Arcot Adapter™ for Cisco® VPN Installation and Configuration Guide (Windows)

Version 2.1.6

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot Adapter for Cisco VPN Installation and Configuration Guide
Version 2.1.6
February 2010
Part Number: AAA01-002DC-02160

Trademarks

Patents

Arcot Systems, Inc., 455 West Maude Avenue, Sunnyvale, CA 94085

Contents

Preface

This guide describes the process to install and configure Arcot Adapter 2.1.6 with Cisco® IPSec VPNs.

This guide includes information on:

- High-level architecture of the integration process
- Requirements for installing the Arcot Adapter
- Installation of Arcot Adapter
- Post-installation tasks
- Configuration files
- Uninstallation of Arcot Adapter

Intended Audience

This guide is intended for system integrators who are responsible for configuring Cisco® IPSec VPNs with Arcot WebFort to seamlessly work with each other. This guide requires that the reader must be familiar with WebFort and the Cisco® IPSec VPN technology.

> **NOTE:** This guide assumes that Cisco® IPSec VPN appliance(s) and Arcot WebFort have been installed and are independently operational, before you follow the procedures in this guide.

Information Included in this Guide

This guide is organized as follows:

- **Chapter 1, "Arcot Adapter for Cisco® IPSec VPN Overview"**, describes the high-level integration architecture of Arcot Adapter and describes the other Arcot products that Adapter interacts with.
- **Chapter 2, "Preparing for Installation"**, lists the pre-requisite software and configurations required to install Arcot Adapter.
- **Chapter 3, "Installing Arcot Adapter"**, describes the steps to install the Arcot Adapter.
- **Chapter 4, "Deploying and Configuring Customization Engine"**, describes the steps to configure Arcot Customization Engine (ACE).
- **Chapter 5, "Configuring the Components"**, describes the steps to configure Arcot WebFort and the Cisco® VPN to communicate with each other.
- **Chapter 6, "Preparing for the Arcot VPN Client Distribution"**, provides information on the Arcot VPN Client (AVC) properties file and how to get it ready for distribution to your end users.
- **Chapter 7, "Uninstalling Arcot Adapter Components"**, lists the steps to uninstall the Arcot Adapter components and the related files that are used by the Arcot Adapter.
- **Appendix A, "Third-Party Software Licenses"**, lists the third-party software that are used with Adapter.
- **Appendix B, "Glossary"**, describes the terms that are used in this guide.

Related Publications

Other related Arcot publications are as follows:

Arcot WebFort 6.0 Installation and Deployment Guide	This guide describes the procedure for installing and deploying WebFort on supported platforms.
Arcot WebFort 6.0 Administration Guide	This guide provides information to administer and configure WebFort.
ArcotID Client 6.0 Reference Guide	This guide provides complete information about ArcotID Clients.
Arcot RiskFort 2.0 Installation and Deployment Guide	This guide describes the procedure for installing and deploying RiskFort on supported platforms.
Arcot RiskFort 2.0 Administration Guide	This guide provides information to administer and configure RiskFort.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the **System** tab.
Italic	Names of Publications	For more information, see the *ArcotID Client 6.0 Reference Guide*.
	Emphasis	*Never* give anyone your password.
Cross reference	Links in the guide	Refer to the chapter **Preparing for Installation** for more information.

`Fixed-width`	Text File Content	`##### Cisco VPN Profile to AAP URL mapping #####`
		`# Mapping Format`
		`aap.profile.serverurl.mapping.<profilename>`

	File names	`arcotauthui.properties`

Contacting Support

If you need help, contact Arcot Support as follows:

Email	support@arcot.com
Web site	http://support.arcot.com

Chapter 1

Arcot Adapter for Cisco® IPSec VPN Overview

Many organizations use Virtual Private Networks (VPNs) to provide secure access to the resources available in their private networks. Although VPNs protect the integrity of data transmissions, they rely on simple user name and password to authenticate users. This approach exposes organizations to the risk of identity fraud. VPN implementations that utilize hardware authentication devices, such as One-Time Password (OTP) tokens, are expensive to deploy and manage.

By integrating Arcot WebFort Server with the Cisco IPSec VPN appliances, you enable a solution that combines flexible, software-based strong authentication with a full-featured IPSec VPN system that does not change the users' login experience or your organization's critical business processes. This integrated solution leverages Arcot's unique software-based credential protection cryptographic camouflage technology (which is the basis of ArcotID) to provide authenticated access to the Cisco VPN appliances.

This chapter explains the basic concepts of the Arcot Adapter and the features introduced in this release. This chapter includes the following sections:

Adapter Architecture

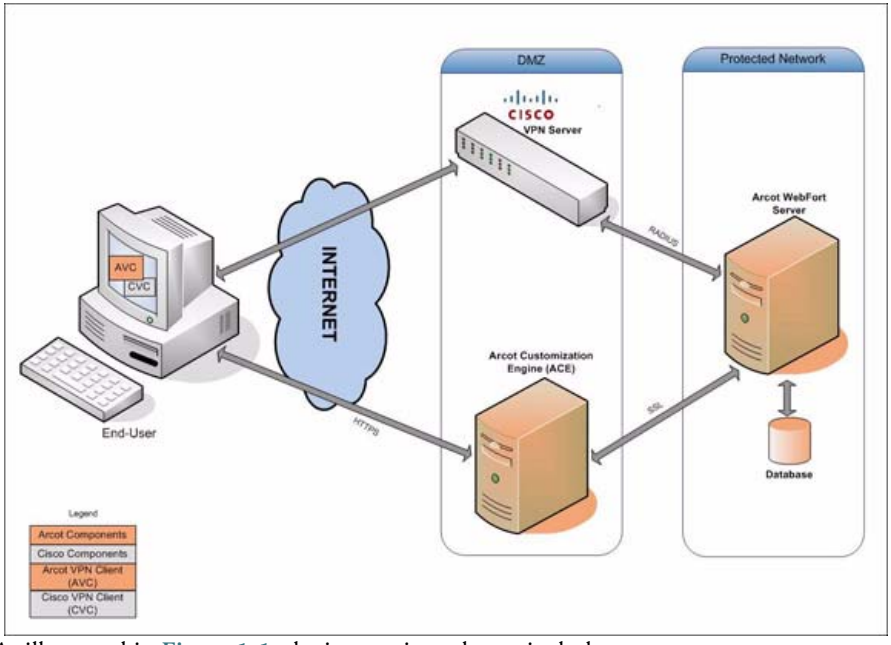
This section explains the architecture of the Adapter and the typical information flow between these components. This section includes the following topics:

- Architecture
- Typical Adapter Workflow

Architecture

Figure 1-1 illustrates how Arcot Adapter 2.1.6 and its components integrate with Cisco IPSec VPNs.

Figure 1-1 Architecture Diagram



As illustrated in Figure 1-1, the integration adapter includes:

- Arcot VPN Client
- Arcot Customization Engine (ACE)
- Arcot WebFort

Arcot VPN Client

The *Arcot VPN Client* (AVC) is an end-user Adapter component that is installed on the user's computer. As a result, it is the only component of the Adapter that a user interacts with directly.

When the user specifies the ArcotID user name and password, AVC interacts with **Arcot Customization Engine (ACE)** for the ArcotID authentication. After successful authentication when ACE returns a One-Time-Token (OTT), AVC invokes the Cisco VPN Client and passes the user name along with the OTT.

Arcot Customization Engine (ACE)

The *Arcot Customization Engine* is a state machine that maintains the state data of the user flow, conducts WebFort authentication, and reads or writes information. It controls the enrollment and authentication workflows that an end user must undergo (at their end) by "instructing" the AVC to show the required input fields, buttons, and other UI elements.

> **NOTE:** The ACE communicates with the AVC using XML over HTTPS.

Arcot WebFort

Arcot WebFort protects users from identity theft and fraud by providing strong, two-factor authentication, without changing their familiar user name/password-based sign-on experience. As a result, it significantly enhances the varied authentication management capabilities (including step-up authentication) of a Cisco IPSec VPN deployment by adding a transparent layer of strong multi-factor authentication.

> **NOTE:** Arcot WebFort is packaged separately and should be installed separately. Refer to Arcot WebFort documentation for more information.

Typical Adapter Workflow

As illustrated in **Figure 1-1**, the generic login workflow when you integrate WebFort with Cisco IPSec VPN is as follows:

1. User invokes Arcot VPN Client to connect to their enterprise network.
2. User specifies their ArcotID credentials and clicks the **Login** button to connect.
3. ACE conducts ArcotID authentication and returns an OTT to AVC.

> **NOTE:** ArcotID and ArcotID Password that are a part of ArcotID authentication are used to extract the private key of the user. This private key is then used to sign the challenge. Refer to *ArcotID Client 6.0 Reference Guide* for more information on ArcotID authentication.

