# Table of Contents

## Chapter 1
**Introduction** .......................................................................................... 1
Features of Your Aventail Appliance .......................................................... 2
   Administrator Components ........................................................................ 2
   User Components ...................................................................................... 3
What’s New in This Release ........................................................................... 6
   User Interface Changes in This Release .................................................... 7
About the Documentation .............................................................................. 8
   Document Conventions ............................................................................ 8

## Chapter 2
**Installation and Initial Setup** ................................................................. 9
Network Architecture .................................................................................... 9
Preparing for the Installation ...................................................................... 10
   Deployment Checklist ............................................................................... 10
   Verifying Your Firewall Policies .............................................................. 11
   Helpful Management Tools ...................................................................... 12
Installation and Deployment Process .......................................................... 12
   Installation and Configuration Overview ............................................... 13
   Moving the Appliance Into Production ................................................... 14
Installing the Appliance ............................................................................. 15
   Rack Installation ...................................................................................... 15
Front Panel Controls and Indicators .......................................................... 16
Connecting the Appliance ......................................................................... 17
   Powering Up ............................................................................................ 17
   Powering Down and Rebooting the Appliance ....................................... 17
Performing Initial Network Setup .............................................................. 18
   Tips for Working with Setup Tool .......................................................... 18
   Running Setup Tool ................................................................................. 18
Next Steps .................................................................................................... 19

## Chapter 3
**Working with AMC** ............................................................................... 21
Accessing AMC ............................................................................................ 21
   Logging In to AMC ................................................................................. 21
   Logging Out ............................................................................................. 22
AMC Basics .................................................................................................. 22
   A Quick Tour of the AMC Interface ....................................................... 22
   Getting Help ............................................................................................ 24
Administrator Accounts .............................................................................. 24
   Managing Administrator Accounts ......................................................... 25
   Avoiding Configuration File Conflicts with Multiple Administrators .... 26
Working with Configuration Data ............................................................... 27
   Saving Configuration Changes to Disk ................................................... 27
   Applying Configuration Changes ........................................................... 27
Deleting Referenced Objects ...................................................................... 29

## Chapter 4
**Network and Authentication Configuration** ......................................... 31
Configuring Basic Network Settings ......................................................... 31
   Specifying System Identity .................................................................... 31
   Configuring Network Interfaces ............................................................. 32
   Configuring IP Routes ............................................................................ 33
Configuring Name Resolution .................................................................... 36
Configuring SSL Certificates .................................................................... 38
   Overview: SSL Certificates .................................................................... 38
   Using a Self-Signed Certificate ............................................................... 38
   Obtaining a Certificate from a Commercial CA ................................... 41
Chapter 8
System Administration ........................................... 121
- Optional Network Configuration ........................................... 121
  - Enabling SSH Access from Remote Hosts ... 121
  - Enabling ICMP .......................................................... 121
  - Configuring the Time Settings ........................................ 123
- System Logging and Monitoring ............................... 124
  - Overview: System Logging and Monitoring ............... 124
  - Log File Formats ...................................................... 124
  - Message Log ............................................................... 125
  - Client/Server Access Log ............................................ 129
  - Web Access Log .......................................................... 130
  - Viewing Logs .............................................................. 132
  - Configuring Log Settings ............................................ 133
  - Log File Locations ....................................................... 134
  - Monitoring the Appliance ............................................ 135
  - Monitoring Active Users .......................................... 136
  - SNMP Configuration ...................................................... 137
- Backup, Restore, and System Update ............... 143
  - Backing Up and Restoring Configuration Files ........... 144
  - Patching, Upgrading, Rolling Back, and Resetting the System ............... 151
- Managing the Aventail Services ....................... 155
  - Stopping and Starting the Aventail Services ............. 155
  - Configuring the Aventail Services ................. 155
- SSL Encryption .......................................................... 159
  - Configuring SSL Encryption .................................... 159
- Software Licenses ...................................................... 160
  - Viewing License Details ......................................... 161
  - Managing Licenses ..................................................... 161

Chapter 9
End Point Control ...................................................... 163
- Overview: End Point Control ........................................... 163
  - How the Appliance Uses Zones and Device Profiles for End Point Control ............................... 164
  - End Point Control Scenarios ........................................ 165
- Managing EPC with Zones and Device Profiles ........... 167
  - Enabling and Disabling End Point Control ............... 168
  - Viewing Zones and Device Profiles ......................... 168
  - Defining a Zone ......................................................... 169
  - Creating Zones for Special Situations ...................... 173
- Removing Data Left On the Client ............................. 176
  - Configuring Aventail Cache Control ....................... 177
  - Aventail Secure Desktop .......................................... 178
  - Sygate On-Demand ..................................................... 180
  - Validating Client Integrity ...................................... 181

Chapter 10
Configuring User Access Components ..................... 183
- Aventail ASAP WorkPlace ........................................... 183
  - A Quick Tour of ASAP WorkPlace ......................... 183
  - User Access Agents .................................................. 186
Chapter 11

Installing and Administering a Cluster ................................................................. 215

Overview: An Aventail Cluster .............................................................................. 215
Cluster Architecture ............................................................................................... 215
The Load Balancing Service ................................................................................... 216
Stateful Failover ...................................................................................................... 216
Synchronized Cluster Administration ...................................................................... 217

Installing and Configuring a Cluster ................................................................. 217
Step 1: Connect the Cluster Network ..................................................................... 218
Step 2: Run Setup Tool on Both Nodes of the Cluster ........................................... 218
Step 3: Assign the Master Node ............................................................................ 220
Step 4: Configure the Cluster’s Virtual IP Address .............................................. 220
Step 5: Perform the Remaining Configuration Tasks ............................................ 221
Step 6: Configure the Managed Switch Connection (if applicable) ................. 221

Managing the Cluster ............................................................................................. 222
Viewing and Configuring Network Information for Each Node ................. 222
Powering up a Cluster ............................................................................................ 223
Starting and Stopping Services ............................................................................ 223
Monitoring a Cluster ................................................................................................ 224
Backing up a Cluster ............................................................................................... 224
Performing Maintenance on a Cluster ................................................................. 224
Upgrading a Cluster ............................................................................................... 224
Upgrading a Single Appliance to a Cluster Configuration ............................. 225
Troubleshooting a Cluster ..................................................................................... 226

Cluster Scenarios .................................................................................................... 226
Normal Flow of Traffic ......................................................................................... 226
Node Failure ........................................................................................................... 227

Appendix A

Troubleshooting .................................................................................................... 229
General Networking Issues .................................................................................. 229
AMC Issues ............................................................................................................. 230
Authentication Issues ............................................................................................ 230
Aventail Services .................................................................................................... 230
Aventail OnDemand Issues .................................................................................. 231
General OnDemand Issues .................................................................................. 231
Specific OnDemand Issues .................................................................................... 233
Troubleshooting Tools in AMC ............................................................................. 234
Ping Command ...................................................................................................... 234
Traceroute Command ............................................................................................. 234
DNS Lookup ........................................................................................................... 235
Viewing the Current Routing Table ...................................................................... 236
UNIX Command Reference .................................................................................... 236
Appendix B
Best Practices for Securing the Appliance ......................................................... 239
Network Configuration ....................................................................................... 239
Appliance Configuration ..................................................................................... 240
Administrator Accounts ..................................................................................... 240
Access Policy ..................................................................................................... 240
SSL Ciphers ....................................................................................................... 241
Client Access ..................................................................................................... 241

Glossary ........................................................................................................ 243

Index ................................................................................................................... 251
Chapter 1
Introduction

The Aventail SSL VPN appliance provides secure access—including clientless access to Web applications, access to client/server applications, and file sharing—to employees, business partners, and customers. All traffic is encrypted using Secure Sockets Layer (SSL) to protect it from unauthorized users.

The Aventail appliance makes applications available from a range of access methods— including a standard Web browser, a Java applet, or a Windows client—on a wide range of platforms including Windows, Macintosh, and Linux. You might use the appliance to:

- Create a remote access VPN that enables remote employees to securely access private company applications such as e-mail over the Internet.
- Create a business partner VPN that provides designated suppliers with access to an internal supply chain application over the Internet.

The appliance’s granular access control enables you to define policy and control access down to the user and resource level. To increase efficiency, the appliance is managed from a Web-based management console. This enables you to quickly and easily manage policy and configure the appliance from a standard Web browser.
Features of Your Aventail Appliance

This section highlights the key components provided with your appliance.

Administrator Components

- **Aventail® Web access service** provides users with secure access to Web-based applications, Web servers, and network file servers from a Web browser. The Web access service (formerly known as the ExtraWeb server) contains a secure HTTP reverse proxy that brokers and encrypts access to Web-based resources. It includes user log-off capability to enhance security for users at public Web kiosks.

- **Aventail® client/server access service** provides a secure proxy for accessing standard client/server applications. It works in conjunction with the Aventail Connect client or the Aventail OnDemand agent to provide authenticated and encrypted access over the Internet. The client/server access service (formerly known as the Anywhere VPN server) is based on the SOCKS v5 protocol.

  The client/server access service brokers and encrypts access to internal applications and networks. Its proxy-based architecture and use of SSL enables the client/server access service to traverse firewalls, NAT devices, and other proxy servers that can interfere with traditional VPN devices. The client/server access service works in conjunction with an agent on the user’s computer; the agent securely routes application requests to the appliance. Two agents are available: Aventail OnDemand (a Java applet or application) and Aventail Connect (a Windows application).
- **Aventail® Secure Access Policy (ASAP™) Management Console (AMC)** is a Web-based administrative tool used to manage the appliance. It provides centralized access for managing security policies, configuring the system (including networking and certificate configuration), and monitoring. AMC is accessible from a Web browser.

### User Components

The appliance includes several components that provide users with access to resources on your network.

- **Aventail® ASAP™ WorkPlace** provides your users with access to Web-based resources protected by the Web access service. After a user logs in to ASAP WorkPlace, a home page appears that contains an administrator-defined list of shortcuts. These shortcuts point to the Web-based resources and Windows file system resources to which the user has access privileges. ASAP WorkPlace is accessible from a standard Web browser.

Web resources and file system resources can be accessed from any Web browser that supports SSL. By default, the appliance is configured to deploy a Microsoft ActiveX control (the “standard Web agent”) on newer versions of Microsoft Windows systems running Internet Explorer. The standard Web agent proxies Web content directly through the appliance. For users running other browsers, the appliance will automatically provide translated Web access.
If you’d rather not install an agent or your users’ systems don’t support ActiveX, you can configure the appliance to provide translated Web access.

- **Aventail® OnDemand™** is a secure, lightweight Java applet that provides access to network resources protected by the Aventail client/server access service. Aventail OnDemand can be downloaded from any Web server "on demand" to give users clientless VPN access—ideal for partners or vendors that do not have standard VPN access to your network or for mobile employees that may need to access network resources from a non-work computer such as a public kiosk.
• **Aventail® Connect™** is a Windows application that provides access to network resources protected by the Aventail client/server access service. Installed on the user’s computer, Aventail Connect can provide additional security by requiring personal firewalls and antivirus applications. In most cases, users interact with Aventail Connect only when it prompts them to type authentication credentials or to select their local and remote networks.

![Aventail Connect](image)

• **End Point Control** components ensure that your network is not compromised when accessed from PCs in untrusted environments. The Aventail appliance includes support for several End Point Control (EPC) components designed to protect sensitive data and your network. Aventail’s data protection agents—Aventail Secure Desktop and Aventail Cache Control—automatically remove session data from the PC. The appliance also supports integration with third-party client integrity controls that automatically check for malware on the client system before allowing access.
What's New in This Release

Version 8.0 of the Aventail ASAP platform includes the following new and enhanced features:

- **Simplified access policy management:** The separate access control lists for Web, client/server, and file system resources have been consolidated into a single Access Control page, resulting in fewer steps required to create, manage, and audit access policies.

- **Support for a new Web proxy client access method:** The new, standard Web access method for Windows 2000/XP clients running Internet Explorer 5.5 or later eliminates the need for Web content translation and provides enhanced access to enterprise Web applications.

- **Enhanced End Point Control capabilities:** New End Point Control (EPC) configuration options give administrators greater control over VPN access by defining zones and device profiles. EPC zones classify connection requests based on selected end-user device attributes that define the degree of trustworthiness allowed for client devices. EPC zones can also be associated with access control rules.

- **Improved update and rollback functionality:** The new System Maintenance page includes options to update the system configuration or roll back to a previous version of the system software. This provides an easier alternative—but not a replacement—to using the command line tools.

- **User monitoring and termination:** The new Active Users page displays the current number of active user sessions, and displays a searchable list of sessions that can be sorted by username and realm. This page also includes a new End session option that temporarily terminates all VPN connections for selected users.

- **Expanded authentication and user management support:** The use of authentication realms has been expanded to include support for selecting which EPC zones and access methods are available to realm members.

- **Group affinity checking** accommodates network environments where authentication and authorization are handled by different servers. This allows you to configure a secondary authentication server (either LDAP or Microsoft Active Directory) that is queried for group affinity.

- **Enhanced OnDemand configuration:** The new Configure OnDemand page requires less data entry to configure port-mapped applications. The new network Redirection List shows all network resources that are automatically redirected in Dynamic Mode.

- **Enhanced Simple Network Management Protocol (SNMP) configuration:** The Configure SNMP page has a new option for enabling support for SNMP traps, and provides the ability to download the new Aventail Management Information Base (MIB) file, which adds ASAP-specific data to already supported MIBs.

- **Policy replication between Aventail appliances:** The new Import/Export page allows you to export the current configuration from one appliance and then import all or part of the configuration on another appliance. This is an easy way to ensure that multiple appliances are using the same access policies.

- **License management:** With the new Licensing page you can review and manage software licenses for the appliance, and view status information about concurrent users and expiration dates.

- **Improved usability throughout AMC:** This release includes numerous functional enhancements to the user interface including the grouping of common tasks, navigation “breadcrumbs,” sortable lists, easier access to options, and summary pages that provide configuration and status information at a glance. For more information see “User Interface Changes in This Release” on page 7.
User Interface Changes in This Release

The AMC user interface has undergone significant design improvements for version 8.0 that resulted in some pages, commands, and options being moved to new locations. To assist administrators who are familiar with earlier versions of AMC, the following table shows the old and new locations for these features. Locations that begin with a command name refer to commands on the main navigation menu.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Old Location</th>
<th>New Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Management page</td>
<td>Administrators command</td>
<td>General Settings command&gt; Administrators tab</td>
</tr>
<tr>
<td>Apply Changes button</td>
<td>Apply Changes page</td>
<td>Maintenance command&gt; Maintenance page</td>
</tr>
<tr>
<td>ASAP WorkPlace Configuration page</td>
<td>Services page&gt; ASAP WorkPlace link</td>
<td>ASAP WorkPlace command&gt; WorkPlace Configuration tab</td>
</tr>
<tr>
<td>Display this realm check box and Realm Status list</td>
<td>• Configure Active Directory Authentication page</td>
<td>Authentication command&gt; select authentication server&gt; Configure Authentication Server page</td>
</tr>
<tr>
<td></td>
<td>• Configure LDAP Authentication page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure RADIUS Authentication page</td>
<td></td>
</tr>
<tr>
<td>Manage Software License page</td>
<td>End Point Control Configuration page&gt; Manage license button</td>
<td>General Settings command&gt; Licensing tab</td>
</tr>
<tr>
<td>Maximum session length option</td>
<td>Services page</td>
<td>General Settings command&gt; General Settings page</td>
</tr>
<tr>
<td>NTLM authentication forwarding options</td>
<td>• Configure Active Directory Authentication page</td>
<td>Authentication command&gt; select authentication server&gt; Configure Authentication Server page</td>
</tr>
<tr>
<td></td>
<td>• Configure LDAP Authentication page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure RADIUS Authentication page</td>
<td></td>
</tr>
<tr>
<td>Restart button</td>
<td>Services page</td>
<td>Maintenance command&gt; Maintenance page</td>
</tr>
<tr>
<td>Shut Down button</td>
<td>Services page</td>
<td>Maintenance command&gt; Maintenance page</td>
</tr>
<tr>
<td>Single Sign-On tab</td>
<td>Authentication page</td>
<td>General Settings command&gt; Single Sign-On tab</td>
</tr>
<tr>
<td>Time zone list</td>
<td>Configure NTP and Time Settings page</td>
<td>General Settings command&gt; General Settings page</td>
</tr>
<tr>
<td>Web Application Profiles tab</td>
<td>Resources page</td>
<td>Services page&gt; Web access link&gt; Web Application Profiles tab</td>
</tr>
</tbody>
</table>

Aventail®
About the Documentation

This document contains detailed information about installing, configuring, and maintaining the appliance. Note that the contents of this document are available as context-sensitive Help from AMC; see "Getting Help" on page 24 for more information.

Document Conventions

Throughout this document, “external” refers to the network interface connected to the Internet. “Internal” refers to the network interface connected to your internal corporate network. This document uses the following typographical conventions:

<table>
<thead>
<tr>
<th>Typographical convention</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>User interface components (such as text boxes or buttons on a Web page).</td>
</tr>
<tr>
<td>Monospace font</td>
<td>Information you are supposed to type.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>File names and directories, and examples.</td>
</tr>
<tr>
<td>commandname -x [-y]</td>
<td>In command-line syntax, square brackets indicate optional parameters.</td>
</tr>
<tr>
<td>ALL CAPS</td>
<td>Key names such as ENTER or BACKSPACE, and key combinations such as CTRL+Q.</td>
</tr>
</tbody>
</table>
Chapter 2
Installation and Initial Setup

This section shows where the appliance fits into your network environment, provides installation and cabling instructions, and explains how to use Setup Tool to perform basic network configuration.

Network Architecture

The appliance includes three physical network interfaces, and can be set up in one of three configurations—dual interface, single interface, or clustered. Dual and single interface configurations are discussed in this section. See "Installing and Configuring a Cluster" on page 217 for a discussion of the cluster configuration.

- **Dual interface configuration.** One network interface is used for external traffic (that is, to and from the Internet), and the other interface is used for internal traffic (to and from your corporate network).
Chapter 2 - Installation and Initial Setup

- **Single interface configuration.** A single network interface is used for both internal and external traffic. In this configuration, the appliance is usually installed in the demilitarized zone (or DMZ, also known as a perimeter network).

  ![Diagram of network configuration]

In both configurations, incoming requests to the Aventail services—including TCP/IP traffic for the client/server access service and HTTP/S traffic for the Web access service—are sent over port 80 (HTTP) and port 443 (HTTPS). Note that traffic from the Aventail Connect client and the OnDemand agent is always sent over port 443. Because most networks are configured to enable traffic over these ports, you won't need to reconfigure firewalls on your network.

You should install the appliance in a location where it can connect to resources on your network, including:

- Application servers and file servers, including Web servers, client/server applications, and Windows file servers.
- External authentication repositories (such as an LDAP, Microsoft Active Directory, or RADIUS server).
- One or more Domain Name System (DNS) servers.
- Optionally, a Windows Internet Name Service (WINS) server. This is required for browsing Windows networks using ASAP WorkPlace.

**CAUTION** Aventail highly recommends that you secure the appliance behind a firewall.

Although not required, enabling the appliance to communicate with these additional resources will provide greater functionality and ease of use:

- Network Time Protocol (NTP) server for synchronizing the time on the appliance.
- External server for storing syslog output.
- Administrator’s workstation for secure shell (SSH) access.

You can configure the appliance to use a self-signed server certificate, or for enhanced security you can obtain a certificate from a commercial certificate authority (CA). For more information, see "Obtaining a Certificate from a Commercial CA" on page 41.

**Preparing for the Installation**

Before beginning the installation, you'll need to gather information about your networking environment and verify that your firewalls are properly configured to permit traffic to and from the appliance.

**Deployment Checklist**

Before configuring the appliance, you'll need to gather the following information. You'll provide some of this information when running Setup Tool (see "Running Setup Tool" on page 18), but most of it will be used when configuring the appliance in AMC (see "Network and Authentication Configuration" on page 31).
• The root password you’ll use to administer the appliance.
• Internal IP address and, optionally, an external IP address.
• Interface speeds for one or both network adapters.
• The name for the appliance. (Because this name will be used only in log files, you don’t need
to add it to DNS.)

Notes
• If you are installing a cluster, you’ll need several pieces of additional information. See
“Installing and Configuring a Cluster” on page 217.

Certificate information
Several pieces of information will be used to generate the server and AMC certificates:
• Fully qualified domain name (FQDN) for the appliance. You’ll need to add this name to your
public DNS, and it will be visible to users when they connect to Web-based resources.
• FQDN for the ASAP Management Console (AMC) server. You’ll use the AMC server name to
access AMC, which is used to administer the appliance.

Name lookup information
• Internal DNS domain name of the network to which the appliance will be connected.
• Primary internal DNS server address (additional DNS servers are optional).
• The IP address for an internal WINS server and the name of your Windows domain (required
to browse files on a Windows network using Aventail ASAP WorkPlace, but are otherwise
optional).

Authentication information
• Server name and login information for your authentication servers (LDAP, Active Directory,
and/or RADIUS).

Routing information
• Default gateway address. If the computer from which you’ll access AMC is on a different
network than the appliance, you’ll need to specify a gateway when you run Setup Tool. In AMC,
you’ll supply the default gateway to the Internet.
• Routing information to any internal resources, which may include static and/or dynamic routes.
To use dynamic routing, your site must support the Routing Information Protocol (RIP).

Optional configuration information
• To enable SSH access from a remote machine, you’ll need the remote host’s IP address.
• To synchronize with an NTP server, you’ll need the IP addresses for one or more NTP servers.
• To send data to a syslog server, you’ll need the IP address and port number for one or more
syslog servers.

Verifying Your Firewall Policies
For the appliance to function correctly, you must open ports on your external (Internet-facing) and
internal firewalls.

External firewall
For secure access to the appliance from a Web browser, Aventail Connect, or Aventail OnDemand,
you must make sure that ports 80 and 443 are open on firewalls at your site. Opening your firewall
to permit SSH access is optional, but can be useful for performing administrative tasks from a
remote system.

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Port/protocol</th>
<th>Usage</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80/tcp</td>
<td>Unencrypted network access</td>
<td>x</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443/tcp</td>
<td>Encrypted network access</td>
<td>x</td>
</tr>
<tr>
<td>SSH</td>
<td>22/tcp</td>
<td>Administrative access to the appliance</td>
<td></td>
</tr>
</tbody>
</table>
Internal firewall

If you have a firewall on the internal network, you may need to adjust its policy to open ports for back-end applications with which the appliance must communicate. In addition to opening ports for standard network services such as DNS and e-mail, you may need to modify your firewall policy in order for the appliance to access the following services.

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Port/protocol</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Microsoft networking  | • 138/tcp and 138/udp  
                        | • 137/tcp and 137/udp  
                        | • 139/udp                | Used by ASAP WorkPlace to perform WINS name resolution, browse requests, and access file shares |
| LDAP (unencrypted)    | 389/tcp       | Communicate with an LDAP directory or Microsoft Active Directory       |
| LDAP over SSL (encrypted) | 636/tcp | Communicate with an LDAP directory or Microsoft Active Directory over SSL |
| RADIUS                | 1645/udp or 1812/udp | Communicate with an RADIUS authentication server                     |
| NTP                   | 22            | Synchronize the appliance clock with an NTP server                     |
| Syslog                | 514/tcp       | Send system log information to a syslog server                         |
| SNMP                  | 161/udp       | Monitor the appliance from an SNMP management tool                     |

Helpful Management Tools

To manage the appliance from a remote system running Microsoft Windows, you may find the following management tools useful. Note that both of these tools use encryption to protect information from eavesdropping, unlike standard FTP or Telnet utilities.

- **A Secure Shell (SSH) client** enables you to securely log in to the appliance and configure it from the command line. This is useful for backing up the system, viewing log files, and configuring advanced network settings. A popular SSH client for Windows is VanDyke Software’s SecureCRT. A trial download is available at [http://www.vandyke.com/products/securecrt/](http://www.vandyke.com/products/securecrt/). Another popular client is PuTTY, a free implementation of Telnet and SSH for Win32 platforms. PuTTY is recommended by Cisco.

  To connect to the appliance using SSH, you type “root” as the username and type the password you created using Setup Tool.

- **A Secure Copy (scp) client** makes it easy to securely transfer files from a PC running Windows to the appliance. This is useful for copying certificates and other data to the appliance. A popular Windows client is WinSCP, available at [http://winscp.sourceforge.net/eng/](http://winscp.sourceforge.net/eng/).

Installation and Deployment Process

This section outlines the process of installing, configuring, and testing the appliance, and deploying it into a production environment.

Notes

- The Aventail appliance ships with a default license that supports 1,000 concurrent users for a three-day evaluation period. To continue using the appliance after this three-day limit, you must upload a valid license file. As a reminder, the Aventail ASAP Management Console (AMC) will display a yellow “license warning” message in the status area that links to the Licensing page.
• It is recommended that you ensure that the appliance’s date and time settings are configured correctly for your time zone before importing a license file. For more information, see “Configuring the Time Settings” on page 123.
• If you are installing a cluster, see “Installing and Configuring a Cluster” on page 217.

Installation and Configuration Overview

The installation process is composed of several steps. The following checklist will help you get started.

1. **Rack-mount the appliance and connect the necessary cables.**
   See “Rack Installation” on page 15 and “Connecting the Appliance” on page 17.

2. **Configure basic network information using Setup Tool.**
   The first time you start the system, Setup Tool automatically runs and you’ll be asked to provide:
   - Administrator password.
   - IP address for the internal network interface.
   - (Optional) The gateway used to access the internal interface.
   See “Running Setup Tool” on page 18.

3. **Log in to AMC and complete the network configuration.**
   Log in to AMC, the Web-based application used to administer the appliance, and configure the following:
   - System identity.
   - External network interface (optional).
   - Routing information.
   - Name resolution settings.
   See “Configuring Basic Network Settings” on page 31.

4. **Configure a server certificate.**
   The appliance encrypts information using the Secure Sockets Layer (SSL) protocol. You can create a self-signed certificate using AMC, or optionally obtain a certificate from a commercial certificate authority (CA).
   See “Configuring SSL Certificates” on page 38.

5. **Define one or more authentication servers.**
   Authentication is used to verify the identity of users. When configuring an authentication realm, you are prompted to specify a directory type (LDAP, Microsoft Active Directory, RADIUS, or local users) and a credential type (username/password, token, or digital certificate).
   See “Managing User Authentication” on page 51.

6. **Define application resources and groups.**
   Application resources include TCP/IP-based resources (such as client/server applications, file servers, or databases), Web-based resources (including Web applications or Web sites) that run over HTTP, and Windows network share resources (to be accessed via ASAP WorkPlace).
   See “Creating and Managing Resources” on page 85.

7. **Define users, groups, and realms.**
   User and group definitions are used in access control rules to control access to application resources. Realms enable the appliance to directly integrate with authentication servers, eliminating the need to create and manage accounts for each user requiring access to your network.
   See “Overview: Users, Groups, and Realms” on page 105.

8. **Create access control rules.**
   Access control rules determine what resources are available to users or groups.
   See “Access Control Rules” on page 95.
9. **Configure Web and network shortcuts for ASAP WorkPlace.**
   To provide your users with easy access to a Web resource and/or a file system resource from within ASAP WorkPlace, you may want to create shortcuts to these resources.
   See “Working with Shortcuts” on page 190.

10. **Optionally, enable and configure End Point Control**
    End Point Control optionally deploys data protection components designed to safeguard sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments.
    See “End Point Control” on page 163.

11. **Apply your changes.**
    To activate your configuration changes, you must apply them.
    See “Applying Configuration Changes” on page 27.

12. **Test system accessibility.**
    Now you can verify that the appliance can access your external user repositories, and make sure that the resources on your network are accessible.
    See “Troubleshooting” on page 229.

---

**Moving the Appliance Into Production**

After you have tested the appliance sufficiently in your network environment and determined how you want it to work, you’re ready to move it into its permanent home. This section describes steps you may need to perform when moving the appliance into production.

- **Reconfigure the appliance with new address information.**
  If the network environment changed when you moved the appliance into production, you will need to reconfigure the basic network settings and adjust any of the following values if they have changed:
  - IP address for the internal interface and external interfaces
  - Default gateway IP address
  - Static routes
  - Default DNS domain and DNS server IP address
  If you have a large number of configuration changes to make, you may find it convenient to restore the appliance to its default settings and start over from scratch. This can be done using Config Reset Tool; see "Restoring Factory Default Configuration Settings" on page 149 for more information.

- **Register the appliance with DNS.**
  If you haven’t already registered the appliance with your company’s DNS, you’ll want to do this now. This ensures that external users can access your network resources using a fully qualified domain name instead of an IP address. Edit your DNS server’s database to include the fully qualified domain name contained in the appliance’s certificate.

- **Obtain a commercial SSL certificate.**
  You may want to obtain a commercial certificate for the appliance to assure users of its identity. (Generally, a self-signed certificate is adequate for AMC.) For more information on generating server certificates, see “Configuring SSL Certificates” on page 38.

- **Adjust your firewall policies.**
  If you have an Internet-facing firewall, you may need to adjust its policy to open ports required by the appliance. By default, both the Web access service and the client/server access service communicate using port 443/tcp. (The Web access service uses port 443/tcp for HTTPS and port 80/tcp for HTTP.) If you want to use SSH to connect to the appliance from outside the network, you’ll need to open port 22/tcp.
  If you have a firewall that faces the internal network, you may need to adjust the policy for that firewall to open ports for any back-end applications with which the appliance must communicate (if these ports are not already open). For instance, if you use an LDAP or Microsoft Active Directory server for authentication, you’ll need to open port 389/tcp on your internal firewall. For RADIUS, you’ll need to open ports 1645/ucp and 1812/udp.
If you’re using Aventail ASAP WorkPlace to access Windows network shares, you will also need to open internal ports on your internal firewall so that WorkPlace can perform name resolution, make browse requests, and connect to file shares. For more information, see “Deployment Checklist” on page 10.

• **Deploy the Aventail Connect client and/or Aventail OnDemand.**
  If you use the client/server access service, your users will need a software component to access your network resources.
  • For Windows-based PCs, you can install the Aventail Connect client on the desktop. See “Aventail Connect” on page 200 or Chapter 3 of the *Aventail Connect Administrator’s Guide*.
  • The Aventail OnDemand agent is available on any Java-enabled platform; see “Aventail OnDemand” on page 201.

• **Create Web and network shortcuts and deploy ASAP WorkPlace.**
  If you use ASAP WorkPlace as an interface to Web-based resources and to provide Web-based access to Windows network share resources, you will need to create shortcuts to these resources (see “Working with Shortcuts” on page 190). You’ll also want to publish the ASAP WorkPlace URL so your users know how to access resources through your VPN.
  You may want to customize the appearance of ASAP WorkPlace for your environment. See “Customizing the Appearance of ASAP WorkPlace” on page 194 for more information.

**Installing the Appliance**

After you’ve unpacked the box, you’re ready to install the appliance on your network and prepare for the configuration process.

**Rack Installation**

Before connecting the appliance, make sure that you have sufficient space and adequate power. The specifications are listed below:

• 1U rack-mount component measuring 16.9" wide by 23.9" deep
• AC power supply: 350W PFC
• AC voltage: 4.96 amp at 115 V, or 2.48 amp at 220 V

To mount the appliance in an equipment rack, you’ll need to install the rack hardware. The product packaging contains a slide rail kit for mounting the appliance in a four-post cabinet. See the documentation provided with the rail kit for detailed installation instructions. Brackets are also provided for mid-mount installation in a two-post rack.
Front Panel Controls and Indicators
Before powering up the appliance, you should familiarize yourself with the front panel controls.

![Front Panel Diagram]

The following table describes the controls and indicators on the front panel.

<table>
<thead>
<tr>
<th>Letter</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>External network interface (adapter 1) activity LED</td>
<td>Continuous or blinking green light indicates network activity.</td>
</tr>
<tr>
<td>B</td>
<td>Internal network interface (adapter 2) activity LED</td>
<td>Continuous or blinking green light indicates network activity.</td>
</tr>
</tbody>
</table>
| C      | Power LED | • Continuous green light indicates the system is on.  
          • No light indicates the power is off. |
| D      | Power button | Toggles the system power on/off. |
| E      | System status LED | • Continuous green light indicates normal system operation.  
          • Continuous amber light indicates system is in a critical or non-recoverable condition.  
          • No light indicates system stop. |
| F      | Fixed disk drive status LED | • Random blinking green light indicates disk activity.  
          • Continuous amber light indicates disk drive fault. |
| G      | ID LED | Continuous blue light indicates ID button is depressed.  
          The ID LED is visible through the rear of the chassis and enables you to easily identify the appliance when you’re working in a rack of servers. |
| H      | ID button | Toggles the ID LED on/off. |
| I      | Reset button | Reboots the system. |
Connecting the Appliance

The appliance uses up to five connections, as shown in the following illustration.

1. Internal network (INT 2)
2. External network (EXT 1)
3. Cluster interface (HA 3)
4. Console
5. Power supply

To connect the appliance

1. Connect a network cable from your internal network into the top Ethernet adapter (marked INT 2).
2. Optionally, connect a cable from your external network into the bottom Ethernet adapter (marked EXT 1).
3. If you are setting up a cluster, connect one end of the supplied network crossover cable into the cluster interface adapter (marked HA 3). Connect the other end to the cluster interface adapter on the other appliance in the cluster.
4. Connect the supplied RJ45 cable and DB9-to-RJ45 adapter from a laptop computer or terminal to the rear serial port. This provides full console access to the appliance; see “Powering Up” on page 17 for more information.
5. Connect a standard AC power cord to the power supply.

Powering Up

After you’ve connected the appliance, you’re ready to power up for the first time and begin the configuration process. The serial connector located on the rear panel provides an interface for configuring the appliance from a laptop or terminal.

To power up the appliance

1. Power up the laptop or terminal.
2. Use a terminal emulation program to establish a serial connection with the appliance. The terminal settings are as follows:
   - Mode: VT100
   - Connection speed: 9600 baud
   - Handshaking CTS/RTS
   - Databits: 8
   - Parity: none
   - Stop bits: 1
3. Power up the appliance by pressing the power button on the front panel.

The LEDs on the front of the device will light up, and the Aventail Setup Tool will automatically run; see “Running Setup Tool” on page 18 for more information.

Powering Down and Rebooting the Appliance

When it’s time to power down or restart the appliance, be sure to follow the proper procedure. The appliance stores important data in memory while it is running, and needs to write the data to the hard disk before you turn off the power.

**CAUTION** Powering down the appliance improperly can result in loss of data and can leave the system’s files in an inconsistent state.
To power down or restart the appliance

1. From the main navigation menu, click Maintenance.

2. On the Maintenance page, click the appropriate button:
   - To restart the appliance, click Restart. AMC will stop responding. When the appliance
     restarts, you can log in to AMC again.
   - To shut down the appliance, click Shutdown. AMC will stop responding; wait a few
     moments and then power down the appliance by pressing the power button on the front
     panel.

Performing Initial Network Setup

Initial network setup is done using a command-line utility called Setup Tool. It displays a series of
prompts, at which you’ll type appropriate configuration information.

Tips for Working with Setup Tool

Here are some tips for working with Setup Tool.

- Yes or no questions include a [y] or [n] at the end of the prompt; type the appropriate letter
  and then press ENTER to display the next question.
- To delete a character, press BACKSPACE. (On a Windows-based PC, you can also press DELETE
to remove a character.)
- When typing an IP address or netmask, use the standard IP address format of four octets
  (w.x.y.z). Setup Tool provides basic error checking (for example, validating that the gateway
  you type is on the same subnet as the appliance).
- Press q to quit Setup Tool and discard your changes.

Running Setup Tool

The first time you start the system, a command-line setup utility called Setup Tool automatically
runs. It prompts you to accept the Aventail End User License Agreement (EULA), create a root
password, and provide an IP address, subnet mask, and default gateway.

If you are installing a cluster, do not use this procedure. Instead, refer to "Installing and Configuring
a Cluster" on page 217 for installation instructions.

To run Setup Tool

1. Make a serial connection to the appliance (see "Powering Up" on page 17) and then turn on
   the appliance using the power button on the front panel.
2. The Setup Tool automatically runs (you can also invoke it by typing setup_tool).
3. When you’re prompted to log in, type root for the username; press ENTER to move to the
   next screen.
4. The Aventail EULA appears. It scrolls over several screens; press ENTER to move to the next
   screen.
   
   Do you accept the terms of the license agreement? [n]:
   - If you accept the license agreement, type y and then press ENTER to continue.
5. You’re prompted to create a new root password for the system; this password will also be
   used to access AMC.
   
   Password:
• Your password must contain between eight and 20 characters, and is case-sensitive. We recommend that you create a "strong" password using a combination of uppercase and lowercase letters and numbers, and avoid using words found in a dictionary. Be sure to record your password somewhere and keep it secure. Press ENTER to continue.

Confirm password:
• Retype the root password exactly as typed previously (it is case-sensitive) and then press ENTER to continue.

6. Next, you’re prompted to type an IP address, subnet mask, and (optionally) a gateway for the internal interface. You’ll use this interface to connect to the appliance from a Web browser and continue setup using AMC.

   IP address:
• Type an IP address for the internal interface connected to your internal (or private) network and then press ENTER.

   Subnet mask:
• Type a netmask for the internal network interface and then press ENTER.

   Gateway:
• If the computer from which you’ll access AMC is on a different network than the appliance, you must specify a gateway. Type the IP address of the gateway used to route traffic to the appliance and then press ENTER.

   If you’re accessing AMC from the same network on which the appliance is located, simply press ENTER.

7. Next, you’re prompted to review the information you provided. Press ENTER to accept the current value, or type a new value and then press ENTER.

8. You are then asked if this node will be part of a cluster.

   Install node in a cluster? [n]:
• Because this is a single node installation, you should accept the default by pressing ENTER. For details on installing a cluster, see “Installing and Configuring a Cluster” on page 217.

9. Finally, you’re prompted to save and apply your changes.

   Do you want to save and apply configuration changes [y]:
• Press ENTER to save your changes.

At this point, Setup Tool saves your changes and restarts the necessary services. It also generates SSL keys (for SSH access) using the information you provided.

During this time, you will receive minimal feedback; be patient and do not assume that Setup Tool is not responding.

When Setup Tool is finished, a message appears indicating that the initial setup is complete. This message also includes the URL for accessing AMC.

**Next Steps**

You’ve now completed the initial network setup, and are ready to use AMC to continue configuring the appliance. AMC is accessible using a Web browser.

If you’re new to AMC, you might want to read “Working with AMC” on page 21. If you’re ready to continue configuring the appliance, see “Network and Authentication Configuration” on page 31.
Chapter 3  
Working with AMC

This section introduces the Aventail ASAP Management Console (AMC), a Web-based interface for managing the appliance. AMC supports Microsoft Internet Explorer version 5.5 and later, Netscape Navigator version 7.0 and later, and Mozilla 1.41 and later.

Accessing AMC

This section explains how to access AMC using your Web browser and how to log out.

Logging In to AMC

Before logging in to AMC, you’ll need the host name or IP address you typed for the internal interface during the initial setup with Setup Tool.

To log in to AMC

1. Start your Web browser and then type https://<ipaddress>:8443/console in the Address box, where <ipaddress> matches the address you typed for the internal interface when you ran Setup Tool. Press ENTER. The login screen appears.

2. Type admin in the Username box.

3. In the Password box, type the “root” password you created using Setup Tool.

4. Click Login. The AMC home page appears.

For information on changing the AMC password, see “Editing Administrator Accounts” on page 25.

Notes

• Your AMC session will automatically time out after 15 minutes of inactivity. If your session times out, you will be prompted to log in again.
Logging Out

It is important to preserve the security of your AMC administrator account. When you’re finished working in AMC, you should log out by clicking the Log out button in the upper right portion of the screen.

If you terminate a session by simply closing your Web browser, that session will remain active until it times out (after 15 minutes of inactivity). Until then, it will appear on the Administrator Sessions page. For more information, see “Avoiding Configuration File Conflicts with Multiple Administrators” on page 26.

AMC Basics

This section describes the basics of working with AMC. All configuration data is encrypted using SSL as it’s transferred between AMC and your browser, ensuring that your data remains secure. To increase security, it is recommended that you use AMC within a trusted network (on an internal network that is behind a firewall). See “Certificate FAQ” on page 50 for more details.

A Quick Tour of the AMC Interface

The AMC interface will be familiar to anyone who has worked with similar Web-based security management applications. Here are some basic notes about working with AMC.

• **Main navigation menu**
  On the left side of the AMC window are the commands you’ll use to manage the appliance. This is known as the main navigation menu.

• **Tables and tabs**
  Many AMC pages use a tabular layout to present the objects you’ll be managing. The tables include scroll bars, which make it easier for you to keep the main elements on the page (including the navigation bar, header, and footer) in view when working with long lists. You can also sort the data displayed in some tables by clicking the underlined column headings.

  In some cases, you’ll use tabs to switch between modes. For example, you’ll use tabs to switch between managing resources and managing groups containing resources.

• **Editing an object**
  In most of the tables used to display lists of objects, notice that the name field (or in the case of the Access Control page, the rule number) is hyperlinked. To edit an object, click its hyperlink.

• **Changing the Page View**
  Some of the longer, more complex pages in AMC hide the edit controls used to configure advanced features. This makes it easier for you to focus on the most important configuration.
options. To view hidden options, click the down arrow button; to hide a set of options, click the up arrow button.

- **Required fields and errors**

  Required fields are indicated in AMC with an asterisk. If you omit a value for a required field and click **Save**, a red message appears beneath the field indicating that it is required. A red message is also used to indicate an error (for example, if you type an invalid value).

- **Assigning names and descriptions**

  Most of your time in AMC will be spent managing three types of objects: access control rules, resources, and users and groups. When you create these objects, AMC will require you to type a name. AMC also has a space for you to type an optional description.

  Although not required, meaningful descriptions can help you remember critical details about the objects you’re managing, such as the purpose of an access rule or what resources are in a subnet range. A good description can be especially helpful when managing a group of objects; when you return to AMC many months from now to manage a large group of network resources, for example, you’ll be glad to have a description reminding you of what’s in the group.

- **Saving changes on a page**

  AMC pages from which you can input or modify data include a pair of buttons—**Save** and **Cancel**—to save the changes. When you’re finished making changes, be sure to click **Save** to save the changes to disk. If you click **Cancel**, or use the Back button in your browser, your changes are not saved.

- **The AMC status area**

  A status area appears just beneath the AMC header displaying important information:

  - If you’ve made configuration changes but have not applied them, "Pending changes" will appear in the status area. Clicking the message text will display the **Apply Changes** page from which you can activate the configuration changes.
  - If more than one administrator is logged into AMC, "Multiple administrator" will appear in the status area. Clicking the message text will display the **Administrator Sessions** page.
  - If your base appliance license or a component license has expired, "License expired" will appear in the status area. Clicking the message text will display the **Licensing** page from which you can review and manage software licenses. If a software license’s expiration date is approaching, "License warning" will appear in the status area.

- **The current ASAP version number**

  The version of the current system software is displayed at the bottom of the left-hand navigation bar on every page in AMC, and is on the **System Status** page. The version
number is useful for planning system updates, and you’ll need to have it ready when contacting technical support.

**Getting Help**

Each AMC page has a *Help* button that displays context-sensitive online Help. To open Help, click the *Help* button in the upper right portion of the screen. Help appears in a new browser window.

The Help navigation bar includes the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Contents" /></td>
<td>Displays the Help navigation pane, containing Contents, Index, and Search buttons. (This button appears when the Help navigation pane is closed.)</td>
</tr>
<tr>
<td><img src="image" alt="Sync" /></td>
<td>Synchronizes the table of contents to display the current topic. (This button appears when the Help navigation pane is in view.)</td>
</tr>
<tr>
<td><img src="image" alt="Next" /></td>
<td>Displays the next or previous Help topic.</td>
</tr>
<tr>
<td><img src="image" alt="Related" /></td>
<td>Displays a list of related Help topics.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Prints the current Help topic.</td>
</tr>
</tbody>
</table>

The Help navigation includes three buttons that change the content in the left frame:

- **Contents** displays a hierarchical list of Help topics.
- **Index** displays an alphabetical list of keywords in Help.
- **Search** displays a full text search engine for Help. Type a word or short phrase in the box, click **Go!**, and then choose a topic from the list of results.

**Administrator Accounts**

This section describes how to manage AMC administrator accounts and how to avoid problems if more than one administrator is managing the appliance.
Managing Administrator Accounts

AMC enables you to create multiple administrator accounts, each with a separate username and password. All administrators have the same level of control over policy and configuration and can change their AMC passwords. Only the “primary” administrator can add, edit, or delete other administrator accounts.

Adding Administrator Accounts

You might want to create additional administrator accounts if you have more than one person responsible for managing policy and you want each person to have his or her own login credentials. Only the “primary” administrator can create secondary administrator accounts.

