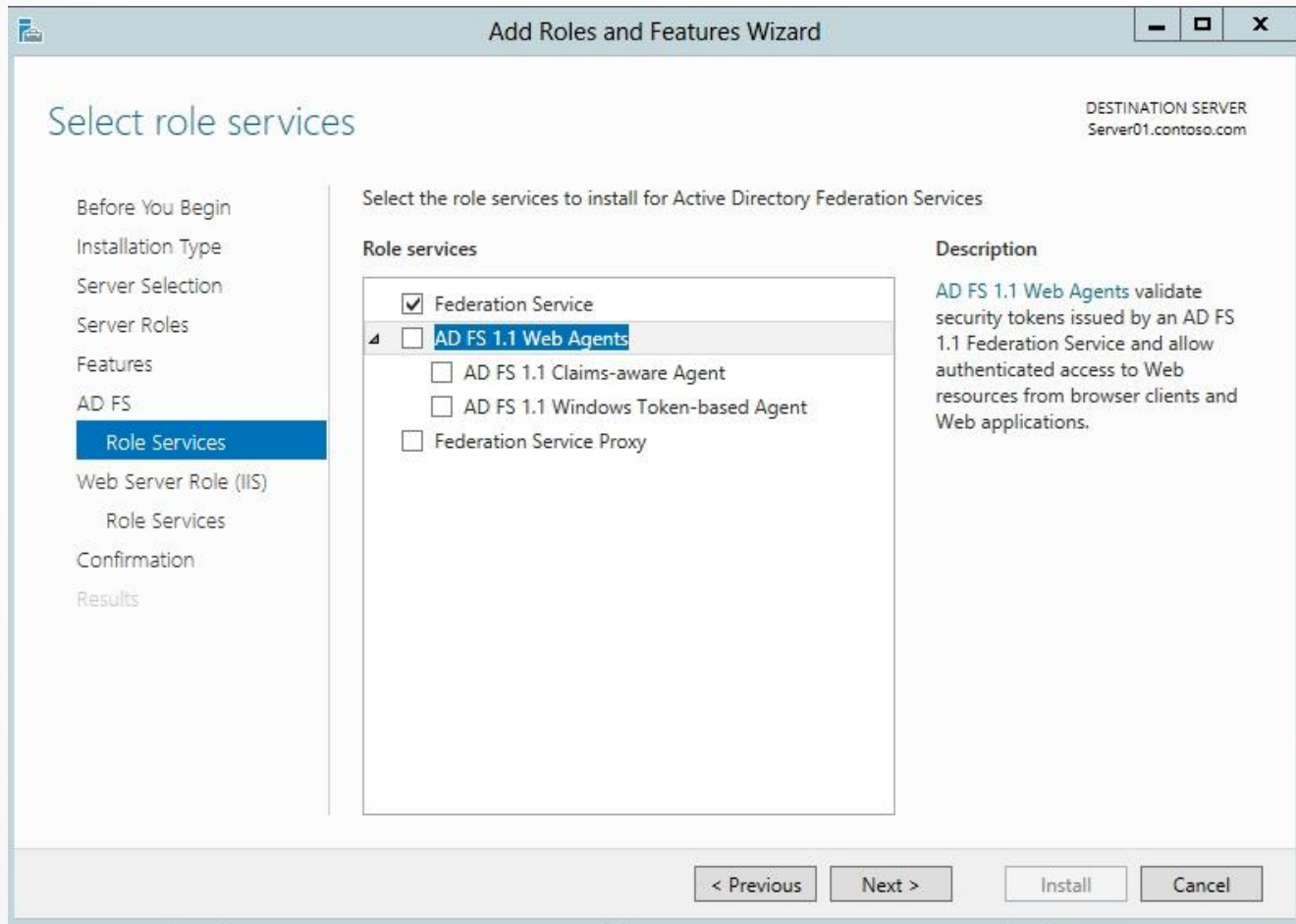
# Implementing AD FS

- AD FS supports the following attribute stores:
  - Active Directory Application Mode (ADAM) in Windows Server 2003
  - Active Directory Lightweight Directory Services (AD LDS) in Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012
  - Microsoft SQL Server 2005 (all editions)
  - Microsoft SQL Server 2008 (all editions)
  - A custom attribute store