4. AVC invokes Cisco VPN Client, which in turn connects to Cisco VPN Server with the user information and the OTT.
5. Cisco VPN validates the OTT with WebFort (which is set up as the RADIUS server.)
6. On successful authentication, user is logged into their enterprise network.

What's in this Release

This section provides information on the new features introduced in the current releases of Arcot Adapter 2.1.6.

- **Support for Arcot WebFort 6.0**

  Adapter 2.1.6 supports the latest Arcot WebFort 6.0 release. This release of WebFort includes many new features, which includes support for LDAP directory server, support for two-way SSL communication, and flexibility to add new authentication and issuance features, among others.

  NOTE: For more information on Arcot WebFort 6.0, see the WebFort documentation.

- **Support for Arcot RiskFort 2.0**

  Adapter 2.1.6 also supports the Arcot RiskFort 2.0 release to evaluate risk of each incoming transaction.

  NOTE: For more information on Arcot RiskFort 2.0, see the RiskFort documentation.

Arcot Adapter Features

This section lists the key features of Arcot Adapter for Cisco IPsec VPN:

- **Support for IPSec VPN**

  Arcot Adapter extends its functionality to support IPSec VPNs. It provides a new component (Arcot VPN Client) that works with Arcot Customization Engine (ACE) to provide VPN capabilities to remote users.

- **Enhancement to Arcot Customization Engine**

  Arcot Adapter added a new controller to the ACE that performs the function of an authentication proxy for the ArcotID authentication in the VPN environment.

Chapter 2

Preparing for Installation

This chapter lists the software requirements for installing the Arcot Adapter and discusses other prerequisites for integration. The following sections are covered in this chapter:

- Adapter Software Requirements
- Checklist for Integration

Adapter Software Requirements

Ensure that the software with specific versions, as listed in this section, is installed and configured.

> **NOTE:** Refer to Chapter 3, "Preparing for Installation" in the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on the software requirements for WebFort.

Table 2-1 WebFort Version Requirement for VPN Integration

Software	Supported Version	Supported Operating System
WebFort Server	6.0	Windows 2003

Database Requirements

The following table lists the database requirements for WebFort Server.

Table 2-2 Minimum Database Version Requirements

	Database Server
WebFort Server	MS SQL Server 2005, Enterprise Edition (SP2)
	Oracle 10*g*

JDK and Application Server Requirements

The following table lists the requirements for the JDK and the application server.

Table 2-3 Minimum JDK and Application Server Version

	JDK	Application Server
WebFort Server	Sun JDK 5.0 Update 10	Apache Tomcat 5.5.23
	Sun JDK 1.4.2 Update 13	Apache Tomcat 5.0.28
	IBM 32-bit v5.0, SR2	IBM WebSphere 6.1
	BEA JRockit JDK 5.0 Update 11	BEA WebLogic Server 10.0 MP1

Checklist for Integration

Before you proceed with the integration, you must ensure that both Arcot WebFort Server and the Cisco IPSec VPN have been installed and are independently operational. You must have the following components installed, configured, and tested:

- Arcot WebFort is installed on the required operating system.

  Refer to *Arcot WebFort 6.0 Installation and Deployment Guide* for installation details.

  IMPORTANT: To ensure the successful implementation of the integrated solution, you must configure WebFort *before* configuring Cisco IPSec VPN appliances.

- The required number of Cisco IPSec VPN appliances have been installed and configured.

  NOTE: For information on how to install and configure your Cisco IPSec VPN appliances, refer to the Cisco documentation or contact your Cisco support.

- Required number of application server instances are running.

  NOTE: If available, run the test scripts to ensure optimal installation.

Chapter 3

Installing Arcot Adapter

This chapter provides instructions for installing the Arcot Adapter for integrating with Cisco IPSec VPN to provide ArcotID authentication. It discusses the following topics:

- Installing Arcot Adapter
- Installation Directory

> **NOTE:** Before proceeding with the instructions in this chapter, ensure that the prerequisites discussed in Chapter 2, "Preparing for Installation" are installed and configured correctly.

Installing Arcot Adapter

Use the **Arcot Adapter InstallAnywhere Wizard** to install the Adapter components. This Wizard supports Complete and Custom installation types. However to install and configure the Adapter for VPN integration, you *must* use the *Custom* option when you run the installer. **Custom** installation enables you to install only the required component (Customization Engine) from the package.

> **IMPORTANT:** Before proceeding with the installation, ensure that all prerequisite software components are installed and the database is set up, as described in the Chapter 2, "Preparing for Installation".

Perform the following steps to install the Arcot Adapter:

1. Navigate to the directory where the **`Arcot-Adapter-2.1.6-Windows-Installer.exe`** file is located and double-click the file to run the installation wizard.

   The Welcome screen appears.

2. Click **Next** to continue.

   The License Agreement screen appears.

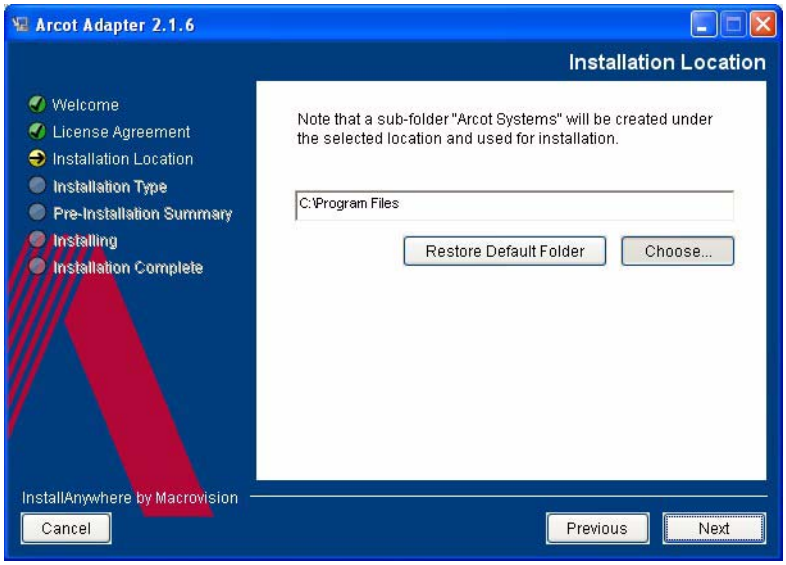
3. Read the license agreement carefully, select the **I accept the terms of the License Agreement** option, and click **Next.**

   The Installation Location screen appears.

4. The installer now verifies if any other Arcot product is installed on the computer.

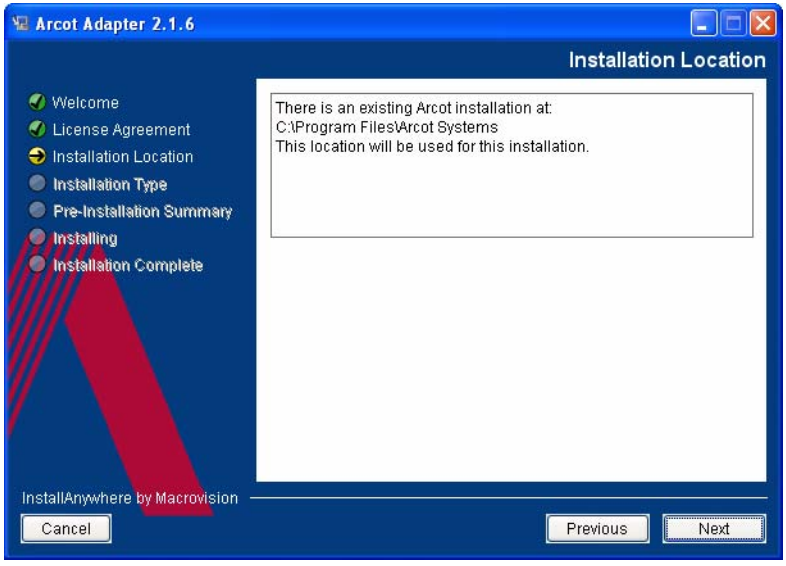
   If it does not find an existing Arcot product installation, then you will be prompted for an installation folder. In this case, the Installation Location screen, as shown in the following figure, appears.

Figure 3-1 The Installation Location Screen (No Arcot Product Found)



If the installer detects an existing Arcot product installation, then you will not be prompted for an installation folder. The following screen appears when an existing *Arcot Systems* folder is located on the computer.

Figure 3-2 The Installation Location Screen (Arcot Product Found)



5. You can accept the default folder specified by the installer to install the Adapter. You can also click **Choose** to navigate and specify a different installation folder.

   Click **Next** to install in the specified folder.

   The Type of Installation screen appears.