► To add an administrator account
1. From the main navigation menu, click General Settings.
2. On the General Settings page, click the Administrators tab, and then click the New button.
3. On the Add/Edit Administrator page, in the Username box, type the secondary administrator’s user name.
4. In the Description box, type a descriptive comment about the administrator. This might be the administrator’s full name or title. This field is optional, but a description can be helpful when viewing the list of administrators later.
5. In the Password box, type a password for the administrator. Be sure to share the password with the administrator. The administrator can change this password at any time.
   Your password must contain at least eight characters, and is case-sensitive. We recommend that you create a password containing a combination of uppercase and lowercase letters and numbers, and avoid using words found in a dictionary.
6. In the Confirm Password box, retype the password to confirm it.
7. Click Save.

Editing Administrator Accounts

To help keep your AMC password secure, you should change it from time to time. Each administrator can edit his or her own account to change the password or update the description. The primary AMC administrator (whose username is “admin”) can edit the account settings for any other administrator.

Your password must contain between eight and 20 characters, and is case-sensitive. We recommend that you create a “strong” password using a combination of uppercase and lowercase letters and numbers, and avoid using words found in a dictionary.

After you change your password, record it somewhere and keep it secure. If you change a secondary administrator’s password, be sure to share the password with the appropriate administrator.

► To edit an administrator account
1. From the main navigation menu, click General Settings.
2. On the General Settings page, click the Administrators tab.
3. In the Username column, click the name of the administrator whose account you want to edit.
4. On the Add/Edit Administrator page, change the textual description or login password.
Notes

• Changing the AMC password will update only the credentials used to log in to AMC. The root password for shell access will still be set to the password you created during the initial setup using Setup Tool. Just as with the AMC password, however, you should occasionally change your root shell password.

To change the root shell password
1. From the command line, type `passwd root` and then press ENTER. The following prompt appears:
   
Enter new UNIX password:
2. Type your new password and then press ENTER. The following prompt appears:
   
   Retype new UNIX password:
3. Retype your new password and then press ENTER. If you retyped your password correctly, a message appears indicating that your password has been updated. Otherwise, an error message appears.

Deleting Administrator Accounts
The primary administrator can delete other administrator accounts. Note that the primary administrator account cannot be deleted.

To delete an administrator account
1. From the main navigation menu, click General Settings.
2. On the General Settings page, click the Administrators tab.
3. In the check box column, select the check box next to the administrator account that you want to delete, and then click the Delete button.

Avoiding Configuration File Conflicts with Multiple Administrators

If more than one administrator is managing your appliance, you should avoid working in AMC at the same time. If multiple administrators make changes to the same object, AMC will save the last change made. This can cause unintentional results, and can potentially cause security problems if conflicting changes are made to access control rules.

If more than one administrator is logged into AMC, a “Multiple administrators” warning message will appear in the AMC status area. Clicking the message shows the username and IP address of all administrators logged into AMC.

To view other administrators logged into AMC
• If the warning message appears, click the hyperlink in the message text to display the Administrator Sessions page.

The page lists the usernames and IP addresses of all administrators logged into AMC. You should contact the other administrators and coordinate your activities to avoid configuration file conflicts.

<table>
<thead>
<tr>
<th>Username</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>10.168.2.176</td>
</tr>
<tr>
<td>admin</td>
<td>10.169.2.55</td>
</tr>
<tr>
<td>admin</td>
<td>10.169.2.7</td>
</tr>
</tbody>
</table>
Notes

• If an administrator has multiple instances of the Web browser logged into AMC, the Administrator Sessions page will list the administrator's user name and IP address more than once. Also, note that you must click Log Out to end an AMC session; if you terminate a session by closing your Web browser, that session will appear in the list of active sessions until it times out (by default, 15 minutes).

Working with Configuration Data

This section explains how to save and activate configuration changes in AMC.

Saving Configuration Changes to Disk

When you're finished making changes on a page in AMC and you click Save, your changes are saved to disk. Note that if you click Cancel or use the Back button in your browser, your changes are not saved.

➤ To save configuration changes to disk
  1. Make any changes on a page in AMC.
  2. Click Save at the bottom of the page.

  Configuration changes are saved to disk, but are not applied to the active configuration. The status area in AMC changes to indicate that you have pending changes that need to be applied to the appliance.

  ![Pending changes](image)

  See “Applying Configuration Changes” on page 27 for information.

Notes

• Changes made on the AMC Administrators page take effect immediately.

Applying Configuration Changes

As you make configuration changes to the appliance, they are saved to disk but are not immediately applied. To activate your changes, you must apply them using the Apply Changes page. You can apply most configuration changes without interrupting service to users. After applying the changes, all new connections will use the new configuration.

If you want to immediately apply new configuration changes to all users, you must manually restart the appropriate services. This will terminate existing user connections and force users to reauthenticate. For details on restarting services, see “Stopping and Starting the Aventail Services” on page 155.

Low-level configuration changes (for example, changing an IP address) will require a restart of network services and will terminate existing user connections, forcing existing users to reauthenticate. If possible, you should apply these configuration changes during off-peak hours (perhaps during a maintenance window) and be sure to notify your users before restarting the server. If a configuration change will require such a restart, AMC displays a warning on the Apply Changes page.

➤ To apply your changes
  1. From the main navigation menu, click Maintenance.
2. On the Maintenance page, click the **Apply changes** button. The **Apply Changes** page appears. (You can also click the **Pending changes** message in the upper right corner of AMC.)

3. Assess the impact of applying your changes by looking at the message on the **Apply Changes** page. One of several messages might appear, as described in the table following this procedure.

4. Click the **Apply Changes** button to apply configuration changes.

Don’t browse to another page in AMC until your changes are applied. After the page refreshes and the “Pending configuration changes” message disappears from the status area in AMC, you can safely display a different page.

One of several messages might appear on the **Apply Changes** page.

<table>
<thead>
<tr>
<th>Warning message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applying changes will restart all services and terminate all user connections.</td>
<td>Applying these changes will terminate existing user connections. CAUTION This will require users to reauthenticate, and may cause them to lose data.</td>
</tr>
<tr>
<td>• Applying changes will terminate existing TCP/IP user connections.</td>
<td>AMCM will become unavailable after your current session ends. Close your browser and then log in to AMC again.</td>
</tr>
<tr>
<td>• Applying changes will terminate existing HTTP user connections.</td>
<td>AMCM will become unavailable after your current session ends. Close your browser and then log in to AMC again.</td>
</tr>
<tr>
<td>Your changes will require AMC to restart, which will end your current administrative session. When the request is complete, open a new browser and log in to AMC again.</td>
<td>AMCM will become unavailable after your current session ends. Close your browser and then log in to AMC again.</td>
</tr>
<tr>
<td>No authentication realms are enabled. This will prevent users from accessing any resources. Click here to configure user authentication.</td>
<td>At least one authentication realm must be enabled for users to have access to resources. Otherwise, the users cannot be authenticated.</td>
</tr>
</tbody>
</table>

**Notes**

- When you apply configuration changes to ASAP WorkPlace, AMC performs a a restart of the service. Users will not need to reauthenticate to WorkPlace, but if they provided Windows login credentials to access a network share, they will be prompted to re-enter them when WorkPlace restarts.

- Any connections that exist when you apply changes will continue to use the old configuration until the connection terminates. Because Web connections are short-lived, most users accessing Web resources will pick up configuration changes fairly quickly. On the other hand, client/server connections can survive for a long period of time. You can use the **Maximum limbo life** setting to control how long existing client/server connections remain active following a configuration change (see “Configuring the Client/Server Access Service” on page 157). This enables you to control how frequently configuration changes are propagated to users accessing TCP/IP applications.
If the new configuration fails to load, existing connections remain in effect but new connection attempts will fail. For details on what to do in this situation, see "AMC Issues" on page 230.

Deleting Referenced Objects

You cannot delete an object (such as a resource or a user) if it is still referenced by another object. If you try to do so, AMC displays an error message. For example, if you try to delete a resource that is still referenced by an access control rule, an error message appears.

Included in the error message is a link to a page that lists all references to the resource you are trying to delete. You must remove all references to the object before you can delete it.

The following table lists the object types that cannot be deleted if they are referenced by other objects.

<table>
<thead>
<tr>
<th>Object type</th>
<th>Objects that may reference this object type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Access control rules, resource groups, WorkPlace Web shortcuts</td>
</tr>
<tr>
<td>Resource groups</td>
<td>Access control rules</td>
</tr>
<tr>
<td>Users</td>
<td>Access control rules</td>
</tr>
<tr>
<td>User groups</td>
<td>Access control rules</td>
</tr>
<tr>
<td>Realms</td>
<td>Users, user groups</td>
</tr>
<tr>
<td>Authentication servers</td>
<td>Realms</td>
</tr>
<tr>
<td>Web application profiles</td>
<td>Resources</td>
</tr>
<tr>
<td>End Point Control zones</td>
<td>Access control rules, realms</td>
</tr>
<tr>
<td>Device profiles</td>
<td>End Point Control zones</td>
</tr>
</tbody>
</table>
Chapter 4
Network and Authentication Configuration

This section provides instructions on the essential network configuration tasks, including configuring the network interfaces, routing, and name resolution settings, and managing SSL certificates. It also explains how to configure user authentication.

This is the minimal network configuration required to get the appliance up and running. For information on configuring additional services—including NTP, SSH, ICMP, and syslog—see “System Administration” on page 121.

Configuring Basic Network Settings

All basic network settings—including IP interfaces, routing, and name resolution—are configurable in AMC.

Specifying System Identity

You must name the appliance and specify the domain name in which it is located.

▶ To specify system identity
1. From the main navigation menu, click Network Settings. The General page appears.

   - General
   - Routing
   - Name Resolution

   Define basic network settings.

   Domain name: *  
   example.com

2. In the Domain name box, type the name of the domain in which the appliance is located. For example, you might type example.com. This name defines the DNS namespace used to identify hosts accessed by the appliance.
3. Click Save to save your changes.
4. In the Network interfaces table, click the appliance name to open the Configure Network Interfaces page for that appliance.
5. In the Appliance name box, type a name for the appliance. This name will appear in system logs, but will not be visible to users. This box is not editable in a cluster environment.
6. Click Save.
Configuring Network Interfaces

To configure the network interfaces, you type the IP address and subnet mask and specify the interface speed. You can run the appliance using just the internal network interface, or optionally enable the external interface if you want to use two interfaces. For more information on the interface configuration options, see "Network Architecture" on page 9.

To configure network interfaces
1. From the main navigation menu, click **Network Settings**. The **General** page appears.
2. In the **Network Interfaces** table, click the appliance name to open the **Configure Network Interfaces** page for that appliance.

3. On the **Configure Network Interfaces** page, configure the settings for the internal interface connected to your internal (or private) network:
   - Type an **IP address** and **Subnet mask** for the interface.
   - Select the appropriate **Interface speed** from the list. You can configure an adapter to automatically sense the speed of your network, but that may cause compatibility issues with some network devices. It’s usually best to manually configure the network interface speed.

4. To run the appliance with both network interfaces, configure the settings for the interface connected to the external network (or Internet):
   - To enable the external interface, select the **Enable external interface** check box.
   - Type the **IP address** and **Subnet mask** settings used to access the Aventail appliance from the Internet. Note that the external IP address must be publicly accessible.
   - Select the appropriate **Interface speed** from the list.

5. Click **Save** to save your changes. After AMC has made your changes, the browser session times out. If you need to perform any other system configuration tasks, log back in to AMC.
Notes

- Many popular switches (for example, Cisco) do not properly detect the duplex mode configured on the appliance. For this reason, it is recommended that you not set them to autonegotiate. If you experience network latency, check the switch port settings to which the appliance is connected to see if they are using the proper configuration. If they are configured incorrectly, configure the switch port to statically assign settings that match the appliance.

- If you configure the appliance to use both interfaces, verify the routing settings to make sure that you have a network route to the internal interface. If the appliance is on a different network than the computer you’re using to access AMC, you’ll need to either define a static route to the network on which the appliance is installed or enable dynamic routing to maintain access to AMC after you apply your network configuration changes. For more information, see “Configuring IP Routes” on page 33.

Configuring IP Routes

To route traffic, you must specify a default gateway. Also, for the appliance to reach your internal network resources, you must provide the appliance with routing information. You can do this by using dynamic routing or by defining static routes.

Configuring the Default Gateway

The default gateway determines where the appliance sends packets that are not explicitly routed. This will be the address of the router that provides access to the Internet.

To configure routing information

1. From the main navigation menu, click Network Settings. The General page appears.
2. On the General page, click the Routing tab.
3. Type the IP address of the router providing access to the Internet in the Default gateway IP address box.

If you’re using AMC for the first time after running Setup Tool, the gateway you specified will appear here. If this is not the gateway that provides access to the Internet (which will often be the case if you’ve enabled both network interfaces) you’ll need to edit this setting accordingly.
4. Click **Save**.

---

**CAUTION!**

If you configure the appliance to use both interfaces, verify the routing settings to make sure that you have a network route to the internal interface. If the appliance is on a different subnet than the computer you’re using to access AMC, you’ll need to either use the dynamic routing option or define a static route to the network on which the appliance is installed.

For example, assume that you’re configuring the appliance to use both interfaces. When you run Setup Tool, you define a default gateway that provides access to AMC from the internal interface. Next, you log in to AMC, enable the external interface, and change the default gateway to point to the router providing Internet access from the external interface. Assuming that the computer you’re using to browse to AMC is on a different subnet than the appliance, applying those changes would cut off your access to AMC.

To avoid this problem, you must do one of the following before applying your network configuration settings:

- Enable the dynamic routing option.
- Define a static route to the subnet on which AMC is located.

---

**Configuring Dynamic Routing**

To use dynamic routing, you must be running version 1 or version 2 of the Routing Information Protocol (RIP) on your internal routers. You can enable dynamic routing on the internal interface, the external interface (if you’ve configured the appliance to use it), or both. For more information on RIP, see [http://www.ietf.org/rfc/](http://www.ietf.org/rfc/) and read RFC 1058 for RIPv1 or RFC 2453 for RIPv2.

**To configure dynamic routing**

1. Confirm that your site supports RIP.
2. From the main navigation menu, click **Network Settings**. The **General** page appears.
3. On the **General** page, click the **Routing** tab.

   ![Dynamic routing](#)

   If the routers on your network support RIP, you can configure the appliance to support dynamic routing.

   - [ ] **Disabled**
   - [ ] **RIP v1**
   - [ ] **RIP v2**

   **RIPv2 authentication:**

   - [ ] **None**
   - [ ] **Password**

   **Interface selection:**

   - [ ] **Internal**

4. In the **Dynamic Routing area**, click the appropriate **Mode**:

   - **RIP v1**, if your site supports version 1 of RIP
   - **RIP v2**, if your site supports version 2 of RIP

5. If you selected **RIP v2**, select the appropriate **RIPv2 authentication**. The options are **None** or **Password**.

6. If you selected **Password** as the **RIPv2 authentication**, type the actual password text in the **Password** box. It can be no longer than 16 characters.

7. In the **Interface selection** box, select the interface(s) on which dynamic routing should be enabled.
8. Click **Save**.

**Notes**
- The RIP route processor on the appliance will not start until you apply the configuration changes. For more information, see “Applying Configuration Changes” on page 27.
- The RIP daemons running on the appliance execute in passive mode only. In other words, they listen for route information from other RIP routers but do not advertise route information.
- You can view a snapshot of the current routing table (including both dynamic and static routes) in AMC. See “Viewing the Current Routing Table” on page 236 for more information.
- If you select an interface that is not enabled, AMC displays an error message (“Interface is not enabled.”) when you try to submit the configuration change.
- It’s best not to enable RIP on the external interface unless you are using RIPv2 with authentication. Otherwise, you could compromise security.

**Configuring Static Routes**

If RIP is not supported at your site or if you prefer not to use dynamic routing, you must explicitly define static routes. This adds entries to the routing table for networks reached from the internal interface. You can add as many static routes as you need.

The decision on whether to use dynamic or static routing depends on your situation. Maintaining static route tables can become quite cumbersome, especially at large sites. Dynamic routing, however, increases network traffic. Choose the option that best fits your situation. You can use both options if needed. The appliance will use all routes it can find.

**To configure static routing information**
1. From the main navigation menu, click **Network Settings**. The **General** page appears.
2. On the **General** page, click the **Routing** tab.

3. To define a static route:
   a. In the **Static routes** section, type the route information in the **IP address**, **Subnet mask**, and **Gateway** boxes.
   b. Click **Add**. The route you just added is displayed in the static route table.
4. Click **Save**.

**To delete a static route**
1. On the **Routing** page, click the **Delete** button to the right of the static route(s) you want to remove.
2. Click **Save**.
Notes

- If you configure the appliance to use both interfaces, verify the routing settings to make sure that you have a network route to the internal interface. If the appliance is on a different network than the computer you’re using to access AMC, you’ll need to define a static route to the network on which the appliance is installed to maintain access to AMC after you apply your network configuration changes. For more information, see “Configuring IP Routes” on page 33.

- If your internal network has a contiguous address space, you can combine multiple static routes into one entry by specifying the proper subnet mask when you create the static route. The following table provides two examples of using a subnet mask to route internal traffic to multiple networks from a single static route entry.

<table>
<thead>
<tr>
<th>To route traffic to these networks:</th>
<th>...type this IP address:</th>
<th>...and this subnet mask:</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0</td>
<td>192.168.0.0</td>
<td>255.255.252.0</td>
</tr>
<tr>
<td>192.168.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.<em>.</em></td>
<td>192.168.0.0</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>(all networks in 192.168 range)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If necessary, you can explicitly create additional static routes for other subnets, because the routing table searches netmasks from most specific to least specific.

Configuring Name Resolution

The appliance needs access to DNS servers to resolve host names to IP addresses. If you use ASAP WorkPlace to browse Windows networks, you also need to specify a Windows Internet Name Service (WINS) server and Windows domain name.

Configuring Domain Name Service

Configuring a DNS server enables the appliance to correctly resolve host names. Properly configuring DNS ensures that the appliance can provide access to your network resources.

To configure DNS name resolution

1. From the main navigation menu, click **Network Settings**. The **General** page appears.
2. On the **General** page, click the **Name Resolution** tab.
3. In the **Search domains** box, type the default DNS domain name for your company (such as *example.com*). This domain name will be appended to unqualified host names to resolve them. You can type multiple domain names, separated by semicolons.

4. In the **DNS server** boxes, type the IP address(es) of your primary and two backup DNS servers. The backup servers are used in case the primary server is unavailable.

5. Click **Save**.

**Notes**

- Changing your DNS settings will require the client/server access service to restart, which will terminate any existing Aventail Connect or Aventail OnDemand connections. You may want to perform these changes during off-peak hours, or during a maintenance window.

### Configuring Windows Network Name Resolution

If you want to browse files on a Windows network using Aventail ASAP WorkPlace, you must specify a Windows Internet Name Service (WINS) server and a Windows domain name. WorkPlace uses this information to perform name resolution and build a list of resources for the user to browse.

**To configure Windows network name resolution**

1. From the main navigation menu, click **Network Settings**. The **General** page appears.
2. On the **General** page, click the **Name Resolution** tab.

3. Under **Windows networking**, type:
   - The IP address of your WINS server in the **WINS server IP address** box.
   - The name of your Windows domain in the **Windows domain name** box, using NetBIOS syntax (for example, *mycompany*).

4. Click **Save**.
Configuring SSL Certificates

The appliance encrypts information using the Secure Sockets Layer (SSL) protocol. You can create a self-signed certificate using AMC, or optionally you can obtain a certificate from a commercial certificate authority (CA). Additionally, you may need to configure the Aventail clients to use the certificate roots file.

Overview: SSL Certificates

The Aventail appliance uses SSL certificates to validate the appliance's identity to connecting users, and provide a public key to secure information that the client computer sends to the server. The appliance requires two SSL certificates:

- AMC uses a certificate to secure management traffic.
- The Aventail services use a certificate to secure end-user traffic.

There are two types of certificates: self-signed and commercial certificates. With a self-signed SSL certificate, you are verifying your own identity. The associated private key data is encrypted using a password. AMC uses a self-signed certificate.

Although a self-signed SSL certificate is secure, you may want to configure the appliance with a certificate from a commercial CA. Commercial certificates are purchased from a CA such as VeriSign (http://www.verisign.com), and are usually valid for one year.

A commercial CA verifies your company's identity, in effect vouching for your identity by providing you with a certificate that the CA signs. A common analogy for a certificate from a commercial CA is a passport. You can present someone with an ID you create yourself, but they may be skeptical about your identity if they do not already know you. If you present someone with a passport issued to you by a trusted country, he or she may be more inclined to accept your identification as valid because a passport office has made an effort to verify your identity.

When deciding which type of certificate to use for the servers, consider who will be connecting to the appliance and how they will use resources on your network:

- If business partners are connecting to Web resources through the appliance, they will likely want some assurance of your identity before performing a transaction or providing confidential information. In this case, you would probably want to obtain a certificate from a commercial CA for the appliance.
  
  On the other hand, employees connecting to Web resources may trust a self-signed certificate. Even then, you may want to obtain a third-party certificate so that end users are not prompted to accept a self-signed certificate each time they connect.

- If users are accessing TCP/IP resources from the appliance, a self-signed certificate is often sufficient because the Aventail Connect client can be configured to trust self-signed certificates.

Using a Self-Signed Certificate

If you plan to use a self-signed SSL certificate (instead of obtaining a certificate from a commercial CA), you can create one using AMC.

▶ To create a self-signed certificate

1. From the main navigation menu, click SSL Settings. The SSL Certificates page appears.
2. Click the appropriate button for the type of certificate you want to create:
   - To create a certificate for the Aventail services, in the Self-signed certificate area click New Certificate.
   - To create a certificate for AMC, in the AMC certificate area click New Certificate.
The **Create Self-Signed Certificate** page or **Create AMC Self-Signed Certificate** page appears.

![Create AMC Self-Signed Certificate](image)

3. In the **Fully qualified domain name** box, type the server name as you want it to appear in the certificate:
   - For the main appliance certificate, you might type something like `vpn.example.com`. You must add this name to your external DNS to make the appliance accessible to users. Your end users will use this name to access Web-based resources on your network. You’ll reference this name when configuring the Aventail Connect or Aventail OnDemand components to provide access to TCP/IP resources.
   - For an AMC certificate, you might type something like `amc.example.com`. In most cases, you should add this name to your internal DNS to simplify access to AMC.

4. In the **Organization** box, type the company or organization name as you want it to appear in your SSL certificate.

5. In the **Country** box, type the two-letter abbreviation for your country. For a list of valid country codes, go to the International Organization for Standardization (ISO) Web site at [http://www.iso.org](http://www.iso.org) and look for information on ISO 3166-1.

6. Click **Save**.

7. To create the certificate, you must apply changes (see “Applying Configuration Changes” on page 27).

### Creating the Trusted Roots File for a Self-Signed Certificate

If you use a self-signed certificate, you will need to provide your users with a trusted roots file.

**To create a trusted roots file for a self-signed certificate**

1. Log in to the appliance.

2. Make a copy of the `server.cert` file, which is located in `/usr/local/extranet/etc`.

3. Open the copied file in a text editor and remove everything except the root certificate. The file will contain one or more certificates as well as the private key. The root certificate is the last
certificate block in the file, including the banners. In the following example, you would delete
the first certificate block and the private key block:

```
Certificate 1
-----BEGIN CERTIFICATE-----
MIIDjgCCqjxiaqAwIBAgIQFQqPVRyCHe8HvynCvam+FyTmkY
OwVTfrVeSglVhJjdeC0uRmFm0sCr0JKn+96g+0gjaMS27Yz2U=
-----END CERTIFICATE-----

Root certificate
-----BEGIN CERTIFICATE-----
MIIDjgCCqjxiaqAwIBAgIQFQqPVRyCHe8HvynCvam+FyTmkY
OwVTfrVeSglVhJjdeC0uRmFm0sCr0JKn+96g+0gjaMS27Yz2U=
-----END CERTIFICATE-----

Private key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIDjgCCqjxiaqAwIBAgIQFQqPVRyCHe8HvynCvam+FyTmkY
OwVTfrVeSglVhJjdeC0uRmFm0sCr0JKn+96g+0gjaMS27Yz2U=
-----END ENCRYPTED PRIVATE KEY-----
```

The resulting file would look like this:

```
-----BEGIN CERTIFICATE-----
MIIDjgCCqjxiaqAwIBAgIQFQqPVRyCHe8HvynCvam+FyTmkY
OwVTfrVeSglVhJjdeC0uRmFm0sCr0JKn+96g+0gjaMS27Yz2U=
-----END CERTIFICATE-----
```

4. Distribute this file to your end users. This increases security and prevents users from being
prompted to accept the SSL certificate each time they connect. See “Adding a New Roots

- For users connecting to the client/server access service via the Aventail Connect client,
  configure the client on each of your users’ computers to use this trusted roots file. The
  file should also become part of the Aventail Connect provisioning package.
- If you want increased security for your Web-based users, this file should be included in
  the browsers for these users.

Notes

- The Setup Tool included with the appliance creates a self-signed certificate for AMC. For most
deployments, this self-signed certificate is sufficient and there is no need to obtain a certificate
from a commercial CA. It is important, however, to use AMC within a trusted network. Self-
signed certificates protect against passive eavesdroppers but not against active attackers.
- If you’re deploying Aventail OnDemand for Microsoft Internet Explorer users on the Apple
Macintosh, you’ll need to obtain a commercial SSL certificate. A self-signed certificate will not
work because the Macintosh Java Virtual Machine (JVM) won’t accept a certificate signed from
an unknown CA.
Obtaining a Certificate from a Commercial CA

Obtaining a certificate from a commercial CA provides verification of your identity for people who connect to your network through the appliance. You’ll need to perform several steps to obtain and configure a certificate from a commercial CA. The steps in this process are shown below.

1. **Generate a CSR**
   - Create a Certificate Signing Request (CSR)

2. **Submit the CSR to a CA**
   - Submit the CSR to a commercial Certificate Authority (CA)

3. **Add CA’s roots file to CSR response**
   - (Optional) If the CA didn’t include a trusted roots file in the CSR response, add it

4. **Import the CSR response**
   - Import the CSR response into AMC to create a certificate

5. **Apply your changes**
   - This restarts the services to activate the certificates

6. **Configure Aventail clients**
   - Configure Aventail Connect or OnDemand to use the trusted roots file

The steps in this process are described in the following sections. This section focuses on obtaining a commercial certificate for the Aventail servers. (AMC is configured to use a self-signed certificate.)

**Step 1: Generate a Certificate Signing Request**

Using AMC, you can generate a certificate signing request (CSR). This process creates an RSA keypair that will be used to secure server information, and a CSR containing your public key and identity information. The information you provide is used by the commercial CA to generate your certificate, and may be visible to end users who connect to the appliance.

- **To generate a CSR**
  1. From the main navigation menu, click **SSL Settings**. The **SSL Certificates** page appears.
2. In the **Certificate signing request** area, click the **Create New CSR** button. The **Create Certificate Signing Request** page appears.

3. Complete the information under the **Certificate information** area. This information is stored in the CSR and used by the commercial CA when generating your certificate. Note that this information may be visible to end users who connect to the appliance.
   a. In the **Fully qualified domain name** box, type the server name as you want it to appear in the certificate. Also known as a "Common Name" (or CN), this is usually composed of a host and a domain name; for example, you might type `vpn.example.com`. Note that your Web-based end users will use this name to access the appliance (in other words, to access ASAP WorkPlace) so it’s best to use a name that is easily remembered. You’ll also reference this name when configuring the Aventail Connect or Aventail OnDemand components to provide access to TCP/IP resources. You must add this name to your external DNS to make the appliance accessible to users.
   b. In the **Organizational unit** box, type your division or department name (for example, **IT Department**).
   c. In the **Organization** box, type your company or organization name as you want it to appear in your SSL certificate.
   d. In the **Locale** box, type the name of your city or town. Spell out the name in full (don’t use an abbreviation).
   e. In the **State** box, type the name of your state or province. Spell out the name in full (don’t use an abbreviation).
   f. In the **Country** box, type the two-letter abbreviation for your country. For a list of valid country codes, see the International Organization for Standardization (ISO) Web site at [http://www.iso.org](http://www.iso.org) and search for ISO 3166-1.
   g. In the **Key length** list, select the key length you want to use for the key. You can choose either 512, 768, 1024 (the default), 1280, or 1536. Larger keys increase security, but make the appliance run more slowly. A key length of 1024 or 1280 is recommended for most installations.
4. Review the information to verify that you’ve typed it correctly, and then click **Save** to generate the CSR. The **Create Certificate Signing Request** page appears.

5. Copy the contents of the CSR text from AMC to the clipboard or into a text file, and then click **OK**.

**Notes**

- The **Status** area beneath the **Certificate signing request** area indicates that you have a pending CSR. Do not resubmit the CSR, or you may be billed twice by the CA. This would also change the internal private key, making the response from the CA unusable.

- Some commercial CAs may have problems reading CSRs that contain shifted characters (characters produced by pressing the SHIFT key) such as “&” or “!”. When specifying your company name or other information, you may want to spell out “&” (if used) as “and” and omit other shifted characters.

### Step 2: Submit the CSR to a Commercial CA

The process of submitting a CSR will vary, depending on which commercial CA you choose. VeriSign is a popular commercial CA that provides SSL certificates through their Secure Site Services; for information see [http://www.verisign.com](http://www.verisign.com).

**To submit a CSR to a commercial CA**

1. Copy the contents of your certificate signing request from the **Certificate Signing Request** page in AMC.
2. Submit it to the CA using the method they request. Usually you’ll either copy and paste the CSR text into a form on the CA’s Web site, or attach it to an e-mail message.
Depending on what is specified by the CA, you may need to paste all the text, or only the text between the BEGIN NEW CERTIFICATE REQUEST and END NEW CERTIFICATE REQUEST banners (including the banners themselves). If you’re not sure, contact the CA.

3. Wait for the commercial CA to verify your identity. You may be asked to produce one or more documents attesting to your corporate identity (such as a business license or article of incorporation).

**Step 3: Review CSR Response and Add CA’s Root Certificate (if necessary)**

After you’ve submitted your CSR, you must wait for the CA to verify your identity. After they complete this process, the CA will send you the certificate reply. It usually comes to you in one of two formats:

- **A file attached to an e-mail message.** In this case, you can save the file to your local file system (the one from which you’ll access AMC) and then import it into AMC.
- **Text embedded within an e-mail message.** In this case, you’ll copy the text and paste it into a text box provided in AMC. Be sure to include the BEGIN CERTIFICATE and END CERTIFICATE banners.

If the CA does not provide a full certificate chain in the CSR response (a common practice), AMC will try to complete the certificate chain when you import the CSR response. If it is unable to complete the chain, AMC will display the following error message: “The certificate chain is not complete.” If this occurs, you must upload the CA’s root certificate and/or any intermediary public certificate(s) to the appliance. If you are acting as your own CA, you will probably need to perform this step.

- **To complete a certificate chain**
  1. Obtain the trusted root certificate or intermediary public certificate from the CA. Most external commercial CAs provide the certificates on their Web site; if the CA is run by your company, check with the server administrator.
  2. From the main navigation menu, click **SSL Settings** and then click the **CA Certificates** tab.
  3. In the **Appliance root certificates** section, click the **Import** button. The **Import Root Certificate** page appears.
  4. Upload the certificate:
     - If the certificate is in binary format, click the **Browse** button and then upload the certificate reply from your local file system (that is, the computer from which you’ve logged in to AMC).
     - If the certificate is in base-64 encoded (PEM) text format, select the **Certificate text** button and then paste the certificate into the text box. Be sure to include the BEGIN CERTIFICATE and END CERTIFICATE banners.
  5. Click **Save** to return to the **CA Certificates** page.
  6. To verify that the certificate was properly uploaded, click the **Manage CA Certificate** button at the top of the page. The new certificate should appear at the top of the **Manage Root Certificates** page.

**Step 4: Import the CSR Response Into AMC**

- **To import a certificate reply**
  1. From the main navigation menu, click **SSL Settings**. The **SSL Certificates** page appears.
  2. In the **Certificate Signing Request** area, click **Import CSR Response**. The **Import CSR Certificate** page appears.
  3. Upload the certificate:
• If the certificate is in binary format, click the **Browse** button and then upload the certificate reply from your local file system (that is, the computer from which you've logged in to AMC).

• If the certificate is in base-64 encoded (PEM) text format, select the **Certificate text** button and paste the certificate into the text box. Be sure to include the **BEGIN CERTIFICATE** and **END CERTIFICATE** banners.

4. Click **Save** to return to the **SSL Certificates** page.

5. To verify that the certificate was properly uploaded, click the **View details** button. The certificate should appear at the top of the **Certificate Details** page.

**Step 5: Apply Your Changes**

To start using a new certificate, you need to apply your configuration changes. For more information, see “Applying Configuration Changes” on page 27.

After applying the change, the appliance examines the new certificate and begins using it for all new connections. If the appliance fails to correctly process the certificate, you’ll see a failure message and the event log will contain information about the failure. Typically, this occurs if there is no certificate, the certificate has expired (or is not yet valid), or the cached password in the encrypted password file is incorrect.

**Step 6: Configure Aventail Connect to Use the Roots File**

Client/server applications are accessed using the Aventail Connect client. When the client receives a certificate from the appliance, it examines the root of the certificate chain and matches it against its own list of trusted roots. If the roots match, the client knows the appliance identity is valid and does not prompt the user to validate the certificate. To avoid requiring the user to validate the certificate, configure Aventail Connect to use the roots file.

For instructions on configuring Aventail Connect with a roots file, see "Configuring Server Validation Options" in the **Aventail Connect Administrator’s Guide**.

**Notes**

• If your users authenticate using digital certificates, you’ll need to configure trusted roots files on the servers as well as on the clients. See “Configuring Client Certificates” on page 49.

**Importing an Existing Certificate from Another Computer**

If you already have a certificate from a commercial CA, you may want to transfer it and its private key to the appliance. After you import the certificate, it will be used by the servers to secure end-user traffic on the appliance.

Note that the appliance stores certificates in the PKCS#12 format. If your certificate is stored in a different format, you’ll need to convert it to PKCS#12 using a tool such as OpenSSL (see “Helpful Management Tools” on page 12 for more information) before importing. After performing the conversion, confirm that the PKCS#12 file contains the complete certificate chain.

**To transfer an existing certificate to the appliance**

1. From the main navigation menu, click **SSL Settings**. The **SSL Certificates** page appears.

2. In the **Appliance certificate** area, click **Import**. The **Import Certificate** page appears.

3. Click the **Browse** button and upload the certificate from your local file system (that is, the computer from which you’ve logged into AMC).

4. Type the password that was used to encrypt the private key in the **Password** box.

5. Click **Save**.

Note that the appliance will use the previous certificate until you apply your configuration changes.
Managing Certificates

This section describes a variety of tasks related to managing certificates. It discusses configuring the Aventail clients to use a roots file and how to verify the roots file from back-end Web resources. It also explains how to review a certificate’s details, change the password for a certificate, and renew a certificate using an existing key.

Overview: CA Certificates

Every CA requires a root certificate so that it can be “trusted” by entities that request digital certificates from it. If a client trusts the root certificate of a CA, it automatically trusts any other certificates that are issued by that CA. Root certificates thus form one of the foundations of public key cryptography. The root certificate is either signed by the CA itself (self-signed) or by a higher authority in a hierarchy of CAs in a public key infrastructure (PKI).

The appliance includes over 100 certificates from leading commercial CAs. If you’ve obtained a certificate from a commercial CA, their root certificate and/or intermediary public certificate is likely already installed on the appliance. However, if you are acting as your own CA you will need to import a root and/or intermediary public certificate to the appliance.

The appliance is configured with several certificates:

- **Appliance’s SSL certificate.** In most deployments, you’ll obtain the main server certificate from a commercial CA. If so, the necessary CA certificates are already installed on the appliance. However, if you are acting as your own CA you will need to import a root and/or intermediary public certificate to the appliance.

- **Secure LDAP or AD server connections.** Securing your LDAP or Active Directory (AD) connection with SSL enhances security by preventing attempts to impersonate the LDAP or AD server. To configure LDAP or AD over SSL, the appliance must be configured with the root and/or intermediary public certificates for the CA that granted your LDAP or AD certificate.

- **Client certificate authentication** If your users authenticate using client certificates, the appliance must be configured with the root and/or intermediary certificates for the CA that issued the client certificates to your end users. These CA certificates are used to verify the validity of certificates submitted by users who connect to the appliance.

- **Connections to back-end HTTPS Web servers** If you have a back-end Web resource that is secured with SSL (that is, it uses HTTPS instead of HTTP), the appliance can be configured with the root and/or intermediary public certificates for the CA that issued the server certificate.

If you can successfully establish a connection with the back-end Web resource, then the appliance is already configured with the necessary CA certificates. If you cannot establish a connection, you will need to upload the CA certificate to the appliance.

You can view the list by clicking the Manage CA Certificate button on the CA Certificates tab of the SSL Certificates page. This displays the Manage Root Certificates popup window, which can also be used to delete CA certificates.

Viewing Certificate Details

You can view the details for the appliance certificate, such as the subject, issuer, start and end time, serial number, and MD5 checksum. Details of a newly imported certificate are not available until you have applied the configuration change.

- **To view the certificate details**

  1. From the main navigation menu, click SSL Settings. The SSL Certificates page appears.
2. On the **SSL Certificate** page, you can review the fully qualified domain name for the certificate, who issued the certificate, and its expiration date.

<table>
<thead>
<tr>
<th>SSL Certificates</th>
<th>CA Certificates</th>
<th>SSL Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage SSL server certificates used by the appliance and AMC.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Appliance certificate**

The appliance is currently configured with the following certificate:

- **Issued to:** vpn.example.com
- **Issued by:** vpn.example.com
- **Valid through:** Sun Sep 20 04:01:60 PDT 2009

3. Click **View details** to view more detailed information about the certificate.

![Certificate Details](image)

**Notes**

- If the CA doesn’t include a common name (CN) in the certificate, the **Issued To** and **Issued By** fields will display the full subject/issuer name (for example, C=US,O=Example Corp,CN=vpn.example.com).

**Exporting the SSL Certificate**

You can export the SSL certificate used to secure end-user traffic on the appliance. It will be saved in PKCS#12 format.

1. From the main navigation menu, click **SSL Settings**. The **SSL Certificates** page appears.
2. In the **Appliance certificate** area, click **Export**. The **Export Certificate** page appears.
3. In the **Password** box, type the password that you want to use to encrypt the private key.
4. Click **Save**, then download the certificate file to your local file system (that is, the computer from which you’ve logged into AMC).
5. Click **OK** to return to the **SSL Certificates** page.
Adding a CA Certificate to the Appliance

If the appliance is not configured with the necessary CA certificate, you’ll need to obtain a copy and upload it to the appliance.

To add a new CA certificate to the appliance

1. Obtain the trusted root certificate or intermediary public certificate from the CA. Most external commercial CAs provide the certificates on their website; if the CA is run by your company, check with the server administrator.
2. From the main navigation menu, click SSL Settings and then click the CA Certificates tab.
3. Click the appropriate Import button:
   • For certificates used to secure connections with an LDAP or AD server or for use with client certificates, click the Import button in the Appliance root certificates area.
   • For certificates used to secure connections with back-end HTTPS Web resources, click the Import button at the bottom of the page in the Back-end server root certificates area.
4. Upload the certificate:
   • If the certificate is in binary format, click the Browse button and then upload the certificate reply from your local file system (that is, the computer from which you’ve logged in to AMC).
   • If the certificate is in base-64 encoded (PEM) text format, click the Certificate text button and then paste the certificate into the text box. Be sure to include the BEGIN CERTIFICATE and END CERTIFICATE banners.
5. Click Save to return to the CA Certificates page.
6. To verify that the certificate was properly uploaded, click the Manage CA Certificates button. The new certificate should appear at the top of the Manage Root Certificates page.
7. If you uploaded a roots file for use with client certificate authentication, you must stop and restart the Web access service and the client/server access service.

Since this will briefly interrupt service to users, it’s best to perform this procedure during a maintenance window. See “Stopping and Starting the Aventail Services” on page 155 for details.

Notes

• By default, the Web access service is configured to verify the root certificate presented by back-end HTTPS Web servers. This important security check will help ensure that you can trust the identity of the back-end server. See “Configuring the Web Access Service” on page 156 for details.

Adding a New Roots Certificate for a Back-End HTTPS Resource

If you have a back-end Web resource that is secured with SSL (that is, it uses HTTPS instead of HTTP), you should configure the Web access service to verify the root certificate presented by the back-end server. This important security check will help ensure that you can trust the identity of the back-end server. See “Configuring the Web Access Service” on page 156 for details.

If the back-end server’s roots certificate is not pre-installed on the appliance, you’ll need to obtain a copy and import it in AMC.

To add a new back-end HTTPS roots certificate on the appliance

1. From the main navigation menu, click SSL Settings and then click the CA Certificates tab.
2. In the Back-end server root certificates area, click the appropriate Import button.
3. Upload the certificate:
- If the certificate is in binary format, click the **Browse** button and then upload the certificate reply from your local file system (that is, the computer from which you've logged in to AMC).
- If the certificate is in base-64 encoded (PEM) text format, click the **Certificate text** button and then paste the certificate into the text box. Be sure to include the **BEGIN CERTIFICATE** and **END CERTIFICATE** banners.

4. Click **Save** to return to the **CA Certificates** page.

5. To verify that the certificate was properly uploaded, click the **Manage CA Certificates** button. The new certificate should appear at the top of the **Manage Root Certificates** page.

**Notes**
- The Web access service is configured to verify the back-end certificates for HTTPS. You can review the downstream Web server configuration settings in AMC; for more information, see "Configuring the Web Access Service" on page 156.
- If you do not want to trust a CA listed in the **Manage Root Certificates** page, you delete it by selecting the check box next to the certificate and clicking **Delete**.

**Adding a New Roots Certificate for LDAP or Active Directory over SSL**

Securing your LDAP or Active Directory (AD) connection with SSL enhances security by preventing attempts to impersonate the LDAP or AD server. To configure LDAP or AD over SSL, you must add the root certificate for the CA that granted your LDAP or AD certificate to the SSL trusted roots file. Also, if you are using digital certificates to authenticate users, you must add the root certificate for the CA that issued the client certificates to your end users.

To add the CA root certificate for your LDAP or AD server to the appliance

1. From the main navigation menu, click **SSL Settings** and then click the **CA Certificates** tab.
2. In the **Appliance root certificates** area, click the appropriate **Import** button.
3. Upload the certificate:
   - If the certificate is in binary format, click the **Browse** button and then upload the certificate reply from your local file system (that is, the computer from which you've logged in to AMC).
   - If the certificate is in base-64 encoded (PEM) text format, click the **Certificate text** button and then paste the certificate into the text box. Be sure to include the **BEGIN CERTIFICATE** and **END CERTIFICATE** banners.
4. Click **Save** to return to the **CA Certificates** page.
5. To verify that the certificate was properly uploaded, click the **Manage CA Certificates** button. The new certificate should appear at the top of the **Manage Root Certificates** page.

Note that this trusted roots file must contain both the root certificate for the CA that issued the LDAP or AD certificate as well as the CA that issued client certificates to your end users (if you are using client certificates).

**Configuring Client Certificates**

If your users authenticate using client certificates, you must configure the trusted roots file (for verifying client certificates) on the appliance. The roots file is used to verify the validity of certificates submitted by users who connect to the appliance. It's best to perform this procedure during a maintenance window as service to users will be briefly interrupted.

To configure the appliance to use your roots file

1. Rename the roots file to `ldapca.cert`.
2. Copy the `ldapca.cert` file to the `/usr/local/aventail/etc` directory.
3. Stop and restart the Web access service and the client/server access service. This will briefly interrupt service to users, but this step is necessary for the services to begin recognizing the new roots file. See “Stopping and Starting the Aventail Services” on page 155 for details.

Notes
• To work correctly, the roots file should be in PEM format (base64-encoded). See “Certificate FAQ” on page 50 for details on how to convert the file.

Certificate FAQ

This section addresses frequently asked questions about working with certificates.

• **How do I obtain a certificate from a non-commercial CA?**
  The process is identical to that used to obtain a certificate from commercial CA, except that you submit the CSR to a non-commercial CA (such as a Microsoft Self-Signed Certificate Authority). This portion of the process is outlined in “Step 2: Submit the CSR to a Commercial CA” on page 43.

• **When do certificates expire?**
  Self-signed certificates are valid for five years. The expiration date for third-party certificates will vary, depending on who issued the certificate; contact the CA for more information.

• **What are the different CA roots files on the appliance and how are they used?**
  The `ldapca.cert` file in `/usr/local/aventail/etc` should contain any roots certificates from any of several sources:
  • If you have users who authenticate using client certificates, it will contain the trusted roots from the CA that issued the certificates.
  • If you are using secure LDAP (LDAPS) with username and password authentication, it will contain the trusted roots from the CA that issued the certificate for the LDAP server.
  • If you are using secure LDAP (LDAPS) with client certificate authentication, it will contain the trusted roots from the CA that issued the certificate for the LDAPS server. (If the LDAPS and client certificates are issued by the same CA, then you only need one signer key.)

  The `backendca.cert` file in `/usr/local/extranet/etc` should contain any roots certificates from CAs that issued SSL certificates in use on back-end secure Web servers (HTTPS) managed by the Web access service. This is not required if the Web access service is managing non-secure (HTTP) resources. For more information, see “Adding a New Roots Certificate for a Back-End HTTPS Resource” on page 48.