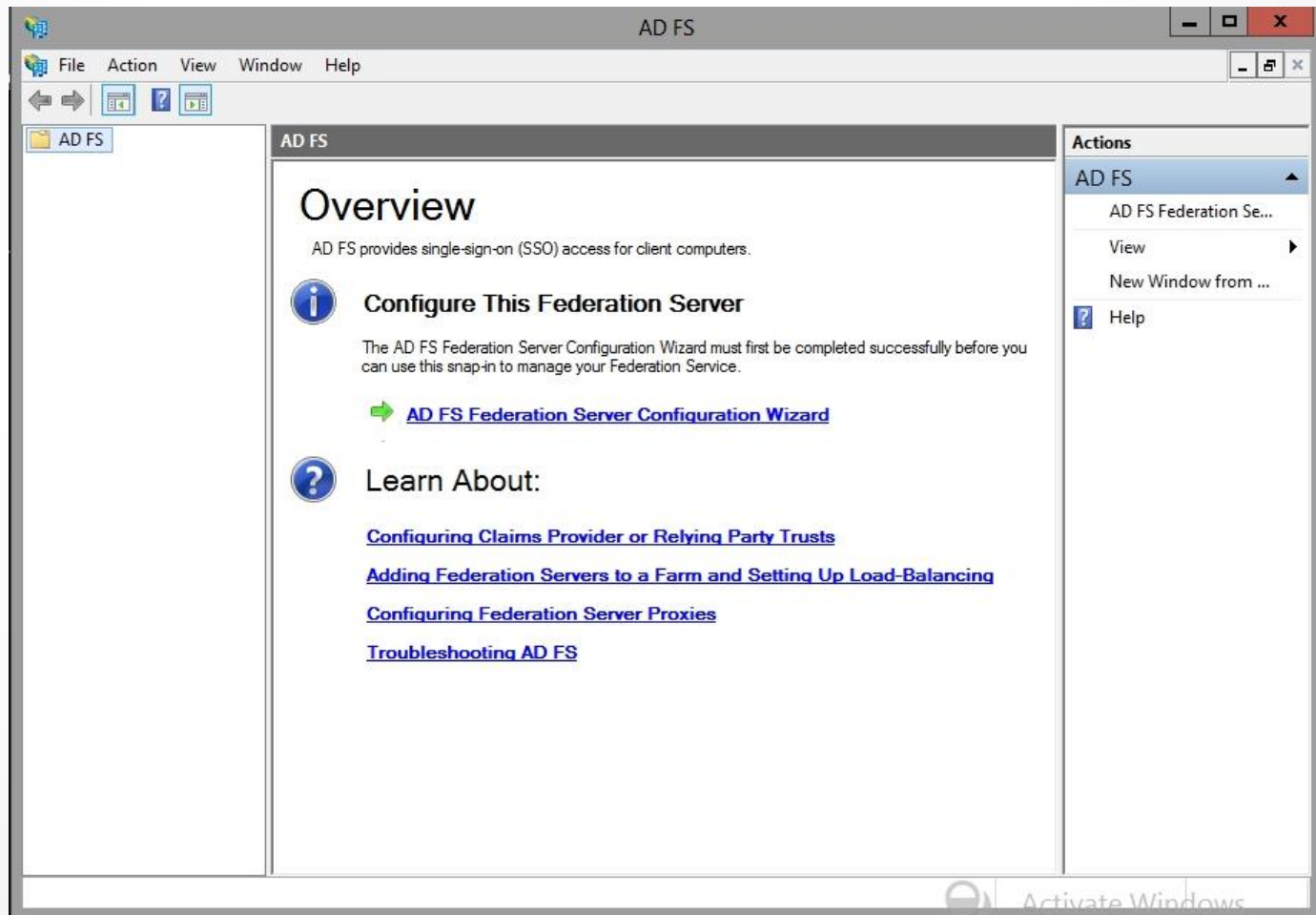
# Implementing AD FS

- AD FS requires DNS names for internal federation servers to which they connect, and the web application that they are trying to use.
- External users need to resolve the name of the internal federation server through the proxy server.