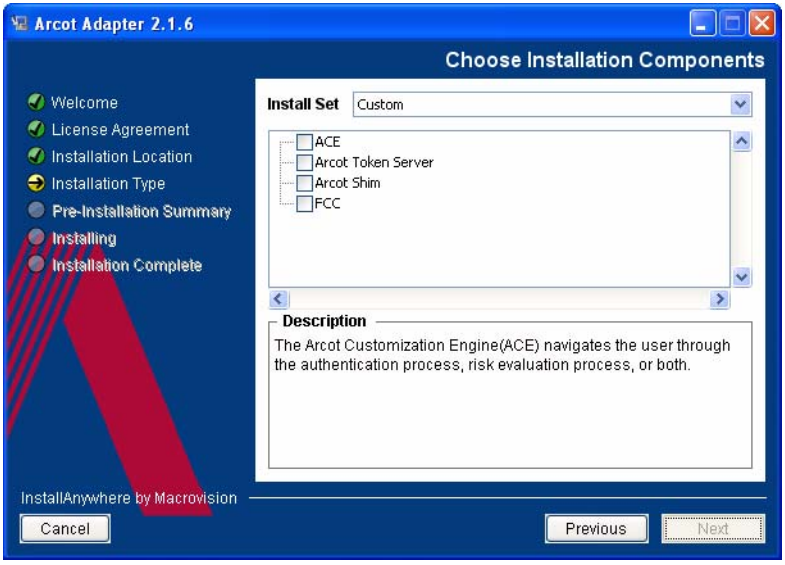
6. Ensure that the **Custom** option is selected.

   This option enables you to install only the selected components of the Adapter on the current system.

7. Click **Next** to continue.

   The Choose Installation Components screen appears (Figure 3-3).

Figure 3-3 The Choose Installation Components Screen



8. Select the **ACE** option, ensuring that all other components are deselected.

   IMPORTANT: The ACE performs the function of an authentication proxy server for the VPN integration and navigates the user through the authentication process. In this guide, the Arcot Customization Engine is also referred to as *Arcot Authentication Proxy* (AAP).

9. Click **Next** to continue.

   The Pre-Installation Summary screen appears.

   Review the information on this screen, and if you need to change a previous selection, then click **Previous** to do so. After changing the required selection, click **Next** to go to the next screen.

10. Click **Install** to begin the installation process.

    The Installing Arcot Adapter 2.1.6 screen appears. This might take several minutes.

    On successful installation, the Installation Complete screen appears.

11. Click **Done** to complete the installation.

    NOTE: If for some reason, the installation failed, then the error log is available in the same location where you ran the Installer from.

Installation Directory

The Arcot Adapter installs the files listed in the following table.

Table 3-1 Directory Structure

Location	Files
<*installation_dir*>\adapterACE	Contains the certificate files, key files, WAR, and properties files required by the Customization Engine.
<*installation_dir*>\docs	Contains the Java documents for Customization Engine API.
<*installation_dir*>\ext-license	Contains the licenses of the third-party software that are used with Adapter.
<*installation_dir*>\Uninstall Arcot Adapter 2.1.6	Contains the files required for uninstalling the Adapter.

Chapter 4

Deploying and Configuring Customization Engine

This chapter lists the tasks that you must perform to deploy and configure the Customization Engine successfully. It covers the following topics:

- Deploying Customization Engine
- Editing the Customization Engine Properties File
- Editing the Log Properties File
- Testing the Configuration

IMPORTANT: Before deploying and configuring the Customization Engine, ensure that the WebFort Server is started and running.

Deploying Customization Engine

You need the `arcotauthui.war` file to deploy the Customization Engine. This file is available at the following location:

`<installation_dir>\adapterACE\`

To deploy the ACE application:

1. Install `arcotauthui.war` on the application server. For example, on Apache Tomcat the location to install the **WAR** file is as follows:

   `<APP_SERVER_HOME>\webapps`

   NOTE: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.

2. Restart the application server.

   The application server must now contain a folder `arcotauthui`.

Editing the Customization Engine Properties File

After deploying the `arcotauthui.war` file in the application server, you must edit the Customization Engine properties file by using any of the following methods:

- Method 1
- Method 2

Method 1

Perform the following steps to edit the `arcotauthui.properties.src` file available in the folder:

```
<APP-SERVER-HOME>\webapps\arcotauthui\WEB-INF\classes\
```

> **NOTE:** The location mentioned here is specific to Apache Tomcat. If you are using other application severs, then refer to the application server vendor documentation for corresponding path.

1. Make a copy of this file in the same folder and rename it to `arcotauthui.properties`.
2. Edit the `arcotauthui.properties` file by setting only those parameters that are described in the Table 4-1.

> **IMPORTANT:** You will also find other parameters in the `arcotauthui.properties` file, however, you *do not* need to change them for the VPN integration.

Table 4-1 Customization Engine Configuration Parameters

Parameter	Description
`WebFortHostName`	Specify the Fully Qualified Distinguished Name (FQDN) or IP address of WebFort.
`WebFortPort`	Specify the port at which WebFort is available. Default value: `9742`

Table 4-1 Customization Engine Configuration Parameters

Parameter	Description
`WebFortTransport`	Specify the default protocol for WebFort to start up. Default value: `TCP` **NOTE:** It is highly recommended that Customization Engine communicates with WebFort using SSL. Refer to *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on how to configure WebFort for SSL.
`WebFortCA_CERT_FILE`	Provide the path for the CA certificate file of the server. The file *must* be in `.PEM` format. Provide the *complete path* for the file.
`WebFortMaxConnPoolSize`	Specify the maximum number of connections that can exist between the Customization Engine and WebFort. At any given instance, the number of connections cannot exceed this value. Default value: `32`

3. Restart the application server or reload the application using your application server.

Method 2

The Adapter installs `arcotauthui.properties` on the file system, you can also use this file to edit the required parameters by performing the following steps:

1. Open the `arcotauthui.properties` file, which is available in the folder:

   `<installation_location>\adapterACE\`

2. Edit the file parameters as described in Table 4-1.

3. Copy the modified `arcotauthui.properties` file at the following location within the `arcotauthui.war` file:

   `\WEB-INF\classes\`

4. Re-create `arcotauthui.war` with the edited `arcotauthui.properties` file.

5. Deploy or re-deploy the `arcotauthui.war` file in the application server.

Editing the Log Properties File

After deploying the `arcotauthui.war` file on the application server, you must edit the log properties file for the Customization Engine by using any of the following methods:

- Method 1
- Method 2

Method 1

In case of **Apache Tomcat**, perform the following steps to edit the `log4j.properties.src` file available at:

```
<APP-SERVER-HOME>\webapps\arcotauthui\WEB-INF\classes\
```

> **NOTE:** The location mentioned here is specific to Apache Tomcat. If you are using other application severs, then refer to the application server vendor documentation for corresponding path.

1. Make a copy of this file in the same folder and rename it to `log4j.properties`.
2. Edit the `log4j.properties` file to set the log information as mentioned in the following table.

Table 4-2 Log Parameters

Parameter	Description
`log4j.appender.authuiout.File`	Specify the log file name and the location where the Customization Engine logs must be written to. By default, the Customization Engine log file name is `arcotauthui.log` and is created in the *`<APP-SERVER-HOME>`*`\logs` folder.

3. Restart the application server or reload the application using your application server.

Method 2

The Adapter installs the `log4j.properties` file on the file system. You can also use this file to edit the required parameters by performing the following steps:

1. Open the `log4j.properties` file, which is available in `<installation_location>\adapterACE\`.
2. Edit the file parameters as described in Table 4-2.

3. Copy the modified `log4j.properties` file at the following location within the `arcotauthui.war` file:

   `\WEB-INF\classes\`

4. Re-create `arcotauthui.war` with the edited `log4j.properties` file.
5. Deploy or re-deploy the `arcotauthui.war` file in the application server.

Testing the Configuration

To test the Customization Engine configuration:

1. Restart the application server.
2. Open the Customization Engine log file from the location you have configured it in the `log4j.properties` file. If you have not changed the `log4j.properties` file, then it is available in the following folder:

For Apache Tomcat 5.5

`<APP_SERVER_HOME>\logs`

For Apache Tomcat 5.0.x

`C:\Windows\system32`

3. Locate the following entry, which indicates that the Customization Engine is configured successfully, in the log file:

```
InitializeTokenSvrClientServlet for Adapter ACE Frontend
version 2.1
WebFort connection test successful
```

Chapter 5

Configuring the Components

After installing the Arcot Adapter and configuring the Arcot Customization Engine (ACE), which performs the function of a proxy between the Arcot WebFort and the Arcot VPN Client, you must now configure the following components to communicate with each other:

- WebFort
- Cisco IPSec VPN appliance

This chapter walks you through the configuration of WebFort and then the configuration of the Cisco VPN IPSec appliance that enable you to integrate WebFort with your primary authentication method. This chapter covers the following sections:

Configuring WebFort

Cisco IPSec VPN uses the **Remote Authentication Dial In User Service** (**RADIUS**) protocol for centralized access, authorization, and accounting management.

To enable WebFort Server for the RADIUS protocol support, use the WebFort Administration Console, which is available at the following location, *after* you have configured WebFort *and* the WebFort Administration Console successfully:

`http://<appserver_host_name>:<port_number>/arcotadmin/adminlogin.htm`

In the preceding URL, *<appserver_host_name>* indicates the host name or the IP address of the application server where you configured the Administration Console and *<port_number>* indicates the port at which the server listens to incoming requests.