• **How many trusted root certificates can go in the trusted roots files?**
  The roots file can contain as many certificates as you want to trust. When placing certificates in a trusted roots file, we recommend that you append the file with the `>>` command (for example, type `cat myfile >> ldapca.cert`). Encode the certificate in PEM format (base64-encoded) and be sure to include the beginning (`---BEGIN CERT...`) and ending (`----END CERT...)` banners.

• **Can private keys or CSRs generated from other tools be imported to the appliance?**
  Private keys and CSRs must be generated on the appliance using Setup Tool or the certificate generation tool. However, you can copy private keys and CSRs from one Aventail appliance to another using secure copy (scp). Note that any copied certificates will be overwritten if you make changes to them from within AMC.

• **Where is the AMC certificate stored?**
  AMC’s self-signed certificate is stored in `/usr/local/app/mgmt-server/sysconf/active/keystore.jetty`. For AMC, a self-signed certificate is sufficient for most environments. It is important, however, to use AMC within a trusted network. Self-signed certificates protect against passive eavesdroppers but not against active attackers.
• **What are the different CA roots files on the appliance and how are they used?**

The `ldapca.cert` file (stored in `/usr/local/aventail/etc`) contains roots certificates from any of several sources:

- If you have users who authenticate using client certificates, it will contain the trusted roots from the CA that issued the certificates.
- If you are using secure LDAP (LDAPS) with username and password authentication, it will contain the trusted roots from the CA that issued the certificate for the LDAP server.
- If you are using secure LDAP (LDAPS) with client certificate authentication, it will contain the trusted roots from the CA that issued the certificate for the LDAPS server. (If the LDAPS and client certificates are issued by the same CA, then you only need one signer key.)

The `backendca.cert` file (stored in `/usr/local/extranet/etc`) contains roots certificates from CAs that issued SSL certificates in use on back-end secure Web servers (HTTPS) managed by the Web access service. This is not required if the Web access service is managing non-secure (HTTP) resources. For more information, see “Adding a New Roots Certificate for a Back-End HTTPS Resource” on page 48.

• **I don’t want to trust a CA listed in one of the appliance’s root certificates. How do I modify a trusted certificate?**

If you do not want to trust a CA, you can establish an SSH connection to the appliance, open the certificate file (either `backendca.cert` or `ldapca.cert`) in a text editor and then remove the CA’s certificate from the list.

• **How many trusted root certificates can go in the trusted roots files?**

The roots file can contain as many certificates as you want to trust. When placing certificates in a trusted roots file, we recommend that you append the file with the `>>` command (for example, type `cat myfile >> ldapca.cert`). Encode the certificate in base64-encoded (PEM) format and be sure to include the beginning (`---BEGIN CERT...`) and ending (`---END CERT...`) banners.

### Managing User Authentication

Authentication is the process of verifying a user’s identity to ensure that the individual really is who he or she claims to be. (Authentication differs from authorization. Authentication verifies identity, while authorization specifies access rights.) This section describes how to configure user authentication.

To manage user authentication, you must define one or more external authentication servers. Authentication servers are referenced by the realms you set up for users to log in the appliance. Realms serve two distinct purposes for the Aventail VPN: in addition to managing user authentication, they also define user communities by deploying access agents and establishing zones of trust. For information on using realms to define user communities, see “Managing Realms” on page 108.

### Configuring Authentication Servers

Using AMC to set up authentication involves configuring the combination of a directory (LDAP, Microsoft Active Directory, RADIUS, or local users), an authentication method (username/password, token or smart card, or digital certificate), and other configuration items that make the authentication process unique (for example, the LDAP search base or the specific directory server). The Aventail appliance supports the following directories and authentication methods:

- LDAP with username/password or digital certificate
- Microsoft Active Directory with username/password
- RADIUS with username/password or token-based authentication (such as SecurID or SoftID)
- Local users (used primarily for testing purposes and not recommended in a production environment)
After you reference an authentication server in a realm and associate users with the realm, the appliance checks users’ credentials against the credentials stored in the specified authentication repository.

**Defining Multiple Authentication Servers**

The appliance supports the definition and use of multiple authentication servers. Following are examples of what might constitute different authentication servers referenced by realms:

- **Multiple combinations of directory/authentication method** such as LDAP with username/password or LDAP with digital certificate. For example, suppose your company employees log in with usernames and passwords but the employees of your call center subdivision log in with digital certificates. You would create an *employee* realm and a *callcenter* realm, each referencing the appropriate authentication method and LDAP search base.

- **Multiple instances of the same directory/authentication method that are using different back-end servers** such as two RADIUS/password instances using different RADIUS servers. In this case you would define two authentication servers, each with the appropriate server information.

- **Multiple instances of the same directory/authentication method on the same server but configured in a different way** such as two instances of LDAP with username/password on the same server but using different search bases (which results in each realm searching a different subtree within the directory). For example, suppose Partner A is in one LDAP subtree and Partner B is in another. You would define a *partnerA* realm and a *partnerB* realm, each configured with the appropriate search base.

AMC also provides “group affinity checking,” which accommodates network environments where authentication and authorization are handled by different servers. For more information, see “Enabling Group Affinity Checking in a Realm” on page 114.

**Referencing an Authentication Server in a Realm**

When you create a realm in AMC, you are required to associate the realm with an authentication server before you can save the realm configuration. This is described in "Creating and Configuring a Realm" on page 110. If at a later date your authentication process changes, you can reconfigure a realm to reference a different authentication server.

► **To reference an authentication server in realm**

1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.

2. In the **Realms** table, click the name of the realm you want to configure to reference the authentication server. The **Configure Realm** page appears.

3. In the **Authentication server** list, select the name of the authentication server you want the realm to use for verifying users’ identities.

   Alternatively, you can click **New** to create a new authentication server and then reference it in the realm.

4. Click **Save** to return to the **Authentication** page.
Configuring LDAP and LDAPS Authentication

The Aventail appliance supports authentication via the LDAP or LDAPS (LDAP over SSL) protocols. Either protocol can be used to validate username and password credentials or digital certificates. The following illustration shows typical LDAP configuration options.

Securing your LDAP connection with SSL requires additional configuration. You must add the root certificate of the CA that granted your LDAP certificate to the SSL trusted roots file. This enhances security by preventing attempts to impersonate your LDAP server. See "Adding a New Roots Certificate for LDAP or Active Directory over SSL" on page 49.

After configuring an LDAP or LDAPS server, you can validate the realm configuration settings by establishing a test connection. For more information, see "Testing Authentication Configurations" on page 68.

Notes

- You'll need to modify your firewall or router to allow the appliance to communicate with your LDAP server. Standard LDAP uses port 389/tcp; LDAPS communicates over port 636/tcp.

Configuring LDAP with Username and Password

Perform the following steps to configure an LDAP authentication server with username and password validation.

To configure LDAP for username/password validation
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Authentication servers area, click the New button.
3. On the New Authentication Server page, under Directory type/protocol, click LDAP.
4. Under Credential type, click Username/Password, and then click Continue. The Configure Authentication Server page appears.

5. In the Name box, type a name for the authentication server.
6. Complete the information listed under **General**:

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server:</td>
<td></td>
</tr>
<tr>
<td>Login DN:</td>
<td></td>
</tr>
<tr>
<td>Password:</td>
<td></td>
</tr>
<tr>
<td>Search base:</td>
<td>Begin searching at a specified base.</td>
</tr>
<tr>
<td>Username attribute:</td>
<td>Examples: cn, uid</td>
</tr>
</tbody>
</table>

- In the **LDAP server** box, type the host name or IP address of your LDAP server. If the LDAP server is listening on a port other than 389 (the well-known port for LDAP), you can specify a port number as a colon-delimited suffix (for example, `myldap.example.com:1300`).
- In the **Login DN** box, type the distinguished name (DN) used to establish a connection with the LDAP server.
- In the **Password** box, type the password used to establish a connection with the LDAP server.
- In the **Search base** box, type the point in the LDAP directory from which you want to begin searching for user information. Usually, this will be the lowest point in the directory tree that contains user information. For example, you might type `ou=Users,o=xyz.com`. Note that the user binding to the LDAP directory must have permissions to view the directory at this level.
- In the **Username attribute** box, type the attribute used to match usernames. This is usually `cn` or `uid`.

7. Complete the information listed under **Group lookup**:

<table>
<thead>
<tr>
<th>Group lookup</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Find groups in which a user is a member</td>
<td>[ ] Look in static groups for user members</td>
</tr>
<tr>
<td>Group attribute: memberOf</td>
<td>Cache group checking</td>
</tr>
<tr>
<td>Cache lifetime: 120 sec</td>
<td>this searches each group for a list of members</td>
</tr>
</tbody>
</table>

- If you want the LDAP search to determine a user's group membership by searching the group attribute in the user container, select the **Find groups in which a user is a member** check box and type the **Group attribute**. This attribute is most often `memberOf`. Do not select this option unless attribute-based groups are supported by and enabled on your LDAP server.
- To have the appliance look for group membership in static groups, select the **Look in static groups for user members** check box. This type of search requires searching the entire LDAP tree, which can sometimes be quite large.
  
  If your LDAP server does not support attribute-based groups or you have not enabled this functionality, you should select this option.
- If you want to save time by caching the attribute group and/or static group search results, select the **Cache group checking** check box and type the **Cache lifetime**, in seconds, that you want (the default is 120 seconds).
8. To secure the LDAP connection with SSL, complete the information under **LDAP over SSL**:

SSL encrypts passwords sent to the LDAP server. Be sure to enable SSL if your internal network is untrusted; if this option is disabled, passwords will be sent in the clear.

- To secure the LDAP connection with SSL, select the **Use SSL to secure LDAP connection** check box.
- To view your certificate details and verify that the root certificate can be used by the appliance, click **View CA Certificate**. This file should contain the root certificate of the CA that issued the LDAP certificate. If it does not, you must add it. See “Adding a New Roots Certificate for LDAP or Active Directory over SSL” on page 49 for details.
- To have the appliance verify that the LDAP host name is the same as the name in the certificate presented by the LDAP server, select the **Match certificate CN against LDAP server name** check box. Typically, your server name will match the name specified in its digital certificate. If this is the case with your server, Aventail recommends enabling this option in a production environment. This makes it more difficult for an unauthorized server to masquerade as your LDAP server if your digital certificate or DNS server becomes compromised.

9. Optionally, complete the information listed under **Advanced**:

- To enable LDAP referrals, select the **Enable LDAP referrals** check box. When this is enabled, an LDAP server that cannot answer a client’s query can refer the client to a different LDAP server that knows the answer. Use caution when enabling this feature as it can slow down the authentication process. If you are configuring LDAP to authenticate against Microsoft Active Directory, you may want to disable this feature.
- In the **Server timeout** box, type the number of seconds to wait for a reply from the LDAP server. The default value is 60.
- To enable NTLM authentication forwarding, click one of the **NTLM authentication forwarding** options. For more information, see “Configuring NTLM Authentication Forwarding” on page 69.

**Notes**

- The **Login DN** and **Password** fields are not always required to connect to an LDAP server. However, if they are not provided (or you don’t specify a password) the appliance will bind to LDAP anonymously, which usually won’t provide the appropriate permissions to perform the necessary searches to find user and group information.
• If you define multiple LDAPS servers, the `ldapca.cert` file must contain the CA root certificates needed for all of them. You should also configure the **Match certificate CN against LDAP server name** setting to be the same for each realm. (Aventail recommends enabling this option for a production environment.) Although AMC allows you to configure this setting per realm, the appliance actually uses the setting configured in the last loaded LDAPS realm. In other words, if you selected this check box for three LDAPS servers, but cleared it for a fourth LDAPS realm, the functionality would be disabled for all four servers.

### Configuring LDAP with Digital Certificates

Perform the following steps to configure an LDAP authentication server with digital certificate validation.

**To configure LDAP for digital certificate validation**

1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.
2. In the **Authentication servers** area, click the **New** button.
3. On the **New Authentication Server** page, under **Directory type/protocol**, click **LDAP**.
4. Under **Credential type**, click **Digital certificate**, and then click **Continue**. The **Configure Authentication Server** page appears.
5. In the **Name** box, type a name for the authentication server.
6. Complete the information listed under **General**:

   - In the **LDAP server** box, type the host name or IP address of your LDAP server. If the LDAP server is listening on a port other than 389 (the well-known port for LDAP), you can specify a port number as a colon-delimited suffix (for example, `myldap.example.com:1300`).
   - In the **Login DN** box, type the distinguished name (DN) used to establish a connection with the LDAP server.
   - In the **Password** box, type the password used to establish a connection with the LDAP server.
   - In the **Search base** box, type the point in the LDAP directory from which you want to begin searching for user information. Usually, this will be the lowest point in the directory tree that contains user information. For example, you might type `ou=Users,o=xyz.com`. Note that the user binding to the LDAP directory must have permissions to view the directory at this level.
7. Complete the information listed under **Matching LDAP Attributes**:

**Matching LDAP attributes**

<table>
<thead>
<tr>
<th>Attribute mapping:</th>
</tr>
</thead>
</table>

- In the **Attribute mapping** box, type a mapping of the user ID field in the certificate to the corresponding user ID field in LDAP. For example, if the `cn` field in the certificate maps to the `cn` field in LDAP, type `cn=cn`. Or, if the `cn` field in the certificate maps to the `uid` field in LDAP, type `cn=uid`. Note that the text you type here is case-sensitive.

- In the **Certificate attribute** box, type the name of the LDAP attribute that stores user certificates. This is usually `userCertificate`.

8. Complete the information listed under **Group lookup**:

**Group lookup**

- If you want the LDAP search to determine a user’s group membership by searching the group attribute in the user container, select the **Find groups in which a user is a member** check box and type the **Group attribute**. This attribute is most often `memberOf`. Do not enable this option unless attribute-based groups are supported by and enabled on your LDAP server.

- To have the appliance look for group membership in static groups, select the **Look in static groups for user members** check box. This type of search requires searching the entire LDAP tree, which can sometimes be quite large.

  If your LDAP server does not support attribute-based groups or you have not enabled this functionality, you should select this option.

- If you want to save time by caching the attribute group and/or static group search results, select **Cache group checking** and type the **Cache lifetime** that you want (the default is 120 seconds).

9. To secure the LDAP connection with SSL, complete the information under **LDAP over SSL**:

**LDAP over SSL**

SSL encrypts passwords sent to the LDAP server. Be sure to enable SSL if your internal network is not trusted; if this option is disabled, passwords will be sent in the clear.

- To secure the LDAP connection with SSL, select the **Use SSL to secure LDAP connection** check box.

- To view your certificate details and to verify that the root certificate can be used by the appliance, click **View CA certificate**. This should list the name of the CA (or CAs) who issued the client certificates and the LDAP certificates. If it does not, you must add them. See “Adding a New Roots Certificate for LDAP or Active Directory over SSL” on page 49 for details.
58 | Chapter 4 - Network and Authentication Configuration

- To have the appliance verify that the LDAP host name is the same as the name in the certificate presented by the LDAP server, select the **Match certificate CN against LDAP server name** check box. Typically, your server name will match the name specified in its digital certificate. If this is the case with your server, Aventail recommends enabling this option in a production environment. This makes it more difficult for an unauthorized server to masquerade as your LDAP server if your digital certificate or DNS server becomes compromised.

10. Complete the information listed under **Advanced**:

- To enable LDAP referrals, select the **Enable LDAP referrals** check box. When this is enabled, an LDAP server that cannot answer a client’s query can refer the client to a different LDAP server that knows the answer. Use caution when enabling this feature as it can slow down the authentication process. If you are configuring LDAP to authenticate against Microsoft Active Directory, you may want to disable this feature.

- In the **Server timeout** box, type the number of seconds to wait for a reply from the LDAP server. The default value is **60**.

11. Click **Save** to return to the **Authentication** page.

**Notes**

- The **Login DN** and **Password** fields are not always required to connect to an LDAP server. However, if they are not provided (or you don’t specify a password) the appliance will bind to LDAP anonymously, which usually won't provide the appropriate permissions to authenticate users.

- If your users authenticate using client certificates, you must configure the trusted roots file (for verifying client certificates) on each server that the users will connect to. For more information, see “Configuring Client Certificates” on page 49.

- If you define multiple LDAPS realms, the **ldapca.cert** file must contain the CA root certificates needed for all of them. You should also configure the **Match certificate CN against LDAP server name** setting to be the same for each realm. (Aventail recommends enabling this option for a production environment.) Although AMC allows you to configure this setting per realm, the appliance actually uses the setting configured in the last loaded LDAPS realm. For example, if you selected this check box for three LDAPS realms, but cleared it for a fourth LDAPS realm, the functionality would be disabled for all four realms.

**Configuring Microsoft Active Directory Servers**

The appliance can validate username/password credentials against Microsoft Active Directory (AD). If you are using Active Directory with digital certificates, you will need to configure it as an LDAP server. See “Configuring LDAP to Authenticate Against Active Directory” on page 62.

The following illustration shows typical Active Directory configuration options:
After configuring an Active Directory server, you can validate the realm configuration settings by establishing a test connection. For more information, see “Testing Authentication Configurations” on page 68.

Notes

- You’ll need to modify your firewall or router to allow the appliance to communicate with your Active Directory server. The appliance uses standard LDAP and LDAPS ports to communicate with Active Directory. The standard LDAP port is 389/tcp; LDAPS communicates over port 636/tcp.

Configuring Active Directory with Username and Password

Perform the following steps to configure an Active Directory authentication server with username/password validation.

Note that if you are using Active Directory with digital certificates, you will need to configure it as an LDAP realm. See "Configuring LDAP to Authenticate Against Active Directory” on page 62.

To configure Active Directory

1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Authentication servers area, click the New button.
4. The only Credential type that is available for Active Directory is Username/Password, so you do not need to make a selection. Click Continue. The Configure Authentication Server page appears.
5. In the Name box, type a name for the authentication server.
6. Complete the information listed under **General**:

- **Active Directory domain controller**: Enter an FQDN or IP address.
- **Active Directory domain name**: To specify a particular AD domain to use as a search base, enter its FQDN (e.g., example.com).
- **Login name**: Enter the login name you want to use to log in to the Windows domain (such as jdoe or jdoe@example.com). You may also specify a non-administrator user who has these privileges.
- **Password**: Type the password that corresponds with the login name.

7. To secure the Active Directory connection with SSL, complete the information under **Active Directory over SSL**.

- **Use SSL to secure Active Directory connection**: Make sure SSL is enabled.
- **View CA certificate**: To import a certificate, go to the SSL Settings page.
- **Match certificate CN against Active Directory domain controller**: This should list the name of the CA (or CAs) who issued the client certificates and the SSL certificates. If your Active Directory server’s CA is not listed in the file, or if you use a self-signed certificate, you must add your certificate to this file. See “Adding a New Roots Certificate for LDAP or Active Directory over SSL” on page 49 for details.

In the **Active Directory domain controller** box, type the IP address or host name of the Active Directory domain controller.

If you want to specify a particular Active Directory domain, type it in the **Active Directory domain name** box. This should be the domain that you want to use as the search base (in other words, the domain that contains the appropriate \( \text{cn} = \text{users} \) container). For example, if you want to search a single domain such as marketing, you would type marketing.example.com. If you want to search your entire company’s domain, you would type example.com. If you do not specify a domain, the appliance searches the first available default naming context on the domain controller.

To perform Active Directory searches, the appliance must log into Active Directory (unless you have configured Active Directory to allow anonymous searches). In the **Login name** box, type the user name or \( \text{sAMAccountname} \) attribute used to log in to the Windows domain (such as jdoe or jdoe@example.com).

The login should be for a user who has privileges to perform searches and view user records, such as the administrator on that domain controller. You may also specify a non-administrator user who has these privileges.

If you specify an Active Directory domain, the appliance searches that domain for users. If you do not specify a domain, the appliance searches the first available default naming context on the domain controller. If the user information is not stored in either of these locations, you will need to configure this realm as an LDAP realm. See “Configuring LDAP to Authenticate Against Active Directory” on page 62.

Type the **Password** that corresponds with the **Login name**.
To have the appliance verify that the Active Directory domain controller host name is the same as the name in the certificate presented by the Active Directory server, select the **Match certificate CN against Active Directory domain controller** check box. Typically, your server name will match the name specified in its digital certificate. If this is the case with your server, Aventail recommends enabling this option in a production environment. This makes it more difficult for an unauthorized server to masquerade as your AD server if your digital certificate or DNS server becomes compromised.

8. In the **Advanced** area, you can configure NTLM authentication forwarding options, as well as options for notifying users prior to the expiration of their Active Directory passwords. Users cannot change their passwords via the appliance, but an advance notification gives them time to change their passwords through other means.

   ![Advanced](image)

   - **Prompt user before password expires**
     - Begin prompting: **5** days before expiration

   **NTLM authentication forwarding**
   Forward NTLM credentials to back-end Web servers.

   - **Forward a custom domain name**
     - Domain name: 
   - **Forward the realm name as domain name**

   - To activate the notification functionality, select the **Prompt users before password expires** check box. Indicate when the advance notice should begin by typing the number of **days before expiration** (the default is 5 days). Your users will see the following prompt:
     
     Your password is about to expire in **<n>** days.

     where **<n>** is the value in **days before expiration**.

   - To enable NTLM authentication forwarding, click one of the **NTLM authentication forwarding** options. For more information, see “Configuring NTLM Authentication Forwarding” on page 69.

9. Click **Save** to return to the **Authentication** page.

**Notes**

- The **Login name** and **Password** fields are not always required to connect to an Active Directory server. However, if they are not provided (or you don’t specify a password) the appliance will bind anonymously. In this case, if you have not configured Active Directory to allow anonymous searches, the search will fail.

- **CAUTION** If Active Directory over SSL is not enabled, passwords will be transmitted in the clear to the Active Directory server. If the internal network is not trusted, you should enable SSL. Your Active Directory server must also be enabled to use SSL. See your Microsoft Active Directory documentation for details.

- If you define multiple Active Directory with SSL (ADS) servers, you should specify the same **Match certificate CN against Active Directory domain controller** setting for each server. (Aventail recommends enabling this option for a production environment.) Although AMC allows you to configure this setting on a per-realm basis, the appliance actually uses the setting specified in the last loaded ADS realm. For example, if you selected this check box for three ADS realms, but cleared it for a fourth ADS realm, the functionality would be disabled for all four realms.
Configuring LDAP to Authenticate Against Active Directory

If you are using Active Directory with digital certificates, you need to authenticate to Active Directory using LDAP. The procedure for configuring an LDAP server is defined in “Configuring LDAP and LDAPS Authentication” on page 53. When configuring LDAP, you should pay special attention to the attributes you're using to query the directory. Because every implementation of Active Directory is different, you must know how the object classes and related attributes are configured in your Active Directory schema.

The following table describes the key Active Directory attributes used to validate username and password credentials. Note that all attributes are case-insensitive.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login DN</td>
<td>The DN used to establish a connection with your Active Directory server. In</td>
</tr>
<tr>
<td></td>
<td>a generic Active Directory configuration located in the example.com domain,</td>
</tr>
<tr>
<td></td>
<td>the DN for a user named &quot;John Doe&quot; would be:</td>
</tr>
<tr>
<td></td>
<td>cn=John Doe,cn=users,dc=example,dc=com</td>
</tr>
<tr>
<td>Search base</td>
<td>The point in the AD directory from which you want to search for user</td>
</tr>
<tr>
<td></td>
<td>information. Usually, this will be the lowest point in the directory tree</td>
</tr>
<tr>
<td></td>
<td>that contains user information. Note that the user binding to AD must have</td>
</tr>
<tr>
<td></td>
<td>permissions to view the directory at this level.</td>
</tr>
<tr>
<td></td>
<td>For a generic installation, a search base of</td>
</tr>
<tr>
<td></td>
<td>cn=users,dc=example,dc=com will find most users. You may want to</td>
</tr>
<tr>
<td></td>
<td>search from a higher level (such as dc=example,dc=com) if some users</td>
</tr>
<tr>
<td></td>
<td>are stored in a different branch.</td>
</tr>
<tr>
<td>User name</td>
<td>The attribute used to match user names. In most AD implementations,</td>
</tr>
<tr>
<td>attribute</td>
<td>sAMAccountName will match the user ID (for example, jdoe). You can use</td>
</tr>
<tr>
<td></td>
<td>cn instead, but that would require users to authenticate with their full</td>
</tr>
<tr>
<td></td>
<td>names (John Doe) instead of their user IDs (jdoe).</td>
</tr>
</tbody>
</table>

If you've imported client certificates into Active Directory, pay close attention to the **Attribute mapping** and **Certificate attribute**. The following table describes the attributes you use to authenticate users via client certificates stored in Active Directory.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute mapping</td>
<td>This creates a mapping between the user ID field in the certificate and the</td>
</tr>
<tr>
<td></td>
<td>corresponding user ID field in Active Directory. The mapping takes the form</td>
</tr>
<tr>
<td></td>
<td>a=b, where a is the SSL attribute and b is the LDAP alias.</td>
</tr>
<tr>
<td></td>
<td>• In most implementations, <strong>cn=cn</strong> will match the CN field in the certificate with the CN field in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>• If the user’s e-mail address is defined as <strong>Email</strong> in the certificate, then <strong>Email=mail</strong> will match the corresponding field in the directory (as specified in Active Directory’s <strong>User General</strong> tab).</td>
</tr>
<tr>
<td>Certificate attribute</td>
<td>Active Directory stores user certificates in an attribute named userCertificate; therefore, type userCertificate.</td>
</tr>
</tbody>
</table>

**Notes**

- If you create an access control rule referencing a group, a user must be an explicit member of that group for his or her request to match the rule. Membership in a nested group will not result in a match. This may affect large Active Directory deployments containing nested user groups.

  For example, assume that the "SeattleCampus" group contains a group named "Marketing." Employee "John Doe" is a member of the "Marketing" group, but is not explicitly a member of "Seattle Campus". Because membership is not inherited by nested groups, the appliance will

![Image](https://via.placeholder.com/150)
not recognize him as a member of the "SeattleCampus" group unless he is an explicit member of that group.

- Microsoft provides a graphical tool that makes it easy to perform LDAP operations, including connecting, browsing, and modifying a directory. The tool—called LDP (ldp.exe)—is available with the Windows 2000 Server Support Tools; see the Microsoft Product Support site for more information.

**LDAP Examples for Active Directory Authentication**

Here are a few LDAP configuration examples.

**Example 1—Active Directory**

| Login DN | CN=AVtest,CN=Users,DC=testusr,DC=example,DC=com |
| Search base | DC=testusr,DC=example,DC=com |
| User name attribute | sAMAccountName |

**Example 2—Active Directory**

| Login DN | CN=JohnDoe,CN=Users,DC=na,DC=example,DC=com |
| Search base | CN=Users,DC=na,DC=example,DC=com |
| User name attribute | sAMAccountName |

**Example 3—Active Directory with Digital Certificate**

| Attribute mapping | Email=mail |
| Certificate attribute | UserCertificate |

**Example 4—LDAP with Domino Server**

| Login DN | CN=Aventail,O=peoplesoft |
| Search base | o=peoplesoft |
| User name attribute | cn |

**Configuring RADIUS Realms**

The appliance can validate username/password or token-based credentials against a RADIUS database. The following illustration shows typical RADIUS configuration options.
Notes

- You’ll need to modify your firewall or router to allow the appliance to communicate with your RADIUS server. The RADIUS authentication protocol typically uses port 1645/udp. In addition, you must configure your RADIUS server to include the IP address of the appliance as a RADIUS client (most often referred to as a Network Access Server).

Configuring RADIUS with Username and Password

Perform the following steps to configure the RADIUS authentication method for username and password validation.

► To configure RADIUS for username and password validation
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Authentication servers area, click the New button.
3. On the New Authentication Server page, under Directory type/protocol, click RADIUS.
4. Under Credential type, click Username/Password, and then click Continue. The Configure Authentication Server page appears.

5. In the Name box, type a name for the authentication server.
6. In the Primary RADIUS server box, type the host name or IP address of your primary RADIUS server. If your RADIUS server is listening on a port other than 1645 (the well-known port for RADIUS), you can specify a port number as a colon-delimited suffix (for example, myradius.example.com:1812 would set the port to that used by Steel-Belted Radius).
7. In the Secondary RADIUS server box, type the host name or IP address of your secondary RADIUS server. You can also add a port number as a suffix if necessary.
8. In the Shared secret box, type the password used to secure communication with the RADIUS server. This must be the same secret that is specified on the designated RADIUS server.
9. In the Match RADIUS groups by list, select the attribute containing the groups of which the user is a member. The value returned from RADIUS will be used in the group portion of the appliance access rule. There are three possible values:
   - None: Ignores the group attribute.
   - filterid attribute (11): Matches against the FilterID attribute.
   - class attribute (25): Matches against the Class attribute.
10. In the Retry interval box, type the number of seconds to wait for a reply from the RADIUS server before retrying the connection.
11. Complete the information listed under **Advanced**:

- **RADIUS identifier**: The unique identity of the RADIUS client; defaults to the machine's host name.
- **Service type**: An integer, usually 1 for Login or 8 for Authenticate Only.

**NTLM authentication forwarding**
Forward NTLM credentials to back-end Web servers.

- In the **RADIUS identifier** box, type information that uniquely identifies the RADIUS client. This information is placed in the NAS-Identifier attribute when the RADIUS request is composed. This field is necessary only if the RADIUS server is having problems accepting the host name of the appliance, which is used as the default identifier.
- In the **Service type** box, type a RADIUS Service-Type integer to tell the RADIUS server what type of service is being requested. For most RADIUS servers, you should type 1 (for Login) or 8 (for Authenticate Only).
- To enable NTLM authentication forwarding, click one of the **NTLM authentication forwarding** options. For more information, see “Configuring NTLM Authentication Forwarding” on page 69.

12. Click **Save** to return to the **Authentication** page.

### Configuring RADIUS with Tokens

The appliance supports token-based user credentials, such as SecurID or SoftID, that are validated against a database on a RADIUS server. Perform the following steps to configure the RADIUS authentication method for token-based credentials.

**To configure RADIUS for token validation**

1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.
2. In the **Authentication servers** area, click the **New** button.
3. On the **New Authentication Server** page, under **Directory type/protocol**, click **RADIUS**.
4. Under **Credential type**, click **Token/SecurID**, and then click **Continue**. The **Configure RADIUS Authentication** page appears.

5. In the **Name** box, type a name for the authentication server.

6. In the **Primary RADIUS server** box, type the host name or IP address of your primary RADIUS server. If your RADIUS server is listening on a port other than 1645 (the well-known port for RADIUS), you can specify a port number as a colon-delimited suffix (for example, `myradius.example.com:1812` would set the port to that used by Steel-Belted Radius).

7. In the **Secondary RADIUS server** box, type the host name or IP address of your secondary RADIUS server. You can also add a port number as a suffix if necessary.

8. In the **Shared secret** box, type the password used to secure communication with the RADIUS server. This must be the same secret that is specified on the designated RADIUS server.

9. In the **Match RADIUS groups by** list, select the attribute containing the groups of which the user is a member. The value returned from RADIUS will be used in the group portion of the appliance access rule. There are three possible values:
   - **None**: Ignores the group attribute.
   - **filterid attribute (11)**: Matches against the **FilterID** attribute.
   - **class attribute (25)**: Matches against the **Class** attribute.

10. In the **Retry interval** box, type the number of seconds to wait for a reply from the RADIUS server before retrying the connection.

11. Complete the information listed under **Advanced**:

   - In the **RADIUS identifier** box, type information that uniquely identifies the RADIUS client. This information is placed in the NAS-Identifier attribute when the RADIUS request is composed. This field is necessary only if the RADIUS server is having problems accepting the host name of the appliance, which is used as the default identifier.
• In the **Service type** box, type a RADIUS Service-Type integer to tell the RADIUS server what type of service is being requested. For most RADIUS servers, you should type 1 (for Login) or 8 (for Authenticate Only).

• Select the **Use RADIUS server password prompt** check box if you want to display the user password prompt that is configured on the RADIUS server. If your RADIUS server is not configured with a prompt, the appliance will prompt the user with the contents of the **Custom password prompt** box.

If you want the appliance to generate the user password prompt, leave the **Use RADIUS server password prompt** box cleared and type a prompt in the **Custom password prompt** box. For example, if you're creating a SecurID prompt you might type **Please enter your PASSCODE:**. If no prompt is specified here or on the RADIUS server, the appliance will generate an “Enter Password:” prompt.

12. Click **Save** to return to the **Authentication** page.

**Configuring Local User Authentication**

The appliance can check username and password credentials against those stored locally in `/etc/passwd`. By default, the only local user account is “root.” You cannot create local user accounts in AMC; use the standard `adduser` command from a command prompt.

Local user authentication is intended for testing purposes and is not recommended in a production environment.

► **To configure local user authentication**

1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.
2. In the **Authentication servers** area, click the **New** button.
3. On the **New Authentication Server** page, under **Directory type/protocol**, click **Local users**.
4. Under **Credential type**, click **Username/Password**, and then click **Continue**. The **Configure Authentication Server** page appears.

<table>
<thead>
<tr>
<th>Configure Authentication Server</th>
<th>Configure authentication settings for local users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential type: Username/Password</td>
<td>Name:*</td>
</tr>
</tbody>
</table>

5. In the **Name** box, type a name for the authentication server.
6. Click **Save** to return to the **Authentication** page.
7. Click the name of the realm you want to edit. This opens the configuration page for that realm.
8. Make your configuration changes and then click **OK**.
Testing Authentication Configurations

To help you validate your authentication configuration settings, the AMC pages used to configure Microsoft Active Directory and LDAP servers include a Test connection button. This button establishes a connection with your external user repository and provides status:

If you've correctly configured the appliance, a message reading "Valid connection!" appears beside the button. If there is an error in the configuration settings, the message will provide helpful text briefly describing the problem.

Notes

- The test connection feature is intended only to test whether the appliance can bind an external directory. If you enter login credentials, the appliance will use them, but it will otherwise attempt to bind to the directory anonymously. Because it does not actually search the directory, testing a connection will not validate that your login credentials provide access to the configured domain.

Configuring Single Sign-On

Single sign-on (SSO) allows you to configure the appliance to forward user credentials to back-end Web resources. In addition to basic HTTP authentication forwarding, you can configure the following SSO options:

- **NTLM authentication forwarding** sends a Windows domain name along with the user’s authentication credentials.

- **Support for Netegrity SiteMinder** forwards user authentication credentials to a SiteMinder server.

Using single sign-on prevents the user from having to log in multiple times (once to get to the appliance, and again to access an application resource).

Overview: Single Sign-On

Single sign-on (SSO) allows you to configure the appliance to forward user credentials to back-end Web resources. This prevents the user from having to log in multiple times (once to get to the appliance, and again to access an application resource).

The appliance support several types of Web SSO:

- **Basic authentication forwarding** is a widely supported form of authentication forwarding, but is not very secure because it sends passwords in the clear across the network. The appliance can be configured to send each user's authentication credentials, or "static" credentials (that is, the same credentials for all users). Basic authentication forwarding is configured within a Web application profile. See "Adding a Web Application Profile" on page 92.

- **NTLM authentication forwarding** provides a secure method for sending Windows network credentials to a Microsoft IIS (Internet Information Services) Web server. NTLM (short for "Windows NT LAN Manager") uses a challenge/response mechanism to securely authenticate users without sending passwords in the clear across the network. NTLM authentication forwarding passes a Windows domain name along with the user’s authentication credentials.

- **Netegrity SiteMinder** is a third-party product that provides a centralized mechanism for administering single sign-on. You can configure the appliance to forward user authentication credentials to a SiteMinder server, which then forwards the credentials on to any back-end Web resources it is protecting.
Notes

- Aventail’s standard Web access agent does not support single sign-on to back-end Web servers secured with SSL. Any links to these resources accessed through the standard Web agent will not provide single sign-on. To provide either basic authentication or NTLM authentication forwarding to an HTTPS resource, you should create an alias for the Web resource and add it as a link in ASAP Workplace. That will force the appliance to provide translated Web access.

As a security measure, SSO is disabled by default. The following table summarizes the steps involved in configuring the various types of SSO.

<table>
<thead>
<tr>
<th>SSO Type</th>
<th>Configuration Steps</th>
</tr>
</thead>
</table>
| Basic authentication forwarding | • Configure a Web application profile to use SSO and specify which user credentials to use  
                                 | • Attach the Web application profile to any Web resources for which you want to use SSO |
| NTLM authentication forwarding | • Configure a Web application profile to use SSO and specify which user credentials to use  
                                 | • Attach the Web application profile to any Web resources for which you want to use SSO  
                                 | • Configure a domain name for each authentication server for which you want to use SSO |
| Netegrity SiteMinder          | • Configure the settings used to communicate with your SiteMinder server               
                                 | • Create an agent for the Aventail appliance on the SiteMinder policy server             |

Configuring NTLM Authentication Forwarding

Windows NT LAN Manager (NTLM) authentication enables users accessing Web resources on Windows networks to be securely authenticated without sending passwords in the clear across the network.

There are two steps to configuring NTLM authentication forwarding. First, you configure the authentication server to include the Windows domain name you want to forward. Next, you enable the SSO options in a Web application profile, and then attach the profile to the Web resource(s) to which you want to forward user credentials. Ensure that you have completed these preliminary steps before configuring NTLM authentication forwarding.

To configure NTLM authentication forwarding

1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Authentication servers area, click the name of server you want to configure. The Configure Authentication Server page appears.
3. In the Advanced area, specify the domain name you want to forward in the NTLM authentication forwarding section:

   NTLM authentication forwarding
   Forward NTLM credentials to back-end Web servers.

   - [ ] Forward a custom domain name
     Domain name: [ ]
   - [ ] Forward the realm name as domain name

For resources configured with NTLM authentication forwarding, this will be used for the domain name portion of the credentials.
• To specify a domain name, click **Forward a custom domain name**. You can type a custom domain name in the **Domain name** box, but it is not required. If you do not specify a domain name, an empty (or “null”) domain name will be forwarded along with the user credentials.

• To forward the realm server (as specified in the **Name** box at the top of the page) along with the user credentials, click **Forward the server name as domain name**.

4. Enable the **Single Sign-On** options for a Web application profile. For information on Web application profiles, see “Adding a Web Application Profile” on page 92.

**Notes**

• To use NTLM authentication forwarding in situations in which the credentials do not match, users must be running a Web browser that supports NTLM.

• When single sign-on is enabled, the Web access service and the back-end server will determine which authentication method is used. If only one authentication method (basic authentication or NTLM authentication) is enabled in AMC, that enabled authentication method will be used. However, if both basic authentication and NTLM authentication are enabled in AMC, NTLM authentication will be used as it is the more secure method.

### Configuring Netegrity SiteMinder Authentication Forwarding

You can configure the appliance to forward user credentials to a Netegrity SiteMinder server using SiteMinder’s native API. SiteMinder then forwards those credentials to any back-end Web resources it is protecting. The SiteMinder configuration is a global setting: If enabled, username credentials will be forwarded to SiteMinder for all Web resources. The appliance is compatible with Netegrity SiteMinder version 4 and above.

Before configuring Netegrity SiteMinder settings in AMC, you must create an agent for the Aventail appliance on the SiteMinder policy server. See the Netegrity documentation for more details.

**To configure Netegrity SiteMinder authentication forwarding**

1. From the main navigation menu, click **General Settings**.

2. Click the **Single Sign-On** tab.

3. To enable SSO to Web applications protected by SiteMinder, select the **Enable Netegrity SiteMinder authentication forwarding** check box.
4. In the **Name** box, type the shared name you used when creating the Aventail agent in SiteMinder.

5. In the **Secret** box, type the shared password for the Aventail agent.

6. In the **Cookie domain** box, enter the domain to be included in the single sign-on cookie.

7. In the **Primary server** box, type the host name or IP address of the SiteMinder policy server to which you are forwarding credentials.

8. In the **Secondary server** box, type the name of the server that will be used if the **Primary** server is unavailable.

9. In the **HA configuration mode** list, specify whether the appliance will reach the Netegrity policy server in round-robin or failover mode.

10. In the **Timeout** box, type the maximum number of seconds the appliance waits before determining whether it can reach the Netegrity policy server. The default is **20**. After this period, the Aventail appliance ends the connection with SiteMinder.

11. Under **Advanced**, specify the port numbers used to communicate with the SiteMinder server:
   - The default **Accounting port** is 44441.
   - The default **Authentication port** is 44442.
   - The default **Authorization port** is 44443.

12. Click **Save**.

### Next Steps

After you’ve performed the basic network setup, obtained an SSL certificate for the appliance, and configured authentication settings, you’re ready to start managing users and user groups, defining resources, and configuring access control rules.
Chapter 5
Designing Your VPN

This chapter provides guidelines on how to design a VPN and contains examples of common VPN configurations.

The first phase of the design process is planning, in which you identify your users, the resources you want to make available, and the access methods used to reach those resources. Next, you're ready to begin the nuts and bolts of security administration—defining resources and creating access control rules that determine who can access those resources. You may also want to deploy End Point Control components to your users to protect sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments. Finally, you'll be ready to deploy the VPN to your user community.

For more specific information on the mechanics of security administration, see “Security Administration” on page 85.

Planning Your VPN

To effectively design your VPN, you must identify who will access your VPN, what types of resources you will make available, and which access methods you will provide to end users so they can reach your network.

Who Will Access Your VPN?

Your user community will obviously have a major impact on how you design and administer your VPN. Most VPN users generally fall into one of two camps: remote employees or business partners.

- **Remote employees.** When serving remote and mobile employees, you'll generally provide relatively open access to enterprise resources. Of course, you can also define a more granular access policy for specific resources that contain sensitive information (such as a payroll application).

  Employee computer systems under IT control provide the flexibility to install client software—such as Aventail Connect—on the desktop. Aventail Connect provides direct integration with Windows Network Neighborhood and allows you to enforce desktop security (such as requiring a personal firewall or virus detection software) for users accessing the network from a remote location.

- **Business partners.** Suppliers, vendors, contractors, and other partners generally have restricted access to resources on your network. This requires you to administer more granular resource definitions and access control rules than those typically used for a remote access VPN.

  For example, instead of simply defining a domain resource and granting employees open access privileges, you'll often need to define specific host resources and manage a more complex access policy. Additionally, when defining a Web resource you may want to obscure its internal host name to maintain the privacy of your network.
Because of the administrative and support issues associated with installing client software on PCs outside the control of your IT organization, a Web-based access method is usually best for business partners.

What Types of Resources Are You Deploying?

The Aventail appliance manages a wide variety of corporate resources, which fall into three categories:

- **Web resources** are Web-based applications or services that run over HTTP or HTTPS. Examples include Microsoft Outlook Web Access and other Web-based e-mail programs, Web portals, and standard Web servers.

- **Client/server resources** are enterprise applications that run over TCP/IP (including applications that use UDP). Examples include thin-client applications such as Citrix, full client/server applications such as Microsoft Outlook, Lotus Notes, or SAP, or terminal servers. You define these types of client/server applications by specifying a host name, an IP address or IP range, a subnet IP address, or a DNS domain.

- **Windows file shares** include Windows network servers or computers containing shared folders and files.

See “Creating and Managing Resources” on page 85 for detailed information on managing resources.

How Will Users Access Your Resources?

End users can access VPN resources secured by the Aventail appliance using three methods. This gives you a range of deployment options for both "managed" desktops controlled by your IT department and systems outside your control, including employees’ home PCs, partner desktops, and other systems such as kiosks or PDAs.

- **Standard Web browser.** Web resources and file system resources can be accessed from any Web browser that supports SSL. By default, the appliance is configured to deploy a Microsoft ActiveX control (the “standard Web agent”) on Microsoft Windows systems running Internet Explorer. The standard Web agent proxies Web content directly through the appliance. For users running other browsers, the appliance will automatically provide translated Web access. If you’d rather not install an agent or your users’ systems don’t support ActiveX, you can configure the appliance to provide translated Web access. Browser-based access is ideal for providing remote access from virtually any PC, including public kiosks or wireless LANs. It’s also a good option for providing business partner access, because it does not require any client configuration or administration.

- **Java-enabled platform.** Aventail OnDemand provides access to client/server applications and Web resources. It is accessible from a Java-enabled Web browser or any environment—such as Macintosh or Linux systems—configured with a stand-alone Java environment. If you’ve licensed OnDemand, by default it is configured to run automatically (“embedded mode”) when the user connects to ASAP WorkPlace. Alternatively, you can configure OnDemand in “standalone mode” so the user launches it manually by clicking a link on ASAP WorkPlace. For optimum performance, OnDemand is installed on the user’s computer the first time it is accessed, minimizing download time for returning users.

Aventail OnDemand is a good choice for providing access to users who are connecting with a device that is not managed by IT staff, such as a home PC or a PDA.

- **Windows client.** Aventail Connect is a 32-bit Windows client that provides access to a broad range of resources, including traditional client/server applications, thin-client applications, file servers, or Web resources. It offers complete integration with the Windows desktop, including support for Microsoft single sign-on and seamless access to network share resources from Network Neighborhood. It also provides advanced security options that help protect your corporate network, including personal firewall integration and antivirus software detection. Aventail Connect’s support for auto-updating simplifies ongoing administration tasks.