# Implementing AD FS

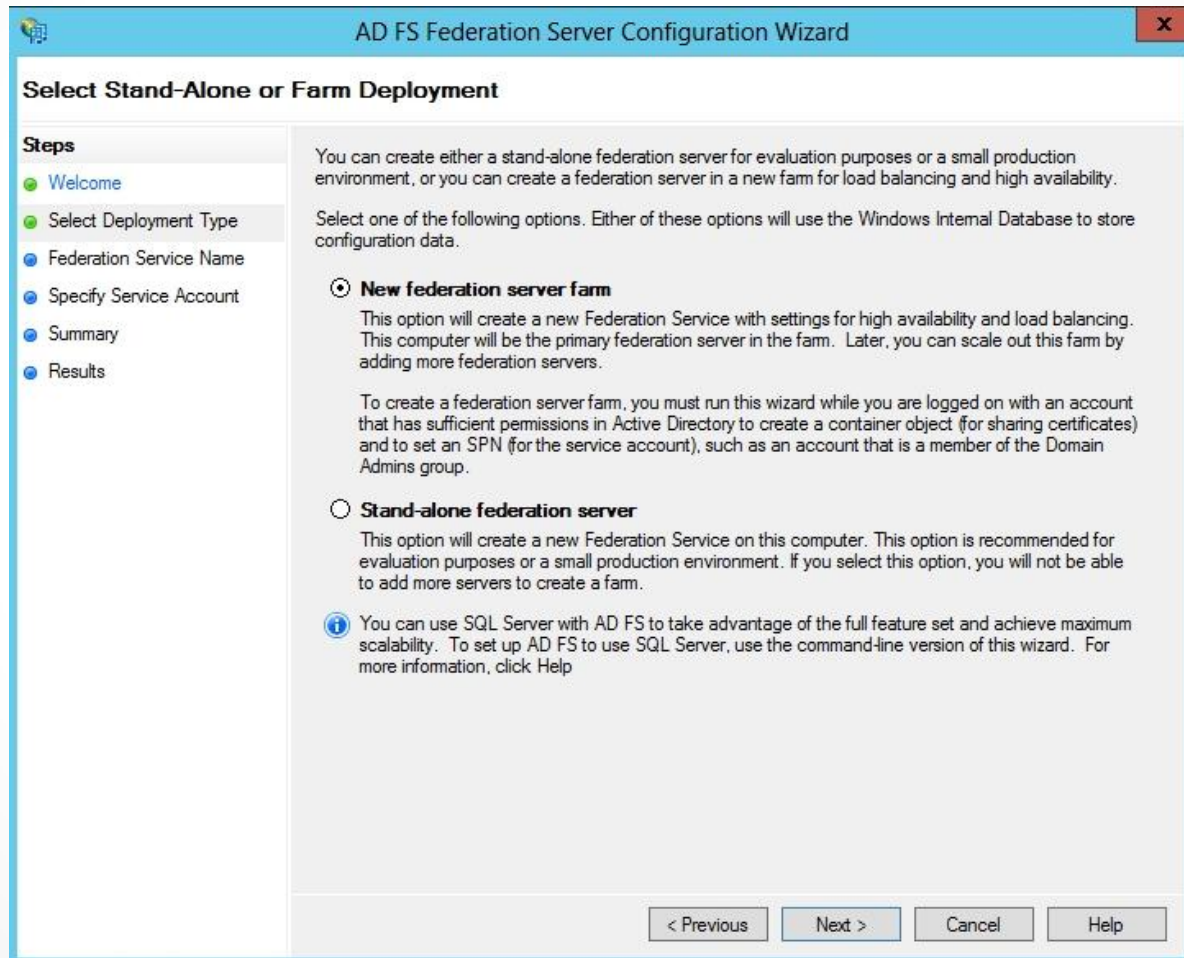


# Implementing AD FS





# Implementing AD FS



# AD FS Certificates

- The necessary digital certificates include:
  - **Server communications certificate:** The certificate installed on the web server and federation server proxy that the clients access to provide SSL communications. If AD FS needs to be accepted by clients on the Internet, you should use third-party certificates.
  - **Token-signing certificate:** The certificate used by the claims provider to identify itself and by the relying party to verify that the token is coming from a trusted federation partner. The relying party also requires a token-signing certificate to sign the tokens it prepares for AD FS.
  - **Token-decrypting certificate:** The certificate used to decrypt the user token before transmitting the token across the network.