You can use the RADIUS Configuration page of the WebFort Administration Console (**Figure 5-1**) to configure RADIUS settings.

> **NOTE:** Refer to the chapter "Configuring WebFort" in the *Arcot WebFort 6.0 Administration Guide* for detailed information on the configuration process.

To configure the RADIUS protocol support for WebFort:

1. Ensure that you are logged in to the WebFort Administration Console with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the *<ORGANIZATION_NAME>* link for the required organization.

   The Organization Information page appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane.
7. Under **RADIUS**, click the **RADIUS Clients** link to display the RADIUS Configuration page (**Figure 5-1**).

Figure 5-1 The RADIUS Configuration Page

8. Provide the following information in the respective fields:

   - **RADIUS Client IP Address** - Enter the IP Address of the RADIUS client through which users authenticate to WebFort RADIUS Server.
   - **Shared Secret Key** - The secret key that is shared between the RADIUS client and the WebFort Server.

     NOTE: The minimum length of key is **1** and the maximum is **512** characters.

   - **Description** - Enter a string to describe the RADIUS client. The description helps to identify the RADIUS client, when multiple clients are configured.
   - **Authentication Type** - Select **RADIUS OTP** as the type of authentication that is used with VPNs.
   - **Maximum Packet Size (in Bytes)** - Select the appropriate packet size for RADIUS messages.

     NOTE: Refer to the *RFC 2865* for more information on the packet format.

   - **RADIUS Version** - Select the required RADIUS version.

9. Click the **Add** button to add the IP address of the new RADIUS client.

   NOTE: The RADIUS Configuration page also displays the **Existing RADIUS Clients** table, which helps to update or delete the RADIUS client IP addresses.

Configuring the Cisco IPSec VPN Appliance

You must configure the Cisco IPSec VPN appliance *after* you have successfully configured WebFort and its components. You must ensure the following while configuring your VPN:

1. Create a group for all users in the VPN Server who will be authenticated by WebFort.
2. Specify the appropriate IPSec settings for the group.
3. Add WebFort as the authentication server for this group, specifying the following information correctly:
   - **Server Type:** RADIUS
   - **Authentication Server:** IP address of the WebFort Server
   - **Used For:** User Authentication
   - **Server Port:** `<WebFort_Server_Port>`

     NOTE: The default port for WebFort Server is **`1812`**.

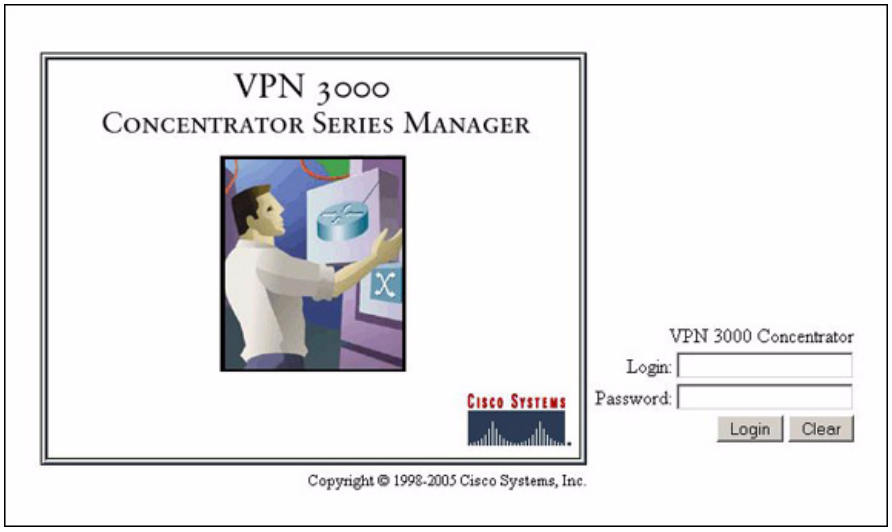
For example, the steps to configure a Cisco VPN 3000 Series Concentrator are:

1. Navigate to the following URL:

   `https://<VPN_host_name_or_IP_address>/admin.html`

   The login page (**Figure 5-2**) for the VPN Administration Console appears.

Figure 5-2 Login Screen of the Cisco IPSec VPN Administration Console



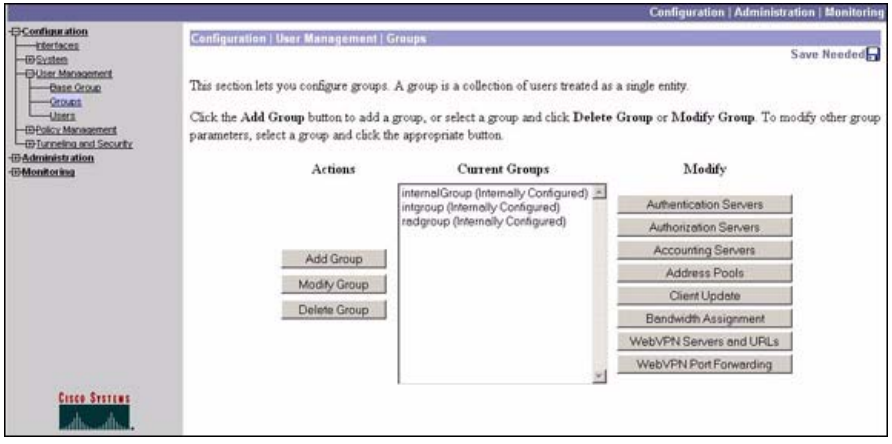
2. Log in to the Cisco IPSec VPN administrative interface.

   On successful authentication, Cisco IPSec VPN appliance displays the main menu.

3. In the left-hand pane, under **Configurations**, click the **User Management** link.

4. Click the **Groups** link to display the Groups page, as shown in Figure 5-3.

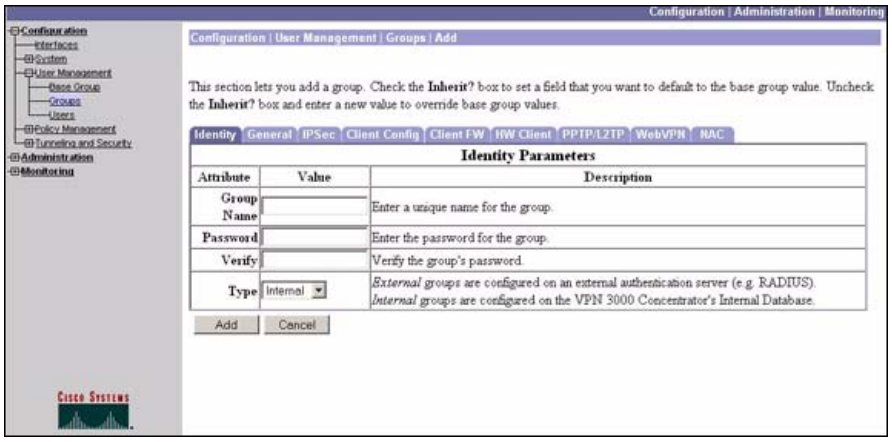
Figure 5-3 The Groups Page



5. Click the **Add Group** button to add a new group to the list of existing groups.

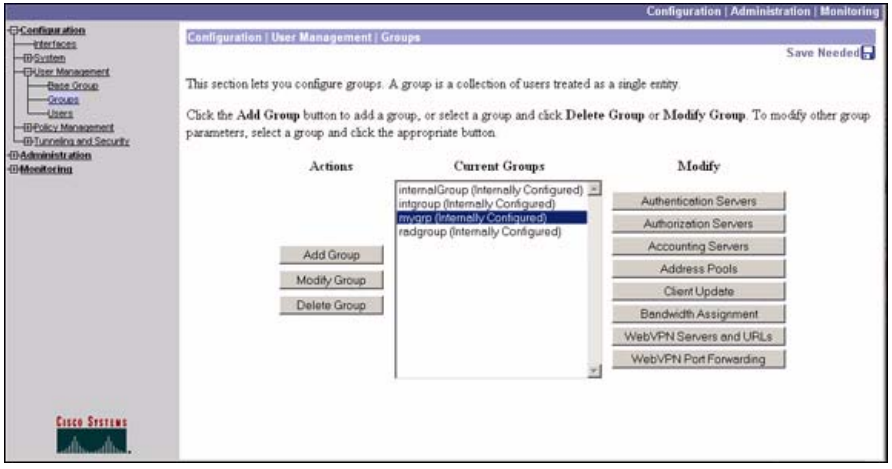
   The Add Groups page, shown in Figure 5-4, appears.

Figure 5-4 The Add Groups Page



6. Specify the appropriate information in the **Group Name**, **Password**, and **Verify** fields.
7. From the **Type** list, select **Internal**.
8. Click **Add** to add the group to the Current Groups list, as shown in Figure 5-5.