Aventail Connect is typically used for remote access on systems that can be readily managed by IT, such as a corporate laptop used by a traveling or remote employee.
The following table summarizes the available access methods and the advantages of each.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Provides access to</th>
<th>Advantages</th>
</tr>
</thead>
</table>
| **Standard Web mode**         | Any Web resource, (including Web-based applications, Web portals, Web servers) | • Convenient access from any ActiveX-enabled browser  
• Defaults to “translated mode” on other browsers  
• Minimal client configuration or administration tasks  
• Users can access any network URL by typing its actual URL in the browser’s **Address** box  
• Broader access to enterprise applications |
| **Translated Web browser**    | Any Web resource, (including Web-based applications, Web portals, Web servers) | • Convenient access from virtually any PC  
• No client configuration or administration tasks  
• Supports the use of aliases to hide internal host names in the browser **Address** bar  
• Single sign-on to back-end Web servers |
| **Aventail OnDemand**         | Client/server applications and Web resources from any Java-enabled platform       | • Broad cross-platform support  
• Lightweight (~300K) Java agent is easy to administer and deploy |
| **Aventail Connect**          | Client/server applications, Web resources, and Windows network shares             | • Offers seamless integration with Windows Network Neighborhood  
• Enhanced security options, including split-tunneling, personal firewall detection, and virus software detection |

Your choice of access methods will be based on a variety of factors, including:

- **Technical considerations**, such as the hardware platform, operating system, or Web browser in use by end users.
- **Security requirements**, such as the safeguards you want to put in place on the desktop.
- **End-user profile**, including their level of technical sophistication.
- **Administrative resources** available to manage and support a VPN.

**Security Administration**

Administering your security policy involves defining resources and then creating access control rules that determine the availability of those resources.

**Defining Resources**

When managing resources, you have some flexibility to decide which resource type to use for a given object on your network. The type you choose will vary depending on your VPN design. For example, you might define a Web application as a URL resource for use by a business partner and “alias” the host name for an extra measure of security. Alternatively, you could define the domain in which the Web application is located as a network resource, which is a convenient way to enable remote employee access to multiple Web resources.
This section discusses your options for defining resources.

**URL Resources**

Any Web resource—such as a Web application, a Web portal, or a Web server—can be defined as a URL resource; they are specified in AMC using the standard `http://` or `https://` URL syntax. Defining a Web resource as a URL provides several advantages:

- You can create a Web shortcut for ASAP WorkPlace to make it simple for users to quickly access a URL resource.
- You can define very specific access rules to control which users can access the URL.
- You have the option of obscuring (or “aliasing”) the internal host name so it is not publicly exposed. When a user accesses an alias in translated mode, the Aventail Web access service proxies the request to the downstream Web resource and translates its private URL using an alias name you define. The user sees only the public (or “aliased”) URL. The following figure illustrates how the private address for an inventory application might be translated into a public URL.

The private URL for this resource is `http://inventory.in.example.com`. The administrator has created an alias named “supplier” and associated it with the private URL for the inventory application.

Of course, suppliers won’t access the resource using its private URL (which would publicly expose a sensitive host name). Instead, they access a public URL composed of the appliance’s fully qualified domain name, followed by the resource’s alias name. Notice that the public URL uses the `https://` prefix rather than the standard `http://` prefix (this is because all traffic to and from the Aventail appliance is secured using SSL).

**Notes**

- Even if you don’t alias the private address, the URL is slightly modified by the appliance when accessed in translated mode. See “Content Translation” on page 292 for more information.
- Some Web-based applications use Java applets or other browser extensions that submit traffic using protocols other than HTTP. Examples of such applications include Citrix NFuse, Oracle J-Initiator, and certain versions of SAP and PeopleSoft. Although accessed using a Web browser, these applications may need to be defined as a network resource and proxied through OnDemand using the client/server access service.

**Network Resources**

As the name implies, “network resources” are flexible enough to encompass virtually anything on your network, including applications, file servers, or multiple Web resources. Network resources are specified in AMC using either a domain, subnet, IP range, host name, or IP address.
Here are some examples of network resources:

- **Client/server applications** include "traditional" applications developed for a particular operating system, or thin-client applications designed to be run over the Web. Users access client/server applications using either Aventail Connect or Aventail OnDemand.

- **Network shares** include Windows file servers or file shares. When defined as a network resource, network shares are accessible using either Aventail Connect or Aventail OnDemand. (To access a network share using a Web browser, you must instead define it as a file system resource.)

- **Source networks** are referenced in an access rule to permit or deny a connection to a destination resource based upon the location from which the request originates. This provides you with even greater security. For example, you might permit connections from only a particular domain, or even from an individual IP address.

- **Multiple Web resources** on your network—whether in a domain, subnet, or IP range—can be defined as a network resource. This approach provides a convenient way for you to administer multiple Web servers from a single object in AMC. For example, if you specify a domain (and create the appropriate access rule), users will be able to access any Web resources contained within that domain from their Web browsers (or from Aventail OnDemand or Aventail Connect).

  On the downside, however, your users cannot access those resources from a link on ASAP WorkPlace; instead, they must know the internal host name of the resource. If the standard Web agent is running, they can enter any URL directly into their browser. However, in translated mode, users must manually type URLs in the **Intranet Address** box in WorkPlace.

With such a wide scope of resource definitions—from broad resources such as a domain or subnet, down to a single host or IP address—you may wonder how best to define your network resource definitions. Broad resource definitions simplify your job as network administrator, and are typically used when managing a remote access VPN with an open access policy. For example, you could define your internal DNS namespace as a domain and create a single policy rule granting employees access privileges.

On the other hand, a more restrictive security policy will require you to define network resources more narrowly. This approach is typically used when administering a partner VPN. For example, to provide an external supplier with access to an inventory application, you might specify its host name as a resource and create a policy rule specifically granting the supplier access privileges.

**File System Resources**

To access a Windows network share from a Web browser, you create a file system resource. A file system resource can be defined as a Windows domain or a UNC path name. This provides you with the flexibility to create an open policy that provides access to the entire domain, or to create a more granular policy that controls access at the server, share, or folder level.
Managing Access Control

After you’ve defined your VPN resources, you control which resources are available to users by creating an access policy.

Overview: Access Control Rules

After a user successfully authenticates (that is, verifies his or her identity), the appliance evaluates the access rules to control authorization to specific resources. Rules appear on the Access Control page:

Access control rules are stored as a list, with each rule assigned a specific order. When the appliance evaluates a connection request, it begins at the top of the list and works down the list (that is, in ascending numeric order) until it finds a match. When it finds a match, the action required by the rule—either “permit” or “deny”—is applied and no further rules are evaluated. If the appliance reaches the end of the list without finding a match, it applies an implicit “deny” rule to prohibit access.

Access to a resource can be based on several criteria. Most access rules control access based on who the user is—that is, the user’s name or group membership—and the destination resource he or she is trying to reach. (If you don’t restrict access to a particular user or destination resource, the word “Any” appears in the access control list.)

Additionally, you can control access based on several other criteria:

- **The access method used to reach the resource.** You might want to enable broad access to resources within an internal domain from Aventail Connect or Aventail OnDemand, but prevent browser-based access to Web servers within the domain.

- **The End Point Control zone from which the connection request originates.** Suppose you want to require users accessing a sensitive financial application to run a cache cleaner after each session. If so, you could configure a rule restricting access to systems in a “trusted” zone running Aventail Secure Desktop.

- **The source network from which the connection request originates.** You might control access to a resource based on an IP range, subnet, or domain.

- **The day and/or time of the request.** For example, you might allow business partners to access a particular application only from 9:00 A.M. to 5:00 P.M. on weekdays.

- **The encryption strength of the connection.** You might require connections to a particularly sensitive resource to use strong 128-bit encryption.

- **The SOCKS command offered by the client.** For connections proxied through the client/server access service, you can limit access to particular types of connections; for example, you might allow bind or connect requests, but deny ping requests. For UDP connections, you can restrict access based on whether encryption is used.

To summarize the authorization process:

1. A user initiates a connection.
2. The appliance analyzes the connection request to identify its attributes (including user and group information, the destination being requested, source network from which the request originates, and the day or time of the request).

3. The appliance reads the first rule in the access control list and compares it to the request criteria:
   - If a match is found, the action (“permit” or “deny”) specified in the rule is applied. After this occurs, no further rules are evaluated.
   - If no match is found, the appliance evaluates the next rule in the list to see if it matches the request.

4. If the appliance processes all of the rules without finding a match, it applies an implicit end rule to deny access.

Design Guidelines for Access Rules

Because the appliance processes your access control rules sequentially, the order in which you organize them has great significance in terms of whether access is permitted or denied. Carefully review your security policy settings to avoid inadvertently placing rules in the wrong order.

- **Put your most specific rules at the top of the list.** As a general rule, it is usually best to put your most specific rules at the top of the list. Putting the least restrictive rules at the top of the list may cause the appliance to find a match before it has a chance to process your more restrictive rules.

- **Be careful with “Any” rules.** If you create a rule that does not restrict access to a particular user or destination resource, the word “any” appears in the access control list. Carefully consider the impact of “any” in your policy rules. For a “permit” rule, too many “any” criteria could expose a security hole. On the other hand, too many “any” criteria in a “deny” rule could unnecessarily restrict network access.

- **Optimizing performance.** Because the appliance evaluates rules in sequential order, you can optimize performance by placing the network resources that are accessed most frequently at the top of the list.

- **Avoid resource and access method incompatibilities.** In some very specific cases, certain combinations of resource types and access methods can create problems with your access policy. For more information, see “Resolving Deny Rule Incompatibilities Between Access Methods and Resources” on page 103.

For more information on best practices for designing access control rules, see “Access Policy” on page 240.

Services Managing Your Access Policy

Your VPN resources are secured and managed by three different services:

- **The Web access service** controls browser-based access to URL resources, or to any network resources containing Web resources. The Web access service is a secure gateway that enables access to Web resources using any standard Web browser that supports SSL. By default, the appliance is configured to deploy a Microsoft ActiveX control (the “standard Web agent”) on Microsoft Windows systems running Internet Explorer. The standard Web agent proxies Web content directly through the appliance. For users running other browsers, the appliance will automatically provide translated Web access. If you’d rather not install an agent or your users’ systems don’t support ActiveX, you can configure the appliance to provide translated Web access.

- **The client/server access service** controls access to any network resources, such as a domain, subnet, IP range, or host. The client/server access service is a proxy based on the SOCKS v5 protocol. The service’s proxy-based architecture and use of SSL allow it to traverse firewalls, NAT devices, and other proxy servers that often interfere with traditional VPN devices.

- **The ASAP WorkPlace service** controls access to network file shares accessed from a Web browser. The ASAP WorkPlace service communicates with Windows file servers and network shares (including Microsoft Distributed file system, or Dfs, resources) using the Server Message Block (SMB) file-sharing protocol.
In addition to the standard permit/deny privileges available with the other access control rules, file system rules also include read/write permissions. This allows you to supplement (though not override) the native Windows permissions. For example, the appliance policy can prevent a user from browsing the network or modifying a file on a network share.

All file system access privileges specified on the Aventail appliance are additive to those specified in Windows, and do not override the privileges set in the operating system. For example, if you provide a user with read/write access to a network folder, but the native Windows permissions only provided the user with read privileges, he or she would be unable to modify the contents of the folder.

**End Point Control**

Traditional VPN solutions typically provide access only from the relative safety of a corporate laptop. In that environment, the major security concern is unauthorized network access. Because an SSL VPN enables access from any Web-enabled system, it may bring additional risks from PCs in untrusted environments, such as a kiosk at an airport or hotel, or an employee-owned PC.

The Aventail appliance includes support for several End Point Control (EPC) components designed to protect sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments. Aventail's data protection agents—Aventail Secure Desktop and Aventail Cache Control—automatically remove session data from the PC. The appliance also supports integration with third-party client integrity controls that automatically check for malware on the client system before allowing access.

The appliance's EPC configuration options give you granular control over VPN access using device profiles and zones:

- **A device profile** is a set of attributes that characterize the type of device requesting the connection. These attributes can include a Windows domain name, the presence of a software program such as personal firewall or anti-virus program, or a registry entry.

- **A zone** classifies a connection request based on the presence or absence of a device profile, and is used to provision data protection components or determine which resources are available.

When a user connects to the appliance, the appliance interrogates the user's computer, then determines if its attributes match those defined in the zone's device profile. If the device matches the profile, the appliance classifies the computer into the zone. The following diagram illustrates the evaluation process performed by the appliance when a user logs in to a realm configured with End Point Control:

To configure EPC, you first create one or more device profiles that identify the client attributes you want to look for. Next, you define an EPC zone and reference the device profiles required for a device to be classified into that zone. The zone is in turn referenced in a realm; this determines which users...
can be classified into the specified zone and which data protection agents are deployed to those users. Optionally, you can reference a zone in an access control rule to determine which resources are available to users in that zone.

For more information on configuring EPC, see “End Point Control” on page 163.

Deployment

After you’ve defined your resources and access policy, it’s time to deploy your resources to users. Web resources and Windows file shares can be easily deployed using ASAP WorkPlace. Aventail OnDemand offers access to client/server applications, and Aventail Connect provides Windows users with broad access to resources throughout your network.

This section provides an overview of deploying your VPN resources. For more detailed information, see “Configuring User Access Components” on page 183.

Deploying Web Resources

ASAP WorkPlace, a Web service that provides users with dynamically personalized access to Web resources and Windows file shares, makes it easy to deploy Web resources directly from the appliance. It provides access to the major components of your VPN:

- **Web shortcuts** provide users with fast access to specific Web resources. Likewise, **network shortcuts** enable users to directly access specific file shares. Both lists are filtered based on your access policy to show each user only those resources he or she has privileges to use.

- The **Network Explorer** page provides Web-based access to Windows file shares. Its Windows Explorer-like interface supports most common file management tasks, such as opening, uploading, downloading, and copying files. The appliance's file system access policy is used to control each user’s access privileges. You can also disable file uploads from ASAP WorkPlace, or disable access to file shares entirely.

- The **Intranet Address** box enables users to type URLs and/or UNC path names to access resources for which you haven’t created specific links. For example, a user could type the host name of a Web server, or a specific folder on a Windows share.

If you prefer to use an existing corporate intranet or Web portal, you can have users authenticate to the appliance from ASAP WorkPlace, and then automatically redirect them to the internal site. This is done by modifying the WorkPlace template to link to your internal resource. See “Redirecting Users to Another Site” on page 198 for information.

For complete information on configuring ASAP WorkPlace, see “Aventail ASAP WorkPlace” on page 183.

Deploying Aventail OnDemand

Aventail OnDemand—a Java applet used to access client/server applications—can be deployed from ASAP WorkPlace in one of two modes. In **embedded mode**, OnDemand automatically starts when a user connects to ASAP WorkPlace. In **stand-alone mode**, the user manually starts OnDemand by clicking a link on WorkPlace. OnDemand appears in a separate browser window.

For Microsoft Windows users, OnDemand can be configured to dynamically redirect connection requests to the appliance. This requires the user to manually start any client/server applications he or she wants to use. Alternatively, you can set up OnDemand to automatically run a client/server application when the user clicks a link in ASAP WorkPlace (this configuration is also required for users on non-Windows platforms).

For complete information on configuring OnDemand, see “Aventail OnDemand” on page 201.

Deploying Aventail Connect

Aventail Connect—a Windows application used to access a broad range of VPN resources—is configured using a separate Windows program called the Aventail Connect Configuration Tool. You can also customize Connect setup packages using the Aventail Connect Customizer tool.
To deploy Aventail Connect, you distribute the setup package on a Web server, FTP server, or file server. For complete information on configuring Aventail Connect, see the *Aventail Connect Administrator’s Guide*.

**VPN Configuration Examples**

This section describes common deployment scenarios.

**Remote Access VPN Scenarios**

To better understand how to deploy a remote access VPN, let’s look at some common scenarios.

<table>
<thead>
<tr>
<th>Access scenario</th>
<th>Common configuration steps</th>
</tr>
</thead>
</table>
| 1—Provide access to a specific Web resource | 1. Define a URL resource.  
2. Create a rule referencing the URL.  
3. Add a Web shortcut to ASAP WorkPlace. |
| 2—Provide access to all Web resources in your network | 1. Define a network resource (such as a domain or subnet) for all internal DNS domains.  
2. Create a rule referencing the network object.  
3. Instruct users to type the host name or URL for any Web resources in the **Intranet Address** box on ASAP WorkPlace. |
| 3—Provide access to any Web resources in a portion of your network | 1. Define a network resource (such as a domain or subnet) for the portion of the network containing the Web resources.  
2. Create a rule referencing the network object.  
3. Instruct users to type the host name or URL for any Web resources in the **Intranet Address** box on ASAP WorkPlace. |
| 4—Provide Windows users with broad access to network resources | 1. Define a resource referencing your DNS domain.  
2. Create a rule referencing the domain.  
3. Configure and distribute the Aventail Connect client. |
| 5—Provide Web-based file access to entire network | 1. Define a resource referencing your Windows domain.  
2. Create a rule referencing the domain.  
3. Add a network shortcut referencing the domain.  
4. Make sure ASAP WorkPlace’s **Network Explorer** tab is enabled (this is the default state). |

**Partner VPN Scenarios**

Here are examples of common steps for deploying a partner VPN.

<table>
<thead>
<tr>
<th>Access scenario</th>
<th>Common configuration steps</th>
</tr>
</thead>
</table>
| 1—Provide access to a specific Web resource and obscure its internal host name | 1. Define a URL resource and specify an alias.  
2. Create a rule referencing the URL.  
3. Add a Web shortcut to ASAP WorkPlace. |
End Point Control Scenarios

Here are some basic examples of how to deploy End Point Control.

### Access scenario

<table>
<thead>
<tr>
<th>Access scenario</th>
<th>Common configuration steps</th>
</tr>
</thead>
</table>
| **2—Provide Web-based access to a client/server application**                  | 1. Define a network resource referencing the application’s host name or IP address.  
2. Create a rule referencing the network resource.  
3. Configure Aventail OnDemand (if accessing a thin client or terminal server application, you can optionally configure OnDemand to automatically start the application).  
4. Add an Aventail OnDemand link to ASAP WorkPlace.                                                                 | |
| **3—Provide Web-based access to a specific folder on a Windows network, but prevent general network browsing** | 1. Define a file system resource referencing the folder’s UNC path name.  
2. Create a rule enabling read (and optionally, write) access to the folder.  
3. Add a network shortcut referencing the resource.  
4. Make sure ASAP WorkPlace’s Network Explorer tab is enabled (this is the default state).                       | |

### Access scenario

<table>
<thead>
<tr>
<th>Access scenario</th>
<th>Common configuration steps</th>
</tr>
</thead>
</table>
| **1—Deploy Aventail Cache Control to employees accessing the network from an untrusted system, but not from a “trusted” system (such as an IT managed laptop)** | 1. Define a device profile with attributes identifying a trusted system (such as a Windows registry key, the name of a corporate application, or your Windows domain name).  
2. Reference the device profile in a zone, and configure the zone to require no data protection tools.  
3. Reference the zone in any realms used by your employees.  
4. Configure the Default zone to require Aventail Cache Control.                                                                 | |
| **2—Deploy Aventail Secure Desktop to partners accessing the network from their domain** | 1. Define a device profile with an attribute referencing the partner’s Windows domain name.  
2. Reference the device profile in a zone, and configure the zone to require Aventail Secure Desktop.  
3. Reference the zone in the realm used by your partners.  
4. Configure the Default zone to block VPN access (will prevent unknown systems from accessing the network). | |
| **3—Allow employees on home PCs to bypass Aventail Cache Control, but deploy it to everyone else** | 1. Define a device profile with an attribute referencing a unique corporate application.  
2. Reference the device profile in a zone, and configure the zone to require Aventail Secure Desktop.  
3. Reference the zone in the realm used by your employees.  
4. Configure the Default zone to block VPN access (will prevent unknown systems from accessing the network). | |

---

Aventail

---

**EX-1500 Installation and Administration Guide | 83**
### Access scenario

<table>
<thead>
<tr>
<th>Access scenario</th>
<th>Common configuration steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>4—Deploy Aventail Cache Control to a user on a Macintosh</td>
<td>1. Define a device profile referencing <strong>Macintosh</strong> as the operating system.</td>
</tr>
<tr>
<td></td>
<td>2. Reference the device profile in a zone, and configure the zone to require Aventail Cache Control.</td>
</tr>
<tr>
<td></td>
<td>3. Reference the zone in any realms used by your Macintosh users.</td>
</tr>
</tbody>
</table>
Managing security is perhaps your most important job as an administrator. The Aventail ASAP Management Console (AMC) makes it easy for you to manage the elements of security administration: resources and access control rules. For details on how to plan your resource definitions, see “Designing Your VPN” on page 73.

Creating and Managing Resources

This section explains how to create and manage resources, resource groups (a collection of resources), and Web application profiles (configuration settings for Web resources). You can define a resource before referencing it in an access control rule or, alternatively, you can define a new resource directly from the access control rule interface. For more information, see “Adding Users and Resources From Within Access Control Rules” on page 101.

Viewing Resources and Resource Groups

Resources and resource groups are displayed on the Resources page and the Groups page, respectively.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Web, network, and file system resources.</td>
<td></td>
</tr>
<tr>
<td>Show</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAP Workplace</td>
<td>ASAP Workplace, built-in</td>
<td>URL</td>
</tr>
<tr>
<td>Company Domain</td>
<td>lorenfig.com</td>
<td>Windows domain</td>
</tr>
<tr>
<td>CRM Application</td>
<td>Customer Relationship Mgmt.</td>
<td>Host</td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>Outlook Web Access for Employees</td>
<td>URL</td>
</tr>
<tr>
<td>Payroll Application</td>
<td>Host Payroll App.</td>
<td>Host</td>
</tr>
</tbody>
</table>

To view your list of available resources and resource groups
1. From the main navigation menu, click Resources.
2. Click the Resources tab to view your available individual resources, or click the Groups tab to view your available resource groups.
   
   The Type column displays the type of each resource or resource group. Remember that a network resource can contain both Web and client/server applications.
3. Use the Show list to control the types of resources that are displayed on the page.
4. To view more detail on a particular resource or profile, click the name in the Resource column.

Notes
• By default, there may be one or more read-only resource definitions shipped with the appliance. These definitions, which appear in the resource list, are required by the appliance services.

Adding a Network Resource

Network resources are typically used to define client/server resources on your network. They can also be used to define a network object containing multiple Web resources (such as a domain), or to define a network object that can be used to control access based on the source of a connection request. Network resources are defined as domains, IP addresses and ranges, subnet IP addresses, and host names. See "Designing Your VPN" on page 73 for a more detailed discussion.

To add a network resource
1. From the main navigation menu, click Resources. The Resources page appears.
2. On the Resources page, click the New button. The Add/Edit Resource page appears.
3. In the Name box, type a name for the resource.
4. In the Description box, type a descriptive comment about the resource.
5. In the Resource definition area, select the option you want and provide the appropriate network information.

- A host is any computer on your network. In the Host name or IP box, type a host name (it can be qualified or unqualified) or type the full IP address for the host in dotted decimal form (w.x.y.z).

- An IP range typically identifies a shorter range of computers within a subnet. Under the IP range area, type the IP addresses at the beginning (From) and end (To) of the IP range in dotted decimal form (w.x.y.z).

- A subnet is a portion of a network that shares a common address component. Under the Subnet area, type the IP address and Subnet mask in dotted decimal form (w.x.y.z).

- A domain encompasses one or more hosts. In the Domain box, type the name of the domain (such as example.com).

6. If the network resource you’re defining is a Web resource, in the Advanced area select a Web application profile from the list. The list contains preconfigured Web application profiles that are recommended for several popular Web applications, custom Web profiles (see “Adding a Web Application Profile” on page 92), and a default Web profile. If you are unsure of which profile to select, it’s best to choose the default. To view the profile, click View selected profile. Note that when users access this resource via Aventail Connect or OnDemand, Web profiles are ignored. For more information on Web application profiles, see "Adding a Web Application Profile" on page 92.
If the network resource you're defining is not a Web resource, select None for the Web profile.

7. After you've finished, you can define another resource by clicking Save and Add Another, or click Save to return to the Resources page.

**Notes**

- A network resource can be defined using a host name, IP address, domain name, subnet, or IP range. The following table explains the syntax used to define each of these resource types. Note that host names can be fully qualified or unqualified.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>bart.private.example.com bart</td>
</tr>
<tr>
<td>Host IP address</td>
<td>192.0.34.72</td>
</tr>
<tr>
<td>IP range</td>
<td>192.0.34.72 - 192.0.34.74</td>
</tr>
<tr>
<td>Subnet</td>
<td>192.0.34.0 / 255.255.255.0</td>
</tr>
<tr>
<td>Domain name</td>
<td>private.example.com</td>
</tr>
<tr>
<td>Windows domain</td>
<td>example or example.com</td>
</tr>
</tbody>
</table>

- Microsoft Outlook connects to Microsoft Exchange using an unqualified host name. Therefore, when defining a Microsoft Exchange server as a network resource, you must define it as an unqualified name (such as FRED).

**Adding a URL Resource**

URL resources include Web-based applications that are accessed using HTTP or HTTPS. Web traffic is proxied through the Aventail Web access service, a secure gateway through which users can access intranet resources from the Internet. A URL resource can be used only as a destination in a Web access control rule. For more information, see "Configuring Access Control Rules" on page 95.

▶ To add a URL resource

1. From the main navigation menu, click Resources. The Resources page appears.
2. On the Resources page, click the New button. The Add/Edit Resource page appears.
3. In the Name box, type a name for the resource.
4. In the Description box, type a descriptive comment about the resource.
5. In the Resource definition area, select URL and then type the appropriate URL. You must include the http:// or https:// protocol identifier.

- If an HTTPS resource, include the https:// protocol.

6. If you want to automatically add a shortcut to the URL resource in WorkPlace, select the Create ASAP WorkPlace shortcut check box. The name you assign to the URL resource will appear in the Resource column in WorkPlace.
7. Click the down-arrow button to view the **Advanced** options.

![Advanced Options]

- **Alias name**: 
- **Synonyms**: 

- **Allow public access** (do not authenticate user)
- **Web application profile**: 
  - Default

8. Optionally, specify an **Alias name**—a public alias that will represent the private URL. The alias name will be visible to users, so try to make it easy to remember (the shorter and more descriptive, the better). You should provide an **Alias name** if:

- You want to obscure the internal host name for this resource.
- The URL resource is not contained within one of the search domains configured on the appliance (configured on the **Name Resolution** tab of the **Network Settings** page, under **Domain Name Service**).

For more information about aliases, see “URL Resources” on page 76.

9. In the **Synonyms** box, you can define any alternative names (or “synonyms”) for the URL resource name. This is useful if users access the server using a different name (perhaps an unqualified or condensed name) or if a Web page contains links pointing to a DNS alias and the name is not properly translated by the Web access service. Separate multiple synonyms with semicolons.

The appliance will automatically define the resource shortname as a synonym. For example, if the URL is `http://mail.example.com`, the appliance adds the synonym `mail`. It does not appear in the **Synonym** box, however.

10. Select the **Allow public access** check box if you want to allow unrestricted access to this URL. If this option is enabled, no authentication is used to verify the user's identity. This is useful if you want to provide public access to an internal Web resource. (Note that to enable public access to a resource, you must also create a rule allowing “Any” user to access the resource.)

11. Select a **Web application profile** from the list. The list contains preconfigured Web profiles that are recommended for several popular Web applications, custom Web profiles (see “Adding a Web Application Profile” on page 92), and a default Web profile. If you are unsure of which profile to select, it's best to choose the default. To view the profile, click **View selected profile**. For more information on Web application profiles, see “Adding a Web Application Profile” on page 92.

12. After you've finished, you can define another resource by clicking **Save and Add Another**, or click **Save** to return to the **Resources** page.

### Notes

- A URL resource can be defined in various ways.

<table>
<thead>
<tr>
<th>URL Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard URL</td>
<td><a href="http://host.example.com/index.html">http://host.example.com/index.html</a></td>
</tr>
<tr>
<td>Standard URL with port number</td>
<td><a href="http://host.example.com:80/index.html">http://host.example.com:80/index.html</a></td>
</tr>
<tr>
<td>URL for secure site</td>
<td><a href="https://host.example.com/index.html">https://host.example.com/index.html</a></td>
</tr>
<tr>
<td>URL containing IP address</td>
<td><a href="http://192.0.34.0/index.html">http://192.0.34.0/index.html</a></td>
</tr>
</tbody>
</table>
• Some Web-based applications use Java applets or other browser extensions that submit traffic using protocols other than HTTP. Although accessed using a Web browser, these applications must be defined as network resources (not URL resources) and proxied using the client/server access service. Examples of such applications include Citrix NFuse, Oracle J-Initiator, and certain versions of SAP and PeopleSoft.

Adding a File System Resource

File system resources represent the Windows files and folders that users can access via ASAP WorkPlace.

Note that file system resources cannot be accessed by Aventail Connect users. To give Connect users access to Windows files and folders, you must define the appropriate network resources and apply client/server access control rules.

To add a file system resource

1. From the main navigation menu, click Resources. The Resource Management page appears.
2. On the Resources page, click the New button. The Add/Edit Resource page appears.
3. In the Name box, type a name for the resource.
4. In the Description box, type a descriptive comment about the resource.
5. In the Resource definition area, define a Windows file resource. You can define a specific file system share by typing a UNC path or you can define an entire Windows domain.

   ![Image](image.png)

   - To define a specific file system resource, click the Network share button and type a UNC path. This can be an entire server (for example, `\ginkgo`), a shared folder (for example, `\john\public`), or a network folder (`\ginkgo\news`).
   - To reference a user’s personal folder on the network, click the Network share button and type a UNC path containing the variable `XXX_Username_XXX`. This feature allows you to create a single shortcut on ASAP WorkPlace that dynamically references a personal folder for the current user. For example, say you create a resource by typing `\users\XXX_Username_XXX` in the Network share box. Next, you create a WorkPlace shortcut referencing this resource, time entering `\users\XXX_Username_XXX` in the Link text box. When the user `jdoe` connects to ASAP WorkPlace, the variable will be automatically replaced with his username and provide access to a folder named `\users\jdoe`. When user `rsmith` access the same link, it will provide access to the `\users\rsmith` folder.

   For more information, see “Creating Network Shortcuts to Personal Folders” on page 192.
   - To define an entire Windows domain, click Domain, select the Windows domain check box, and then type the name of the domain in either NetBIOS or DNS syntax (such as `example` or `example.com`). Defining an entire Windows domain gives authorized users access to all the network file resources within the domain.

6. You can optionally add a shortcut to a the file system resource in WorkPlace by selecting the Create ASAP WorkPlace shortcut check box. The name you assign to the URL resource will appear in the Resource column in WorkPlace.
7. After you’ve finished, you can define another resource by clicking Save and Add Another, or click Save to return to the Resources page.

**Editing Resources**

Before modifying a resource, carefully examine the associated rules to understand how your changes will affect your security policy.

**Notes**

- You cannot change an existing network resource’s definition setting (for example, change a host name to an IP range); instead, you must create a new network resource and apply the appropriate definition setting.
- You cannot change an existing ASAP WorkPlace shortcut’s definition setting; instead you must create a new shortcut on the WorkPlace Shortcuts page and apply the appropriate resource definition setting.

▶ **To edit a resource**

1. From the main navigation menu, click Resources.
2. On the Resources page, and then click the name of the resource that you want to edit.
3. On the Add/Edit Resource page, make your edits as needed.
4. Click Save.

**Deleting Resources**

You cannot delete a resource that is referenced in an access control rule, resource group, or WorkPlace shortcut. Before deleting a resource, you must first remove it from any rules in which it is referenced. See “Deleting Referenced Objects” on page 29 for more details.

▶ **To delete a resource**

1. From the main navigation menu, click Resources.
2. On the Resources page, select the check box to the left of any resources that you want to delete.
3. Click the Delete button. If this resource is still referenced by an access control rule, resource group, or WorkPlace shortcut, AMC displays an error message. Click the link in the error message to see a list of all references to this resource.

**Creating and Managing Resource Groups**

You can define individual resources or manage them in resource groups, which are collections of individual resources. Grouping resources provides a convenient way to manage access to a set of resources with similar characteristics. For example, you might define a resource group containing your remote employee applications to simplify the process of managing access to those resources.

There is no limit to the number of resources that a resource group can contain. When you create a new resource group, it is added to your list of available resources and groups; you can then use the resource group in access control rules.

**Adding Resource Groups**

When you create a new resource group, it is added to the list of available groups on the Groups tab of the Resources page.

▶ **To add a resource group**

1. From the main navigation menu, click Resources.
2. On the **Resources** page, click the **Groups** tab, and then click the **New** button. The **Add/Edit Resource Group** page appears.

3. Type a **Name** for the resource group.
4. In the **Description** box, type a descriptive comment about the group.
5. Select the check box for each resource you want to include in the group. There is no limit to the number of resources that a resource group can contain.
6. After you’ve finished, you can define another resource group by clicking **Save and Add Another**, or click **Save** to return to the **Groups** page.

### Editing Resource Groups

Before modifying a resource group, carefully examine the associated rules to understand how your changes will affect your security policy.

**To edit a resource group**

1. From the main navigation menu, click **Resources**.
2. On the **Resources** page, click the **Groups** tab, and then click the name of the group that you want to edit.
3. On the **Add/Edit Resource Group** page, make your edits as needed.
4. After you’ve finished, you can edit another resource group by clicking **Save and Add Another**, or click **Save** to return to the **Groups** page.

### Deleting Resource Groups

You cannot delete a resource group that is referenced in an access control rule. Before deleting a resource group, you must first remove it from any rules in which it is referenced. See “Deleting Referenced Objects” on page 29 for more details.

**To delete a resource group**

1. From the main navigation menu, click **Resources**.
2. On the **Resources** page, click the **Groups** tab.
3. Select the check box for any groups that you want to delete.
4. Click the **Delete** button. If this resource group is still referenced by an access control rule, AMC displays an error message. Click the link in the error message to see a list of all references to this resource group.
Viewing Web Application Profiles

Web application profiles are displayed on the Web Application Profiles page.

To view your list of available Web application profiles
1. From the main navigation menu, click Services. The Services page appears.
2. In the Access Services area, click the Configure link for Web resources. The Configure Web Access Service page appears.
3. Click the Web Application Profiles tab to view your available Web profiles.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Use for most sites without SSO</td>
</tr>
<tr>
<td>DWA</td>
<td>Domino Web Access</td>
</tr>
<tr>
<td>RPC Agents</td>
<td>RPC Agents</td>
</tr>
<tr>
<td>Notes 5.x</td>
<td>Lotus Notes (6.x versions)</td>
</tr>
<tr>
<td>Onyx</td>
<td>Onyx CRM</td>
</tr>
</tbody>
</table>

The table includes preconfigured Web application profiles that are recommended for several popular Web applications, any custom Web profiles you created, and a default Web profile.
4. Click the name of a Web application profile to view its settings.

Adding a Web Application Profile

Web application profiles control single sign-on characteristics as well as content translation options for a particular resource. All Web resources, whether defined as a network resource or a Web resource, should have a Web application profile associated with them.

- **Single sign-on** options control whether and how a user’s login credentials are forwarded to downstream Web applications. These options are turned off by default.
- **Content translation** options control whether hyperlinks in JavaScript code, in cookie bodies and in cookie paths, are translated by the Web access service. Content translation is for more information on how the service performs translation, see the “Aventail SSL VPN Web Developer’s Guide” on the Aventail Assurance Web site. The options are used only by the translated Web access agent, but are ignored by standard Web access.

To add a Web application profile
1. From the main navigation menu, click Services. The Services page appears.
2. In the Access Services area, click the Configure link for Web resources. The Configure Web Access Service page appears.
3. Click the **Web Application Profiles** tab, and then click the **Add** button. The **Add/Edit Web Application Profile** page appears.

![Add/Edit Web Application Profile](image)

4. In the **Name** box, type a name for the profile. If you are creating a profile to associate with a specific application, you may want to give it a profile name that reflects this. For example, a profile for the **xyz** Web application could be named **xyz**.

5. In the **Description** box, type a descriptive comment about the profile.

6. In the **Single Sign-On** area, specify if and how you want user credentials to be passed along to the Web resource. Forwarding user credentials prevents the user from having to log in multiple times (once to get to the appliance, and again to access an application resource).

   - If you select the **Forward each user's individual username and password** check box, the username and password used to authenticate to WorkPlace will be forwarded to the back-end Web server.
   - If you select the **Forward static credentials** check box, the appliance forwards the same username and password for all users. This is useful for Web sites that require HTTP basic authentication, but don't provide personalized content for each user based on the login name. It's also useful for users who authenticate with a client certificate or token.
   - If you do not select either option, single sign-on functionality is disabled. If you select both options, the individual username and password option takes precedence. For example, if the user provides a username/password pair, it will be forwarded, but if username/password is not provided, the Web access service will forward the static credentials.

7. In the **Content Translation** area, select the items that you want the Web access service to translate.

   ![Content Translation](image)
• Select the **Translate JavaScript code** check box if you want the Web access service to translate links embedded in JavaScript code used by the Web resource. This is useful for JavaScript that contains absolute URLs or absolute references ("/to/path/xyz"), or that dynamically generates URLs (for example, location="http://" + host name + "/index.html"). This improves compatibility with Microsoft Outlook Web Access and other applications that rely on JavaScript.

• Select the **Translate DHTML content** check box if you want the Web access service to translate URLs written dynamically by DHTML. This option is useful if a Web resource uses JavaScript’s `document.write` method to dynamically create URLs. This option is disabled by default.

• Select the **Translate cookie body** check box if you want the Web access service to translate URLs embedded in the body of a cookie. Embedding URLs in the body of a cookie is not common practice, but if a Web resource is doing this and you do not have this option enabled, users can experience problems (a common symptom is being redirected to another URL unexpectedly).

• Select the **Translate cookie path** check box if you want the Web access service to translate the path attribute of cookies sent by back-end resources. The browser uses cookie paths to determine when to send a cookie back to the server. The appliance changes the path that the browser sees, so if the cookie path is not translated, the browser will never send the cookie. A common symptom of this situation is a user being prompted repeatedly for login credentials after already entering valid ones. If this occurs, you should enable this option. It is enabled by default.

• Select **Ignore MIME types** if you want the Web access service to determine content type by examining the file extension, not the MIME type. Normally, the Web access service translates certain content types (including text and HTML). It determines the content type from the MIME type in the HTTP header. If a Web resource is sending the incorrect MIME type, select this option and the Web access service will decide whether or not to translate a file based on its file extension. This option is disabled by default.

8. Click **Save**.

**Notes**

- Shipped with the appliance are several preconfigured Web application profiles that are recommended for certain commonly used Web applications. Profiles shipped with the appliance include:
  - **Default**: A default profile that you can use for most Web applications
  - **OWA**: A profile for Microsoft Outlook Web Access
  - **Onyx**: A profile for the Onyx Employee Portal
  - **WorkPlace**: A read-only profile for ASAP WorkPlace

- Because Web resources can be defined quite broadly, the appliance follows a set of rules for determining which Web application profile to apply to an incoming request. The appliance chooses the profile associated with the most specific resource. For example, suppose you’ve defined a DNS domain (xyz.com) as a resource and have attached Web application profile A to it. You’ve also defined a specific Web server (web1.xyz.com) as a resource and have attached Web application profile B to it. A user request comes in for https://web1.xyz.com/timesheet.html. The appliance uses Web application profile B because it is associated with a more specific resource (the Web server) than Web application profile A (the domain). The actual order that the appliance uses is as follows:

  URL --> Host name --> IP address --> Subnet/IP range --> DNS domain

- If you want to associate the same Web application profile to all resources within a single domain, you can associate a profile with that domain, then select **None** as the profile for any individual resources you define that are within that domain. The individual resource will "inherit" the domain’s profile. If there is no profile associated with a particular resource, and there is no profile to inherit, the appliance uses the system defaults for the profile.
Editing Web Application Profiles

Before modifying a profile, confirm that the changes will be compatible with the applications to which the profile is associated.

To edit a Web application profile
1. From the main navigation menu, click Services. The Services page appears.
2. In the Access Services area, click the Configure link for Web resources. The Configure Web Access Service page appears.
3. Click the Web Application Profiles tab, and then click the name of the profile that you want to edit.
4. On the Add/Edit Web Application Profile page, make your edits as needed.
5. Click Save.

Deleting Web Application Profiles

If a profile is still associated with one or more resources, AMC prevents you from deleting it. You must remove all remaining associations if you still want to delete the profile. See “Deleting Referenced Objects” on page 29 for more details.

To delete a Web application profile
1. From the main navigation menu, click Services. The Services page appears.
2. In the Access Services area, click the Configure link for Web resources. The Configure Web Access Service page appears.
3. Click the Web Application Profiles tab, and then select the check box to the left of any profiles that you want to delete.
4. Click the Delete button. If this profile is still referenced by a resource, AMC displays an error message. Click the link in the error message to see a list of all references to this profile.
5. Click Save.

Access Control Rules

Access control rules determine what resources are available to users or groups. Rules can be defined broadly to provide access from any access methods or defined narrowly so that only a specific access method—Web browser, Network Explorer, or Aventail Connect and Aventail OnDemand—is permitted.

In addition to evaluating whether users can access resources based on who they are, access control rules can also factor in the trustworthiness of users' access points using End Point Control zones and device profiles, which are described on “Managing EPC with Zones and Device Profiles” on page 167.

Configuring Access Control Rules

As your network changes over time, you will need to configure the access control rules that determine what application resources are available to your various users and groups.

Before adding an access control rule, carefully examine your list of existing rules; you might find that you can modify an existing rule instead of creating a new one. To save time, you can also copy an existing rule and modify its parameters.

If you decide to add a new rule, reviewing your current configuration will help you determine where the new rule should fit in the rule order. New rules are added to the top of the access control list by default; you can then move them to their proper positions in the list.
Viewing Access Control Rules

Access control rules are displayed in numerical order on the Access Control page. The appliance evaluates the rule in the first position first, the rule in second position second, and so on. All access control rules are displayed by default, but you can use the Display list to filter them by resource type.

To view access control rules

1. From the main navigation menu, click Access Control. The Access Control page appears.

2. Select the rule set that you want to view from the Display list:
   - To view all access rules regardless of resource type, select All.
   - To view access rules controlling access to Web-based (HTTP and HTTPS) resources, select Web browser.
   - To view access rules controlling access to client/server (TCP/IP) resources, select Aventail Connect/OnDemand.
   - To view access rules controlling access to Windows file system resources via ASAP WorkPlace, select Network Explorer.

3. Review the data listed in the access control rule table:
   - The check box column is used to select one or more rules. You’ll use this to delete rules (using the Delete button) or reorder them (using the Move Up and Move Down buttons).
   - The number column indicates the order in which the rule will be evaluated. To edit a rule, click its corresponding number.
   - The Action column indicates whether a rule is used to permit or deny access, or whether it is disabled. When match is found, the appliance takes the action specified here. A rule that permits access displays a green indicator in the Action column, while a rule that denies access displays a red indicator.
   - A disabled rule displays a gray indicator in the Action column. When a rule is disabled, it is not evaluated. This provides a convenient way to temporarily disable a rule without having to delete it.
   - The Description column lists the descriptive text you typed when creating the rule.
   - The Users column indicates the users to whom the rule applies. “Any” indicates that the rule applies to all users.
   - The Destination column lists the destination resources to which the rule applies. “Any” indicates that the rule applies to all resources.
   - The Method column indicates whether a specific access method is associated with a rule. A globe icon signifies Web browser access; a globe icon with a folder represents Network
Explorer, which provides Web access to file system resources; the Aventail logo indicates access via Aventail Connect or Aventail OnDemand. “Any” indicates that the rule applies to all access methods.

- The Zone column indicates whether an access rule is associated with a particular End Point Control zone. EPC zones are used to classify a connection request based on the attributes of the client device. “Any” indicates the rule applies to all EPC zones. A red “restricted” icon indicates that the rule controls access for one or more specific zones.

### Adding Access Control Rules

Perform the following steps to add an access control rule.

**To add an access control rule**

1. From the main navigation menu, click **Access Control**.
2. On the **Access Control** page click **New**. The **Add/Edit Access Rule** page appears.

![Add/Edit Access Rule](image)

3. Type a number in the **Number** box to specify the rule's position in the access rule list. By default, new rules are added to the top of the list, but you can use this box to place the rule anywhere you want. For example, if you assign the number 3 to a new rule, the new rule will be inserted before the current rule 3 (which will become rule 4). This field is required.

4. In the **Description** box, type a descriptive comment about the rule. This step is optional, but a description can be helpful when viewing your list of rules later, and also appears in log files where it is useful in debugging. The **ID** is a unique identifier automatically assigned by AMC; it cannot be edited.

5. Use the **Action** buttons to specify whether the rule will be used to **Permit** or **Deny** access, or if the rule is **Disabled**.

6. Complete the information listed under **Basic settings**:  

   ![Basic Settings](image)

   - The **Users/groups** box specifies the users or user groups to whom the rule applies. Click **Edit** to select from a list of users and groups. If no users or groups are specified, the value for this field defaults to “Any.”