# Implementing Claims-Based Authentication

1. Install the AD FS server role.
2. Create and configure a server authentication certificate in IIS.
3. Create a stand-alone federation server.
4. Install and configure Windows Identity Foundation (WIF) and a sample application.
5. Create and configure the WIF application pool.
6. Configure the WIF sample application to trust incoming claims.
7. Configure AD FS to send claims to the application.
8. Configure the claim rule for the sample application.
9. Test access to the application.

# Relying Party Trusts

- A relying party trust
  - Identifies the relying party so that the federation server knows which applications can use AD FS.
  - Defines the claim rules, from the claims provider.
- The relying party is defined on the federation server.

# Relying Party Trusts

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main area is titled "Select Data Source". On the left, a "Steps" pane lists five steps: "Welcome", "Select Data Source" (highlighted), "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main content area contains the following text and controls:

Select an option that this wizard will use to obtain data about this relying party:

- Import data about the relying party published online or on a local network  
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.  
Federation metadata address (host name or URL):  
  
Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file  
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.  
Federation metadata file location:
- Enter data about the relying party manually  
Use this option to manually input the necessary data about this relying party organization.

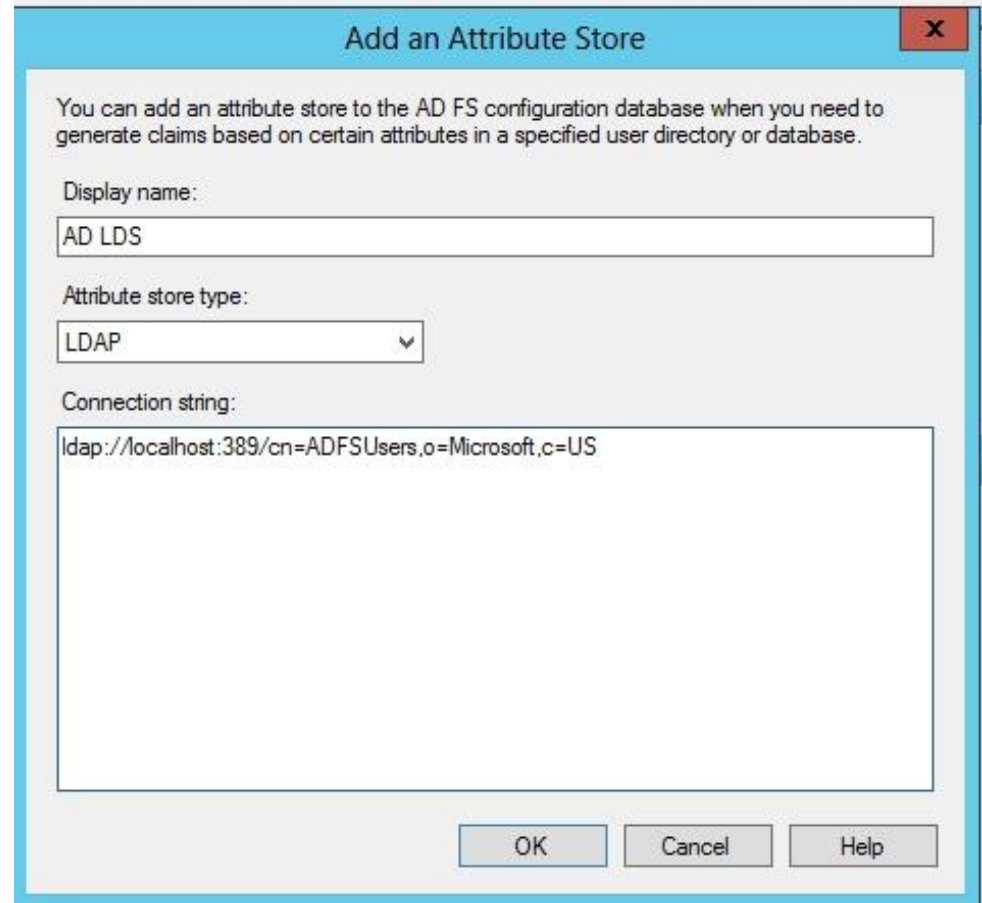
At the bottom of the dialog, there are four buttons: "< Previous", "Next >", "Cancel", and "Help".