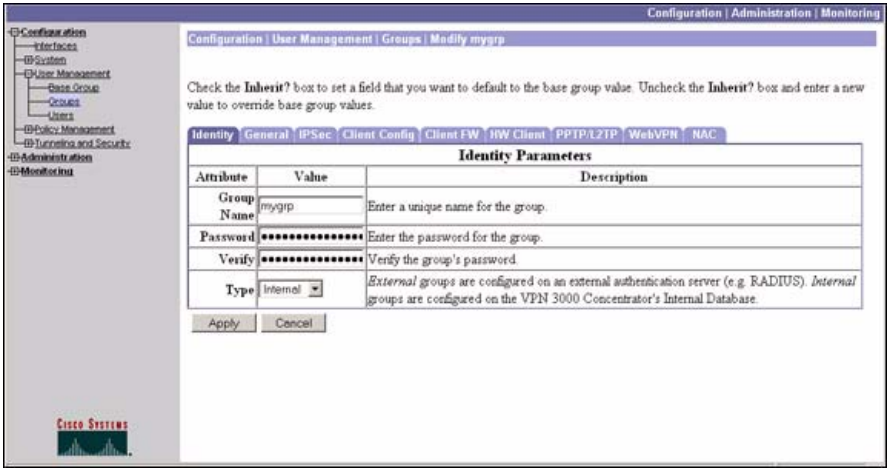
Figure 5-5 The Added Group



9. Select the group you created in the **Current Groups** list and click **Modify Group**.

   The Modify <*Group_Name*> page, as shown in Figure 5-7, appears.

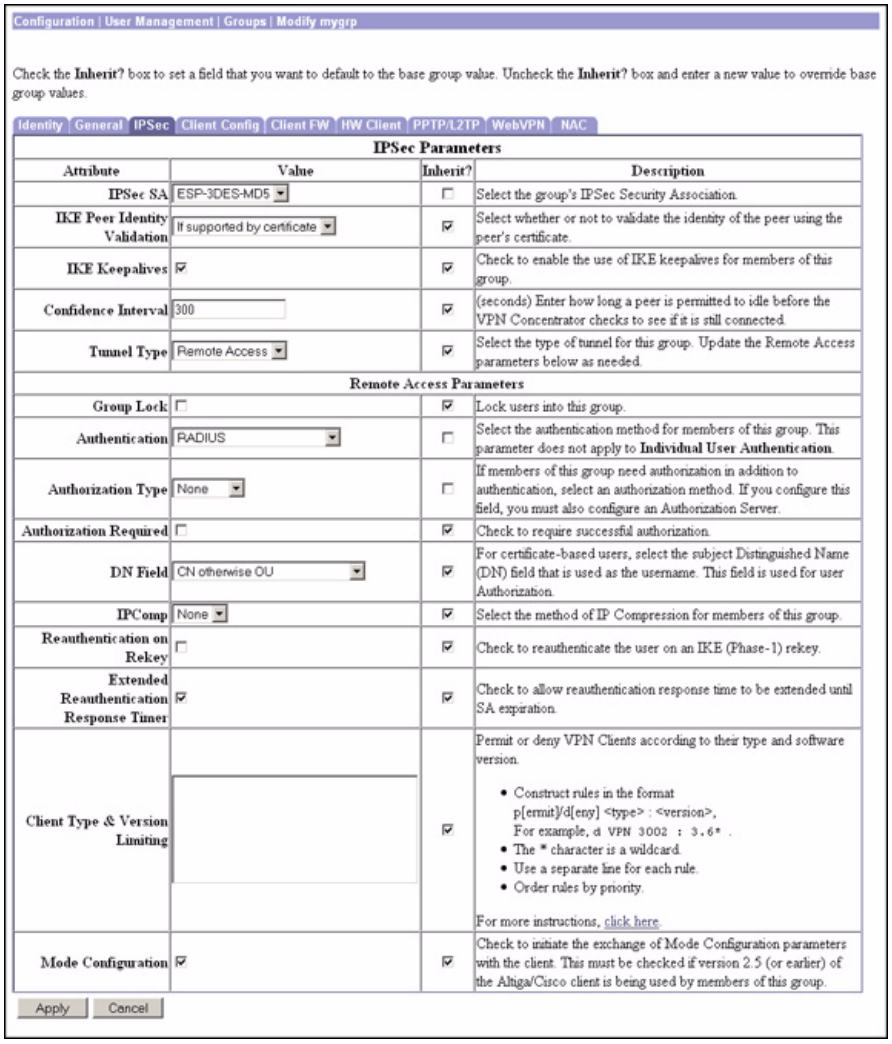
Figure 5-6 The Modify <*Group_Name*> Page



10. Activate the **IPSec** tab.

    The IPSec tab for the Modify <*Group_Name*> page, as shown in Figure 5-7, appears.

Figure 5-7 The Modify Groups Page: IPSec Tab

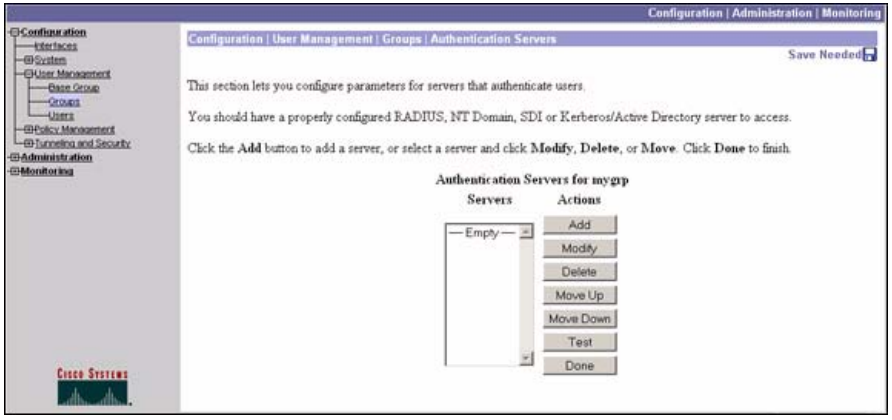


11. Specify the required configuration information in the **IPSec Parameters** section.
12. Under the **Remote Access Parameters** section, select **RADIUS** as the **Authentication Type**.
13. Specify all other configurations required for you setup.
14. Click **Apply** to modify the settings of the selected group and return to the Current Groups list.

15. From the **Current Groups** list, select the group that you just modified and click the **Authentication Servers** button (under **Modify**.)

    The Authentication Servers page, as shown in Figure 5-8, appears. This page enables you to add an authentication server (WebFort Server you configured in the preceding section, in our case) for the group.

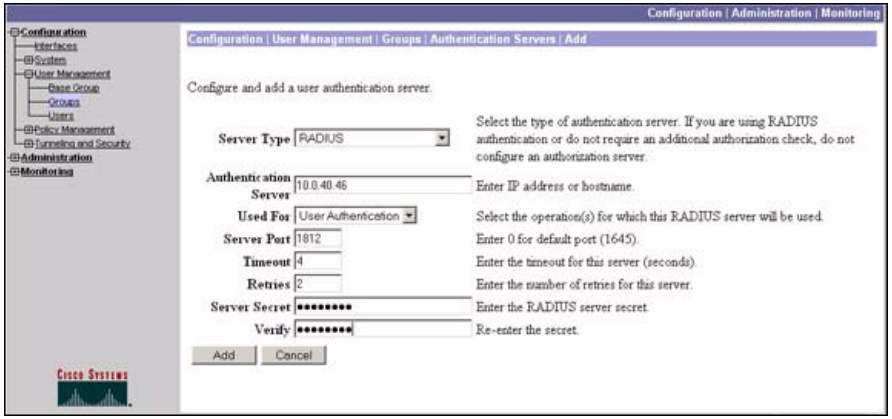
Figure 5-8 The Authentication Servers Page



16. Click **Add** to add and configure an authentication server.

    The Authentication Servers Add page, as shown in Figure 5-8, appears.

Figure 5-9 The Authentication Servers Add Page



17. Specify the required information for the authentication server. Ensure that you select:

    - **Server Type:** RADIUS

- **Authentication Server:** IP address of the WebFort Server
- **Used For:** User Authentication
- **Server Port:** `<WebFort_Server_Port>`

  NOTE: The default port for WebFort Server is **`1812`**.

18. Click **Add** to add the specified server.

    You can use the **Test** button to test the connectivity between VPN and WebFort Server. This operation throws an error in the Authentication Activity report in the WebFort Administration Console.

19. Click **Done** to complete the configuration.

You can now follow the Cisco VPN configuration documentation to create a connection profile on the client system. After you are done, you can use Arcot VPN Client to connect to the VPN.

Chapter 6

Preparing for the Arcot VPN Client Distribution

Arcot VPN Client (AVC), an end-user component of the Adapter, must be installed by the users themselves. For this, the **`Arcot-VPN-Client-1.1-Windows.zip`** package must be distributed to the users. This package contains the configuration files needed to successfully connect to an enterprise network.