   - The **Destination resources** box specifies the destination resources or resource groups to which the rule applies. Click **Edit** to select from a list. If no destination resources are selected, the value for this field defaults to “Any.”
7. In the **Access methods** area, select one or more access methods from which you will control access to the resource.

- **Any** manages access to all resources in the rule, regardless of the access method making the request. This is the recommended setting in most circumstances, unless your security environment requires you to limit access to a resource to a particular access method.
- **Web browser** manages access from HTTP or HTTPS resources for users connecting via a Web browser.
- **Network Explorer** manages access from Windows file system resources for ASAP WorkPlace users connecting via Network Explorer.
- **Aventail Connect and Aventail OnDemand** manages access from TCP/IP resources such as client/server applications, file servers, or databases, for users connecting via either Aventail Connect or Aventail OnDemand.

For example, suppose you want to provide access to a network domain for users who have Aventail Connect or Aventail OnDemand, but you don’t want to allow browser access to Web resources within that domain. You could do that by creating a rule that specifies the network domain in the **Destination resources** box and selects **Aventail Connect and Aventail OnDemand** as the only access method.

8. In the **End Point Control zones** area, select the zones from which you will permit or deny access to the resources. Click **Edit** to select from a list. The default for this field is "Any” zone. See “Managing EPC with Zones and Device Profiles” on page 167 for information configuring and using zones.

9. When you are finished creating the rule, you can define another rule by clicking **Save and Add Another**, or click **Save** to return to the **Access Control** page.

**Notes**

- Because AMC gives you the flexibility to assign multiple access methods to resources, situations may arise where there is a mismatch between access methods and resources. This happens if you create a rule that assigns an access method that is incompatible with the specified resource. For example, designating **Web access** as the method for accessing a Windows domain resource will trigger an "Invalid destination resources” error message in AMC. For more information see “Resolving Invalid Destination Resources” on page 104.
- In some cases you can create a "deny” rule that contains a mix of resources and access methods that may prevent subsequent rules from being evaluated. This could inadvertently block user access to other resources referenced in the access policy. The logic used to determine access method and resource compatibility is described in "Resolving Deny Rule Incompatibilities Between Access Methods and Resources” on page 103.
Using Advanced Access Control Rule Attributes

For most rules, a basic configuration that includes users or groups, destination resources, and access methods will be sufficient. However, more options are available to provide even tighter access in the Advanced area of the Add/Edit Access Rule page.

For example, if you want to permit connections from only a particular domain, or even from an individual IP address, you would use the Source networks option. Source networks are referenced in an access rule to permit or deny a connection to a destination resource based upon the location from which the request originates. This provides you with even greater security.

To use Advanced settings for an access control rule
1. Click the down-arrow button for the Advanced area on the Add/Edit Access Rule page.

2. Use Source networks to specify the names of any source networks you want evaluated in the rule. This is useful for controlling access based on the origin of the connection request. Click Edit to select from the list of network resources. If no source network is specified, the value of this field defaults to “Any.”

3. Use Permissions to specify whether the rule will allow Read and/or Write access to the file system resource(s). These access privileges work in conjunction with the Windows access control rules associated with the same file system resource(s). Permission must be granted by both entities (that is, Windows and the appliance) for a user to receive a certain privilege. Note that if you disable file uploads, all users will be unable to write to files. Users with write access will be able to move and delete files, however.

4. Use Destination ports to restrict access over individual ports or a range of ports. For example, if you are building a policy to control access to an SMTP mail server, you might allow access only over port 25 (the well-known port for SMTP traffic). A list of the latest port number assignments is available at http://www.iana.org/assignments/port-numbers.

To enable access on any port, click Any. To specify multiple ports, click Selected and type the port numbers, separating each with a semicolon. To specify a port range, type the beginning and ending numbers separated by a hyphen.

5. Specify the Minimum key length required on the user’s device when making SSL connections. To require the greatest security on the user’s device, choose 128-bit. If your environment does not support strong encryption, choose a shorter key length.
6. Under **Time and date**, specify when the rule will be in effect. You can specify a **Shift** or a **Range**, or you can specify that the rule remain in effect at all times.

```
<table>
<thead>
<tr>
<th>Any</th>
<th>Range</th>
<th>Shift</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

7. Specify the **SOCKS commands** that the client/server access service will accept from the client. For example, you might allow **Bind** or **Connect** requests, but deny **Ping** connections. A brief description of each command is included here, but for more details, see [http://www.ietf.org/rfc/rfc1928.txt](http://www.ietf.org/rfc/rfc1928.txt).

- **Bind** is used in protocols that require the client to accept connections from the server. FTP is a notable example. Bind usually occurs with a Connect/Bind pair of connections.
- **Connect** is used for all normal TCP connections (for example, SSH, telnet, scp, and so forth).
- **Ping** and **Traceroute** are common network troubleshooting commands. Selecting these commands will configure the client/server access service to perform these operations on your behalf.
- **UDP** allows the client/server access service to make a UDP data transfer. This is necessary for operations such as streaming audio and Microsoft Outlook new mail notification. For UDP connections, you can restrict access based on whether encryption is used by selecting **Match encrypted**, **Match unencrypted**, or **Match either**.

8. When you are finished creating the rule, you can define another rule by clicking **Save and Add Another**, or click **Save** to return to the **Access Control** page.

**Notes**

- When you select one or two access methods, the advanced options are enabled or disabled based on whether they apply to the access method(s). However, if you select “Any” as the access method, all the advanced options will be available. When AMC validates the rule it prevents you from selecting rule attributes that are not relevant to the access methods. The following table shows the advanced options that apply to each access method.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Applicable Advanced Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser (HTTP/HTTPS)</td>
<td>• Source networks</td>
</tr>
<tr>
<td></td>
<td>• Minimum key length</td>
</tr>
<tr>
<td></td>
<td>• Time and date</td>
</tr>
<tr>
<td>Network Explorer (Web access to file system resources)</td>
<td>• Source networks</td>
</tr>
<tr>
<td></td>
<td>• Read/write permissions</td>
</tr>
<tr>
<td></td>
<td>• Time and date</td>
</tr>
</tbody>
</table>

Aventail
Adding Users and Resources From Within Access Control Rules

Some administrators prefer to define all policy objects (users, groups, and resources) before creating access control rules. Although this structured approach works particularly well for the initial configuration, you may find it inconvenient for ongoing management. If so, you can define new resources directly from the interface used to create access control rules.

To add a user or resource from within an access control rule

1. From the Add/Edit Access Rule page, click Edit beside the Users/groups box or the Destination resources box.

A popup window appears displaying your current users and groups, or resources.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Applicable Advanced Options</th>
</tr>
</thead>
</table>
| Aventail Connect & Aventail OnDemand (TCP/IP) | • Source networks  
• Destination ports  
• Minimum key length  
• Time and date  
• SOCKS command |
2. Click the New button. The next page displayed depends on the type of object (user, group, or resource) you are creating.
3. Define the settings for the new user, group, or resource.
4. After you’re finished, you can define another object by clicking Save and Add Another, or click Save to return to the previous page. The new object appears in the user, group, or resource list.
5. Select the check box beside the object you want to add to the access rule and then click Save to return to the Add/Edit Access Rule page.

Editing Access Control Rules
Before modifying an access control rule, carefully examine your existing rules to understand how your changes will affect your security policy. Pay close attention to the rule order.

▲ To edit an access control rule
1. From the main navigation menu, click Access Control.
2. On the Access Control page, click the number of the rule that you want to edit. For example, if you want to edit the rule in the third position in the list, click 3.
3. Make any edits, as needed, on the Add/Edit Access Rule page, and then click Save.

Copying an Access Control Rule
Rather than creating a new access control rule from scratch, you may be able to save time by making a copy of an existing rule and changing some parameters to fit the new rule. Choose a rule to copy that shares the most characteristics with the rule you plan to create. Copying a rule is also useful when testing your access policy.

▲ To copy an access control rule
1. From the main navigation menu, click Access Control.
2. On the Access Control page, select the check box next to the rule that you want to copy.
3. Click Copy. The Add/Edit Access Rule page appears. Note that all the fields for the new rule are the same as those for the rule you based it on, with the exception of the Number field, which is set to 1.
4. Leave the Number field set to 1 if you want the new rule added to the top of the list, or type a different number to assign the rule to another position.
5. Type a new Description for the rule. AMC will not prevent you from creating rules with the same description, but the best practice is to assign each rule a unique and meaningful description.
6. Change the settings for any other fields on the Add/Edit Access Control page as needed.
7. When you are finished defining the rule, you can define another rule by clicking Save and Add Another, or click Save to return to the Access Control page.

Deleting Access Control Rules
Before you delete an access control rule, carefully examine your existing rules to understand how the deletion will affect your security policy. Note that you will not be prompted to confirm the deletion; use caution when deleting rules.

▲ To delete an access control rule
1. From the main navigation menu, click Access Control.
2. On the Access Control page, select the check box for any access rules that you want to delete.
3. Click the Delete button.
Moving Access Control Rules

You can reorder the placement of one or more rules in the access control list. Before you reorder your access control rules, carefully examine them to understand how the reordered list will affect your security policy.

To move access control rules

1. From the main navigation menu, click Access Control.
2. On the Access Control page, select the check box for each rule that you want to move.
3. Click the Move Up or Move Down button as appropriate. Each click of the button moves the selected rules up or down one position on the list.

Notes

- When you use the Display option to filter the view of the access rules by a specific access method, you cannot use the Move Up and Move Down buttons to reorder the list. You can only move an access control rule when Display is set to “All.”
- To move a rule multiple positions in the list, you may find it faster to change the Number box on the Add/Edit Access Rule page.

Resolving Deny Rule Incompatibilities Between Access Methods and Resources

If you attempt to define a “deny” rule referencing any of the three combinations described in the following table, AMC will display the warning message “Some of the resources in this rule are not supported by the selected access method(s), which could inadvertently deny access to some resources.”

In a “permit” rule, you can safely mix and match resources and access methods. However, “deny” rules containing specific combinations of resources and access methods may prevent subsequent rules from being evaluated. This could inadvertently block user access to resources referenced later in your access policy.

During its policy evaluation, the appliance may in some cases be unable to determine whether a deny rule matches an incoming connection request. As a security precaution, it stops processing your rule set and blocks user access. This occurs during evaluation of a deny rule containing any of the following combinations of resource types and access methods.

<table>
<thead>
<tr>
<th>Rule Action</th>
<th>Resource Type</th>
<th>Access Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Windows domain</td>
<td>• Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web browser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Aventail Connect and OnDemand</td>
</tr>
<tr>
<td>Deny</td>
<td>URL</td>
<td>• Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Aventail Connect and OnDemand</td>
</tr>
<tr>
<td>Deny</td>
<td>Network share</td>
<td>• Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Aventail Connect and OnDemand</td>
</tr>
</tbody>
</table>

Example

For example, suppose you create a deny rule blocking access to a Windows domain and leave Access methods set to “Any.” Since a Windows domain is accessible from ASAP WorkPlace, when the appliance receives a connection attempt from ASAP WorkPlace, it would match the rule and deny access.

However, assume the user makes a connection request from Aventail Connect or OnDemand, or from a standard Web browser. In this case, the appliance would be unable to determine whether the Windows domain rule matched the request (regardless of what destination resource is being requested). The appliance would then stop evaluating any further rules in your policy and
immediately deny access. If the Windows domain rule were at the top of your access control list, it would very likely prevent the user from accessing any VPN resources. For example, if the next rule in the list were a permit rule allowing the user to access a VPN resource, it would not be evaluated.

**Resolving the Problem**

To resolve rule incompatibilities, we recommend you modify the rule so it doesn’t reference indeterminate access methods. In the case of a Windows domain or Network share, you should select only Network Explorer as the access method. For a URL, you should select only Web browser or ASAP WorkPlace as the access method.

**Resolving Invalid Destination Resources**

If you attempt to create a rule that assigns an access method to an incompatible destination resource, AMC will prevent a mismatch by displaying the warning: “Invalid destination resources: These resources are not accessible from the selected access method(s).” The following table lists the access method/destination resource combinations that will trigger this warning.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Invalid Destination Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>• Windows domain</td>
</tr>
<tr>
<td></td>
<td>• Network share</td>
</tr>
<tr>
<td>Network Explorer</td>
<td>• URL</td>
</tr>
<tr>
<td>Aventail Connect and Aventail OnDemand</td>
<td>• URL</td>
</tr>
<tr>
<td></td>
<td>• Windows domain</td>
</tr>
</tbody>
</table>

**Example**

For example, suppose you create a rule to access a Windows domain resource, and then designate Web browser as the access method. When you select that combination, the “Invalid destination resource” warning appears on the Add/Edit Access Rule page immediately above the Access methods area. AMC will not permit you to save this rule while it contains a method/resource mismatch. If you click Save with this mismatch still selected, AMC removes the invalid resource from the rule. If the rule contains only one mismatched resource, it is replaced with “Any.”

**Resolving the Problem**

To resolve a destination resource error, modify the rule so that the type of access method is compatible with the destination resource. The simplest way to avoid an access method/destination resource mismatch is to set the Access method option on the Add/Edit Access Rule page to "Any."
Chapter 7
Users, Groups and Realms

Most access control rules determine which resources are available for users or groups of users. Accordingly, you must define users and groups in AMC that map to users or groups stored in external user directories. The appliance directly integrates with leading back-end authentication systems, eliminating the need to create and manage user accounts directly on the appliance. At a higher level, realms unite users and groups into user communities that share common characteristics, most notably access policy.

- Managing Realms
- Managing Users and Groups

Overview: Users, Groups, and Realms

A user is an individual who needs access to resources on your network. A user group is a collection of users. After you’ve created a user or user group on the appliance, you can reference it in an access control rule to permit or deny access to resources.

Realms serve two distinct purposes for the Aventail VPN: they define user communities, and they configure user authentication. This section describes the role of realms in setting up your user communities.

Realms let you determine which access agents are provisioned to the members of a user community when they log in to a realm. For example, you may want to enable OnDemand for your employee realm, but provide only Web access to your partner realm. If End Point Control is enabled, realms can also be used to determine which “zones of trust” members belong to within the realm.

Users and groups are not actually stored on the appliance. Instead, you create references to existing users or groups stored in an external LDAP, Microsoft Active Directory, or RADIUS repository. This eliminates the need to create and manage users directly on the appliance.

In most directories, similar user accounts are grouped together to grant them similar rights and permissions. Assuming that your directory is organized this way, most of your user management on the appliance will usually be centered around user groups, not individual users. First, you’ll set up the appliance to reference user groups stored in your directory, and then you’ll reference those groups in access control rules. In most cases, you’ll need to manage individual users only when you need to assign them permissions that are different from what their group membership would allow.

You can define a user or group before referencing it in an access control rule or, alternatively, you can define a new user or group directly from the access control rule interface. For more information, see “Adding Users and Resources From Within Access Control Rules” on page 101.

Notes
- The appliance also supports local users, which are stored locally on the hard disk. Local users are recommended only for testing purposes, and are not intended to be used in production. You cannot create local user accounts in AMC; instead, use the standard UNIX commands. See “UNIX Command Reference” on page 236 for details.
Default, Visible, and Hidden Realms

To authenticate a user, the appliance must know which realm the user belongs to. If only one realm is enabled, the appliance automatically uses that realm. But if multiple realms are enabled, the appliance needs to know which one to use. When users log in, they will typically choose the appropriate realm from a list.

You can make their choice easier, however, by defining a default realm within AMC. (See “Selecting the Default Realm” on page 112.) If a default realm is defined, the realm selection box is automatically populated with the default realm (there is one exception to this rule with the Connect client). The specific behavior of each access method is outlined in this section.

It is strongly recommended that you select a default realm.

You can also choose which realm names are visible to end users. If a user needs to log in to a realm that is hidden, the user must know the realm name and must manually type it into the login box. For example, suppose you have created realms for various suppliers and you’d prefer that the suppliers not know about one another. You would hide these realm names, requiring each supplier to type in their realm name when logging in to the appliance.

The following table describes the typical end-user login experience for various realm configurations.

<table>
<thead>
<tr>
<th>Realms enabled</th>
<th>Default realm configured?</th>
<th>Hidden realm(s) configured?</th>
<th>User’s login experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>N/A</td>
<td>N/A</td>
<td>User does not have to select a realm during login. Access methods automatically use the one enabled realm for authentication.</td>
</tr>
<tr>
<td>Multiple</td>
<td>Yes</td>
<td>None</td>
<td>User must select a realm from the list. Realm text box is initially populated with the default realm.</td>
</tr>
<tr>
<td>Multiple</td>
<td>No</td>
<td>None</td>
<td>User must select a realm from the list. Realm text box is initially populated with the first realm (sorted alphabetically).</td>
</tr>
<tr>
<td>Multiple</td>
<td>Yes</td>
<td>Yes</td>
<td>User must select a realm from the list. Realm text box is initially populated with the default realm. Realm list also contains an entry called Other and a second text box appears. If login requires a hidden realm, user selects Other and types realm name in the second text box.</td>
</tr>
</tbody>
</table>

Following is a detailed description of the user’s login experience for each access method.
ASAP WorkPlace

When users first access ASAP WorkPlace, they are presented with one or more login pages. If only one realm is enabled, they see only the page requesting their user credentials. If multiple realms are enabled, they see the following login page on which they select the appropriate realm:

Please log in

Log in here to establish a secure connection to your network resources.

Log in to Employees

If there are one or more hidden realms, the login page looks like this:

Please log in

Log in here to establish a secure connection to your network resources.

Log in to Other...

To type a name, choose Other from the list above

Next

After clicking Next, users authenticating with username and password are presented with the page for typing credentials.

Please log in

Log in here to establish a secure connection to your network resources.

Log in to Employees

User name:

Password:

Login

Aventail Connect

A Connect user’s login experience differs depending on how Connect is configured (see the Aventail Connect Administrator’s Guide for configuration information).
Chapter 7 - Users, Groups and Realms

If Connect is configured to use the default realm and a default realm is configured on the appliance, Connect automatically uses the default realm and does not prompt the user for a realm. If no default is defined or if Connect is not configured to use the default, the user sees an empty box and must select a realm from the list or type a realm name. Hidden realms do not appear in the list.

Notes

• If a user logs in with a pre-5.3 version of Connect, Connect will automatically use the default realm without prompting the user. If no default is defined, it will automatically use the first realm (in alphabetical order).

Managing Realms

When using realms to set up user communities, AMC allows you to determine which access agents are provisioned to members of a specific realm, and optionally classify realm members’ devices into “zones of trust.” Realms can also be configured to use zones for providing special access to subsets of users. See “Creating Zones for Special Situations” on page 173.

The following illustration shows how a realm authenticates users, provisions access agents, and if End Point Control is enabled, assigns them to different zones based on the trustworthiness of their computers.

In this example, two separate realms for employees and business partners use the same LDAP server to authenticate users. When a user authenticates and logs in to the appropriate realm, the appliance classifies the connection request based on attributes it detects on the device, assigns it to a zone, and provisions the appropriate access agent.
This example shows members of the employees realm being assigned to one of two zones, depending whether they’re connecting from a home computer that’s authorized to have standard Web access, or from an IT-managed computer that’s considered more trustworthy and authorized access to network resources. Business partners log in to a separate realm with access only to specific Web resources:

**Best Practices For Defining Realms**

When defining realms, there are several best practices to follow to simplify your users’ login experience.

- Keep in mind that your end users choose a realm name when logging in; therefore you should choose realm names that clearly describe the user community. For example, a realm that includes all internal employees might be called "employees," while a realm that includes external suppliers might be called "suppliers."

- If some of your users will be logging in to realms that are hidden, you should tell your users the realm name they need to type as well as how to type it in (choose Other from the realm list and then type the realm name in the text box).

- Enable multiple realms only if necessary. If only one realm is enabled, users do not need to select a realm as part of the login process. When moving from a test to a production environment, verify that all test realms have been removed.

**Viewing Realms**

Realms configured in AMC are displayed on the Authentication page.
To view configured realms

1. From the main navigation menu, click Authentication. The Authentication page appears.

2. Review the data listed in the Realms table:
   - The check box column is used to select one or more realms. You'll use this to delete realms, or to copy them.
   - The Enabled column indicates whether a realm is enabled or disabled. A green indicator means the realm is enabled, while a red indicator means the realm is disabled. When a realm is disabled, users and groups associated with that realm will be unable to log in.
   - The Name column displays the name you assigned when creating a realm. You can edit a realm by clicking its name.
   - The Authentication server column lists the name of the authentication server that is referenced by each realm for verifying users’ identities.
   - The Description column lists the descriptive text you typed when creating a realm.

Creating and Configuring a Realm

Perform the following steps to create and configure a realm for a user community. If you create more than one realm, you’ll need to choose one as the default realm, which is described later in this section.

1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Realms area, click New. The Configure Realm page appears.
3. In the Name text box, type a meaningful name for the realm. Keep in mind that your end users select a realm name when logging in, so choose a name that clearly describes the user community.
4. In the Description text box, type a descriptive comment about the realm.
5. Enable or disable this realm by selecting the appropriate **Status**. See “Enabling and Disabling Realms” on page 112 for more information.

6. If you want this realm to appear in the list of realms seen by your users (recommended in most cases), select the **Display this realm** check box.

7. Select the **Authentication server** that the realm will use to verify users’ identities. This field is required. You can also click **New** to configure a new authentication server. For more information, see “Managing User Authentication” on page 51.

8. In the **Zones** area, you can optionally assign one or more End Point Control zones to the realm. Zones determine which devices are authorized to belong to a realm. If you don’t select a zone, realm users will be assigned to the default zone, which could limit or even deny access to resources, depending on your access policy. Select an entry from the **Available zones** list and then click **Add**.

   Zones are matched in the order they are listed, so it is important to you consider which devices are authorized in each zone. We recommend placing your most specific zones at the top of the list. For information about zones, see “Managing EPC with Zones and Device Profiles” on page 167.

9. Select which **Web access** agent will be provisioned to members of this realm for accessing URL resources through ASAP WorkPlace:

   - Select **Use standard Web agent** if you want to provide improved application compatibility to any URL resource. The standard Web agent is available only for Windows XP or 2000 users; other platforms will default to translated Web access. You can also set the inactivity timer to end inactive user connections by choosing a time limit from the **End inactive user connections** list.

   - Select **Use translated Web access** if you want to provide cross-platform access to URL resources that are specifically configured to run with WorkPlace, and let users specify other URLs.

   For more information on configuring WorkPlace, see “Aventail ASAP WorkPlace” on page 183.
10. Select whether you want to provision realm users with the access agent for **Client/server access with OnDemand**:

- Select the **Enable OnDemand** check box to provision access to client/server (TCP/IP) resources from WorkPlace.
- Select **Dynamically redirect connection** if you want OnDemand to dynamically redirect traffic to any network destination resources defined in AMC. Dynamic redirection is available only for Windows users with administrator privileges.
- Select **Embed Aventail OnDemand agent in WorkPlace** if you want OnDemand to start automatically when users connect to WorkPlace. If this option is not selected, users will have to click a link in WorkPlace to automatically start OnDemand.

For more information on configuring OnDemand, see page "Aventail OnDemand" on page 201.

11. Click **Save** to enable the realm settings and return to the **Authentication** page.

**Selecting the Default Realm**

If you use more than one realm, you will need to select one as the default. To authenticate a user, the appliance must know which realm the user belongs to. If only one realm is enabled, the appliance automatically uses that realm. But if multiple realms are enabled, the appliance needs to know which one to use. When users log in, they will typically choose the appropriate realm from a list. You can make their choice easier, however, by defining a default realm within AMC.

Even if you configure only one realm, if that realm is not specified as the default, AMC will display the warning message “There is no default realm selected” on the **Authentication** page.

**To select a default realm**

1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.
2. In the **Default realm** list, select the realm that will be the default. This list shows only those realms that are enabled and configured to be displayed. Hidden realms cannot be set as the default and thus are not included. If you select **None** (which is not recommended), users will need to choose the appropriate realm when logging in.

**Enabling and Disabling Realms**

The appliance supports the simultaneous use of multiple realms. You can control which realms are active by enabling and disabling them. When a realm is disabled, users and groups associated with that realm will be unable to log in. If no authentication realm is enabled, users will not have access to the network.

**To enable or disable an authentication realm**

1. From the main navigation menu, click **Authentication**. The **Authentication** page displays the list of defined realms. If a realm is enabled, its indicator icon in the second column from the left appears green. If a realm is disabled, its indicator icon is gray.
2. Click the name of the realm you want to enable or disable. This opens the **Configure Realm** page for that realm.
3. Select whether the **Status** for the realm is **Enabled** or **Disabled**, and then click **Save**.
Editing a Realm

Perform the following steps to edit a realm’s configuration.

► To edit an authentication realm
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. Click the name of the realm you want to edit. This opens the Configure Realm page for that realm.
3. Make your configuration changes and then click Save.

Copying a Realm

To save data entry when you’re creating multiple realms, you can copy the settings from an existing realm and use them as the basis for configuring a new realm.

► To copy a realm
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Realms area, select the check box to the left of the realm that you want to copy, then click the Copy button. This opens the Configure Realm page for that realm. Note that all the settings from the original realm are displayed in the fields.
3. In the Name text box, type a meaningful name for the new realm. Keep in mind that your end users chose a realm name when logging in, so choose realm names that clearly describe the user community.
4. Change any Available zones, Access methods, and Advanced settings as needed. See “Creating and Configuring a Realm” on page 110 for information on these settings.
5. Click Save to create the new realm and return to the Authentication page.

Deleting a Realm

Perform the following steps to delete a realm.

► To delete a realm
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Realms area, select the check box to the left of the realm that you want to delete, then click the Delete button.

You cannot delete a realm that is still associated with users or groups. You must either delete the users and groups, or associate them with a different realm. For more information see "Deleting Referenced Objects" on page 29.

Restricting User or Group Membership to a Realm

If a realm references a user directory on an external authentication server, you can configure the realm to permit only a subset of all users and groups from that directory to log in to the realm. This creates, in effect, “virtual realms” derived from selected users and groups that are currently configured in AMC.

► To restrict the users or groups who can log in to a realm
1. From the main navigation menu, click Authentication. The Authentication page appears.
2. In the Realms area, click the name of the realm whose membership you want to modify. This opens the Configure Realm page for that realm.
3. In the **User or group restrictions** area under **Advanced**, specify which users or groups can log in to the realm.

   **User or group restrictions**
   
   To restrict the users or groups who can log in to this realm, specify their names below.

   ![User or group restrictions table](image)

   - If the realm references an LDAP or Microsoft Active Directory authentication server, click **Search** to add users or groups by searching the contents of the directory. For information, see “Adding Users or Groups by Searching a Directory” on page 115.
   - If the realm references a RADIUS server, type a group name or a username in the **Name** box, then click **Add**.

4. Click **Save** to return to the **Authentication** page.

   > To delete a user or group from the realm restriction list
   
   1. Select the check box next to the name of the each user or group you want remove from the list.
   2. Click **Delete**.
   3. Click **Save** to return to the **Authentication** page.

   If you delete all the users or groups that were added to a realm’s restriction list, the result is that the realm returns to its default membership configuration, which includes all users as defined by the authentication server referenced by the realm.

### Enabling Group Affinity Checking in a Realm

The appliance enables “group affinity checking,” which accommodates network environments where authentication and authorization are handled by different servers, and facilitates increased security through two-factor authentication. Group affinity checking allows you to configure a secondary authentication server—either Active Directory or LDAP—that is queried for group affinity.

A common situation for using group affinity checking involves a RADIUS database with authentication tokens configured as the primary authentication server, and an LDAP or Active Directory server configured for determining group affinity.

   > To enable group affinity checking
   
   1. From the main navigation menu, click **Authentication**. The **Authentication** page appears.
   2. In the **Realms** area, click the name of the realm you want to modify. This opens the **Configure Realm** page for that realm.
3. In the **Advanced** area, select the **Enable group affinity checking** check box.

   ![Enable group affinity checking](image)

   This controls authorization by performing a group affinity check against an LDAP or Active
   Directory server.

   - Enable group affinity checking
   - Server: None

4. Select the name of the LDAP or Active Directory server that will perform group affinity
checking from the **Server** list. You can also click **New** to define a new group affinity server
using the **New Authentication Server** page.

5. Click **Save** to return to the **Authentication** page.

### Managing Users and Groups

User and group management is an ongoing job. Users and groups are not stored directly on the
appliance, but are instead referenced from external user directories. Although most user
management is done through the external user repository, keeping the AMC list current is essential
for delivering secure, reliable access.

The users and groups defined in AMC will be associated with any directories currently configured on
the appliance.

### Adding Users or Groups by Searching a Directory

For Microsoft Active Directory and LDAP directories, you can add users by searching the contents
of the directory and selecting users or groups from a list, instead of manually typing a distinguished
name (DN). Note that this feature is not available for adding users contained in a RADIUS realm (or
in the local user store).

When you add a user or group, it appears in the list on the **Users page** or **Groups page**, respectively. You can then add the user or group to access control rules.

1. To add users or groups by searching a directory
   1. From the main navigation menu, click **Users & Groups**. The **Groups** page appears.
   2. Choose the type of object you want to add:
      - To add a group, click the **Groups** tab.
      - To add a user, click the **Users** tab.
   3. Click the **Search** button. The **Search Directory** window appears.
   4. In the **Look in** list, choose the directory you want to search.
   5. Define your search criteria:
      - In the **Search for** box, type all or part of a user or group name. The default is *, which
        will return all records in the realm. You can use the wildcard character (*) anywhere in
        the search string. For example, to find group names beginning with the letter "j," you
        would type j*. Or, to find a users named "Mary" or "Marty" (but not "Max"), you could
type m*y.
      - To narrow your search, type an LDAP attribute in the **Attribute** box. For example, you
        might type sn to look for a user's surname, or cn to find a common name.
      - Type the number of results you want returned on each page in the **Show** box. The
default is 25.
      - To specify more detailed search criteria, click the **Advanced** tab; see “Advanced Search
Methods” on page 117 for details.
6. Click **Search**.

7. Locate the objects you want to add:
   - Use the arrow buttons in the lower left pane to page through the results. < and > move forward and back one page at a time. << and >> display the first and last pages, respectively.
   - To view detailed information about a user or group, click its name. A detailed list of attributes appears in the right pane.
   - Select the check box to the left of any users or groups you want to add to the appliance.

8. Click the **Insert Selected** button to add the selected users or groups to the appliance. To select (or deselect) all users or groups on the current page, select the check box next to **Select all/none**.

9. When you’re finished, click the **Close** button in the upper right to close the popup window and return to the main AMC page.

**Notes**
- By default, the basic search is configured to locate users and groups by querying the `sAMAccountName`, `cn`, `uid`, and `userid` attributes.
Advanced Search Methods

If you are familiar with LDAP syntax, you can create an advanced search to further narrow the scope of your query. This is especially useful for reducing the number of search results, particularly when querying a large directory. In some cases, you may also need to perform an advanced search in order to query a directory using a non-standard schema.

To perform an advanced search, click the **Advanced** tab. The fields used to specify advanced search criteria are explained in the following table.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter box</strong></td>
<td>Specify an LDAP search filter that will reduce the scope of the search.</td>
</tr>
</tbody>
</table>

**Syntax**

```
filter=(operator(LDAP attribute=value)(..))
```

**Operators**

- **OR** = "|
- **AND** = "&"
- **NOT** = "!"

**Examples**

- `{cn=Babs Jensen}`
- `{(cn=Tim Howes)}`
- `(&(objectClass=Person) ((sn=Jensen) (cn=Babs J*))`
Chapter 7 - Users, Groups and Realms

Notes

• For more information on LDAP search filters, see RFC 2254 at http://www.ietf.org/rfc/rfc2254.txt.

• The LDAP search syntax is flexible and provides several ways to accomplish the same result. For example, you might use the object class to search for all groups in a directory:

objectclass=group

Alternatively, you could accomplish the same result using a search filter:

(|(objectclass=group)(objectclass=groupOfNames))

Adding a User or Group Manually

When you create a user or group, it appears in the list on the Groups page or the Users page. You can then add the user or group to access control rules.

To add a user or group

1. From the main navigation menu, click Users & Groups. The Groups page appears.
2. Choose the type of object you want to add:
   • To add a group, click the Groups tab, and then click the New button. The Create Group Mapping page appears.
   • To add a user, click the Users tab, and then click the New button. The Create User Mapping page appears.
3. In the **Realm name** list, select the realm to which the user or group belongs. If it exists in multiple realms and you want the appliance to search for any occurrence, select **Any** from the realm list.

4. In the **Group name** or **User name** box, type the group or user information. Type the name exactly as it appears in the external repository. The following table explains the syntax used to define users and groups.

<table>
<thead>
<tr>
<th>Object</th>
<th>Directory type</th>
<th>What to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Active Directory</td>
<td>Type a common name (CN) or distinguished name (DN). Although a CN is easier to enter than a DN (for example, you can type <code>Sales</code> instead of <code>cn=Sales,cn=Users,dc=example,dc=com</code>), the CN is not guaranteed to be a unique match. When in doubt, it’s safer to use a DN.</td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
<td>Type a distinguished name (DN). For example, you might type <code>cn=Sales,cn=Users,dc=example,dc=com</code>.</td>
</tr>
<tr>
<td></td>
<td>RADIUS</td>
<td>Type a group name. For example, you might type <code>Sales</code>.</td>
</tr>
<tr>
<td>User</td>
<td>Active Directory or RADIUS</td>
<td>Type a username. For example, you might type <code>jsmith</code>.</td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
<td>Type a distinguished name (DN). For example, you might type <code>cn=jsmith,cn=Users,dc=example,dc=com</code>.</td>
</tr>
</tbody>
</table>

**Notes**
- Usernames and group names are case-sensitive.
- If you enter the name incorrectly (for example, `mktg` or `Marketing` instead of `marketing`), the user or group members will be unauthorized to access any resources.
- For Active Directory or LDAP directories, you can also click **Browse** to search the directory.

5. In the **Description** box, type a descriptive comment about the user or group.

6. Click **Save** to return to the **Groups** page or **Users** page, or click **Save and Add Another** to add another user or group.

**Notes**
- When you add a user group in AMC, you are not actually grouping users. You are merely adding the name of a user group that is defined in your external user repository.
- The appliance also supports local users (stored in `/etc/password`) for use in testing. You cannot create local user accounts in AMC; instead, use the standard UNIX commands. See “UNIX Command Reference” on page 236 for details.

### Editing a User or Group

If a user or group name or distinguished name changes in your external directory, you’ll need to modify the account on the appliance.

**To edit a user or group**

1. From the main navigation menu, click **Users & Groups**. The **Groups** page appears.
2. Choose the object you want to edit:
• To edit a group, click the Groups tab, and then click the name of the group that you want to edit. The Create Group Mapping page appears.
• To edit a user, click the Users tab, and then click the name of the user that you want to edit. The Create User Mapping page appears.

3. Make any edits as needed.
   Note that if the user or group is in an Active Directory or LDAP realm, you can click the Browse button and search for the user. Clicking Insert Select User or Insert Selected Group will update the user or group mapping on the appliance.

4. Click Save to return to the Groups page or Users page, or click Save and Add Another to edit another user or group.

Deleting a User or Group

When you delete a user or group, its mapping is removed from the system. Deleting a user or group does not remove it from the external user directory.

▷ To delete a user or group
1. From the main navigation menu, click Users & Groups. The Groups page appears.
2. Choose the object you want to delete:
   • To remove a group, click the Groups tab, and then select the check box to the left of any groups that you want to delete.
   • To remove a user, click the Users tab, and then select the check box to the left of any users that you want to delete.
3. Click the Delete button.

Notes
• If the user or group is referenced in an access control rule, AMC displays an error message. In this case, you must first remove the user or group from any rules in which it is referenced. Click the link in the error message to see a list of all references to this user group. See "Deleting Referenced Objects" on page 29 for more details.
Chapter 8
System Administration

This section describes how to manage the Web access and client/server access services, how to configure and use the system logging, and how to configure Secure Sockets Layer (SSL) encryption options. It also describes how to use a variety of command-line tools to upgrade, rollback, or reset software versions and to back up or reset configuration files.

You may occasionally need to use a few UNIX commands when managing the system. If you are new to UNIX, see “UNIX Command Reference” on page 236 for more information.

Optional Network Configuration

This section describes how to configure a variety of network services and tools. It explains how to enable SSH access from remote hosts and how to enable Internet Control Message Protocol (ICMP) so you can ping the appliance. It also describes how to configure the time settings on the appliance.

For information about configuring and using SNMP, see “SNMP Configuration” on page 137.

Enabling SSH Access from Remote Hosts

Enabling SSH provides an easy way to access the appliance console from another system. You can enable SSH access from your internal network or from an external network. The local SSH server daemon (sshd) listens on port 22 (the well-known port number for SSH).

To enable SSH access
1. From the main navigation menu, click Services.
2. Click the Configure link for SSH in the Network Services area. The Configure SSH page appears.
3. To enable SSH, select the **Enable SSH** check box.

4. To add a host from which you want to enable SSH access, type the IP address and subnet mask for the host you want to add, then click **Add**.

5. Click **Save**.

   **To delete a host:**
   1. Click the **Delete** button to the right of any hosts you want to remove.
   2. Click **Save**.

**Notes**
- Do not use SSH when performing upgrades from the command line. It is recommended that you perform upgrades from a serial console instead.
Enabling ICMP

Enabling ICMP allows you to use the ping command to test network connectivity to the appliance from another computer on the same subnet. Note that this will not enable broadcast pings.

**CAUTION** Enabling ICMP makes it possible to ping the appliance from both network interfaces. Unless you suppress ICMP Echo Request traffic using a firewall or other network device, it will be possible to discover the appliance from the Internet.

**To enable ICMP**
1. From the main navigation menu, click **Network Settings**. The **General** page appears.
2. In the **ICMP** area, select the **Enable ICMP pings** check box.
3. Click **Save**.

Configuring the Time Settings

By default, the appliance is set to Greenwich Mean Time (GMT). If you want the logs to reference your local time, you'll need to configure the time settings on the appliance. You can configure the appliance to use Network Time Protocol (NTP) to accurately set the system clock. You can also manually configure the date, time, and time zone.

**To configure the time settings using NTP**
1. From the main navigation menu, click **Services**. The **Services** page appears.
2. Click the **Configure** link for **NTP** in the **Network Services** area. The **Configure NTP Settings** page appears.
3. To enable NTP, select the **Enable NTP** check box.
4. To configure NTP, type the IP addresses for one or more NTP servers in the **Primary server** and **Backup server** boxes. The appliance will attempt to synchronize with the primary server, and will use the secondary servers as needed if the primary server is unavailable.
5. Click **Save**.

**Notes**
- The appliance does not use NTP authentication keys, making it possible for someone to spoof an NTP server and provide the appliance with incorrect time settings. We recommend that you only synchronize with NTP servers on your internal network.
To manually configure the time settings

1. From the main navigation menu, click **General Settings**. The **General Settings** page appears.

2. Complete the information listed under **Date/Time**:

   - To change the time zone, select your current time zone from the **Time zone** box.
   - To set the current time, type the current date in **mm/dd/yyyy** format in the **Date** box, and type the current time in **hh:mm** format in the **Time** box using 24-hour notation. Click **Set now** to apply your changes immediately.

3. Click **Save**.

**Notes**
- If you are using an Aventail-provided evaluation license, do not move your system time backward from the current time; doing so will disable all services on your appliance for licensing reasons.

**System Logging and Monitoring**

The Aventail appliance logs a variety of useful information, including user access and system events. This section provides information about how to configure and view logs, discusses the various log file formats, and describes how to send messages to an external syslog server. It also describes the system status information displayed by AMC.

**Overview: System Logging and Monitoring**

The appliance logs data for the services on the appliance. All system logs are collected and stored in the syslog format. Log messages are handled using syslog-ng (or syslog "next generation"), an updated version of the standard syslog format. Syslog-ng provides enhanced log filtering options (using regular expressions) and its ability to forward logs over TCP and keep track of forwarding hops makes it ideal for firewalled environments.

The appliance is initially configured to store log files locally. If you configure the appliance to send log files to a central syslog server, you can monitor system-level events in near real time, and receive notifications about significant events. If a central syslog server is not available, you can manually review log files from the command-line interface on the appliance itself (using standard UNIX commands such as `tail`, `cat`, and `more`).

**Log File Formats**

The appliance generates several types of log files:
- **Message log** The message log displays server processing and diagnostic information about both the Web and client/server services. It also provides detailed messages about all access control decisions: each time a user request matches a policy rule, a log file entry is recorded explaining the action taken.
  
  You can access this log from AMC by choosing **Web and client/server message log** from the **View Logs** page. The file name is `/var/log/aventail/access_servers.log`

- **Access logs** The appliance generates two access logs, one for the Web service and one for the client/server service. These two logs provide detailed information about connection activity, including a list of users accessing your network and the amount of data transferred.
You can access this log from AMC by choosing **Client/server access log** or **Web access log** from the **View Logs** page. The file name is either /var/log/aeventail/extranet_access.log or /var/log/aeventail/extraweb_access.log

- **ASAP WorkPlace log** The appliance generates a single log file for ASAP WorkPlace, documenting error conditions and informational messages.

  You can access this log from AMC by choosing **ASAP WorkPlace access log** from the **View Logs** page. The file name is /var/log/aeventail/workplace.log

The following section outlines the file formats used for the various log files.

**Message Log**

The message log displays server processing and diagnostic information about both the Web and client/server services. It also provides detailed messages about all access control decisions: each time a user request matches a policy rule, a log file entry is recorded explaining the action taken.

The message log is generated in the syslog format (RFC 3164) and contains message logs for the Web access service, the client/server access service, and the policy server (an internal service that controls policy for the other services).

The following is a portion of the message log:


<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying data generated by syslog</td>
<td>This data, which is generated by syslog, is stamped as it is sent from the log server to syslog. It includes the date and time (Nov 10 12:22:01), the host that sent it to syslog (appliance), and the process that sent it to syslog (logserver).</td>
<td>Nov 10 12:22:01 appliance logserver:</td>
</tr>
<tr>
<td>Precise time stamp</td>
<td>This time stamp indicates when the message was generated by the service (Web, client/server, or policy). It’s recommended that you rely on this time stamp instead of the one generated by syslog.</td>
<td>[10/Nov/2003:12:22:01.132120 -0800]</td>
</tr>
</tbody>
</table>
Chapter 8 - System Administration

Auditing Access Policy Decisions

One of the main uses for the message log is to audit access policy decisions. Each time a user request matches a policy rule (including Web, client/server, and file system), the appliance will write an entry to the message text field (the last field in the message log) explaining the action taken.

A sample message for an access policy decision looks like this:

```
f0005393 Info    CS ACL  Matched  C/S Rule #10 'Allow access to ALL!', User
'tester@(business partner)' connecting from '192.168.2.100:1234': Attempting
to access 'w5.example.com:80'
```

For each connection request that matches a rule, a log message is generated at the \textit{Info} level. Requests that don't match a rule are logged at the \textit{Verbose} level (except in cases where no rule match is found at all; these are logged at the \textit{Info} level). To summarize, a connection request will generate one \textit{Info} message (for a rule match), and one or more \textit{Verbose} messages (for non-matches).

For policy decisions, the message text field in the log messages will include the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying data generated by the service</td>
<td>This data identifies the origin of the message. The components of this portion of the message are as follows:</td>
<td>016527 en 00000001 Verbose System</td>
</tr>
<tr>
<td></td>
<td>• The first number (016527) is the process ID (PID), which identifies the server process that generated the message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The code following the PID (en in the example) identifies the server. The codes are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ps (policy service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ew (Web access service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• en (client/server service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pt (client/server service ping/traceroute tools)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The next number (00000001 in the example) is the session ID. Each user session is assigned a unique number that is then used in messages from all four services (Web, client/server, policy, WorkPlace). It is therefore easy to search for all messages related to a single user session. If a message is not tied to a particular user session, it is assigned a number lower than 00000010. The first digit of this ID indicates which service originally generated the session, as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 (policy service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 (Web access service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 (client/server service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3 (WorkPlace service)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The text following the session ID indicates the level of the message (Verbose in the example).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The next text (System in the example) indicates the message type.</td>
<td></td>
</tr>
<tr>
<td>Message text</td>
<td>The text following all the identifying information is the actual message itself.</td>
<td>Acceptor: Socks Server is now Listening on 192.168.1.200:1081, fd=14.</td>
</tr>
</tbody>
</table>

See “Auditing Access Policy Decisions” on page 126 for an explanation of the message text for access policy decisions.
If no rule matched, an **Info** level message will be generated indicating that no matching rule was found.

**Examples**

Here are a few examples of log messages auditing access control.

**Example 1—Verbose Level**


**Example 2—Success at Info Level**

**Example 3—Failure at Info Level**


**Viewing Client Certificate Errors in the Log**

If the appliance is unable to verify a certificate chain, a message like this appears in the Web and client/server message log file:

ps 10000006 Info Module CERT: Certificate validation status 0, error is 10: error:0000000A:lib(0):func(0):DSA lib

This message includes an error code (in this case "10") reporting why the certificate check failed. These error codes include:

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Unable to get issuer certificate</td>
<td>The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found</td>
</tr>
<tr>
<td>7 Certificate signature failure</td>
<td>The signature of the certificate is invalid.</td>
</tr>
<tr>
<td>9 Certificate is not yet valid</td>
<td>The certificate is not yet valid.</td>
</tr>
<tr>
<td>10 Certificate has expired</td>
<td>The certificate has expired.</td>
</tr>
<tr>
<td>18 Self signed certificate</td>
<td>The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.</td>
</tr>
<tr>
<td>19 Self signed certificate in certificate chain</td>
<td>The certificate chain could be built up using the untrusted certificates but the root could not be found locally.</td>
</tr>
<tr>
<td>20 Unable to get local issuer certificate</td>
<td>The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.</td>
</tr>
<tr>
<td>21 Unable to verify the first certificate</td>
<td>No signatures could be verified because the chain contains only one certificate and it is not self-signed.</td>
</tr>
<tr>
<td>22 Certificate chain too long</td>
<td>The certificate chain length is greater than the supplied maximum depth.</td>
</tr>
<tr>
<td>23 Certificate revoked</td>
<td>The certificate has been revoked.</td>
</tr>
<tr>
<td>24 Invalid CA certificate</td>
<td>A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.</td>
</tr>
</tbody>
</table>
Client/Server Access Log

The client/server access log provides detailed information about connection activity, including a list of users accessing your network and the amount of data transferred. You can access this log from AMC by choosing **Client/server access log** from the **View Logs** page, or by opening `/var/log/aventail/extranet_access.log`.

The messages are stored in Aventail SOCKSSLF format. The following example illustrates a portion of a client/server access service log file:

```
   connect 192.168.136.254:22 0 21722 60631 263
```

The log entries contain the following fields (separated by spaces):

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-IP</td>
<td>IP address and port number of the computer</td>
<td>12.230.158.210:1110</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method used (<strong>ssl:LDAP</strong>, <strong>ssl:Radius</strong>, or <strong>none</strong>).</td>
<td>ssl:LDAP</td>
</tr>
<tr>
<td>&quot;Username&quot;</td>
<td>User accessing the resource. If multiple realms are defined on the appliance, this field will take the form of &quot;Username@realm&quot;.</td>
<td>&quot;fred figment&quot;</td>
</tr>
<tr>
<td>&quot;Date/Time&quot;</td>
<td>Date (in date/month/year format) and time (hours, minutes, seconds, and milliseconds in 24-hour-clock format) of the connection.</td>
<td>&quot;13/Sep/2002:19:18:28 -0700&quot;</td>
</tr>
<tr>
<td>SOCKS version</td>
<td>Version of the SOCKS protocol in use.</td>
<td>v5</td>
</tr>
<tr>
<td>SOCKS command</td>
<td>SOCKS command (either <strong>bind</strong>, <strong>connect</strong>, <strong>udp</strong>, <strong>traceroute</strong>, <strong>ping</strong>, or <strong>none</strong>).</td>
<td>connect</td>
</tr>
<tr>
<td>Destination-IP</td>
<td>IP address (and port number) of the resource being accessed.</td>
<td>192.168.136.254:22</td>
</tr>
<tr>
<td>Connection status</td>
<td>Status of the connection, where:</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>• 0 is success.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Values less than 256 indicate general failure codes sent to the client.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Values greater than 256 are internal debugging codes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See &quot;Auditing Connection Status Messages&quot; on page 130 for an explanation of the various status codes.</td>
<td></td>
</tr>
<tr>
<td>Bytes-received</td>
<td>Number of bytes received.</td>
<td>21722</td>
</tr>
<tr>
<td>Bytes-sent</td>
<td>Number of bytes sent.</td>
<td>60631</td>
</tr>
<tr>
<td>Connection duration</td>
<td>Connection duration (in seconds).</td>
<td>263</td>
</tr>
</tbody>
</table>
Auditing Connection Status Messages

The connection status code (which appears as the fourth-to-last field in the client/server access log; see “Client/Server Access Log” on page 129 for details) is often useful in debugging client/server connection problems. The following table describes each code:

<table>
<thead>
<tr>
<th>Connection status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Successful connection attempt</td>
</tr>
<tr>
<td>Less than 256</td>
<td>Values less than 256 indicate general failure codes sent to the client:</td>
</tr>
<tr>
<td></td>
<td>• 1 = general SOCKS server failure</td>
</tr>
<tr>
<td></td>
<td>• 2 = connection not allowed by ruleset</td>
</tr>
<tr>
<td></td>
<td>• 3 = network unreachable</td>
</tr>
<tr>
<td></td>
<td>• 4 = host unreachable</td>
</tr>
<tr>
<td></td>
<td>• 5 = connection refused</td>
</tr>
<tr>
<td></td>
<td>• 6 = TTL expired</td>
</tr>
<tr>
<td></td>
<td>• 7 = command not supported</td>
</tr>
<tr>
<td></td>
<td>• 8 = address type not supported</td>
</tr>
<tr>
<td></td>
<td>• 9 = invalid address</td>
</tr>
<tr>
<td></td>
<td>• 10 = address failed to resolve</td>
</tr>
<tr>
<td>Greater than 256</td>
<td>Values greater than 256 are internal debugging codes:</td>
</tr>
<tr>
<td></td>
<td>• 257 = no authentication method</td>
</tr>
<tr>
<td></td>
<td>• 258 = authentication failed (e.g., the end-user entered an invalid username/password)</td>
</tr>
<tr>
<td></td>
<td>• 259 = authentication I/O fail</td>
</tr>
<tr>
<td></td>
<td>• 260 = authentication quiet fail</td>
</tr>
<tr>
<td></td>
<td>• 261 = lost client connection</td>
</tr>
<tr>
<td></td>
<td>• 262 = cannot load module</td>
</tr>
<tr>
<td></td>
<td>• 263 = not authorized (e.g., access denied due to policy)</td>
</tr>
<tr>
<td></td>
<td>• 264 = encrypt failure</td>
</tr>
<tr>
<td></td>
<td>• 265 = unknown failure</td>
</tr>
</tbody>
</table>

Examples

If an end-user enters an invalid username/password, error number 258 would appear in the log:

```
192.168.2.69:3127 ssl "testing" "26/Feb/2004:21:31:51.947 +0000" v5 none -:- 258 385 0 14
```

If the RADIUS secret was incorrectly configured on the appliance, a user connection request would generate error number 259 in the log:

```
192.168.2.69:3127 ssl "testing" "26/Feb/2004:21:31:51.947 +0000" v5 none -:- 259 385 0 1
```

Web Access Log

The Web access log provides detailed information about connection activity, including a list of users accessing your network and the amount of data transferred. You can access this log from AMC by choosing Web access log from the View Logs page or by opening `/var/log/aventail/extraweb_access.log`.

The messages are stored in the World Wide Web Consortium (W3C) Common Log Format (CLF). See [http://httpd.apache.org/docs/logs.html](http://httpd.apache.org/docs/logs.html) for more information on CLF logs. This example shows a sample log message:
The log entries contain the following fields (separated by spaces):

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-IP</td>
<td>IP address of the computer accessing the Web access service (note that this field may contain a translated address if NAT is in use).</td>
<td>10.0.0.5</td>
</tr>
<tr>
<td>Identity</td>
<td>This field is not used by the Web access service and will always contain a hyphen.</td>
<td>-</td>
</tr>
<tr>
<td>Username</td>
<td>Username with which the user has authenticated to the Web access service.</td>
<td>jsmith</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time at which the request was finished processing (not the time at which the request was made).</td>
<td>[16/Apr/2003:21:36:38 +0000]</td>
</tr>
<tr>
<td>&quot;Request&quot;</td>
<td>First line of the HTTP request, containing the HTTP command (such as GET or POST), the requested resource, and the HTTP version number.</td>
<td>&quot;GET /alias2/bar.jpg HTTP/1.1&quot;</td>
</tr>
<tr>
<td>HTTP-Return-Code</td>
<td>Return code that the server responded with:</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>• 2xx codes indicate a successful request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3xx codes indicate some form of redirection or cached response.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4xx codes indicate an error (such as a resource that is not found or an unauthorized request).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5xx codes indicate a server error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information on these codes, see <a href="http://www.ietf.org/rfc/rfc2616.txt">http://www.ietf.org/rfc/rfc2616.txt</a></td>
<td></td>
</tr>
<tr>
<td>Bytes-Sent</td>
<td>Number of bytes sent in the body of the response (this does not include the size of the HTTP headers).</td>
<td>140</td>
</tr>
</tbody>
</table>

**Examples**

- If an authentication attempt fails—for example, because the user enters an invalid username or password—a single message will appear in the log with a return code of 200 (short for “OK,” indicating the client request was understood). Notice that the source IP address in the message is the only way for you to identify who made the request:
For a successful authentication, a similar message appears, but with a return code of 302 (short for "Found"). It is immediately followed with another message that contains the end-user's authentication credentials and a return code of 200:


192.168.2.69 - (jsmith)@ (AD) [26/Feb/2004:21:44:25 +0000] "GET /workplace/access/home HTTP/1.1" 200 15424

- If an end-user successfully authenticates, but is denied access to a Web resource by an access rule, a message containing a return code of 403 (short for "Forbidden") is logged:

192.168.2.69 - (jsmith)@ (AD) [26/Feb/2004:21:52:25 +0000] "GET /dukes HTTP/1.1" 403 3358

- If an end-user successfully authenticates and is permitted to access a URL, a message appears that is identical to that used for a failed authentication (again, notice the return code of 200), except that this one includes the user's credentials:

192.168.2.69 - (jdoe)@ (AD) [26/Feb/2004:21:51:03 +0000] "GET /dukes HTTP/1.1" 200 262

Viewing Logs

You can use AMC to view access log and message log data for the Aventail services.

- **To view logs**
  1. From the main navigation menu, click **Logging**. The **View Logs** page appears.
  2. Use the **View messages from** box to select the Aventail service and log file you want to view. You can view the following log files:
     - Log file for the ASAP WorkPlace service
     - The access log for the client/server service (called Anywhere VPN in the log files)
     - The message log, which contains information for both services (Web service and client/server service)
     - The access log for the Web service (called ExtraWeb in the log files)
  3. Use the **Show last** box to select the number of log messages you want to display. You can choose **50**, **100**, or **250**.
4. Click the **Refresh** button to update the page to show the most recent log messages.

![View Logs]

**Configuring Log Settings**

If you are debugging the system, you can set the message log level for the Aventail services in AMC. Additionally, you can configure the appliance to send log files to an external syslog server.

**Setting Log Levels**

You can use AMC to specify how much detail is written to the message logs for each service. Increasing the message log detail will require more disk space and will have a greater impact on system performance.

▲ **To set the logging level**

1. From the main navigation menu, click **Logging**. The **View Logs** page appears.
2. Click the **Configure Logging** tab.

![Configure Logging]

3. Use the **Web**, **Client/server**, and **ASAP WorkPlace** lists to select the appropriate level of message detail for each service:
   - The log levels for Web and client/server, in increasing order of detail, are: **Fatal**, **Error**, **Warning**, **Info**, **Verbose**, and **Debug**. For example, the **Info** log level will generate more log information than the **Error** level.
   - The log levels for ASAP WorkPlace are **Normal** and **Debug**. Typically, selecting **Normal** is recommended. **Debug** might be necessary if you are troubleshooting a problem.
4. Click **Save**.

**Notes**

- The highest detail log levels are valuable for debugging purposes, but can have a significant performance impact and should not be used in normal operation.

**Sending Log Files to a Syslog Server**

The Aventail appliance can send system logs to a syslog server. Regardless of whether you configure syslog, all system events are logged locally. In order to avoid flooding the network with log information, the appliance only forwards log messages for the three highest severity levels (warn, error, and fatal).

**To send log files to a syslog server**

1. From the main navigation menu, click **Logging**. The **View Logs** page appears.
2. Click the **Configure Logging** tab.
3. Under **Syslog configuration**, type the IP address and port numbers for one or more syslog servers. Note that the appliance defaults to port 514/tcp for the syslog-ng port, but you can use another port as needed to match your server configuration.

```
| Server #1: | Port: |
| Server #2: | Port: |
| Server #3: | Port: |
```

4. Click **Save**.

**Notes**

- Because syslog data is not encrypted, sending log messages to an external server is a potential security issue.

**Log File Locations**

The following table lists the location of the log files on the appliance.

<table>
<thead>
<tr>
<th>Aventail Server</th>
<th>Log File Format</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client/server access service</td>
<td>syslog</td>
<td>/var/log/aventail/access_servers.log</td>
</tr>
<tr>
<td></td>
<td>SOCK5SLF</td>
<td>/var/log/aventail/extranet_access.log</td>
</tr>
<tr>
<td>Web access service</td>
<td>syslog</td>
<td>/var/log/aventail/access_servers.log</td>
</tr>
<tr>
<td></td>
<td>W3C CLF</td>
<td>/var/log/aventail/extraweb_access.log</td>
</tr>
<tr>
<td>ASAP Management Console (AMC)</td>
<td>syslog</td>
<td>/var/log/aventail/management.log</td>
</tr>
<tr>
<td>ASAP WorkPlace</td>
<td>syslog</td>
<td>/var/log/aventail/workplace.log</td>
</tr>
</tbody>
</table>
To minimize storage requirements for log files, the appliance rotates the files. The process is described in the following table.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every 20 minutes</td>
<td>• Rotate any log files that are larger than 3MB.</td>
</tr>
<tr>
<td></td>
<td>• Force rotate the syslog log file.</td>
</tr>
<tr>
<td></td>
<td>• Check disk free space on <code>/var/log</code>. If less than 25% free space,</td>
</tr>
<tr>
<td></td>
<td>delete oldest log files until free space reaches 25%.</td>
</tr>
<tr>
<td>Every day</td>
<td>• Force rotate all log files.</td>
</tr>
<tr>
<td></td>
<td>• Delete any log files that are older than 7 days.</td>
</tr>
</tbody>
</table>

Log files more than one day old are stored in compressed format using the gzip compression utility. Compressing the logs conserves disk space and network bandwidth when sending files to a central syslog server, or when manually transferring the log files from the server for storage or review later.

The log file names contain a suffix that is numbered sequentially from 1 (one day old) through 7 (one week old). For example:

- `extraweb_access.log` is the current log file for Web access service.
- `extraweb_access.log.1` is the previous day’s log file (stored in uncompressed format).
- `extraweb_access.log.2.gz` through `extraweb_access.log.7.gz` are the logs from the previous six days (stored in compressed format).

**Monitoring the Appliance**

AMC displays a variety of information that is helpful in monitoring basic system settings, disk and memory usage, current connections, and network bandwidth utilization.

To monitor the appliance

1. From the main navigation menu, click **System Status**. The System Status page appears, displaying information about the appliance’s current status.

2. To update the page, click **Refresh**.
Notes
• This page displays the version number for the ASAP Platform, which is useful for planning system updates or requesting technical support.

Monitoring Active Users
You can view the total number of active user sessions at any given time, and you can temporarily terminate all VPN connections for any selected users. This section describes how to view active user sessions, search for active user sessions, and temporarily end active user sessions.

Viewing Active Users
You can view the number of currently active user sessions, and you can view a list of all active user sessions sorted by user name, realm name, or session start time.

To view all active user sessions
1. From the main navigation menu, click **Active Users**. The **Active Users** page appears.

2. Review the active user session data:
   • The **Current active users** field displays the total number of active user sessions.
   • The **Username** column displays the name of each individual user with an active session.
   • The **Realm** column displays the name of the realm to which the user belongs.
   • The **Session start time** column displays the time at which the session started.

3. By default, the active user session list is sorted by user name. To sort the list by a different method, click **Username**, **Realm**, or **Session start time** at the top of each column.

Searching for Active Users
You can search the list of current user sessions by user name.

To search for an active user session
1. From the main navigation menu, click **Active Users**. The **Active Users** page appears.
2. In the **Search for** box, type all or part of a user name. You can use the wildcard character (*) anywhere in the search string. For example, to find user names beginning with the letter “j,” you would type j*. Or, to find a users named “Mary” or “Marty” (but not “Max”), you could type M*y.
3. In the Show box, type the maximum number of results you want returned. The default is 200 users. (This field can be useful if, for example, you have exceeded your concurrent user count and want to terminate the 10 oldest connections. In this example, you would first sort the user session list by Session start time. You would then type 10 in the Show box and then, after the search results are returned, you would select the Select all check box and click End session.)

4. Click Search.

   AMC refreshes the active user session list and displays only any users that match your search criteria.

**Ending Active User Sessions**

You can immediately terminate a user’s session, even if the user has multiple active connections on different services or nodes. Ending an active user session only temporarily disables the user’s network access for 10 minutes; the user can still log in to the VPN again after that period if your access policy allows it. To permanently prevent a user from logging in to your VPN, you must modify the applicable access control rules, modify or delete the applicable user and group definitions, or delete the user from your user directory.

- **To temporarily end an active user session**
  1. From the main navigation menu, click Active Users. The Active Users page appears.
  2. In the list of active user sessions, locate the user or users whose access you want to temporarily disable. Alternatively, you can search for a specific user.
  3. Select the check box next to any users whose access you want to disable, and then click End session. You can select all users in the list by selecting the Select all checkbox at the top of the list; you could use this method to end all active user sessions, which is similar to stopping the appliance services.

**SNMP Configuration**

If you have a Simple Network Management Tool (SNMP) tool such as Hewlett-Packard OpenView or IBM Tivoli, you can use it to monitor the appliance as an SNMP agent. The appliance supports SNMP versions 1, 2c, and 3, and provides a variety of management data in Management Information Base (MIB) II format.

**Configuring SNMP**

This section describes how to configure SNMP using AMC.

- **To configure SNMP**
  1. From the main navigation menu, click Services. The SNMP Settings page appears.
2. Under **Network Services**, click **SNMP Configuration**.

   
   ![Configure SNMP](image)

   - Enable SNMP by selecting the **Enable SNMP** check box. (Note that if you leave this page to configure SNMP hosts before clicking **OK**, the status of this setting will not be saved.)

   - Select the network interface you want SNMP to use by selecting the appropriate option (**Internal**, **External**, or **Both**) from the **Interface selection** list.

   - Use the **Agent properties** area to identify the appliance:
     - Type the string your network management tool uses to query the Aventail appliance in the **Community string** box. This field is required, and set to **public** by default. It is a good security practice to change your community string to a secure passphrase because “public” is not secure.
     - Describe the appliance agent in the **System location** and **System contact** boxes. For example, you might specify the physical location of the appliance (for example, **Floor 2 – server lab**) and the system administrator contact information (such as **Jim Jamerson, 206-555-1212**).

   - Define the management systems from which the appliance will allow SNMP requests:

     ![SNMP hosts](image)

     - In the **SNMP hosts** area, click **Add**. The **Add/Edit Allowed Hosts** page appears.
     - Type the **IP address** and a **Subnet mask** for the host.

   - Click **Save**.

   **Notes**

   - You must configure your SNMP manager with the Management Information Base (MIB) used by the appliance. The appliance supports version 4.2.3 of the University of California, Davis (UCD) MIB, and MIB II.

   You must also configure your SNMP manager with the community string required to query the appliance.
• Ensure that your internal firewalls are configured to allow port 161/udp traffic.

Downloading the Aventail MIB File

AMC allows you to download the Aventail MIB file, which adds Aventail VPN-specific data to already supported MIBs. See "Aventail MIB Data" on page 140 for details on the information provided by the Aventail MIB.

To download the Aventail MIB
1. From the main navigation menu, click Services. The Services page appears.
3. Click the Download Aventail MIB button. A file download message appears.
4. Click Save, then browse to the correct directory and save the aventailCustomMibs.tar file.

Retrieving Management Data Using SNMP

SNMP data is arranged in a standardized hierarchy made up of structured text files that describe valuable management data. These text files (called MIBs), contain descriptions of specific data variables, such as system information or status.

To retrieve information through SNMP, you query the system for an "object identifier," or OID. Each OID includes a text name, but is usually referenced using a number. For example, the OID for system uptime (sysUpTime) is 1.3.6.1.2.1.1.3.

If you don’t have an SNMP management package, you can retrieve SNMP data by connecting to the appliance, logging in as "root," and running the snmpwalk or snmpget command. For example, to retrieve information about disk space availability, you could type the following snmpwalk command to query OID 1.3.6.1.4.1.2021.9:

```
snmpwalk -v 1 localhost -c public 1.3.6.1.4.1.2021.9
```

To view a list containing all of the MIB variables, type:

```
snmpwalk -O n localhost -c public |more
```

This command returns a list like this:

```
.1.3.6.1.2.1.1.1.0 = Linux aventailvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50 PDT 2003 i686
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.2021.250.10
.1.3.6.1.2.1.1.3.0 = Timeticks: (1707979) 4:44:39.79
.1.3.6.1.2.1.1.4.0 = Root < root@localhost> (configure /etc/snmp/snmp.local.conf)
.1.3.6.1.2.1.1.5.0 = aventailvpn
.1.3.6.1.2.1.1.6.0 = Unknown (configure /etc/snmp/snmp.local.conf)
.1.3.6.1.2.1.1.8.0 = Timeticks: (7) 0:00:00.07
.1.3.6.1.2.1.1.9.1.2.1 = OID: .1.3.6.1.2.1.31 ...
```

To view a list containing all of the MIB names (which are helpful for use with the snmpget command) type:

```
snmpwalk -O S localhost -c public |more
```

This command returns a list like the following:

```
SNMPv2-MIB::sysDescr.0 = Linux aventailvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50 PDT 2003 i686
SNMPv2-MIB::sysObjectID.0 = OID : SNMPv2-SMI::enterprises.2021.250.10
SNMPv2-MIB::sysUpTime.0 = Timeticks: (1712451) 4:45:24.51
SNMPv2-MIB::sysContact.0 = Root (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysName.0 = aventailvpn
SNMPv2-MIB::sysLocation.0 = Unknown (configure /etc/snmp/snmp.local.conf)
```
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (7) 0:00:00.07
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB

Notes
• See the UNIX man pages for more information on `snmpget` and `snmpwalk` (for example, typing `man snmpwalk` would provide help for `snmpwalk`).
• For more information on the UCD MIB SNMP agent, see `http://www.ece.ucdavis.edu/ucd-snmp/`.
• For more information on MIB II (including an explanation of the MIB II variable names), see `http://www.ietf.org/rfc/rfc1213.txt`.

Aventail MIB Data
The Aventail MIB comprises four modules whose object identifiers (OIDs) provide the following information about the Aventail VPN:
• System information
• System health
• Service health
• Service history

System Information Module
The OIDs in the System Information module provide basic information about the appliance.

<table>
<thead>
<tr>
<th>Item</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAP version</td>
<td>1.3.6.1.4.1.4331.1.1.0</td>
<td>The version of ASAP running on this node in major.minor.micro-patch-build format. For example: 8.0.0-64.</td>
</tr>
<tr>
<td>Hardware model</td>
<td>1.3.6.1.4.1.4331.1.2.0</td>
<td>The model number of the appliance, either EX-750 or EX-1500.</td>
</tr>
</tbody>
</table>

System Health Module
The OIDs in the System Health module provide information about the operational status of the appliance.

<table>
<thead>
<tr>
<th>Item</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently logged in</td>
<td>1.3.6.1.4.1.4331.2.1.1.0</td>
<td>The number of currently authenticated users.</td>
</tr>
<tr>
<td>Peak logged in</td>
<td>1.3.6.1.4.1.4331.2.1.2.0</td>
<td>The maximum number of concurrent users the appliance has had since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>Maximum licensed users</td>
<td>1.3.6.1.4.1.4331.2.1.3.0</td>
<td>The maximum number of concurrent users the appliance is licensed for.</td>
</tr>
<tr>
<td>Current connections</td>
<td>1.3.6.1.4.1.4331.2.2.1.0</td>
<td>The number concurrent connections being serviced by the Aventail client/server access service and the Aventail Web access service.</td>
</tr>
<tr>
<td>Peak connections</td>
<td>1.3.6.1.4.1.4331.2.2.2.0</td>
<td>The maximum number of concurrent connections the appliance has had since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>CPU utilization</td>
<td>1.3.6.1.4.1.4331.2.3.0</td>
<td>The current CPU percent utilization of the sum of CPUs on the single appliance node.</td>
</tr>
<tr>
<td>Item</td>
<td>OID</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RAM utilization</td>
<td>1.3.6.1.4.1.4331.2.4.1.0</td>
<td>The current average virtual memory (RAM) percent being utilized.</td>
</tr>
<tr>
<td>Swap utilization</td>
<td>1.3.6.1.4.1.4331.2.4.2.0</td>
<td>The current average virtual memory (swap) percent being utilized.</td>
</tr>
<tr>
<td>Internal interface current</td>
<td>1.3.6.1.4.1.4331.2.5.1.0</td>
<td>The current VPN throughput in megabits per second as measured on the internal interface of the node since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>peak throughput</td>
<td>1.3.6.1.4.1.4331.2.5.2.0</td>
<td>The peak VPN internal interface throughput in megabits per second since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>External interface current</td>
<td>1.3.6.1.4.1.4331.2.5.3.0</td>
<td>The current VPN throughput in megabits per second as measured on the external interface of the node since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>peak throughput</td>
<td>1.3.6.1.4.1.4331.2.5.4.0</td>
<td>The peak VPN external interface throughput in megabits per second since the last reset interval. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>Cluster interface current</td>
<td>1.3.6.1.4.1.4331.2.5.5.0</td>
<td>The current mean average VPN cluster interface throughput in megabits per second since the last reset. The reset interval is every 24 hours.</td>
</tr>
<tr>
<td>peak throughput</td>
<td>1.3.6.1.4.1.4331.2.5.6.0</td>
<td>The peak VPN cluster interface throughput in megabits per second since the last reset. The reset interval is 24 hours.</td>
</tr>
</tbody>
</table>
Service Health

The OIDs in the Service Health module provides information about the status of each service running on the appliance. For each service, the MIB provides a service ID, service description, and a service state of “up” or “down.”

<table>
<thead>
<tr>
<th>Item</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>1.3.6.1.4.1.4331.3.1.1.1.0</td>
<td>The service ID number for the Aventail ASAP Management Console is 0.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.1.1</td>
<td>The service ID number for the Aventail Client/server access service is 1.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.1.2</td>
<td>The service ID number for the Aventail Web access service is 2.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.1.3</td>
<td>The service ID number for Aventail ASAP WorkPlace is 3.</td>
</tr>
<tr>
<td>Service</td>
<td>1.3.6.1.4.1.4331.3.1.1.2.0</td>
<td>Aventail ASAP Management Console.</td>
</tr>
<tr>
<td>Description</td>
<td>1.3.6.1.4.1.4331.3.1.1.2.1</td>
<td>Aventail Client/server access service.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.2.2</td>
<td>Aventail Web access service.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.2.3</td>
<td>Aventail ASAP WorkPlace.</td>
</tr>
<tr>
<td>Service State</td>
<td>1.3.6.1.4.1.4331.3.1.1.3.0</td>
<td>The current state of AMC: 1=up and 0=down.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.3.1</td>
<td>The current state of the Aventail Client/server access service: 1=up and 0=down.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.3.2</td>
<td>The current state of the Aventail Web access service: 1=up and 0=down.</td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.4.1.4331.3.1.1.3.3</td>
<td>The current state of Aventail ASAP WorkPlace: 1=up and 0=down.</td>
</tr>
</tbody>
</table>

Security History Module

The OIDs in the Security History module provide information on login and access denials.

<table>
<thead>
<tr>
<th>Item</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of login denials</td>
<td>1.3.6.1.4.1.4331.4.1.0</td>
<td>The number of login denials since the last reset interval. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>Last user denied login</td>
<td>1.3.6.1.4.1.4331.4.2.1.0</td>
<td>The last user who was denied authentication, shown in the format user@realm.</td>
</tr>
<tr>
<td>Last denied login time</td>
<td>1.3.6.1.4.1.4331.4.2.2.0</td>
<td>The time and date when the last user was denied authentication.</td>
</tr>
<tr>
<td>Number of access denials</td>
<td>1.3.6.1.4.1.4331.4.3.0</td>
<td>The number of access denials since the last reset. The reset interval is 24 hours.</td>
</tr>
<tr>
<td>Last user denied access</td>
<td>1.3.6.1.4.1.4331.4.4.1.0</td>
<td>The last user who was denied access in the format user@realm.</td>
</tr>
<tr>
<td>Last resource access denied</td>
<td>1.3.6.1.4.1.4331.4.4.2.0</td>
<td>The URL of the last resource to which access was denied.</td>
</tr>
</tbody>
</table>
Other SNMP Data

Here is some other information about the appliance that you can retrieve using SNMP.

<table>
<thead>
<tr>
<th>Item</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last access denied</td>
<td>1.3.6.1.4.1.4331.4.4.3.0</td>
<td>The time and date when the last user was denied access.</td>
</tr>
</tbody>
</table>

**Backup, Restore, and System Update**

Included on the appliance are a number of command-line administrative tools for backing up configuration settings, patching and upgrading the software, and restoring previous versions or configurations. These tools can be divided into two groups: one for managing the backup and restoration of configuration files; and one for patching, upgrading, rolling back, and resetting the system software. The tools are listed in the following table, followed by detailed explanations of the use of these tools.

Use the following tools for managing the backup and restoration of configuration files. These files include all the information that you configure within AMC (for example, certificates, IP addresses, resource definitions, users and user groups, access control rules, and so forth).

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Backup Tool</td>
<td>Back up current configuration files.</td>
</tr>
<tr>
<td>Config Restore Tool</td>
<td>Restore a previous version of one or more configuration files.</td>
</tr>
<tr>
<td>Config Compare Tool</td>
<td>Compare backup configuration files to the current configuration files.</td>
</tr>
</tbody>
</table>
As an alternative to backing up and restoring configurations through the command-line tools, you can import and export configurations through AMC. For more information, see “Importing and Exporting Configurations Through AMC” on page 144.

Use the following tools for patching, upgrading, or rolling back the appliance system software.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Reset Tool</td>
<td>Reset configuration files to the factory defaults.</td>
</tr>
<tr>
<td>Update Tool</td>
<td>Install a patch to the existing version of the system software or upgrade to a new version.</td>
</tr>
<tr>
<td>Rollback Tool</td>
<td>Roll the system software back to its most recent state prior to a patch or upgrade.</td>
</tr>
<tr>
<td>Factory Reset Tool</td>
<td>Restore the appliance to its original state when received from the vendor. Use this tool as a last resort.</td>
</tr>
</tbody>
</table>

### Backing Up and Restoring Configuration Files

You can back up the appliance configuration files at any time. This is good practice when you make many system changes and want to preserve your previous configuration. From a backup file you can restore your entire appliance configuration to a previous state, or just restore a single file. This enables you to ensure that multiple appliances are using the same access policies. A file comparison tool lets you compare backup files to current configuration files.

The Aventail appliance offers two methods for backing up and restoring configurations: the Import/Export feature in AMC and the command-line utilities Backup Tool and Config Restore Tool. The AMC Import/Export feature is more convenient, but the command-line tools are more robust.

### Importing and Exporting Configurations Through AMC

Through AMC, you can export the current configuration from one appliance and then import all or part of the configuration to another appliance. This is similar to the functionality provided by the command-line Backup Tool and Config Restore Tool; however, while the AMC method is more convenient, it imports and exports only a subset of the data that can be backed up and restored using Backup Tool and Config Restore Tool. See “Backing up the Current Configuration Using Backup Tool” on page 147 and “Restoring Configuration Files Using Config Restore Tool” on page 148.

The following table lists the types of data that can be imported and exported using the AMC Import/Export feature versus the command-line Backup Tool and Config Restore Tool.

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>AMC</th>
<th>Command-line tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access policy</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Certificates</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>ASAP WorkPlace customizations</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Node-specific network settings</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>OnDemand configuration files</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Manual configuration-file edits</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Exporting the Current Configuration Through AMC

You can export the current configuration in a single Aventail Export Archive (.aea) file through the AMC interface. Only configuration data that was generated by AMC is exported; no manual configuration-file edits are exported. The following table lists the types of configuration data included in an exported file. Note that you cannot export a partial configuration; the exported file includes all of the configuration data listed below.

<table>
<thead>
<tr>
<th>Type of configuration data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access policy</td>
<td>Includes rules, resources, users and groups, ASAP WorkPlace shortcuts, and EPC signatures and zones.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Includes certificates, private keys, and certificate passwords.</td>
</tr>
<tr>
<td>ASAP WorkPlace customizations</td>
<td>Includes general appearance settings, custom content, and custom templates.</td>
</tr>
<tr>
<td>Node-specific and network-specific settings</td>
<td>Includes host names, IP addresses, default route information, DNS settings, and cluster settings.</td>
</tr>
</tbody>
</table>

Only the current saved configuration data is exported. Any pending changes that you have not applied are not exported. To export pending changes, you must first apply them and then export the configuration. This can be useful if you want to export a saved configuration before applying changes.

To export the current configuration through AMC

1. From the main navigation menu, click Maintenance. The Maintenance page appears.
2. In the **System configuration** area, under **Import or export**, click **Import/Export**. The **Import/Export** page appears.

   ![Import/Export page screenshot]

   **Export**

   Export your current configuration, including your access policy (rules, resources, and users), network settings, and SSL certificates. Note that this will export the active configuration, not including any pending changes.

   ![Export button]

   **Import**

   Import an entire configuration file, or just a subset of the file.

   **Import:**
   - Entire configuration
   - Partial configuration
     - Access policy
     - Certificates
     - ASAP Work-Place customizations

   ![Configuration file browse button]

3. Click **Export**. The **Export Configuration** page appears, and a **File Download** dialog box prompts you to open the **asap.aea** file or save it to your hard drive.

   ![Export Configuration page screenshot]

   **NOTE**

   You have pending configuration changes, and they will not be exported in the current file. To export pending changes, you will first apply them and then export.

   ![OK button]

4. Click **Save**, browse to the correct directory, and then save the **asap.aea** file.

5. Click **OK** on the **Export** page to return to the **Import/Export** page.

**Importing a Full or Partial Configuration Through AMC**

You can import a full or partial configuration through the AMC interface. This is similar to restoring a configuration through the command-line Config Restore Tool, but it does not import as thorough a set of configuration data as the Config Restore Tool can.

The imported file must be compatible with the current ASAP Platform version. Configurations that fall into the same major.minor versions are compatible with one another; for example, you could import an ASAP Platform v7.0.1 file into an existing ASAP Platform v7.0.2-1.3 configuration.
The following table describes the types of data that you can import into an existing AMC configuration.

<table>
<thead>
<tr>
<th>Type of configuration data</th>
<th>Description</th>
</tr>
</thead>
</table>
| Partial configuration      | • **Access policy**: Includes rules, resources, users and groups, ASAP WorkPlace shortcuts, and EPC signatures and zones.  
  • **Certificates**: Includes certificates, private keys, and passwords for LDAP servers secured using SSL, and root certificates for back-end Web servers secured using SSL.  
  • **ASAP WorkPlace customizations**: Includes general appearance settings, custom content, and custom templates. |
| Entire configuration       | • All partial configuration data (see above).  
  • **Certificates**: Includes certificates, private keys, and passwords for AMC and appliance certificates.  
  • **Node-specific and network-specific settings**: Includes host names, IP addresses, default route information, DNS settings, and cluster settings. |

To import a full or partial configuration through AMC

1. From the main navigation menu, click **Maintenance**. The **Maintenance** page appears.
2. In the **System configuration** area, under Import or export, click **Import/Export**. The **Import/Export** page appears.
3. In the **Import** area, specify which type of configuration data you want to import:
   - **Partial configuration**: Select any combination of the **Access policy**, **Certificates**, and **ASAP WorkPlace customizations** check boxes.
   - **Entire configuration**: Click to import all access policy, certificate, and ASAP WorkPlace customization data, and node-specific and network-specific settings.
4. In the **Configuration file** box, type the path of the appropriate asap.kea file, or click **Browse** to locate it.
5. Click **Import**.
6. To activate the imported configuration, you must apply changes. See “Applying Configuration Changes” on page 27.

**Notes**
- If an import fails, you can view details in the /var/log/aventail/management.log file.
- If you import a configuration while you have other configuration changes pending in AMC, those pending changes will be overwritten.

**Back up the Current Configuration Using Backup Tool**

The command-line Backup Tool included with the appliance will back up critical files on the appliance, including:
- Configuration files for the Aventail services
- Network settings
- Access control rules
- Log rotation settings
- Server certificates, keys, and passwords
Backup files are saved to a compressed tar file (by default, /var/backups/cfgback.tgz). It is good practice to back up your system on a regular basis, especially when making many system customizations.

To back up your configuration

1. Connect to the appliance using SSH or a serial connection, and log in as "root".
2. Type `config_backup`, specifying any optional parameters described as follows.

   ```
   config_backup [-t tarfile] [-q] [-d debuglevel] [-h]
   ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t tarfile</code></td>
<td>Backs up your configuration to the specified file. This parameter is required only if you want to back up to a different backup file than the default file: /var/backups/cfgback.tgz. Aventail suggests that you not set this parameter, because the restore program normally looks for the default file when restoring.</td>
</tr>
<tr>
<td><code>-q</code></td>
<td>Turns off the confirmation prompts (making the backup &quot;quiet&quot;). Normally, you are prompted when you might overwrite an existing backup file.</td>
</tr>
<tr>
<td><code>-d debuglevel</code></td>
<td>Specifies how much information to display about the backup operation. Set <code>debuglevel</code> to an integer between 0 and 10. Specify 0 for no information, 10 for complete information. The default is 1 (normal information).</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Shows help listing available parameters.</td>
</tr>
</tbody>
</table>

After you run Backup Tool, it saves your system configuration files to a backup file with the name and location specified above. If a backup file already exists at that location, you are prompted to confirm that you want to overwrite it (unless you use the `-q` parameter).

Notes

- Your configuration is automatically backed up if you install a new system update using Update Tool. This will not overwrite manual backups created by an administrator.
- For additional protection, use a program like scp to copy the `.tgz` file from the appliance to a separate location, such as a drive on your network or removable media.
- You can automate backups by adding the Backup Tool to a script. In this case, you can use the `-q` parameter to suppress confirmation prompts.

Restoring Configuration Files Using Config Restore Tool

You might want to restore from a backup file if you make changes that cause configuration problems. The command-line Config Restore Tool included with the appliance enables you to restore your entire configuration, or restore a single file.

Before you restore configuration files, you might want to compare files in the backup file to current files on your system; for more information, see “Comparing Files in a Backup File to Files on the System” on page 150.
CAUTION Never restore configuration files from a previous major, minor, or micro version of the system software. Because major/minor/micro version updates may contain changes to how configuration files are defined, old configuration files may be out of sync with the newer version and the appliance may not function properly. For example, if you were to upgrade your system to version 7.1.0 and later restore configuration files from version 7.0.0, you could experience problems due to system incompatibilities. Therefore, you should only use Config Restore Tool to restore configuration files created from the same major, minor, or micro version that is currently on your system. It is safe, however, to restore configuration files from a previous patched version, as long as the major, minor, and micro numbers are the same (for example, if your appliance is running version 7.1.0-1.6, you could restore configuration files from 7.1.0-1.2, but not from 7.0.0-1.8).

To restore configuration files from a backup file
1. Log in to the appliance as "root".
2. Type config_restore, specifying any optional parameters described below.

```
class restore [-f filename] [-t tarfile] [-q] [-d debuglevel] [-h]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f filename</code></td>
<td>Restores only the file you specify. Use this program if you want to restore a single file rather than all the configuration files in the backup file. See <code>/var/backups</code> for a list of backup files.</td>
</tr>
<tr>
<td><code>-t tarfile</code></td>
<td>Restores your configuration from the specified backup file. This parameter is required only if you need to restore from a different backup file than the default file: <code>/var/backups/cfgback.tgz</code></td>
</tr>
<tr>
<td><code>-q</code></td>
<td>Turns off the confirmation prompts (making the restore &quot;quiet&quot;). Normally, you are prompted to confirm that you want to restore files.</td>
</tr>
<tr>
<td><code>-d debuglevel</code></td>
<td>Specifies how much information to display about the restore operation. Set <code>debuglevel</code> to an integer between 0 and 10. Specify 0 for no information, 10 for complete information. The default is 1 (normal information).</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Shows help listing the available parameters.</td>
</tr>
</tbody>
</table>

You are prompted to confirm that you want to restore (unless you use the `-q` parameter) and Config Restore Tool copies all the configuration files (or only the file you specify, if you use the `-f` parameter) from the specified backup file, overwriting any of the same configuration files that exist.

Notes
- If the backup file is not found, Config Restore Tool reports an error; it requires a backup file to run. You can manually back up your system as described in "Backing up the Current Configuration Using Backup Tool" on page 147.

Restoring Factory Default Configuration Settings
You may occasionally want to restore the factory default configuration settings. For example, if you are moving the appliance into a different environment and have a large number of configuration changes to make, you may find it convenient to restore the appliance to its default settings and start over from scratch. To restore factory defaults, you run a command-line utility named Config Reset Tool.

CAUTION Running Config Reset Tool will delete all of your existing system configuration data.
- If you intend to restore a configuration from backup, make sure you have copied your backup files to another system before continuing.
To restore factory default configuration settings
1. Connect to the appliance (using either SSH or a serial connection) and log in as "root".
2. Type `config_reset` to run Config Reset Tool.
3. A prompt appears asking you to confirm whether you want to restore to default settings:
   
   ```
   Reset the appliance configuration to factory defaults? (n)
   ```
   
   Press `y` and then press ENTER to save your changes.
4. A prompt appears asking whether you want to reboot or shutdown (halt) the appliance. Press `r` to reboot, or `h` to halt.
   
   If you reboot the system, a login prompt appears after the system restarts.
5. Rerun Setup Tool to configure the network. See “Running Setup Tool” on page 18.

Comparing Files in a Backup File to Files on the System
You can compare the files in a backup file to the files currently on the system. This is helpful for finding out which files are different or getting details (for text files) on the differences between files.

To compare a backup file to your current configuration
1. Connect to the appliance (using either SSH or a serial connection) and log in as "root".
2. Type `config_compare`, specifying any optional parameters described below.

   ```
   config_compare [-s] [-f filename] [-t tarfile] [-d debuglevel] [-h]
   ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-s</code></td>
<td>Shows details of differences between files on your system and files in the backup file. This is comparable to using a &quot;diff&quot; command; for text files, you’ll see a line-by-line comparison of any differences between files. If you compare binary files, Compare Tool can indicate only that the files differ.</td>
</tr>
<tr>
<td><code>-f filename</code></td>
<td>Compares the file you specify to the same file in the backup file (no other files in the backup file are compared if you use this parameter). See <code>/var/backups</code> for a list of backup files. If you’re comparing two text files, use this parameter in conjunction with the <code>-s</code> parameter to view details of the differences between the files.</td>
</tr>
<tr>
<td><code>-t tarfile</code></td>
<td>Compares files to the backup file you specify. This parameter is required only if you want to compare your system files to a different backup file than the default file: <code>/var/backups/cfgback.tgz</code></td>
</tr>
<tr>
<td><code>-d debuglevel</code></td>
<td>Specifies how much information to display about the restore operation. Set <code>debuglevel</code> to an integer between 0 and 10. Specify 0 for no information, 10 for complete information. The default is 1 (normal information).</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Shows a help listing of the available parameters.</td>
</tr>
</tbody>
</table>

Config Compare Tool produces a report showing which files in the backup file are different from your current configuration files (unless you use the `-f` parameter to compare a single file to the backup). You are also alerted if a file no longer exists in the current configuration.

If you use the `-s` parameter, you’ll also see detailed differences between text files. You’re prompted to press ENTER after viewing the details of each difference.
Patching, Upgrading, Rolling Back, and Resetting the System

Aventail periodically offers system updates that add new functionality for the servers or address existing issues. A system update is a compressed .bin file and can be in the form of a patch or an upgrade. A patch addresses existing issues with a particular version and typically contains only the files that have changed from the original version. An upgrade contains a new version of the software and contains a full image instead of individual files.

You can install updates to your system using the command-line Update Tool, which should always be run from a serial console, or through the AMC interface. After installing an update, you can roll back to the previous version, if necessary, through AMC or using the command-line Rollback Tool.

To view the current version of the system, click **System Status** from the main navigation menu. See “Monitoring the Appliance” on page 135 for more information.

- Verifying the Downloaded Files
- Installing a System Update Through AMC
- Rolling Back to a Previous Version from the Command Line
- Rolling Back to a Previous Version Through AMC
- Performing a Factory Reset

### Downloading a System Update

You can find system updates (patches and upgrades) on the support page of the Aventail Web site. To access this area, you’ll need to create an account and receive a username and password; contact your channel partner or Aventail salesperson for information on getting a support account. After you have an account, you’ll be notified regularly by e-mail when new system updates are available.

**To download a system update**

1. Log in to the support page of the Aventail Web site at [http://aventailassurance.aventail.com](http://aventailassurance.aventail.com)
2. Go to the Downloads area, and view the section for your appliance.
3. Download any update files you want to install. You should also download the .md5 file associated with the update file.

   Each system update is a compressed .bin file and is accompanied by a release-notes file with the same name and a .txt extension. Consult the release notes to see what types of changes can be expected from each update. See the following section for information about the file-naming conventions for update files.