# Claims Provider Trust Rules

- A claims provider trust
  - Identifies the claims provider.
  - Describes how the relying party consumes the claims that the claims provider issues.
- By default, the AD FS server is configured with a claims provider trust named *Active Directory*.
- The claims provider trust options are similar to the relying party trust options:
  - Import data about the claims provider through the federation metadata.
  - Import data about the claims provider from a file.
  - Manually configure the claims provider trust.

# Attribute Stores

AD FS uses an attribute store to look up claim values. Although AD DS is already configured by default as an attribute store, you can configure a database or another directory such as Active Directory Lightweight Directory Services (AD LDS).



**Add an Attribute Store**

You can add an attribute store to the AD FS configuration database when you need to generate claims based on certain attributes in a specified user directory or database.

Display name:  
AD LDS

Attribute store type:  
LDAP

Connection string:  
ldap://localhost:389/cn=ADFSUsers,o=Microsoft,c=US

OK Cancel Help

# AD FS Proxy

- The AD FS proxy
  - Is used for the federation server of two organizations to securely communicate over the Internet using port 443.
  - Is located in the perimeter network.
  - Collects authentication information from the user's browser through the WS-Federation Passive Requestor Profile (WS-F PRP), an AD FS web service, which then passes it on to the federation service.



# AD FS Proxy

The screenshot shows a Windows-style dialog box titled "AD FS Federation Server Proxy Configuration Wizard". The current step is "Specify Federation Service Name". On the left, a "Steps" pane lists: "Welcome", "Specify Federation Service Name" (highlighted), "Ready to Apply Settings", and "Configuration Results". The main area contains the following text and controls:

Specify the name of the Federation Service to which this federation server proxy will redirect client requests.

Federation Service name:  
  
Example: fs.contoso.com

Use an HTTP proxy server when sending requests to this Federation Service

HTTP proxy server address:  
  
Example: http://proxy.contoso.com:9000/

At the bottom right, there are four buttons: "< Previous", "Next >", "Cancel", and "Help".

# Cloud Services

- As servers, services, and applications move to the cloud, those servers, services, and applications (e.g., Windows Azure, SharePoint Online, or Exchange Online) are located away from the organization.
- Therefore, organizations want to rely on AD DS for authentication and authorization using AD DS credentials and by using AD FS to provide claims to those servers, services, and applications on the cloud.
- AD FS provides SSO support for both Microsoft and non-Microsoft cloud services.

# Lesson Summary

- The Active Directory Federation Services (AD FS) role allows administrators to configure Single Sign-On (SSO) for web-based applications across a single organization or multiple organizations without requiring users to remember multiple usernames and passwords.
- Claims are statements made by a trusted entity about an object such as a user that includes key information identifying the user.
- Installing the Active Directory Federation Services role and creating the AD FS server is a simple process when using Server Manager. When you select the AD FS role services, you install the federation server or the federation service proxy.

# Lesson Summary

- A relying party trust identifies the relying party so that the federation server knows which applications can use AD FS. It also defines the claim rules from the claims provider.
- A claims provider trust identifies the claims provider and describes how the relying party consumes the claims that the claims provider issues.
- By default, the AD FS server is configured with a claims provider trust named *Active Directory*.

# Lesson Summary

- AD FS uses an attribute store to look up claim values. Although AD DS is already configured by default as an attribute store, you can configure a database or another directory such as Active Directory Lightweight Directory Services (AD LDS).
- The AD FS proxy is used for the federation server of two organizations to securely communicate over the Internet using port 443. The proxy server is located in the perimeter network.

**Copyright 2013 John Wiley & Sons, Inc.**

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.