Before installing the AVC, to successfully connect to your enterprise network, the user must edit settings in the **`.properties`** and **`.xml`** configuration files. To reduce user errors while editing these files, Arcot strongly recommends that the administrator modifies these files *before* distributing it to the users. This chapter covers the following topics:

- Exploring the Package
- Editing arcotvpnclient.properties File
- Editing arcotvpnclienterrors.properties File
- Editing avcstrings.properties File
- Editing CopyFiles.xml File
- Configuring AVC for Silent Installation

Exploring the Package

The **`Arcot-VPN-Client-1.1-Windows.zip`** package comprises the AVC installer (**`Arcot-VPN-Client-1.1-Windows-Installer.exe`**) and the **`resources`** folder, which contains:

- The `arcotvpnclient.properties` file, which is used to specify the mapping between the Cisco and Arcot Authentication Proxy (AAP) profiles, proxy server settings, and location of image files used in the AVC user interface.
- The `properties` subfolder that contains the following files:
  - `arcotvpnclienterrors.properties`
  - `avcstrings.properties`

  These properties files can be used to customize the error messages and the names of the screen elements used in the AVC user interface.
- The `images` subfolder, which contains the images that are used in the AVC user interface. These images can be customized by replacing them with the new images. While replacing these images, ensure that the new image file name, format, and dimensions matches that of the original image.

  NOTE: The placement of these custom or new images is controlled by the ACE using the corresponding Controller. In this folder, the `arcot_logo.gif` file is used to store the Arcot Logo and `vpnsplashscreen.png` file contains the splash screen image.For information on the other files found in this folder, refer to the topic "**Arcot VPN Client Images Location**" in the **"Editing arcotvpnclient.properties File"** section.
- The `screens` subfolder that contains three XML files, which are used for rendering the AVC user interface.
- The `add-ons` folder that contains the `CopyFiles.xml` file, which can be used for specifying the add-on files that needs to be copied on the end-user's system.

The following sections describe the contents of these configuration files and the way these files can be customized as per your requirements.

NOTE: In the following sections, wherever you need make a change in the default configuration value, you must first uncomment the respective parameter by removing "#" from the beginning of the parameter entry.

Editing arcotvpnclient.properties File

The `arcotvpnclient.properties` file specifies:

- The Default and Failover URLs to connect to the Arcot Customization Engine (ACE), which is also referred to as the Arcot Authentication Proxy (AAP).
- The mapping between the Cisco VPN Profile and the AAP.
- The network timeout settings to specify the connection and read timeout.
- The network proxy server settings.
- The VPN client commands that are used to connect, disconnect, and refresh a connection with the VPN server.
- The connection status messages.
- The location of the image files used in the VPN client user interface.

The following snippet provides the content of a sample configuration file.

```
-----------------------------------------------------------------
############# Base VPN Client Profile to AAP URL mapping ###############
#
# Mapping Format
#aap.profile.serverurl.mapping.<profilename>=<primaryAAPurl>,<failoverS
erver1url>,<failoverServer2url>
#
# Examples : -
# AAP mapping for profile named 'ProfileA'
#aap.profile.serverurl.mapping.ProfileA=https://primaryAAP/arcotauthui/
vpn/controller_vpn.jsp,https://failoverAAP/arcotauthui/vpn/controller_v
pn.jsp
#
# The 'Default' AAP url for profiles that are not mapped to any AAP. A
# required property.
#aap.default.serverurl=https://defaultPrimaryAAP/arcotauthui/vpn/contro
ller_vpn.jsp,https://defaultFailoverAAP/arcotauthui/vpn/controller_vpn.
jsp
#
#################################################################################
################### Network Timeouts ###################################
#
# Connection timeout can be specified as follows : -
# vpnclient.connection.timeout=30000
#
# Read timeout can be specified as follows : -
# vpnclient.read.timeout=30000
#
```

```
# The timeouts are in milliseconds. They will default to 30000
# milliseconds each.
#
#############################################################################

######################### Network proxy settings ########################
#
# If the user is accessing authentication server through a proxy server
# following properties are required.
#
#
# proxyHost=<proxyServerHostName>
# proxyPort=80
#
# The following property specifies whether user needs to be
# authenticated to proxy server or not. If authentication is required at
# proxy server uncomment it.
#
# proxyAuthenticationRequired=true
#
# Proxy username and password should never be commented.Proxy username
# and password has to be stored in base64 encoded format. Proxy username
# and password shouldnot be edited manually.
#
  proxyUser=dXNlcm5hbWU=
  proxyPassword=cGFzc3dvcmQ=
#
#############################################################################

################### Base VPN Client commands ##########################
#
# Examples for windows : -
# Command for vpn connection. A required property.
# Note : -
# The {base.vpn.client.directory} variable will be substituted by Base
# VPN Client install
# location, during Arcot VPN Client installation.
# vpnclient.connect.command={base.vpn.client.directory}\\vpngui.exe -sc
-user "#username#" -pwd "#password#" "#profile#"
#
# Command to be executed before executing vpn connect command. An
# optional property.
# vpnclient.preconnect.command=
#
# Command to be executed after successful vpn connection. An optional
# property.
# vpnclient.postconnect.command=
#
# Command for checking status of connection. A required property.
# vpn.cmd.check.status={base.vpn.client.directory}\\vpnclient.exe stat
# traffic
#
```

```
# Command to disconnect. A required property.
# vpn.cmd.disconnect={base.vpn.client.directory}\\vpnclient.exe
# disconnect
#
#########################################################################

########### Messages to be checked for connection status ###############
#
# Message to check for disconnected status. Use ';' to specify multiple
# values. A required property.
# line.to.grep.for.notconnected=No connection exists.;Your VPN
# Connection is not active.
#
# Message to check for connected status. Use ';' to specify multiple
# values. A required property.
# line.to.grep.for.connected=Time connected
#
#########################################################################

####################### Arcot VPN Client images locations #############
#
# Arcot VPN Client window title bar image location.
image.appicon=images/appicon.gif
#
# System Tray image, when in connected state.
image.connected=images/ArcotTrayIconC.gif
#
# System Tray image, when in disconnected state.
image.disconnected=images/ArcotTrayIconDC.gif
#
#########################################################################
######## PLEASE DO NOT EDIT ANYTHING BELOW THIS LINE ########

##### Base VPN Client profile file extension #####
profile.file.extention=.pcf
################################################
################## System Tray Properties ########################
### System Tray Items ###
systray.action.disconnect=Disconnect
systray.action.connect=Connect
systray.action.exit=Exit
systray.action.refresh=Refresh

### System Tray Messages ###
systray.tooltip.status.connect.message=Arcot VPN Client\nStatus :
Connected
systray.tooltip.status.disconnect.message=Arcot VPN Client\nStatus :
Disconnected
systray.invoke.status.connect.message=Connected to VPN.
systray.message.head=Arcot VPN Client
#################################################################
-----------------------------------------------------------------
```

The configurable parameters found in the `arcotvpnclient.properties` file are explained below:

- **Base VPN Client Profile to AAP URL mapping:** In this section, you need to configure the following parameters:
  - **Cisco Profile to AAP Mapping:** The Cisco client supports multiple VPN server connections. The connection details are stored as a VPN Profile at the client-end, with one profile representing one VPN server.

    In the file, uncomment the **`aap.profile.serverurl.mapping.Profile<`*`name`*`>`** entry and specify the mapping.

    NOTE: You can create as many profile-to-AAP mapping sections in the file, as required.

    IMPORTANT: If the **`Profile<name>`** contains any white space characters, then the profile mapping can be specified by escaping the white space characters with backslash "**`\`**". For example, if the profile name is "**`profile 1`**", then the profile mapping entry should be specified as **`app.profile.serverurl.mapping.profile\ 1= <Server_URL>`**.
  - **Default AAP (`aap.default.server.url`) (*required*):** This ACE URL is used for the profiles that are *not* mapped to any AAP.

    In the file, uncomment the **`aap.default.serverurl`** entry and specify the ACE URL.

    TIP: While specifying AAP mapping or URL in the preceding cases, multiple comma-separated AAPs can be specified using the following format: *`<primaryAAPurl>,<failoverServer1url>,<failoverServer2url>`*
- **Network Timeouts:** In this section you can define the Arcot VPN Client connection timeout and read timeout values. These configurable parameters are defined below:
  - **Arcot VPN Client Connection Timeout:** The connection timeout parameter is used to specify the time interval (in milliseconds) for which the client waits for the server's response to a new connection request. If the client receives a valid response from the server within the specified time frame, the connection is established else the client terminates the connection request.

    By default, this parameter is set to `60000` milliseconds (`1` minute). In the file, uncomment the **`vpnclient.connection.timeout`** entry and specify the required time interval.