4. Transfer the update to the /upgrade/bricks directory on the appliance using scp.

### Naming Conventions for Update Files

**upgrade_<major>_<minor>_<micro>_<build>.bin**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>major</strong></td>
<td>The major release number for this update. If this is the only number that is present, it indicates that this release contains significant new features plus fixes. It also indicates that it contains a full image of the entire system.</td>
</tr>
<tr>
<td><strong>minor</strong></td>
<td>The minor release number for this update. If the version number contains only the major and minor numbers, it indicates that this release contains incremental features plus fixes. It also indicates that it contains a full image of the entire system.</td>
</tr>
<tr>
<td><strong>micro</strong></td>
<td>The micro release number for this update. If the version number contains only the major, minor, and micro numbers, it indicates that this release contains a small number of features plus fixes. It also indicates that it contains a full image of the entire system.</td>
</tr>
<tr>
<td><strong>build</strong></td>
<td>An internal build number used by Aventail. All releases contain a build number.</td>
</tr>
</tbody>
</table>
Examples

- `upgrade_8_0_0_23.bin` would upgrade your appliance to a 8.0 major release (build 23).
- `upgrade_8_1_0_13.bin` would upgrade your appliance to the 8.1 minor release (build 13).
- `upgrade_8_1_1_21.bin` would upgrade your appliance to the 8.1.1 micro release (build 21).
- `upgrade_8_1_5_19.bin` would patch the 8.1.5 minor release. This patch would contain only the packages that were modified since the last micro release, 8.1.5. You must have version 8.1.5 on your system before installing this patch.

Notes

- You don’t need to download the release notes; they are included in the update file and will be expanded to an /upgrade directory when you run the update.

Verifying the Downloaded Files

Before installing an update, it is important to verify that the files downloaded properly.

To verify the downloaded files

1. From a command line, type the following command, which returns a checksum for the downloaded file.
   
   ```
   md5sum <upgrade_filename>.bin
   ```

2. Extract the checksum from the associated .md5 file (which you downloaded from the Aventail Web site).
   
   ```
   cat <update-filename>.md5
   ```

3. Compare the two checksums. If they match, you can safely continue with your update. If they differ, try the download again and compare the resulting checksums. If they still don’t match, contact Aventail Technical Support.

Installing a System Update from the Command Line

After you’ve downloaded a system update and copied it to the appliance, you can install it using the command line. Use this procedure for the installation of version upgrades as well as patches.

For information on updating the software on a cluster, see “Upgrading a Cluster” on page 224.

To install a system update

1. Connect to the appliance using SSH (or use a serial connection) and log in as “root.”
2. Copy the upgrade file to the /upgrade/brick directory on the appliance.
3. Type `/upgrade/bricks/upgrade_<version>.bin`, specifying the appropriate upgrade version number.
4. Some scp programs do not maintain the original file permissions after a transfer. Make sure the update file is executable by typing `chmod +x upgrade_<version>.bin`.
5. Reboot the appliance.
Notes

- It is good practice to perform a backup before rebooting the appliance. For more information, see “Backing up the Current Configuration Using Backup Tool” on page 147.

Installing a System Update Through AMC

You can use the AMC update feature to install version upgrades as well as patches.

For information on updating the software on a cluster, see “Upgrading a Cluster” on page 224.

To install a system update through AMC

1. From the main navigation menu in AMC, click Maintenance. The Maintenance page appears.

2. In the System configuration area, click Update. The Update page appears.

3. If you have not already downloaded the upgrade or patch file, click the Aventail Assurance Web site link and download the appropriate update or patch file to your local file system.

4. Type the path of the update or patch file or click Browse to locate it.
5. Click **Install Update**. A file upload status indicator appears. If necessary, you can stop the upload process by clicking **Cancel**.
   After the file upload process is complete, the update is automatically installed on the appliance. Note that you cannot cancel the installation process.
   After the installation process is complete, the appliance automatically restarts.
6. After the appliance restarts, log in to AMC and verify the new ASAP Platform version number on the AMC home page.

**Rolling Back to a Previous Version from the Command Line**

You can use Rollback Tool to undo up to two system updates that have been installed on the system. If you experience problems after completing an update, you may want to use this tool to roll back to a known state. Each time you run Rollback Tool, it removes the most recent system update and restores the version that existed just prior to the update.

**CAUTION** If you have made any configuration changes since updating the system, running Rollback Tool will erase these changes.

- **To undo a system update**
  1. Connect to the appliance using SSH (or use a serial connection) and log in as “root.”
  2. Type `rollback_tool` to have Rollback Tool remove the most recent update.
  3. When the command prompt reappears, type `reboot` to restart the appliance.

**Rolling Back to a Previous Version Through AMC**

From AMC, you can undo the most recent update installed on the system. If you experience problems after completing an update, you may want to use this feature to roll back to a known state. Each time you roll back the software image, it removes the most recent system update and restores the version that existed just prior to the update.

**CAUTION** If you have made any configuration changes since updating the system, rolling back the software image will erase these changes.

- **To roll back to a previous version through AMC**
  1. From the main navigation menu in AMC, click **Maintenance**. The **Maintenance** page appears.
  2. In the **System configuration** area, click **Rollback**. The **Rollback** page appears.
  3. To roll back to the version displayed on the **Rollback** page, click **OK**.
     After the rollback process is complete, the appliance automatically restarts and applies the changes.
  4. After the appliance restarts, verify the new ASAP Platform version number on the AMC home page.

**Performing a Factory Reset**

A factory reset returns the appliance to the state it was in when you first received it. Running Factory Reset Tool erases all updates and configuration files that have been created since the appliance arrived. For example, if the original appliance contained version 7.0.0, running Factory Reset Tool returns it to version 7.0.0, erasing any updates, configuration files, log files, and so forth that have been created or installed on the appliance. There are a couple of scenarios in which this tool may be appropriate:

- You want to completely clean the machine and reuse it elsewhere.
- The appliance is in an unrecoverable state. In this case, you should contact Aventail Technical Support and confirm that there is no other solution to your problem. Factory Reset should be used only as a last resort to restore the appliance to a working condition.
To return the appliance to its original factory condition
1. On a serial console, log in to the appliance as “root”.
2. Type `factory_reset`. A message appears reminding you to back up your configuration files and then reboot to reset the appliance.
3. Type `reboot` to restart the appliance.

When the reset completes, a prompt similar to the following appears:

```
Debian GNU/Linux 3.0 SSL-VPN ttyS1
SSL-VPN login:
```

4. Log in as “root”, and Setup Tool runs automatically.

**CAUTION** Before running Factory Reset Tool, especially if you are running it to restore the appliance from an unrecoverable state to a known working state, it is best to contact Aventail Technical Support to confirm that this is the best approach to take.

Managing the Aventail Services

This section describes how to start, stop, and configure the Aventail Web access and client/server access services.

Stopping and Starting the Aventail Services

You may occasionally want to temporarily stop one of the Aventail services.

**CAUTION** Aventail recommends stopping the services only during scheduled maintenance periods or during off hours. Also, you should give your users advanced warning that the service will be going down.

To start or stop a service
1. From the main navigation menu, click Services. The Services page appears.

2. Under Access Services, click the appropriate button:
   - Click Stop to stop the service. All existing user connections will be terminated.
   - Click Start to start the service.

Configuring the Aventail Services

This section describes how to configure the Web access and client/server access services. For information on configuring Aventail ASAP WorkPlace, see “Configuring ASAP WorkPlace General Settings” on page 188.

Configuring the Maximum Length of User Sessions

AMC contains a global setting called **Maximum session length** that determines the length of time during which an SSL session can be resumed without requiring reauthentication.
To configure the maximum session length
1. From the main navigation menu, click General Settings. The General Settings page appears.
2. In the Maximum session length box, type the number of minutes that SSL session records should live in the cache. The default is 720 minutes (12 hours).
3. Click Save. Note that you must apply changes for this change to take effect.

Configuring the Web Access Service
This section describes how to configure the service that manages access to Web resources. The appliance supports two modes of Web access. Standard Web access provides improved application compatibility without the need for content translation. It is supported on the Windows XP and 2000 operating systems and requires Internet Explorer 5.5 or later. Translated Web access provides access to any URL and is supported on Windows, Linux, and Macintosh. For more information, see “Standard Web Access vs. Translated Web Access” on page 187.

To configure the Web access service
1. From the main navigation menu, click Services. The Services page appears.

3. The Standard mode — redirection list area provides links that allow you to view redirected Web resources. For Microsoft Internet Explorer users running Windows XP or 2000, standard mode automatically redirects Web connections through the appliance for any destination resources you've defined in AMC.
   • Click the Show network redirection list link to view the list of Web resources to which standard mode users are automatically redirected.
   • Click the realm configuration link to display the Configure Realm page, where you can enable the standard Web agent. User access agents, including the standard Web agent, are configured on a per-realm basis.

4. Complete the information listed under Downstream Web resources:
   • If you want the Web access service to check the validity of certificates presented by backend Web servers, select the Validate SSL server certificates check box. If enabled, the appliance will make sure the CN in the certificate matches the host name and that the certificate is valid. Aventail recommends enabling this feature if you are using downstream HTTPS.
• To view details about the root certificate for CAs that issued certificates to back-end Web servers, click the View CA certificate link.
• To import a certificate click the SSL Settings link.

5. Under Advanced, the Translated mode — redirection list area provides options for configuring translated Web Access:

By default, the appliance proxies content from the domains listed in the DNS search list on the Name Resolution page. If you want to override the resources that should be proxied, you can specify them here.

• To proxy resources from a specific domain through the appliance, select Domain from the Type list, type the domain name in the Value box, and then click Add.
• To proxy resources from a specific host through the appliance, select Host name from the Type list, type the name of the host in the Value box, and then click Add.
• To proxy resources from a specific network through the appliance, select Network address from the Type list, type the IP address of the network in the Value box, and then click Add.

Only resources in the domains, hosts, or network address you specify here would be proxied through the appliance. Referenced resources outside of these would not be proxied.

Notes:
If you want all domains in the DNS search list to be proxied along with one or more additional domains, you must type all those domains in this box, including the ones in the DNS search box. If you leave the Translated mode—redirection list blank, the appliance defaults to only proxying the domains in the DNS search list.

Configuring the Client/Server Access Service

This section describes how to configure the client/server access service options.

Note that the client/server access service uses an internal DNS cache to store successful and failed name lookups. Forward and reverse lookups are cached separately. Caching DNS lookups improves performance; this is especially true for failed lookups because processing a failed connection request takes longer than processing a successful request.

To configure the client/server access service

1. From the main navigation menu, click Services. The Services page appears.
2. Under Client/server click the Configure link. The Configure Client/Server Access Service page appears.
3. Complete the information listed under **Timeout values**:

<table>
<thead>
<tr>
<th>Timeout values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL timeout: *</td>
<td>360</td>
</tr>
<tr>
<td>SSL cache lifetime: +</td>
<td>720</td>
</tr>
<tr>
<td>Default connection timeout: *</td>
<td>60</td>
</tr>
<tr>
<td>Authentication timeout: +</td>
<td>60</td>
</tr>
<tr>
<td>SOCKS client timeout: *</td>
<td>0</td>
</tr>
<tr>
<td>Maximum limbo life: +</td>
<td>0</td>
</tr>
</tbody>
</table>

- In the **SSL timeout** box, type the number of seconds that an SSL handshake can last before timing out. The default is **300**.
- In the **SSL cache lifetime** box, type the number of minutes that SSL session records will live in the cache. The client/server access service will negotiate new SSL sessions when the **SSL cache lifetime** expires. Note that AMC also contains a global setting for SSL session length (see “Configuring the Maximum Length of User Sessions” on page 155). It is recommended that these settings have the same value. If they differ, the shorter value takes precedence. The default value for SSL cache lifetime is **720 minutes** (12 hours).
- In the **Default connection timeout** box, type the number of seconds of inactivity allowed before a user connection times out. If no data is transferred within the specified timeout period, the connection is terminated and the user must reauthenticate.
- In the **Authentication timeout** box, type the timeout value, in seconds, for authentication requests. If no data has been received after the specified period of time in the authentication phase, the request times out. Generally, you should set this and **SOCKS client timeout** to the same value.
- In the **SOCKS client timeout** box, type the timeout value, in seconds, for SOCKS protocol responses. If no data is received from the client during non-authentication connections after this number of seconds, the request times out. Generally, you should set this and **Authentication timeout** to the same value.
- In the **Maximum limbo life** box, type the maximum lifetime, in seconds, that connections can live after the server configuration is modified. If you apply configuration changes to the client/server access service, any existing connections will remain active until they are terminated by the user or until the "maximum limbo life" seconds elapse. A short maximum limbo life increases security at the cost of causing some users to lose their connections unexpectedly.

4. Complete the information listed under **DNS cache**:

<table>
<thead>
<tr>
<th>DNS cache</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward lookup: *</td>
<td>Failure:</td>
</tr>
<tr>
<td>Success:</td>
<td>Failure:</td>
</tr>
<tr>
<td>600 seconds</td>
<td>120</td>
</tr>
<tr>
<td>Reverse lookup: *</td>
<td></td>
</tr>
<tr>
<td>Success:</td>
<td>Failure:</td>
</tr>
<tr>
<td>600 seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

- Under **Forward lookup**, in the **Success** box, type the length of time, in seconds, that you want to cache successful forward DNS lookups. In the **Failure** box, type the length of time, in seconds, that you want to cache failed forward DNS lookups.
- Under **Reverse lookup**, in the **Success** box, type the length of time, in seconds, that you want to cache successful reverse DNS lookups. In the **Failure** box, type the length of time, in seconds, that you want to cache failed reverse DNS lookups.
5. Under **Miscellaneous**, in the **Save performance metrics every** box, type the number of connections that will occur between each save of performance metrics. Metrics are logged to syslog and rotated with the other log information.

```
<table>
<thead>
<tr>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save performance metrics every: 0</td>
</tr>
<tr>
<td>0 out of 100 connections</td>
</tr>
</tbody>
</table>
```

6. Click **Save**.

### SSL Encryption

Encryption is an integral element of user authentication and is the most effective way to ensure data security. The appliance encrypts all data using SSL; for the Web access service and the client/server access service, you must configure at least one cipher to be used with SSL to secure your network traffic. Each of these two services selects the "best" cipher from the available set, balancing security and performance trade-offs (security is weighted much more heavily than performance).

SSL provides some degree of protection from downgrade attacks, but in general you should configure your servers to permit only those ciphers that you consider strong enough for your needs. The cipher order, from most preferred to least preferred, is:

- 128-bit RC4, MD5
- 128-bit RC4, SHA-1
- Triple DES, SHA-1
- 56-bit RC4, MD5
- DES, SHA-1
- 40-bit RC4, MD5
- 40-bit DES, SHA-1 (available for the client/server access service only)

### Configuring SSL Encryption

The appliance uses SSL encryption and other cryptographic algorithms—or ciphers—to secure data transfer over a socket. When configuring the encryption settings for the appliance, you must enable at least one cipher to be used in conjunction with SSL to secure your network traffic. The default settings are typically sufficient for most deployments.
To configure SSL encryption settings

1. From the main navigation menu, click SSL Settings, and then click the SSL Encryption tab.

2. Select the ciphers that each access service (Web and client/server) on the appliance will accept for SSL connections. You must select at least one cipher for each access server.

3. Click Save.

Software Licenses

The Aventail appliance uses two different types of licenses:

- **Base appliance license:** This license is used to monitor and enforce concurrent user counts. If you exceed your concurrent active user limit, by default user access will be restricted until the active user count drops below the licensed user limit.

  Depending on your licensing arrangements, however, you may be allowed to exceed the limit by a certain number of user sessions (the grace count). In that case user access will still be allowed but the excess usage will be logged. However, if the active user count exceeds the grace count, user access will be restricted until the active user count drops to below the grace count.

  If user access is restricted, users attempting to log in to your VPN will see an error message indicating that the license count may have been exceeded and will be denied access to your network.

- **Component licenses:** If the license for an appliance component (such as Aventail OnDemand) has expired, users attempting to use that component will see an error message in ASAP WorkPlace.

The Aventail appliance ships with a default license that supports 1,000 concurrent users for three days; to continue using the appliance after this three-day period, you must upload a valid license file.

This section describes how to view license details and manage software licenses for appliance components.
Viewing License Details

In AMC, you can view the status of your base appliance license and the licenses for any other appliance components you may have purchased, such as Aventail OnDemand or Aventail Connect. This section describes how to view details about the status of your licenses.

To view license details

1. From the main navigation menu, click **General Settings**, and then click the **Licensing** tab. The Licensing page appears.

2. Review the information provided:
   - **Product name** displays the type of Aventail appliance to which the license applies.
   - **License holder** displays the name of the entity to whom the appliance is licensed.
   - **Maximum concurrent users** displays the maximum number of concurrent user sessions allowed by the base appliance license. A concurrent user is a single login from a single IP address. Users are no longer counted when they log off, or when their credentials expire.
   - **Component** and **License type** display details about any individual software component licenses. If the license is a temporary or evaluation license, the expiration date is displayed. If a license expiration date is approaching, or if a license has expired, a warning message is displayed in this area and in the AMC status area.

Managing Licenses

This section describes how to import a license file to the appliance, and how to remove an expired license from the appliance.

Some components—such as Aventail OnDemand, Aventail Connect, and Aventail Secure Desktop—require a separate purchase. After you purchase one of these components, you will receive a software license file. Before you can enable these components, you must upload a valid license file through AMC. For information about purchasing additional components, contact your Aventail channel partner.

You may also need to import a base appliance license file if, for example, you want to replace an evaluation license with a permanent license after deciding to purchase an appliance.

**CAUTION** It is recommended that you ensure that the appliance's date and time settings are configured correctly for your time zone before importing a license file. For information about configuring the system clock settings, see "Configuring the Time Settings" on page 123.

To import a license file

1. From the main navigation menu, click **General Settings**, and then click the **Licensing** tab. The Licensing page appears.
2. Click Import License. The Import License File page appears.

![Import License File](image)

3. In the License file box, type the path for the license file, or click Browse to locate it.

4. Click Save.

You can clear an expired component license from the appliance (for example, if you decide not to purchase a component for which you were issued an evaluation license). To renew an expired license, contact your Aventail channel partner to receive a new license file. Note that you cannot clear the base appliance license.

► To clear an expired component license

1. From the main navigation menu, click General Settings, and then click the Licensing tab. The Licensing page appears.

2. If a component license has expired, an “expired” message appears in the License type area and a Clear Expired License button appears. Click Clear Expired License to remove the expired license file from the appliance.
Chapter 9
End Point Control

The Aventail appliance includes support for several “end-point control” components designed to protect sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments.

Traditional VPN solutions typically provide access only from the relative safety of a corporate laptop. In that environment, the major security concern is unauthorized network access. Because an SSL VPN enables access from any Web-enabled system, it may bring additional risks from PCs in untrusted environments, such as a kiosk at an airport or hotel, or an employee-owned PC. End Point Control requires an additional process to evaluate the state of the end-user device.

Overview: End Point Control

Traditional VPN solutions typically provide access only from the relative safety of a corporate laptop. In that environment, the major security concern is unauthorized network access. Because an SSL VPN enables access from any Web-enabled system, it may bring additional risks from PCs in untrusted environments, such as a kiosk at an airport or hotel, or an employee-owned PC.

Aventail End Point Control reduces your exposure from untrusted environments in two ways:

- **Verifying the user’s environment is secure**
  Corporate IT departments configure PCs under their control with antivirus software, firewalls, and other safeguards designed to protect them from malicious software (“malware”). In contrast, unmanaged PCs can easily contain keystroke recorders, viruses, Trojan horses, and other hazards that can compromise your network.

  Aventail supports integration with third-party “client integrity” controls that automatically check for malware on the client system before allowing the user to authenticate.

  In addition, Aventail lets you define “zones of trust” that provide different levels of access depending on the level of trust at the user’s end point. Connection requests are compared against the “device profiles” you set up in AMC and then assigned to the appropriate zone.

- **Removing user data from a PC after a session**

  Web browsers make it easy to inadvertently leave sensitive data on an untrusted PC. For example, a user logged in from a public kiosk will leave a variety of data in the PC’s cache, including passwords, browser cookies, and bookmarked URLs. Users may also accidentally leave files or e-mail attachments on the hard disk.

  Aventail’s “data protection” agents automatically remove session data from the PC.
How the Appliance Uses Zones and Device Profiles for End Point Control

When a user connects to the appliance and logs in to a realm, the appliance interrogates the user's computer, then determines if its attributes match those defined in the zone's device profile. If the device matches the profile, the appliance classifies the computer into the zone. The following diagram illustrates the evaluation process performed by the appliance when a user logs in to a realm that references a zone and device profile.

If a realm references more than one zone, the appliance evaluates a connection request against the zones listed in sequential order in the realm until it finds a zone with a matching device profile. If no match is found in the first zone, the appliance proceeds to the next zone and checks the connection request for a match against its device profiles, and so on down the list of zones in the realm. If no match is found in any zones, the device is automatically assigned to the global default zone, which is described in "Using the Default Zone" on page 173.

Example

For example, you may want to provide members of the “Employees” realm with access to your company’s network resources, provided that they connect from laptop computers that are maintained by your IT department. You could create a zone named “IT Managed” that references a device profile named “IT Trusted Laptop.” In this example, the device profile would require the presence of several specific attributes on users' company laptops: an antivirus program, the file name and directory for an application unique to your company, the registry key for the company application, a personal firewall, and membership in the company domain. After this zone and device profile are configured in AMC, you would add the zone to the “Employees” realm.

When an employee logs in and selects the “Employees” realm, the appliance checks his or her computer for the required device attributes. If the employee’s laptop matches the device profile exactly, the appliance places it in the “IT Managed” zone. From there the realm provisions the user with the appropriate access agent for that realm, and the user is able to access the network resources.

For more examples of using zones and device profiles, see "End Point Control Scenarios" on page 165.
End Point Control Scenarios

This section describes some typical End Point Control scenarios that employ zones and device profiles to classify connection requests and deploy End Point Control tools to clients.

**Scenario 1: Employees Connecting from IT-Managed Laptops**

This scenario begins with an employee connecting to the appliance using an IT-managed laptop.

The sequence of events in this example is as follows:

1. The user connects to the appliance and logs in to the realm “Employees.”

2. Once the user is authenticated, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the “Employees” realm. Device profiles are evaluated by zone, starting with the first zone listed in the realm, which is the “Trusted – IT” zone.

3. The “Trusted – IT” zone references a device profile named “IT managed laptop.” The appliance determines that user’s device attributes match those configured in the “IT managed laptop” profile (a registry key entry, antivirus software, and an application).

4. Based on that match, the appliance classifies the device into the “Trusted – IT” zone and doesn’t evaluate the subsequent two zones listed in the realm.

5. The “Trusted – IT” zone is not configured to require a data protection tool on the client. At this point the “Employees” realm would provision the user with the access agent configured for that realm, and the user would be able to access the appropriate network resources.
Scenario 2: Employees Connecting from a Home PC

This scenario begins with an employee connecting to the appliance from a home PC.

The sequence of events in this example is as follows:

1. The user connects to the appliance and logs in to the realm "Employees."

2. Once the user is authenticated, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the "Employees" realm. Device profiles are evaluated by zone, starting with the first zone listed in the realm, which is the "Trusted – IT" zone. In this scenario, the appliance finds that the client doesn't match the profile in the first zone, so it continues to the second zone in the list: "Semi-Trusted – Home."

3. The "Semi-trusted – Home" zone references a device profile named "Employee home PC." The appliance determines that user's device attributes match those configured in the "Employee home PC" profile (antivirus software and a personal firewall).

4. Based on that match, the appliance classifies the device into the "Semi-trusted – Home" zone and doesn't evaluate the subsequent zone listed in the realm.

5. Because the "Semi-trusted – Home" zone is configured to require a data protection tool on the client, the appliance deploys Aventail Cache Control to the client. At this point the "Employees" realm would provision the user with the access agent configured for that realm, and the user would be able to access the appropriate network resources.
Scenario 3: Employees Connecting from a Public Kiosk

This scenario begins with an employee connecting to the appliance from a public kiosk.

The sequence of events in this example is as follows:

1. The user connects to the appliance and logs in to the realm “Employees.”

2. Once the user is authenticated, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the “Employees” realm. Device profiles are evaluated by zone, starting with the first zone listed in the realm, which is the “Trusted – IT” zone. In this scenario, the appliance finds that the client doesn’t match the profile in the first zone or in the second zone, so it continues to the final zone in the list, the “Default” zone.

3. The appliance determines that the attributes on the public kiosk client do not match any device profiles in the “Employees” realm.

4. The appliance classifies the public kiosk into the “Default” zone. A client that fails to match any other device profile in a realm is automatically assigned to the “Default” zone.

5. In this scenario the “Default” zone is configured to permit VPN access provided that Aventail Secure Desktop (ASD) can be deployed to the client. ASD is an optional data protection component—purchased separately—that provides enhanced data protection for Windows users. If the public kiosk is running either Windows XP or 2000 and a supported browser, then ASD is deployed, after which the “Employees” realm would provision the user with the access agent configured for that realm, and the user would be able to access the appropriate network resources. However, if the public kiosk’s operating system and browser are not compatible with ASD, the appliance will substitute Aventail Cache Control (ACC). If neither ASD or ACC can be loaded on the client, then the user’s connection request would be denied.

Managing EPC with Zones and Device Profiles

End Point Control provisions data protection components to users through the use of zones. Think of these as “zones of trust” that classify connection requests based on the attributes of the client device, such as the presence of a software application or a device profile. Device profiles, which define the attributes required to identify a client and assign it to a zone, can include any combination of:

- Antivirus software
- Personal firewall
- Applications
- Directory names
- File names
- Windows registry entries
- Windows domains

AMC includes one pre-defined zone called the default zone, which cannot be deleted. You can create as many additional zones as needed to accommodate a variety of access scenarios and levels of trust, such as separate zones for employees and for business partners or contractors. The default zone can serve as a global fail-safe to either allow or block VPN access in situations where connection requests don’t match the criteria for any other zones. See “Using the Default Zone” on page 173 for more information.

Realms are used to specify which zones are available to users after they authenticate. For information on linking zones to realms, see “Managing Realms” on page 108. In addition, zones can be tied to your access policy much the same as users, groups, and resources are.

### Enabling and Disabling End Point Control

End Point Control is disabled by default in AMC. AMC allows you to globally enable or disable EPC.

1. To enable End Point Control
   1. From the main navigation menu, click **End Point Control**. The **End Point Control** page appears.
   2. Select the Enable End Point Control check box.

   When End Point Control is disabled, the appliance stops performing the following EPC actions:
   - Evaluating the attributes of client devices.
   - Classifying connection requests into zones.
   - Enforcing zone restrictions in access control rules.

### Viewing Zones and Device Profiles

Zones and device profiles configured in AMC are displayed on the **Zones and Device Profiles** page.

1. To view configured zones and device profiles
   1. From the main navigation menu in AMC, click **End Point Control**.
   2. The **End Point Control** page provides a summary of the zones and device profiles that are configured in AMC, and a summary of the EPC agent status. You can click the name of a zone or device profile to view or edit its settings.
3. Click the **Zones and Device Profiles** tab. The **Zones and Device Profiles** page appears.

4. Review the data listed in the **End Point Control** zones table:
   - The check box column is used to select one or more zones. You’ll use this to delete zones, or copy them.
   - The **Name** column displays the name you assigned when creating a zone. You can edit a zone by clicking its name.
   - The **Description** column lists the descriptive text you typed when creating a zone.
   - The **Device Profile** column lists the names of one or more device profiles that you assigned to a zone.
   - The **Realms** column indicates whether the zone is currently referenced by any realms. A blue dot indicates a zone is being used by one or more realms. If a zone is not referenced by any realms, this field is blank.

5. Review the data listed in the **Device profiles** table:
   - The check box column is used to select one or more device profiles. You’ll use this to delete profiles.
   - The **Name** column displays the name you assigned when creating a device profile. You can edit a device profile by clicking its name.
   - The **Description** column lists the descriptive text you typed when creating a device profile.

**Defining a Zone**

The following procedure describes how to create a zone. Zones are supported for Windows 2000 or XP computers running Internet Explorer 5.5 or later. If you want to create a zone for Macintosh or Linux computers, see “Defining Zones for Macintosh or Linux Clients” on page 174.

**To define a zone**

1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
2. Click the **Zones and Device Profiles** tab.

3. In the **End Point Control Zones** area, click **New**. The **Zone Definition** page appears.

   ![Zone Definition](image)

   - **Name**: Type a meaningful name for the zone.
   - **Description**: Type a descriptive comment about the zone.
   - **Device profiles**: Select the check box for any **Device profiles** that you want to require in the zone. During the connection process, the appliance will require that all of the attributes defined in a profile are present on a device in order to assign it to this zone. You can also click **New** to create a device profile for the zone.

   ![Device profiles](image)

   In most cases a zone should include at least one device profile. For more information, see "Defining Device Profiles for a Zone" on page 171. If a zone references multiple device profiles, the appliance will accept any profile that matches the connection request and assign the device to the zone.

4. In the **Name** box, type a meaningful name for the zone.

5. In the **Description** box, type a descriptive comment about the zone.

6. Select the check box for any **Device profiles** that you want to require in the zone. During the connection process, the appliance will require that all of the attributes defined in a profile are present on a device in order to assign it to this zone. You can also click **New** to create a device profile for the zone.

   ![Device profiles](image)

   In most cases a zone should include at least one device profile. For more information, see "Defining Device Profiles for a Zone" on page 171. If a zone references multiple device profiles, the appliance will accept any profile that matches the connection request and assign the device to the zone.

7. If you want the zone to require the presence of Aventail Cache Control or Aventail Secure Desktop, select the appropriate option from the **Required data protection tool** list.

   ![Data protection](image)

   Aventail Secure Desktop is an optional component for supported Windows 2000 and XP platforms that is purchased separately. On unsupported platforms, Aventail Cache Control is used instead.

8. When you are finished creating the zone, click **Save** to return to the **Zones and Device Profiles** page.

**Notes**

- If you want to assign Aventail Connect users in to zone, you must take an extra step to configure the zone. See "Assigning Aventail Connect Users to a Zone" on page 172. Note that Aventail Cache Control and Aventail Secure Desktop are not applicable when using Aventail Connect.
Defining Device Profiles for a Zone

A device profile establishes a trust relationship with a client device by looking for one or more attributes such as an antivirus program, application, or registry key. Device profiles can be referenced by one or more zones.

To define a device profile for a zone
1. From the main navigation menu in AMC, click End Point Control. The End Point Control page appears.
2. Click the Zones and Device Profiles tab.
3. In the Device profiles area, click New. The New Device Profile Definition page appears.
4. In the Name box, type a meaningful name for the device profile.
5. In the Description box, type a descriptive comment about the device profile.
6. In the Add attribute area, select the Operating system for the device profile. If you select Microsoft Windows, complete the relevant attribute settings described in the next step.

If you select Macintosh or Linux, see “Defining a Profile for a Macintosh or Linux Client” on page 174.

7. Select the appropriate attributes for the device profile. After you specify the Type and Value for each attribute, click the Add to Current Attributes button. Notice that the device attribute you just added appears in the Current attributes table.
   • For Antivirus program, select either Norton Antivirus or McAfee. If you select both values, any one will be accepted if found on the client device.
     If your users run antivirus programs other than those listed here, you can add them to a device profile by using the Application attribute.
   • For Application, type the name of an application process that must be running on the client device. Application names are not case-sensitive. If you enter more than one application, then all the applications must be present on a device to match the profile.
   • For Directory name, type the name of a directory that must be present on the hard disk of the device. Directory names are not case-sensitive. If you enter more than one directory name, then all the directories must be present on a device to match the profile.
   • For File name, type the name of a file (including its extension) that must be present on the hard disk of the device. File names are not case-sensitive. If you enter more than one file name, then all the file names must be present on a device to match the profile.
   • For Personal firewall program, select Sygate, Microsoft, or Zone Labs. If you select more than one, any one will be accepted if found on the client device.
If your users run personal firewall programs other than those listed here, you can add them to a device profile by using the Application attribute.

- For **Windows registry entry**, type the **Key name**, **Value name**, and **Data**. Use the **Registry entry** list to specify whether the registry key value detected on the client device must be equal to, greater than, greater than or equal to, less than, or less than or equal to, the registry key value entered here. This is useful for keeping the device profile current with software that is automatically updated on client devices without having to manually change the profile each time the software gets updated. For example if a device profile uses a registry key entry for an antivirus program that’s auto-updated on the client, you would specify that registry key value detected on the client device must be greater than or equal to the value entered in this field.

  If you enter more than one Windows registry entry, then all the registry entries must be present on a device to match the profile.

- For **Windows domain**, type the domain name the client belongs to in NetBIOS syntax (for example, *mycompany*) without a DNS suffix. If you enter multiple Windows domains, any one will be accepted. Separate multiple entries with semicolons.

8. When you are finished creating the device profile, click **Save** to return to the **Zones and Device Profiles** page.

### Assigning Aventail Connect Users to a Zone

If you have users who access your network resources by running Aventail Connect, you must assign them all to the same zone so that they will be properly identified by the appliance. This step is required because Aventail Connect is routed to the appliance differently from other connection methods.

You don’t need to create a zone exclusively for Aventail Connect users; they can be placed in an existing zone. Since Aventail Connect will likely be installed only on trusted computers, you may want to assign them to your most trusted zone.

**To assign all Aventail Connect users to a zone**

1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
2. Click the **Zones and Device Profiles** tab.
3. Use the **Place Aventail Connect users in this zone** list to select the appropriate zone for your Aventail Connect users.

### Copying a Zone

To save steps, AMC allows you to copy the attributes of an existing zone and use them in a new zone. When you copy a zone, the device profiles from the original zone are included in the new zone.

**To copy a zone**

1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
2. Click the **Zones and Device Profiles** tab.
3. Select the check box to the left of the zone you want to copy, then click the **Copy** button. The **Zone Definition** page appears. Note that all the information from the original zone is displayed except for the **Name** box, which is blank.
4. In the **Name** box, type a meaningful name for the new zone.
5. Change any **Device profile** and **Data protection** settings as needed.
6. Click **Save** to create the new zone and return to the **Zones and Device Profiles** page.
Deleting a Zone or Device Profile

Perform the following steps to delete a zone.

► To delete a zone
1. From the main navigation menu in AMC, click End Point Control. The End Point Control page appears.
2. Click the Zones and Device Profiles tab.
3. In the End Point Control zones area, select the check box for the zone you want to delete, and then click the Delete button.

► To delete a device profile
1. From the main navigation menu in AMC, click End Point Control. The End Point Control page appears.
2. Click the Zones and Device Profiles tab.
3. In the Device profiles area, select the check box for device profile you want to delete, and then click the Delete button.

Notes
- You cannot delete a zone or a device profile if it is referenced by another object. For example, if you try to delete a zone that is referenced by a realm, AMC will display an error message. You must remove all references to the zone before you can delete it. For more information, see “Deleting Referenced Objects” on page 29.

Creating Zones for Special Situations

While the majority of connection requests—those involving Microsoft Windows and Internet Explorer—can be accommodated by standard zone configurations, you may need to address special situations involving other operating systems and browsers, or connection requests that don’t match any of the zones you’ve defined. You can use zones and device profiles to address the following situations:
- Clients that don’t match the criteria for any defined zones and device profiles.
- Clients running Macintosh operating systems.
- Clients running Linux operating systems.
- Clients running Windows and a non-Microsoft Web browser, or earlier versions of Windows.
- Special classes of users who require access regardless of the client device they’re running.

Be sure to configure the global default zone, which is implicitly present in every realm configured in AMC.

Using the Default Zone

AMC provides a global default zone that serves as a fail-safe to either allow or block VPN access for any connection requests that don’t match the other zones you set up. When the appliance receives a connection request that it can’t classify into a zone—meaning it can’t identify the client device’s operating system, browser, or other attributes—that device is automatically placed in the default zone. Your choice is whether to grant or deny VPN access to users whose devices are assigned to the default zone.

Unlike other zones, the default zone does not include device profiles, but it can be configured to require the presence of a data protection agent. The default zone is implicitly present in every realm configured in AMC.

► To configure the default zone
1. From the main navigation menu in AMC, click End Point Control. The End Point Control page appears.
2. In the **Zones and device profile summary** area, click the **Default Zone** link. The **Zone Definition** page appears with "Default Zone" automatically entered in the Name box.

![Zone Definition Table]

3. In the **Data protection** area, select whether client devices placed in the default zone are required to have **Aventail Secure Desktop** or **Aventail Cache Control** in order to connect.  

   Aventail Secure Desktop is an optional data protection component available on Windows only. On unsupported platforms, Aventail Cache Control is used instead.

4. In the **Access restrictions** area, select whether the appliance will **Allow VPN access** or **Block VPN access** for devices that are placed in the default zone. If **Block VPN access** is selected, users who are assigned to the default zone will be logged off of the appliance.

5. Click **Save** to enable the settings for the default zone.

**Examples**

If you want to provide a limited degree of access to users whose connection requests don’t meet your criteria for a trusted relationship, you can include the default zone in a restrictive access control rule. For example, you could let those users access their e-mail by including the default zone in a “permit” access control rule limited to Web browsers connecting to Outlook Web Access.

If you have a restrictive access policy that requires a high degree of trustworthiness and does not allow connection requests unless they are explicitly defined, then setting the default zone to **Block VPN access** would be the best strategy. Bear in mind that if your other zones and access control rules inadvertently omit legitimate users, the default zone will block them without exception.

**Defining Zones for Macintosh or Linux Clients**

If you have Macintosh or Linux users who need to access your network resources, we recommend that you create unique zones and device profiles for each platform. If the appliance detects the user is running Macintosh or Linux, the device will be assigned to the appropriate zone. If you do not create zones for Macintosh and Linux devices, they will be assigned to the default zone, which could result in blocked access depending on how the default zone is configured.

**To define a zone for Macintosh or Linux**

1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
2. Click the **Zones and Device Profiles** tab.
3. In the End Point Control Zones area, click New. The Zone Definition page appears.
4. In the Name box, type a meaningful name for the Macintosh or Linux zone.
5. In the Description box, type a descriptive comment about the zone.
7. In the Name box, type a meaningful name for the Macintosh or Linux device profile.

Specify the attributes used to establish a trust relationship with a client PC.

Name:  
Description:  

Add attribute

[ ] Microsoft Windows  [ ] Macintosh  [ ] Linux

8. In the Description box, type a descriptive comment about the device profile.
9. Select either Macintosh or Linux as the Operating system. No other attributes are available for these platforms.
10. Click Save to return to the Zone Definition page.
11. Select the check box for the Macintosh or Linux Device profiles that you want to include in the zone.
12. Select Aventail Cache Control from the Required data protection tool list if you want the device profile to require this data protection agent on the Macintosh or Linux client.
13. When you are finished creating the zone, click Save to return to the Zones and Device Profiles page.

Defining Zones for Non-Microsoft Browsers or Earlier Windows Versions

In situations where you have users whose Microsoft Windows PCs are running a browser other than Internet Explorer 5.5 or later—such as Mozilla or Netscape—you can assign them to a special zone. This prevents Windows users with non-Microsoft browsers from being placed in the default zone, which could result in blocked access. The only attribute used to distinguish this type of zone is the presence of the Windows system.

This configuration can also be used to define a zone for users who are running version of Microsoft Windows earlier than Windows XP or 2000.

To define a zone for clients with non-Microsoft browsers

1. From the main navigation menu in AMC, click End Point Control. The End Point Control page appears.
2. Click the Zones and Device Profiles tab.
3. In the End Point Control Zones area, click New. The Zone Definition page appears.
4. In the Description box, type a descriptive comment about the special browser zone.
5. In the Device Profiles area, click New. The New Device Profile Definition popup window appears.
6. In the Name box, type a meaningful name for the device profile.
7. In the Description box, type a descriptive comment about the device profile.
8. In the Add attribute area, select Microsoft Windows as the Operating system for the device profile. Do not specify any other attribute settings.
9. Click Save to return to the Zone Definition page.
10. Select the check box for the browser Device profiles that you want to include in the zone.
11. If you want the device profile to require the presence of a data protection component, select **Aventail Secure Desktop** or **Aventail Cache Control** from the **Required data protection tool** list.

12. When you are finished creating the zone, click **Save** to return to the **Zones and Device Profiles** page.

### Defining Zones for Special Classes of Users

Another method for preventing special classes of trusted users from being assigned to the default zone (and potentially being denied access) involves creating a zone that contains no device profiles, and then assigning that zone to a realm to which only those trusted users belong.

For example, if you want system administrators to be able to access network resources regardless of the client device they’re using, you could assign them to a realm that contains a no-profile zone. Then when system administrators select that realm and log in, they would be placed in the no-profile zone, instead of the global default zone that may be set up to block unrecognized clients.

**To create a no-profile zone**

1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.

2. Click the **Zones and Device Profiles** tab.

3. In the **End Point Control Zones** area, click **New**. The **Zone Definition** page appears.

4. In the **Name** box, type a meaningful name for the zone.

5. In the **Description** box, type a descriptive comment about the zone.

6. Do not select any **Device profiles** for this zone.

7. You can optionally select a **Required data protection tool** for the zone. However, if you want this special class of trusted users to have flexibility regarding the types of devices they’re connecting with, you could leave this field set to “None.”

8. Click **Save**.

Once you’ve defined the no-profile zone, you’ll need to create a realm specifically for this special class of trusted users and configure the realm so that only this special class can log in to it. For more information, see “Restricting User or Group Membership to a Realm” on page 113.

### Removing Data Left On the Client

Aventail’s data protection components are designed to remove data left on the client after each user session. There are two options available:

- **Aventail Cache Control** (ACC) provides basic data protection for all Web sessions. It is included with the base appliance.

- **Aventail Secure Desktop** (ASD) is an optional component—purchased separately—that provides enhanced data protection for Windows users. If the user is on a non-supported platform, ACC is automatically substituted instead.

AMC also supports Sygate On-Demand, which provides advanced End Point Control. For more information see “Sygate On-Demand” on page 180.

Both Aventail components enable you to configure a timeout to automatically end inactive user connections and remove data from the client. This minimizes your exposure in case a user forgets to log out from a kiosk or other shared computer.
When the user ends his or her session, or when the user’s session times out, Aventail Cache Control and Aventail Secure Desktop remove session data from the client’s cache. The following table summarizes the data that gets removed.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser history</td>
<td>All session URLs are permanently removed from the browser’s history, and cannot be recalled from the browser or programmatically from an external application.</td>
</tr>
<tr>
<td>Browser cache</td>
<td>All data files and associated URLs and passwords that are accessed and can be stored on the hard drive by the browser are permanently removed.</td>
</tr>
<tr>
<td>Browser username and password</td>
<td>All usernames and associated passwords that were used in the session are removed from the cache.</td>
</tr>
<tr>
<td>Browser URL AutoComplete list</td>
<td>All URLs that were visited during the session are removed from the browser’s AutoComplete list.</td>
</tr>
<tr>
<td>Windows index.dat</td>
<td>Browser activity details stored in the index.dat file are removed.</td>
</tr>
<tr>
<td>Temporary storage</td>
<td>Most file attachments that users opened from Web applications, such as Outlook Web Access (OWA), are permanently removed when Aventail Cache Control cleans the temporary folder. When using Aventail Secure Desktop, all session-related data files downloaded and stored on the local hard disk are permanently removed. (Note: This is only available using Aventail Secure Desktop.)</td>
</tr>
</tbody>
</table>

### Configuring Aventail Cache Control

Aventail Cache Control removes history, temporary files from the browser cache, passwords, and cookies from the user’s system after each Web session. It also enables you to configure an inactivity timeout.

**To configure Aventail Cache Control**

1. From the main navigation menu, click **End Point Control**. The **End Point Control** page appears.
2. Select the **Enable End Point Control** check box.
3. Under **Post-authentication**, click **Configure data protection**. The **Configure Data Protection** page appears.
4. Set the inactivity timer by choosing a value from the **End inactive user connections** list. This automatically ends a user session and cleans the cache if the user is inactive for the specified interval.

5. In the **Aventail Cache Control** area, select the **Enable Aventail Cache Control** check box.

6. Select the **Close other browser windows at startup** check box to gain a slightly higher level of security in some situations. This setting ensures that ACC can precisely monitor all data associated with the browser context used to access your network, but may inconvenience users who have more than one browser window active when ACC starts.

7. Select the **Allow user to disable cache control** check box if you want to permit the user to prevent the cache cleaner from running at the end of the session. This setting is disabled by default.

8. Click **Save** to return to the **End Point Control** page.

Once you have configured Aventail Cache Control, you must select it as the **Required data protection tool** for a zone. For information, see "Defining a Zone" on page 169.

**Notes**

- You can selectively provide ACC to subsets of your users by enabling it in separate "zones of trust" with different EPC requirements. See "Defining a Zone" on page 169 for information on using zones to control the provisioning of ACC.
- Logging out of ASAP WorkPlace will not cause ACC to clean the cache. The user must close the WorkPlace browser window before ACC will clean the cache and close.
- If ACC cannot load on the user’s computer, the user will not be able to log in to WorkPlace.
- The inactivity timer setting applies to both ACC and ASD; you cannot configure different timeout settings for ACC and ASD.