- **Arcot VPN Client Read Timeout:** In case of a successful client-server connection, the client read timeout parameter specifies the time interval (in milliseconds) for which the client waits for the server's response to a request sent by the client. If the server fails to respond back in the specified time frame, then the connection with the server is dropped.

  By default, this parameter is set to `60000` milliseconds (`1` minute). In the file, uncomment the **`vpnclient.read.timeout`** entry and specify the required time interval.

- **Network Proxy Settings:** In case the end user accesses your enterprise network through a proxy, then the following parameters need to be configured. In the file, uncomment the following entries and specify the appropriate values:

  - **proxyHost**: Specify the proxy server host name.
  - **proxyPort**: Specify the proxy server port.
  - **proxyAuthenticationRequired**: This parameter specifies whether a user needs to authenticate with the proxy server or not. By default, it is commented, which indicates that no proxy server authentication is needed to establish a connection with the VPN server. If proxy server authentication is needed, then you need to uncomment this parameter in the properties file and ensure that it is set to `true`.

    IMPORTANT: The **proxyUser** and **proxyPassword** parameters are used to store the user name and password required to authenticate to the proxy server. As the value of these parameters is set using the Arcot VPN Client's user interface, you *must not* set them manually.

- **Base VPN Client Commands:** In this section you need to specify the VPN client commands that are used to establish a connection with the VPN server, check the connection status, and command to disconnect from the VPN server. In addition, you can also specify the pre- and post-connection commands, if applicable. The following parameters *need* to be specified in this section:

  - **vpnclient.connect.command** (***required***)**:** Specifies the command to establish a connection with the VPN sever. The default value of this parameter is:

    ```
    vpnclient.connect.command={base.vpn.client.directory}\\
    vpngui.exe -sc -user "#username#" -pwd "#password#"
    "#profile#"
    ```

    NOTE: The **`{base.vpn.client.directory}`**, **`#username#`**, **`#password#`**, and **`#profile#`** parameters are automatically replaced by the VPN client with the actual corresponding values, therefore they *need not* be changed. However, the actual command to connect with the VPN server, **`vpngui.exe`**, can be changed, if required.

- **vpn.cmd.check.status** (*required*)**:** Specifies the command to update the connection status. The default value of this parameter is:

  ```
  vpn.cmd.check.status={base.vpn.client.directory}\\
  vpnclient.exe stat traffic
  ```

  NOTE: In the preceding command, the **vpnclient.exe stat traffic** can be replaced with the actual command, if required.

- **vpn.cmd.disconnect** (*required*)**:** Specifies the command to disconnect an active VPN server connection. The default value of this parameter is:

  ```
  vpn.cmd.disconnect={base.vpn.client.directory}\\
  vpnclient.exe disconnect
  ```

  NOTE: In the proceeding command, the **vpnclient.exe disconnect** can be replaced with the actual command, if required.

- **vpnclient.preconnect.command:** Specifies any command that needs to be executed before establishing a connection with the VPN server.

- **vpnclient.postconnect.command:** Specifies any command that needs to be executed after a connection with the VPN server has been established.

- **Messages to be Checked for Connection Status:** This section defines the connection status messages that are read by the VPN client to determine whether the application is connected with the VPN server or not. These connection status messages are a part of the return value of the VPN connection status check command, which is defined in the **vpn.cmd.check.status** parameter. This section includes the following two parameters:

  - **line.to.grep.for.notconnected** (*required*)**:** Specifies the messages that can be returned by the status check command in case of no active connection. The default value of this parameter is:

    ```
    line.to.grep.for.notconnected=No connection exists.;Your
    VPN Connection is not active.
    ```

    NOTE: You can specify multiple messages by separating them with a semicolon (;).

  - **line.to.grep.for.connected** (*required*)**:** Specifies the messages that can be returned by the status check command in case an active connection is found. The default value of this parameter is:

    ```
    line.to.grep.for.connected=Time connected
    ```

- **Arcot VPN Client Images Location**: This section specifies the location of image files used in the AVC user interface. You can replace these images with your own by specifying the path of the image files to be used. This section includes the following parameters:
  - **image.appicon** (***required***)**:** Specifies location of the image used in the title bar of the AVC user interface. By default, it shows the Arcot Logo (**`appicon.gif`**).
  - **image.connected** (***required***)**:** Specifies location of the status bar image used to show an active connection. By default, it is set to display the Arcot Logo with green background color (**`ArcotTrayIconC.gif`**).
  - **image.disconnected** (***required***)**:** Specifies location of the status bar image used to show an inactive connection. By default, it is set to display the Arcot Logo with red background color (**`ArcotTrayIconDC.gif`**).

Editing arcotvpnclienterrors.properties File

The `arcotvpnclienterrors.properties` file specifies the error messages that are displayed to the user in case of any error generated in the AVC. The following snippet provides the content of a sample configuration file.

```
-----------------------------------------------------------------
##### Client side error messages #####
# This file contains error messages that are used by screens on the
# client system.
# If you want to build up locale-specific support, you need to create
# arcotvpnclienterrors_<language>_<country>.properties inside this
# folder.
########################################

profilenotfound=No existing vpn profile found.
defaultaapurlnotfound=Default AAP URL is absent. Please contact
administrator.
required.property.missing=Required property is missing. Please contact
administrator.

# error messages for server communication failures
allaapserversdown=All servers are down. Please try after some time.
communicationfailure=Communication failure, please try again.
communicationproblem=Communication problem, please try again.
vpnconnectfailed=Unable to connect to vpn, please try again.
internalerror=Internal error, please contact administrator.
proxyserverauthfailure=Proxy server authentication failed.
proxydetailsincomplete=Username field is required.
proxyserverconfigurationerror=Invalid proxy server configuration.
Please contact administrator.

# error message on failure to launch browser
browserFailed=The browser failed to launch.

# error message when communication with current server fails in
# middle of a flow, and the client restarts the flow
failovererror=Communication with server failed. Please retry.

# Error message when tried to launc application when one instance is
# running
applicationalreadyrunning=Another instance of application is already
running. Exit already running instance to relaunch.

# Error while parsing error xml
error.parsing.errorxml= Internal error in parsing XML. Please contact
administrator.
-----------------------------------------------------------------
```

The `arcotvpnclienterrors.properties` file uses the following parameter name-value pattern:

```
<ParameterName>=<Value>
```

You can customize an error message by modifying the **`Value`** field of the respective parameter. However, you *must not change* the **`ParameterName`**.

Editing avcstrings.properties File

The `avcstrings.properties` file is used to customize the following screen elements of the AVC user interface:

- The version and copyright information.
- The application title.
- The application's menu names, fields, action button names and their shortcut keys.
- The label for selecting profile.
- The system tray messages.

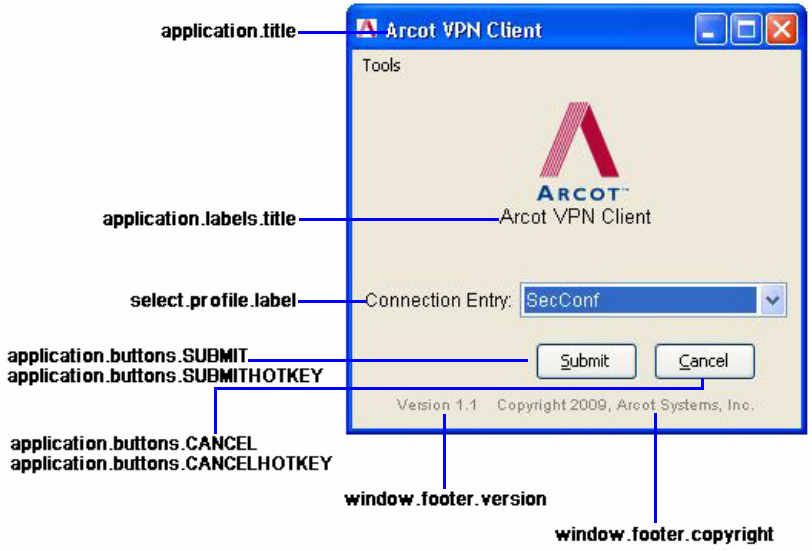
The following snippet provides the content of a sample configuration file.

```
-----------------------------------------------------------------
##### Client side screen messages #####
# This file contains messages that are used by screens on the client
# system.
# If you want to build up locale-specific support, you need to create
# avcstrings_<language>_<country>.properties inside this folder.
########################################

# Version and copyright information
window.footer.version=Version 1.1
window.footer.copyright=Copyright 2009, Arcot Systems, Inc.

# Window title
application.title=Arcot VPN Client

# Title displayed inside client body
application.labels.title=Arcot VPN Client

# Field names
proxysettings.form.USERNAME=Username:
proxysettings.form.PASSWORD=Password:
proxysettings.radio.PROXY_ENABLE=Proxy
proxysettings.radio.PROXY_DISABLE=Direct Connection
proxysettings.checkbox.AUTHENTICATE=Authenticate
#buttons used in screens together with hokeys (shortcuts) to invoke them
application.buttons.OK=OK
application.buttons.OKHOTKEY=O
application.buttons.SUBMIT=Submit
application.buttons.SUBMITHOTKEY=S
application.buttons.CANCEL=Cancel
application.buttons.CANCELHOTKEY=C

# select profile dropdown box in case of profile url mappings
```

```
select.profile.label=Connection Entry:

# Menu names.
tools.menu=Tools
tools.menuitem.enableproxysettings=Enable Proxy
tools.menuitem.changeproxysettings=Proxy Settings

# Proxy setting window instruction
proxy.settings.instruction=Please Configure proxy details.

# system tray messages
systray.connected=Connected to VPN.
systray.disconnected=Disconnected from VPN.
-----------------------------------------------------------------
```

Figure 6-1 shows the screen elements and their corresponding properties that are used to customize them.

Figure 6-1 Customizable Elements of the AVC



NOTE: The `application.buttons.OK` and `application.buttons.OKHOTKEY` properties are applicable only for the error message dialog box, therefore they are not shown in Figure 6-1.

Editing CopyFiles.xml File

The AVC installer can copy extra files that might be required by the VPN client application to work successfully. These files could include the profile configuration or other system files that might be required for successfully running the VPN client.

The `CopyFiles.xml` file is used to specify the location where these extra files need to be copied on the end-user's system. To distribute these extra files with the VPN client installer, perform the following tasks:

1. Copy the files that need to be distributed with the installer in the `\resources\add-ons` folder.
2. In the `CopyFiles.xml` file, specify the location on the end-user's system where these files need to be copied.

The following snippet provides the content of a sample `CopyFiles.xml` file.

```
-----------------------------------------------------------------
...
<Install>
        <OS name="windows">
        <PostInstall>
        <COPY
to_location="$VPN_CLIENT_INSTALL_LOCATION$+$/$"from_location="$EXTRACTO
R_DIR$+$/$+resources+$/$+add-ons+$/$" type="directory">
        <!-- E.g.
           <Object name="Directory Name"/>
        -->
        </COPY>
        <COPY
to_location="$VPN_CLIENT_INSTALL_LOCATION$+$/$"from_location="$EXTRACTO
R_DIR$+$/$+resources+$/$+add-ons+$/$" type="file">
        <!-- E.g.
           <Object name="File Name"/>
        -->
        </COPY>
        </PostInstall>
        </OS>
</Install>
-----------------------------------------------------------------
```

The following table describes the XML tags and the variable names that are used in the `CopyFiles.xml` file:

Table 6-1 Configurable Elements of the CopyFiles.xml File

Element	Description
`to_location`	Specifies the path where the add-on files need to be copied.
`$VPN_CLIENT_INSTALL_LOCATION$+$/$`	This variable contains the location of the VPN client installed on the end-user's system. Typically, this variable should not be changed. However, if you want to store the add-on files on a location other than the VPN client installer, then replace this variable with the required location (say "`c:\Program Files\Profiles`").
`from_location`	Specifies the path from where the add-on files need to be picked up for copying. By default, this is set to the `add-ons` folder that is extracted from the AVC zip file.
`$EXTRACTOR_DIR$+$/$+resources+$/$+add-ons+$/$`	This variable contains the location of the `add-ons` folder that is extracted from the AVC zip file.
`type`	Specifies the type of object being copied. It can be assigned one of the following values: • **directory**: the object that needs to be copied is a directory. • **file**: the object that needs to be copied is a file.
`Object name`	Specifies the name of the object (directory name or filename) that needs to be copied.

After editing the required **`.properties`** and **.xml** files, save them and replace the modified files (shipped by Arcot) in the respective `resources` folder. Re-create the package, which is now ready for distribution to your end users.

Configuring AVC for Silent Installation

The AVC installer can be customized to run in the *Silent Mode*, which does not require any user interaction to install the application. As an administrator, you record the response to the information required by the installer in a separate file and ship this response file along with the installer. After you have created the response file, all that is required to complete the installation process is to double-click on the installer executable file.

To prepare the AVC installer to run in the silent mode, perform the following steps:

1. Modify all configuration files (**`.properties`** and **`.xml`**) as explained in the preceding sections.
2. Create the response file by running the installer from the DOS prompt. Execute the following command to run the installer:

   ```
   <VPN_Client_Installer_Location>\Arcot-VPN-Client-1.1-Windows
   -Installer.exe -r
   "<VPN_Client_Installer_Location>\installer.properties"
   ```

   Executing this command would start the VPN Client installation process. You need to complete the installation process by providing the information required by the installer. The response you provide during the installation process is stored in the **`installer.properties`** file.
3. Open the **`installer.properties`** file in a text editor and add the following two properties at the end of the file:

   ```
   INSTALLER_UI=silent

   USER_INSTALL_DIR=C:\\Program Files\\Arcot Systems
   ```

   Save and close the **`installer.properties`** file.
4. Re-create the final installation package along with the response file, **`installer.properties`**.

   NOTE: Before repackaging, ensure that the `Arcot-VPN-Client-1.1-Windows-Installer.exe` and `installer.properties` files are stored in the same location.

Additional Notes on the Silent Mode

- To install the VPN Client in silent mode, you need to double-click the `Arcot-VPN-Client-1.1-Windows-Installer.exe`. The installer runs as a background process without requiring any user interaction. To verify whether the installation process has completed successfully, look for the folder `Arcot Systems` within the `Program Files` folder on your system.
- If the installer has been configured to run in the silent mode, then the installation and uninstallation processes would not display any interactive dialogs while running.

Chapter 7

Uninstalling Arcot Adapter Components

The steps to uninstall Arcot Adapter include:

- **Uninstalling Arcot Adapter**
- **Post-Uninstallation Steps**

Uninstalling Arcot Adapter

To uninstall Arcot Adapter, you need to remove the packages shipped with Arcot Adapter.

To uninstall Arcot Adapter:

1. Navigate to the following directory:

   `<installation_dir>\Uninstall Arcot Adapter 2.1.6`

2. Double-click the **`Uninstall Arcot Adapter 2.1.6.exe`** file.

   The Uninstall Options screen appears.

3. Select **Complete Uninstall** to uninstall all components of Arcot Adapter and go to Step 5.

   To uninstall only the selected components of the Adapter, select **Uninstall Specific Features** and click the **Next** button.

   The Choose Product Features screen appears.

4. (**For Uninstalling Specific Components Only**) This screen displays all the Arcot Adapter components that are installed on the current system. Select the components that you wish to uninstall and click the **Next** button.

   The Uninstallation Complete screen appears at the end of successful uninstallation.

5. Click **Done** to exit the wizard.

Post-Uninstallation Steps

Perform the following post-uninstallation steps:

1. Delete the installation directory (<*installation_dir*>).

   NOTE: If multiple Arcot products are installed on this system, then delete this folder *only if* Arcot Adapter is the last product to be uninstalled.

2. Uninstall the `arcotauthui.war` file (WAR files for Customization Engine) from the <*APP-SERVER-ROOT*>.

   Here, `APP-SERVER-ROOT` represents the directory path used by your application server.

   NOTE: If you have performed distributed-system deployment, then locate the **WAR** files on the system where you have deployed the particular component.

Appendix A

Third-Party Software Licenses

This appendix lists the third-party software packages that are used by Adapter. These include:

Apache

- The Apache Software License, Version 1.1. Copyright (c) 2000 The Apache Software Foundation. All rights reserved.
  - `log4j-1.2.9.jar`
- Copyright © 2009 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.
  - `commons-codec-1.3.jar`
  - `commons-collections-3.1.jar`
  - `commons-httpclient-3.1.jar`
  - `commons-lang-2.4.jar`
  - `commons-pool-1.4.jar`
  - `ibatis-2.3.0.677.jar`

json-lib-0.7.1.jar

Copyright (c) 2002 JSON.org

Json2.js

Copyright (c) 2002 JSON.org

Microsoft SQL Server 2005 JDBC Driver (sqljdbc.jar)

Copyright © 1993-2008 Microsoft Corporation. All rights reserved.

msvcp80.dll

msvcr80.dll

Oracle Database 10*g* JDBC Driver

SWFObject

Appendix B

Glossary

ArcotID	Is a secure software credential that supports two-factor authentication. To authenticate to WebFort using ArcotID, the user needs the ArcotID file and the associated password.
Arcot Adapter	Arcot product that increases the security of Web resources that are protected by the Cisco IPSec VPN.
Customization Engine	Component of Arcot Adapter that interacts with WebFort to authenticate the user.
Primary authentication	The authentication mechanism used for the primary or main authentication of users. If only one authentication mechanism is used, then it is the primary authentication mechanism.
Question and Answer	Type of authentication method supported by WebFort. In this method, the user sets questions and answers during enrollment. The user has to answer these security questions during authentication.
Roaming Download	The process of downloading ArcotID on multiple systems from the WebFort Server.
WebFort	WebFort provides two-factor software-based strong authentication.