**Aventail Secure Desktop**

Aventail Secure Desktop (ASD) offers more protection than basic cache cleaning. A joint solution developed with Sygate Technologies, ASD creates a "virtual" Windows session that looks and feels like the standard Windows desktop. By default, all data accessed from your network is encrypted before it is written to disk, and is accessible only from within ASD.

When the users end their sessions, ASD permanently removes all session-related data files downloaded and stored on the local hard disk, plus any temporary data associated with the Web browser. It is recommended that you instruct users not to save any data to their local disk when working with ASD. Examples include:

- **Don't save files to the local disk.** For example, if a user downloads a file from your network and saves it to his or her hard disk, it will be deleted when the session ends.
- **Don't save application data to the local disk.** Some client/server applications (such as Microsoft Outlook) allow users to store data locally. Users should be aware of the interaction between these applications and ASD. For example, if an Outlook user is storing data locally (in a .pst file) and moves an e-mail message from the system Inbox to a local mail folder while...
ASD is running, the messages will be deleted from the local disk when the session ends. To help the user identify the virtual session created by ASD, its desktop features a distinctive background color and image.

ASD is available for Windows users with the following environments. Note that Java must be enabled in the browser.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Microsoft Windows XP (with Service Pack 1 or 2 installed)</td>
<td>• Microsoft Internet Explorer 5.5 and later</td>
</tr>
<tr>
<td>• Microsoft Windows 2000 (with Service Pack 3 or 4 installed)</td>
<td>• Microsoft Internet Explorer 6.0 and later (with Service Pack 1 installed)</td>
</tr>
<tr>
<td>• Mozilla 1.6 and later</td>
<td>• Mozilla 1.6 and later</td>
</tr>
<tr>
<td>• Netscape Navigator 7.1 and later</td>
<td>• Netscape Navigator 7.1 and later</td>
</tr>
</tbody>
</table>

**Configuring Aventail Secure Desktop**

This section describes how to configure ASD settings in AMC. Before configuring ASD, ensure that a valid ASD software license has been uploaded to the appliance. For more information, see "Software Licenses" on page 160.

**To configure Aventail Secure Desktop**

1. From the main navigation menu, click End Point Control. The End Point Control page appears.
2. Select the Enable End Point Control check box.
4. Configure the inactivity timer by choosing a value from the End inactive user connections list. This automatically ends a user session and cleans the cache if the user is inactive for the specified interval.
5. In the **Aventail Cache Control** area, configure the ACC settings (described in "Configuring Aventail Cache Control" on page 177). If a user is unable to run ASD (for example, if he or she is using an Apple Macintosh), the appliance will substitute ACC on the client using the specified ACC settings.

6. In the **Aventail Secure Desktop** area, select the **Enable Aventail Secure Desktop** check box.

7. To allow the user to switch between the normal Windows session and the virtual Windows session created by ASD, select the **Allow user to switch between desktops** check box. Note that enabling this option will slightly weaken the data protection provided by ASD.

8. Click **Save** to return to the **End Point Control** page.

Once you have configured Aventail Secure Desktop, you must select it as the **Required data protection tool** for a zone. For information, see "Defining a Zone" on page 169.

**Notes**

- You can selectively provide ASD to a subset of your users by enabling it in separate “zones of trust” with different EPC requirements. See "Defining a Zone" on page 169 for information on using zones to control the provisioning of ASD.
- If a user is unable to run ASD (for example, if he or she is using an Apple Macintosh or Linux computer), the appliance will substitute ACC using the specified settings. If neither ASD nor ACC can load on the user's computer, the user will be logged out.
- The data protection inactivity timer setting applies to ACC and ASD; you cannot configure different timeout settings for ACC and ASD.

**Sygate On-Demand**

Sygate On-Demand provides advanced cache control and data protection. It also validates the host integrity of client computers by verifying the presence of antivirus software, personal firewalls, service packs, and patches. Sygate On-Demand automatically adapts the security of each end point to environmental conditions, such as network location and ownership of the host computer, and has the ability to keep the secure virtual desktop environment persistent on the end point after the Aventail session ends. Sygate On-Demand integrates with the Aventail appliance to provide a seamless user experience, enforce security policies, and eliminate the need for additional hardware. For more information, visit [http://www.sygate.com/ssp/aventail/](http://www.sygate.com/ssp/aventail/).

This component requires a separate purchase. For information about purchasing this component, contact your Aventail channel partner.

◆ **To enable Sygate On-Demand**

1. Obtain the Sygate On-Demand files. (For more information, contact your Aventail channel partner.)

2. Upload the Sygate On-Demand files to the `/usr/local/epcagents/htdocs/postauth/data/ssp` directory on the appliance.

3. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.

4. Under **Post-authentication**, click the **Configure data protection** link. The **Configure Data Protection** page appears.

5. Select the **Enable Sygate On-Demand Protection** check box.
6. Click **Save** to return to the **End Point Control** page.

**Notes**
- Sygate On-Demand requires Sun JVM 1.4 or later.

**Validating Client Integrity**
Aventail supports integration with the WholeSecurity Confidence Online Enterprise Security and Zone Labs Integrity Clientless Security solutions. These solutions provide pre-authentication protection for your network against threats such as viruses, malware, and data theft.

**WholeSecurity Confidence Online Enterprise Edition On-Demand**
WholeSecurity's end-point security solutions provide “zero-hour” protection against known and unknown threats, such as Trojan horses, keystroke loggers, and worms. Delivered on-demand using ActiveX and Netscape plug-ins, WholeSecurity Confidence Online Enterprise Edition On-Demand integrates with the Aventail appliance to protect any computer—even those not owned by the company—at any time. Using a patent-pending behavioral detection technology, WholeSecurity Confidence Online Enterprise Edition On-Demand automatically identifies and eliminates both known and unknown threats without requiring users to update signatures. For more information, visit [http://www.wholesecurity.com/products/on-demand.html](http://www.wholesecurity.com/products/on-demand.html).

► **To enable integration with WholeSecurity Confidence Online Enterprise Edition On-Demand**
1. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
2. Under **Pre-authentication**, click the **Configure client integrity** link. The **Configure Client Integrity** page appears.
3. Click **WholeSecurity Confidence Online**.
4. In the **URL where the Whole Security agent is hosted** box, type the URL from which the Whole Security software will be received. The URL will typically include the internal name of the WholeSecurity server, followed by `/llclient/` and the name of the deployment on the WholeSecurity server. For example:

   ```text
   https://whole.example.com/llclient/<deployment_name>
   ```
5. Click **Save** to return to the **End Point Control** page.

**Zone Labs Integrity Clientless Security**
Zone Labs Integrity Clientless Security protects enterprises from threats on networked guest and employee PCs without requiring the installation of any client software. Zone Labs Integrity Clientless Security is the only product that provides the two essential components of clientless security: disabling spyware and enforcing security policy compliance before remote access is granted. When integrated with the Aventail appliance, Zone Labs Integrity Clientless Security stops ID and password theft, prevents data loss, restores network bandwidth, and improves IT and user productivity. For more information, visit [http://www.zonelabs.com/store/content/company/corpsales/clientSecurity.jsp](http://www.zonelabs.com/store/content/company/corpsales/clientSecurity.jsp).

► **To enable integration with Zone Labs Integrity Clientless Security**
1. Obtain the Zone Labs Integrity Clientless Security files. (For more information, contact your Aventail channel partner.)
2. Upload the Zone Labs Integrity Clientless Security files to the `/usr/local/epcagents/htdocs/preauth/malware/zls` directory on the appliance.
3. From the main navigation menu in AMC, click **End Point Control**. The **End Point Control** page appears.
4. Under **Pre-authentication**, click the **Configure client integrity** link. The **Configure Client Integrity** page appears.
5. Click **Zone Labs Integrity Clientless Security**.
6. Click **Save** to return to the **End Point Control** page.

**Notes**

After enabling integration with Zone Labs Integrity Clientless Security, be sure to keep the Zone Labs software up to date by regularly uploading Zone Labs updates. Zone Labs Integrity Clientless Security cannot perform automatic updates from the Aventail appliance.
Chapter 10  Configuring User Access Components

The Aventail appliance includes several components that enable users to access resources on your network. This section explains how to configure and deploy each component.

One of the components—ASAP WorkPlace—is Web-based and available from any Web browser. ASAP WorkPlace provides dynamically personalized access to Web resources and enables users to browse network file servers from any Web browser. WorkPlace offers two modes of Web access: standard Web access and translated Web access.

Two other components—Aventail Connect and Aventail OnDemand—provide secure access to client/server applications. Aventail Connect is a Microsoft Windows application, and Aventail OnDemand is a secure, lightweight agent.

Aventail ASAP WorkPlace

ASAP WorkPlace, a service that runs on the appliance, provides your users with protected access to Web-based (HTTP) resources. It also gives users access from their Web browsers to files and folders on a Windows file server, and to TCP/IP resources through the Aventail OnDemand agent, which is provisioned from ASAP WorkPlace.

A Quick Tour of ASAP WorkPlace

When a user accesses ASAP WorkPlace, the login page(s) appear. If multiple realms are configured on the appliance, the user is prompted to specify a realm.

```
Please log in

Log in here to establish a secure connection to your network resources.

Log in to Employees

Next
```

The user is then prompted to specify his or her actual credentials. Users authenticating with client certificates do not see this page.
Chapter 10 - Configuring User Access Components

Home Page

Log in to Employees
User name: 
Password: 
Login

After a user has authenticated, the ASAP WorkPlace Home page appears. It displays administrator-defined shortcuts to the Web and file system resources that the user is allowed to access. For information on how to create these shortcuts, see "Working with Shortcuts" on page 190. Note that the network shortcuts, which point to file system resources, do not appear if you have disabled all access to file system resources. For information on how to disable access to file system resources, see "Configuring ASAP WorkPlace General Settings" on page 188. You can also choose whether you want the Intranet Address box to appear and, if so, configure whether it can be used to access Web resources (by typing a URL), file system resources (by typing a UNC path name), or both.

The ASAP WorkPlace Home page includes a Connection Status area that indicates which user access agents are currently running, the zone status, and the session start time. Users can click a Details link in this area to view more information about the user access agent or agents that are running, and to view more detailed connection status information.

If you are deploying Aventail OnDemand to your users, by default OnDemand will launch automatically when users log in to WorkPlace; users can view the status of the OnDemand connection in the Connection Status area. Alternatively, you can configure OnDemand so that users start it by clicking a link on the WorkPlace Home page. You can also create shortcuts that automatically start specific client/server applications that are configured to run with OnDemand. For more information, see “Aventail OnDemand” on page 201.
Users can log out of WorkPlace by clicking the **Log Out** button in the upper right corner. Note that clicking the **Log Out** button logs users out of WorkPlace, but does not necessarily log users out of any applications that are running (depending on which user access agent is being used). To increase security, users should log out of or quit applications when they finish working with them, particularly when working on computers that are shared with other users.

### Intranet Address Box

If enabled, the **Intranet Address** box appears in the upper right corner of ASAP WorkPlace.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource address</strong></td>
<td>A resource can be accessed by typing a complete URL (domain and host name) or just a host name. For example, a resource named “CRM” on a host named “fred” could be accessed using a full URL (such as <a href="http://fred.example.com/CRM/">http://fred.example.com/CRM/</a>) or a host name (such as <a href="http://fred/CRM/">http://fred/CRM/</a> or fred/CRM/).</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>The user does not need to include the http:// protocol identifier to access a standard Web resource (even though it is inserted in the Intranet Address box by default). To access a secure Web site, however, the user must include the https:// protocol identifier.</td>
</tr>
<tr>
<td><strong>Port number</strong></td>
<td>To access a Web resource on a non-standard port (that is, other than 80), the user must type the port number after the host name. For example, fred:8080/SAP and <a href="https://fred:443/SAP">https://fred:443/SAP</a> are both valid entries.</td>
</tr>
</tbody>
</table>

To access a file system resource, the user types the UNC path (for example, \jax\software\download) in the **Intranet Address** box and then clicks **Go**. If the user has appropriate access privileges, the **Network Explorer** page opens, displaying the contents of the requested file system resource.

For information on how to configure the presence and functionality of the **Intranet Address** box, see “Configuring ASAP WorkPlace General Settings” on page 188.
Network Explorer Page

When a user accesses a file system resource (by clicking a network shortcut, typing a UNC path in the Intranet Address box, or clicking the Network Explorer link on the WorkPlace Home page), the Network Explorer page appears.

This page displays the contents of the requested file system resource and, depending on the user’s access privileges, allows the user to perform the following actions on a file: view contents and properties, rename, copy, move, download, and delete. Users may also be able to create new folders. If the administrator has enabled upload functionality (see “Configuring ASAP WorkPlace General Settings” on page 188), and the user has write privileges, the user can upload files. For details on how access privileges defined in AMC combine with Windows access privileges, see “Services Managing Your Access Policy” on page 79.

User Access Agents

ASAP WorkPlace supports a variety of agents that enable users to access different types of resources. The following table describes the various user access agents.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Description</th>
</tr>
</thead>
</table>
| Aventail OnDemand, dynamic mode | • Dynamically redirects to any application that is defined as a network resource in AMC.  
                                 | • Supported only on Windows.                                                |
| Aventail OnDemand, mapped mode  | • Provides access to specific applications that are configured to run with OnDemand.  
                                 | • Supported on Windows, Linux, and Macintosh.                               |
| Standard Web mode             | • Provides access to any URL.                                               
                                 | • Supported only on Windows XP and Windows 2000 with Internet Explorer 5.5 or later. |
| Translated Web mode           | • Provides access to any URL and, optionally, aliases URLs.                
                                 | • Supported on Windows, Linux, and Macintosh.                               |
User access agents are configured on a per-realm basis. When configuring a realm, you can specify the type of Web access realm members get (standard mode or translated mode), and whether they can use OnDemand.

Multiple agents can be active simultaneously. For example, OnDemand in dynamic mode and standard Web access might be active at the same time; OnDemand in dynamic mode would provide users with access to TCP/IP resources, and standard Web access would provide users with access to Web resources.

When a user logs in to ASAP WorkPlace for the first time, WorkPlace automatically provisions and, in some cases, installs the user agent that will provide the broadest range of access based on the user's access privileges and any constraints of the user's system. WorkPlace deploys user access agents in this order, where OnDemand in dynamic mode offers the broadest range of access:

1. OnDemand in dynamic mode
2. OnDemand in mapped mode
3. Standard Web mode
4. Translated Web mode

If the user access agent that provides the broadest range of access cannot be launched (for example, if the user's computer does not meet the agent's system requirements), the next agent will be launched. On subsequent connections, that same user access agent will automatically be launched if the user logs in from the same system.

**Standard Web Access vs. Translated Web Access**

The Aventail appliance supports two modes of Web access through ASAP WorkPlace: standard Web access and translated Web access.

- **Standard Web access** enables users to access a URL from WorkPlace by typing the URL directly in the Internet Explorer Address box. Standard Web access eliminates the need for Web content translation and provides broader access to enterprise Web applications. Standard Web access is automatically provisioned to users and requires no special configuration. Standard Web access provides improved application compatibility, but provisioning the agent can take extra time when a user first logs in to ASAP WorkPlace. Standard Web access is supported on only the Windows 2000 and Windows XP operating systems, and requires Internet Explorer 5.5 or later.

- **Translated Web access** enables users to access a URL that is specifically configured to run with WorkPlace. These URLs are configured in AMC and typically appear as Web shortcuts on the ASAP WorkPlace Home page although, if this feature is enabled, users can also type an appropriate URL in the Intranet Address box. Translated Web access is configured on a per-realm basis and is disabled by default.

The following table summarizes the advantages and disadvantages of each Web access mode.

<table>
<thead>
<tr>
<th>Web access mode</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Web access</td>
<td>• Better application compatibility</td>
<td>• Limited operating system and browser support</td>
</tr>
<tr>
<td></td>
<td>• Users can access any network URL by typing its actual URL in the browser's Address box</td>
<td>• Longer download time when users log in to WorkPlace for the first time</td>
</tr>
<tr>
<td></td>
<td>• Inactivity timer provides tighter end-point control</td>
<td></td>
</tr>
</tbody>
</table>

---

**Aventail**
Chapter 10 - Configuring User Access Components

ASAP WorkPlace Client Requirements

ASAP WorkPlace is compatible with the following operating system and Web browser combinations.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP, Windows 2000, Windows 98</td>
<td>Microsoft Internet Explorer v5.5 or later</td>
</tr>
<tr>
<td>Windows XP, Windows 2000, Windows 98</td>
<td>Netscape Navigator v7.0 or later</td>
</tr>
<tr>
<td>Macintosh OS 10.2 or later</td>
<td>Microsoft Internet Explorer v5.2 or later</td>
</tr>
<tr>
<td>Macintosh OS 9.2 or later (See note below)</td>
<td>Microsoft Internet Explorer v5.1 or later</td>
</tr>
<tr>
<td>Red Hat Linux v0.8 or later</td>
<td>Mozilla v1.4.1 and Netscape Navigator v7.0</td>
</tr>
</tbody>
</table>

Notes

- Standard Web access is supported on only the Windows 2000 and Windows XP operating systems, and requires Internet Explorer 5.5 or later.
- Aventail Cache Control (ACC) is not supported on the Macintosh OS 9.x operating system. If ACC is enabled, users running Macintosh OS 9.x will not be able to access network resources through ASAP WorkPlace.
- Sygate On-Demand requires Sun JVM 1.4 or later.

Configuring ASAP WorkPlace General Settings

This section describes how to configure the ASAP WorkPlace general settings. For details on how to customize the appearance of WorkPlace, see “Customizing the Appearance of ASAP WorkPlace” on page 194.

To configure ASAP WorkPlace general settings

1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Configuration tab.
2. Complete the information in the top section of the tab, which contains options that control Windows file system access.

- If you want your users to have Web-based access to Windows file system resources, select the Enable access to network file shares check box. When enabled, users can access file system resources from within ASAP WorkPlace—through the Network Explorer page, any network shortcuts you create, and the Intranet Address box (if
configured to appear). If this option is disabled, users will not be able to browse or connect to Windows file system resources from ASAP WorkPlace.

- If you want to give users the ability to upload files to a Windows file system resource, select the **Enable file uploads** check box. This functionality is disabled by default. Enabling this feature may have a negative effect on the performance of the appliance, depending on the size of the files that users upload. Also, note that this setting takes precedence over any permissions you set in a file system access control rule. If an access rule grants a user write access to a file system but file uploads are disabled, the user will only be able to move and delete files, not write to them.

3. Complete the information in the **Intranet Address box** area, which contains options that control the presence and functionality of the **Intranet Address** box in WorkPlace. If one or both options are enabled, the **Intranet Address** box appears in the upper right corner of WorkPlace. If neither option is enabled, WorkPlace does not display the box.

### Intranet Address box

This feature enables end users to type UNC path names or URLs in the **Intranet Address** box on ASAP WorkPlace. If you clear the checkboxes, the Intranet Address box will not appear on ASAP WorkPlace.

- **Enable access to Windows network resources**
  - Allows users to reach a Windows network resource by typing its UNC path name in the Intranet Address box.

- **Enable access to Web resources**
  - Allows users to reach a Web resource by typing its URL in the Intranet Address box.

- If you want to give users the ability to reach a Windows file system resource by typing its UNC path in the **Intranet Address** box, select the **Enable access to Windows network resources** check box. This check box is available only if you have enabled Web-based access to file system resources (by selecting the **Enable access to network file shares** check box).

- If you want to give users the ability to reach a Web resource by typing its URL in the **Intranet Address** box on WorkPlace, select the **Enable access to Web resources** check box. This is especially useful if you have defined an entire DNS domain as a resource and want to provide access to all Web servers within the domain (without having to define each individual Web resource in the domain). Note that this setting applies only when WorkPlace is running in translated mode.

For information on defining Web resources, see “Defining Resources” on page 75.

**Notes**

- Note that these options determine only the types of resources that are available from the **Intranet Address** box, and have no effect on your access control policy.

- For a detailed discussion of this box, see “Intranet Address Box” on page 185.

### Customizing ASAP WorkPlace

ASAP WorkPlace is highly customizable. As the administrator, you can control the Web and file system resources that are visible to your users, the ways in which users can access these resources, and the appearance of the user interface. You perform all of this customization in AMC.

The following sections discuss the creation and management of Web and network shortcuts as well as the customization of the WorkPlace user interface. For information on enabling access to file system resources, file uploads, and the Intranet Address box, see “Configuring ASAP WorkPlace General Settings” on page 188.

You’ll use the AMC **WorkPlace Shortcuts** page to manage shortcuts to resources, and the **WorkPlace Appearance** page to customize the appearance of the ASAP WorkPlace application.
You can configure shortcuts to Web and file system resources; this prevents users from needing to type URLs and UNC paths in the Intranet Address box. These shortcuts, which appear on the WorkPlace Home page, are quick and easy to use and do not require that the user know specific URLs or file system paths.

**Working with Shortcuts**

ASAP WorkPlace gives users with appropriate access privileges the ability to work with Web resources, as well as the ability to use a Web browser to browse and work with files and folders on a Windows file server.

For information on system requirements for using WorkPlace to work with Windows files and folders, see “Deployment Checklist” on page 10. For information on enabling access to file system resources, see “Configuring ASAP WorkPlace General Settings” on page 188.

By default, even though you may have defined your resources in AMC, none of them appear in WorkPlace until you create the appropriate shortcuts. This section explains how to create and manage the shortcuts appearing in ASAP WorkPlace.

**Viewing Shortcuts**

You’ll manage shortcuts to resources on the WorkPlace Shortcuts page. As the administrator, you’ll see the entire list of shortcuts on this page; however, when a user accesses ASAP WorkPlace, the list will be filtered to display only the resources that he or she has permission to access. ASAP WorkPlace displays the shortcuts in the same sequence you use to order them on this page.

1. To view shortcuts
   1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.

2. Review the data listed in the fields:
• The checkbox column is used to select one or more shortcuts. Use this to delete shortcuts (using the Delete button) or reorder them (using the Move Up and Move Down buttons).
• The number indicates the order in which the shortcut will be listed in ASAP WorkPlace. You can edit a shortcut by clicking the number.
• The Link text column displays the hyperlink text that is used to access the Web resource. You can edit a shortcut by clicking the link text.
• The Resource column displays the name of the resource.

Adding Web Shortcuts

Web shortcuts provide your users with quick and easy access to Web resources. Before you can create a shortcut to a Web resource, you must first define the resource (see "Adding a URL Resource" on page 87 for more information).

▲ To add a Web shortcut

1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.
2. In the Web shortcuts area, click the New button. The Add/Edit Web Shortcut page appears.
3. In the Number box, type a number that specifies the shortcut’s position in the WorkPlace Web Shortcuts list.
4. In the Link text box, type the hyperlink text that will be used to access the Web resource.
5. In the Description box, type a descriptive comment about the shortcut. Although optional, a description will help users easily identify the Web resource. This description appears beside the link text.
6. In the Resource list, select the resource to which this shortcut will be linked. This list contains all the defined URL resources.
7. Use the Start page box, if necessary, to append more specific information to the selected URL. For example, if you want the link to point to a directory or file other than the root, type a relative path in the Start page box. This is useful for Web applications that store their content in a location other than the root. For example, if the selected URL is for Outlook Web Access and it points to mail.example.com, you could set the start page to /exchange/root.asp. The resulting URL would be https://mail.example.com/exchange/root.asp.
Chapter 10 - Configuring User Access Components

Adding Network Shortcuts

Network shortcuts provide your users with quick and easy access to file system resources. Before you can create a shortcut to a file system resource, you must first define the resource (see “Adding a File System Resource” on page 89 for more information).

To add a network shortcut

1. From the main navigation menu, click ASAP WorkPlace, and then click the Workplace Shortcuts tab.
2. In the Network shortcuts area, click the New button. The Add/Edit Network Shortcut page appears.

3. In the Number box, type a number that specifies the shortcut’s position in the Workplace Network Shortcuts list.
4. In the Link text box, type the hyperlink text that will be used to access the file system resource.
5. In the Description box, type a descriptive comment about the shortcut. Although optional, a description will help users easily identify the file system resource. This description appears beside the link text in ASAP WorkPlace.
6. In the Resource list, select the file system resource to which this shortcut should be linked. This list contains all the defined file system resources.

Creating Network Shortcuts to Personal Folders

You can create a network shortcut that dynamically references a user’s personal folder. This allows you to create a single ASAP WorkPlace link that points to the personal folder for the current user. For example, when the user jdoe connects to ASAP WorkPlace, the link would provide access to a folder named \users\jdoe; for user rsmith, the link would provide access to \users\rsmith.

To create a network shortcut to a personal folder

1. From the main navigation menu, click Resources.
2. Define two file system resources, one to the top-level directory containing the user folders, and another referencing a username variable.

To add a resource, click the Resources tab, and then click the New button. In the Resource definition area, click Network share and then specify the UNC path:

a. The first resource should reference the top-level directory containing the user folders. For example, if the personal folders are stored on a network share named \example\users, you would type \example\users.
b. The second resource should reference the XXX_Username_XXX username variable. For example, for personal folders stored on a network share beneath \example\users\ you would type \example\users\XXX_Username_XXX.

3. Create an access control rule granting users access to the top-level directory (in our previous example, it would reference \example\users\).

The simplest approach is to allow all users to access this resource, and use the native Windows access control to restrict each user to his or her own directory.

4. Create a WorkPlace network shortcut referencing the resource containing the username variable (in our example, \example\users\XXX_Username_XXX).

Note that you can also use the XXX_Username_XXX variable in the Link text box. For example, if you type \example\users\XXX_Username_XXX in the Link text box, the hypertext link on WorkPlace for a user named jdoe would appear as \example\users\jdoe.

Editing Shortcuts

To change the name or description for a resource appearing in ASAP WorkPlace, you’ll need to edit the shortcut. You can create new WorkPlace shortcuts when defining resources; however, to edit settings for an existing shortcut, you must use the WorkPlace Shortcuts page.

► To edit a shortcut

1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.

2. In the Web shortcuts or Network shortcuts area, click the number or the link text of the shortcut that you want to edit. For example, if you want to edit the shortcut in the third position in the Web shortcuts list, you could click 3 in the Web shortcuts area.

3. Make any edits, as needed, and then click Save.

Deleting Shortcuts

If you delete a shortcut, users will no longer see that shortcut in ASAP WorkPlace. You can create new WorkPlace shortcuts when defining resources; however, to delete a shortcut, you must use the WorkPlace Shortcuts page.

► To delete a shortcut

1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.

2. In the Web shortcuts or Network shortcuts area, select the check box to the left of any shortcuts that you want to delete, and then click the Delete button.

Moving Multiple Shortcuts

ASAP WorkPlace displays the list of shortcuts exactly as you order them on the WorkPlace Shortcuts page. You can move one or more shortcuts at the same time; this can be helpful if, for example, you want to place your most frequently used shortcuts at the top of the list.

► To move multiple shortcuts

1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.

2. In the Web shortcuts or Network shortcuts area, select the check box to the left of any shortcuts that you want to move.

3. Click the Move Up or Move Down button as appropriate. Each click of the Move Up or Move Down button moves the block of selected shortcuts up or down one row.
Moving Individual Shortcuts

ASAP WorkPlace displays the list of shortcuts exactly as you order them on the WorkPlace Shortcuts page. You can reorder the placement of individual shortcuts; this can be helpful if, for example, you want to quickly move a shortcut several positions up or down the list.

► To move a shortcut
1. From the main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Shortcuts tab.
2. Click the number or the link text of the shortcut that you want to move. For example, if you want to move the shortcut that is currently in the third position, you could click 3.
3. Type the new list position in the Number box. For example, if you want to move a shortcut to the fifth position in the list, type 5 in the Number box.

For information about moving multiple shortcuts, see "Moving Multiple Shortcuts" on page 193.

Customizing the Appearance of ASAP WorkPlace

From within AMC, you can customize the following components of ASAP WorkPlace:

- Company logo
- WorkPlace title
- Link to custom Help file
- Greeting
- Work Place Shortcuts
- Network Shortcuts
- Internet
- Aventail

The Aventail license agreement stipulates that the “Powered by Aventail” logo, “Licensed to:” content, and the Aventail copyright notice be left intact, unless you’re hosting the content on your own portal page.

► To customize the appearance of ASAP WorkPlace
1. From AMC’s main navigation menu, click ASAP WorkPlace, and then click the WorkPlace Appearance tab.

![ASAP WorkPlace Customization Screenshot]
2. Complete the information in the **Appearance** area:

   **Appearance**
   
   - **Font family**: Serif or Sans-serif
   - **Color scheme**: Dark blue, Light blue, Purple, Red, Green

   a. In the **Font family** list, select the font you want to use (Serif or Sans-serif).
   b. In the **Color scheme** area, select the color scheme you want to use. To view a thumbnail of a color scheme, click the color name (Dark blue, Light blue, Purple, Red, or Green). To display a larger version of the sample page, click the thumbnail image.

3. Complete the information in the **Content** area:

   **Content**
   
   - **Current logo**: av-default-logo.gif
   - **Replace with**: [Browse...]
   - **Title**: ASAP WorkPlace
   - **Greeting**: ASAP WorkPlace provides secure access to network resources on your intranet. To access a resource, click its name from the list below. For help, click the Help button in the upper right or contact your system administrator.
   - **Help file**: [Browse...]

   a. By default, the Aventail logo appears in WorkPlace. To customize the logo, use the **Replace with** box to specify the graphic you want to use. You can type the path of the image file, or you can click the **Browse** button to select the .gif or .jpg file you want to use. For best results, the graphic dimensions should not exceed 200 pixels wide by 100 pixels tall.
   b. In the **Title** box, type the text that should appear as the title on the page and in the browser’s title bar. The title should be no more than 25 characters.
   c. In the **Greeting** box, type the introductory text that should appear below the title. The greeting should contain no more than 250 characters.
   d. In the **Help file** area, click the **Browse** button to upload an HTML file that contains custom Help information. This file must be a well-formed HTML file.

   Your custom Help content is integrated with the default WorkPlace Help system, which contains all the information an end user needs to work with WorkPlace. To further assist the user, you might want to provide more detailed information about the resources available on your VPN, or describe how to get technical support.

### Customizing ASAP WorkPlace Login, Error, and Notification Pages

This section describes how to customize specific pages in ASAP WorkPlace, including authentication, error, and notification pages.
Overview: Customizing WorkPlace Templates

AMC provides support for modifying the appearance of ASAP WorkPlace, including the logo, color scheme, and greeting text on the main WorkPlace page. Although the AMC customizations provide a convenient way to change the general look and feel of WorkPlace, they may not provide enough control for some deployments.

Here are some examples of when you might want to modify the appliance’s templates:

- To make the login and logoff pages visually consistent with your corporate standards.
- To modify the error pages (which appear if a resource is unavailable or a user provides invalid credentials) to include detailed support or troubleshooting information.
- To use your existing corporate portal (where that portal application has been defined as an alias) instead of ASAP WorkPlace. Here you would customize the login, logoff, notification, and error pages to match the look and feel of your existing portal.
- To provide access to a specific application (where that application is defined as an alias) to a business partner. Here you would customize the login, logoff, notification, and error pages to match the look and feel of the application.

The templates you can customize can be broadly grouped into three categories:

<table>
<thead>
<tr>
<th>Template type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>The pages used to gather the user’s credentials, including selecting a realm and entering a username, password, or passcode. You might use these templates to provide the user with helpful information explaining how to log in to your network.</td>
</tr>
<tr>
<td>Error</td>
<td>The pages displayed when an error occurs, such as invalid user input (an authorization-denied message or a failed login) or an error in the appliance. You might use these templates to provide the user with information about how to correct a problem, such as administrator contact information.</td>
</tr>
<tr>
<td>Notification</td>
<td>The pages that provide the user with basic information required to interact with the system, including the logout page (confirming successful logout) and pages containing messages from the authentication module (such as a password-expiration warning). These templates don’t have any special information requirements. If you modify the authentication and error templates, you should also modify the notification templates to ensure consistency.</td>
</tr>
</tbody>
</table>

Although you can redesign the layout or add graphics and text on these pages, you cannot modify or remove the existing elements. For example, on the authentication page you cannot rename the Login button. These elements are dynamically generated by WorkPlace.

Notes

- The WorkPlace pages that are presented to the user after login cannot be customized manually; they are controlled from AMC.
- You can define resource-specific templates only for URLs that have an alias assigned to them in AMC. For more information on aliases, see ”URL Resources” on page 76.

How Template Files are Matched

You can customize templates globally, or on a per-resource basis. For example, you might customize the global templates to use one design, and then override that design for a particular Web resource (provided it is aliased) by modifying its templates.
When a user connects to a resource, the appliance first looks for the most specific template. If one is not found, it checks for the generic template for the category (authentication, error, or notification). If neither is found, the default WorkPlace template (the one under AMC’s control) is used.

The following table explains the various templates and their corresponding file names.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>User selects a realm</td>
<td>realm-select.tmpl</td>
</tr>
<tr>
<td>Authentication</td>
<td>User provides login credentials</td>
<td>authentication-request.tmpl</td>
</tr>
<tr>
<td>Error</td>
<td>Realm selection failed</td>
<td>realm-error.tmpl</td>
</tr>
<tr>
<td>Error</td>
<td>Invalid credentials supplied</td>
<td>authentication-error.tmpl</td>
</tr>
<tr>
<td>Error</td>
<td>Access to resource is denied</td>
<td>authorization-error.tmpl</td>
</tr>
<tr>
<td>Error</td>
<td>Appliance license capacity exceeded</td>
<td>licensing-error.tmpl</td>
</tr>
<tr>
<td>Error</td>
<td>End-point control error</td>
<td>epc-error.tmpl</td>
</tr>
<tr>
<td>Status</td>
<td>Authentication notification (such as password expiration)</td>
<td>authentication-status.tmpl</td>
</tr>
<tr>
<td>Status</td>
<td>Logoff successful page</td>
<td>logoff-status.tmpl</td>
</tr>
<tr>
<td>Generic</td>
<td>End Point Control download page</td>
<td>epc-launch.tmpl</td>
</tr>
<tr>
<td>Generic</td>
<td>User provides login credentials</td>
<td>authentication.tmpl</td>
</tr>
<tr>
<td>Generic</td>
<td>General errors</td>
<td>error.tmpl</td>
</tr>
<tr>
<td>Generic</td>
<td>General status</td>
<td>status.tmpl</td>
</tr>
<tr>
<td>Generic</td>
<td>General page</td>
<td>custom.tmpl</td>
</tr>
</tbody>
</table>

Notes

- The default WorkPlace template file (named extraweb.tmpl) should never be edited: Your changes will be overwritten the next time you customize WorkPlace in AMC.

Customizing the WorkPlace Templates

The appearance of ASAP WorkPlace is controlled using several HTML templates. To customize the templates, you create an HTML file using any standard Web design tool or text editor.

To customize the WorkPlace templates

1. Create an HTML file containing the desired layout, and add the WorkPlace-specific tags:
   - Within the BODY tag, add an HTML COMMENT tag containing the word "EXTRAWEB":

     ```html
     <!-- EXTRAWEB -->
     ```

     This tag determines where to place content dynamically generated by the appliance.
   - Add a reference to the external JavaScript file:

     ```html
     <script language="javascript" src="/__extraweb__/template.js"></script>
     ```

   - To have your templates display any WorkPlace content (including the .css file or the custom logo you configured in AMC), modify your HTML code to reference the __extraweb__/images/ path. For example:

     ```html
     <img src="/__extraweb__/image/mylogo.gif">
     ```

2. Save the file with the appropriate filename (see “How Template Files are Matched” on page 196) using a .tmpl file extension.
Uploading Your WorkPlace Templates

This procedure explains how to upload the templates to the appliance.

▶ To upload ASAP WorkPlace templates
1. Establish a connection to the appliance using SSH.
2. Change to the appropriate directory:
   - General templates are stored in /usr/local/extranet/templates.
   - Alias-specific templates are stored in /usr/local/extranet/templates/<aliasname>, where <aliasname> is the name of the alias you assigned to the URL resource in AMC.
3. Upload your custom templates to the appliance.
4. Copy any supporting files (including cascading style sheets or images) to the /usr/local/extranet/htdocs/__extraweb__/images directory.
5. Change the permissions on your templates to 755 (read-only) by typing the following command:
   
   ```
   find /usr/local/extranet/templates -type d -exec chmod 755 {} \;
   ```

Giving Users Access to ASAP WorkPlace

Because ASAP WorkPlace is a Web application, it can be accessed using a standard Web browser. You will need to provide users with the URL for WorkPlace: https://<server_name> where server_name is the fully qualified domain name (FQDN) contained in the appliance's SSL certificate (see "Configuring SSL Certificates" on page 38).

Redirecting Users to Another Site

If you have a Web portal that provides users with access to network resources, you may want to use it in place of ASAP WorkPlace. If so, you can automatically redirect users to your portal after they authenticate to the appliance. Note that without access to ASAP WorkPlace, your users will not have Web access to Windows file system resources.

To redirect users, you simply modify the Web access service start page to point to your portal home page. By default, the start page is configured to use the meta-refresh tag to automatically display ASAP WorkPlace.

▶ To redirect users to another site
1. Open /usr/local/extranet/htdocs/__extraweb__/index.html in a text editor such as vi.
2. In the <HEAD> section of the file, look for the <meta> tag and change the refresh= attribute to point to your Web portal. This example would redirect the user to the portal page immediately (0 seconds) upon loading the WorkPlace start page:
   
   ```
   <meta http-equiv="refresh" content="0; URL=/servlets/iclient/app">
   ```
3. Save the file.

Accessing ASAP WorkPlace from Other Web Sites

You may want users to access ASAP WorkPlace from another Web page or portal hosted on your network.

▶ To access ASAP WorkPlace from another Web site
1. Create a hyperlink to https://<server_name>/ and replace server_name with the actual name of your appliance. You should use the FQDN contained in the appliance's SSL certificate.
2. To provide a Log out button, create a hyperlink pointing to https://<server_name>/__extraweb__/logoff (again, replacing server_name with the FQDN from your appliance's SSL certificate). This will help preserve the security of user accounts.
End Point Control and the User Experience

When Aventail End Point Control components are enabled, the WorkPlace login process includes additional steps, which vary depending on whether Aventail Secure Desktop (ASD) or Aventail Cache Control (ACC) is used. For more information about Aventail End Point Control, see “Overview: End Point Control” on page 163.

How Aventail Secure Desktop Works

With ASD, the typical WorkPlace session includes the following steps:

1. In a Web browser, the user types the appropriate WorkPlace URL.
2. The user logs in to WorkPlace.
3. The user must accept any Aventail security warnings that appear. The ASD desktop appears, the ASD icon appears in the taskbar notification area, and the WorkPlace login page automatically appears in a new browser window in the ASD desktop.
4. The user accesses his or her network resources as needed.
5. When the user is ready to end the WorkPlace session, he or she exits WorkPlace. This terminates the WorkPlace session and closes the browser window. ASD permanently removes all session-related data files downloaded and stored on the local hard disk, plus any temporary data associated with the Web browser.

Notes

Because ASD permanently removes all session-related data files from the local hard disk, you should instruct users not to save any data to their local disk when working with ASD. Examples include:

- **Don’t save files to the local disk.** For example, if a user downloads a file from your network and saves it to his or her hard disk, it will be deleted when the session ends.
- **Don’t save application data to the local disk.** Some client/server applications (such as Microsoft Outlook) allow users to store data locally. Users should be aware of the interaction between these applications and ASD. For example, if an Outlook user is storing data locally (in a .pst file) and moves an e-mail message from the system Inbox to a local mail folder while ASD is running, the message will be deleted from the local disk when the session ends. To help the user identify the virtual session created by ASD, its desktop features a distinctive background color and image.

How Aventail Cache Control Works

With ACC, the typical WorkPlace session includes the following steps:

1. In a Web browser, the user types the appropriate WorkPlace URL.
2. The user logs in to WorkPlace.
3. The user must accept any Aventail security warnings that appear. The ACC icon appears in the taskbar notification area.
4. The user accesses his or her network resources as needed.
5. When the user ends the ACC session, ACC deletes all data associated with the session.

Notes

- If you configure ACC to close other browser windows at startup, you should notify your users so they can bookmark URLs or avoid losing data that hasn’t been submitted.
Aventail Connect

The Aventail® Connect™ client is a Windows application that provides access to TCP/IP resources protected by the Aventail client/server access service. In most cases, users interact with the Aventail Connect client only when it prompts them to enter authentication credentials or to enable remote network access.

Aventail Connect redirects network traffic and reroutes it according to the routing directives assigned in its configuration file. Configuration files are created using the Aventail Connect Configuration Tool.

When the Aventail Connect client receives a connection request, it determines whether the connection needs to be redirected to the Aventail client/server access service. When redirection is not required, Aventail Connect simply passes the connection request (and any subsequent data transmissions) directly to the TCP/IP stack.

The basic steps for installing, configuring, and deploying the Aventail Connect client are described below. For more detailed information about working with the Aventail Connect client, refer to the Aventail Connect Administrator’s Guide.

► To install, configure, and deploy the Aventail Connect client
1. Install the Aventail Connect administrator tools on your computer. The Aventail Connect administrator tools include the Configuration Tool and the Customizer.
2. Open the Aventail Connect Configuration Tool, and then create a configuration (.cfg) file. The basic steps for creating a configuration file are:
   • Configure the remote network, and the remote network access mode.
   • Specify the destinations on the remote network that Aventail Connect will redirect traffic to.
   • Define any required proxy server settings.
   • Reference the appropriate Aventail client/server access service trusted roots file.

3. Using the Aventail Connect Customizer tool, create an Aventail Connect setup package. You must include the trusted roots file that you referenced in step 2, as well as the configuration file that you created in step 2.

4. Distribute the Aventail Connect setup package to your users. The most common ways of distributing a setup package are:
   • Placing the setup package on an HTTP or HTTPS server.
   • Placing the setup package on an FTP site.
   • Placing the setup package on a network drive that can be accessed as a mapped drive or, for Microsoft networks, via a UNC path name (such as \computer_name\share_name\Connect).
   • Sending the package to users as an e-mail attachment.

5. Instruct your users to retrieve and open the setup package. An executable file automatically extracts the Aventail Connect installation package and initiates setup on the user’s computer.

Notes
   • To enable access to your network resources through Aventail Connect, you must assign users to a zone that specifically allows Aventail Connect access. For more information, see “Assigning Aventail Connect Users to a Zone” on page 172.

Aventail OnDemand

Aventail OnDemand™ is a secure, lightweight agent that provides access to TCP/IP resources protected by the client/server access service. OnDemand uses local loopback proxying to redirect communication to protected network resources according to routing directives defined in AMC. (OnDemand does not support UDP applications.)

This section provides an overview of OnDemand and describes how to configure and deploy OnDemand. Note that the OnDemand options in AMC are disabled if you have not purchased an OnDemand license.

Overview: OnDemand

Aventail OnDemand is a loopback-based proxy solution that secures communication between a client application and an application server. Users can download OnDemand from the Aventail appliance “on demand” to gain clientless VPN access—ideal for partners or vendors who do not have full access to your network, or for mobile employees who may need to access network resources from a public kiosk or home computer.
Chapter 10 - Configuring User Access Components

The following diagram illustrates the connection sequence:

1. By default, OnDemand starts automatically when the user logs in to ASAP WorkPlace. Alternatively, you can configure OnDemand so that the user clicks a link on ASAP WorkPlace to start OnDemand.

2. By default, OnDemand starts and runs within the ASAP WorkPlace window. Alternatively, you can configure OnDemand to run in a separate window in a "stand-alone" mode.

3. OnDemand waits for application requests on the local loopback address (127.0.0.1) and redirects the traffic to the Aventail client/server access service.

4. The Aventail client/server access service proxies the traffic to an application server using the application's required port(s).

5. The application server sends application traffic to the client/server access service.

6. The client/server access service sends the application traffic to OnDemand, which then passes it to the client application.

OnDemand supports TCP applications that use one port or multiple ports, including applications that dynamically define ports. Two types of applications are typically accessed using OnDemand:

- **Resident client/server applications**, such as Internet e-mail applications (including Microsoft Outlook, Outlook Express, Lotus Notes, Netscape Mail, and Eudora), terminal emulation applications (such as WRQ Reflection and NetManage RUMBA PC-to-Host), and remote office connectivity applications (including Citrix ICA/MetaFrame, and Microsoft Windows Terminal Services). Typically, these client applications are installed locally on the client computer. Note that OnDemand supports Microsoft Outlook 2000 and Outlook XP.

- **Downloadable thin client applications**, such as terminal emulation programs (including Attachmate myEXTRA! Terminal Viewers, NetManage RUMBA Web-to-Host, and WRQ Reflection for the Web) and remote office connectivity applications (Citrix ICA client for Java, and Microsoft Windows Terminal Services Advanced Client). Thin client applications are typically Web-based applications that incorporate Java applets or ActiveX controls.

**Notes**

- OnDemand does not support UDP-based applications.

**OnDemand Redirection Modes**

By default, Aventail OnDemand starts automatically when users log in to ASAP WorkPlace. AMC also provides an option to manually start Aventail OnDemand when the user clicks a link in ASAP WorkPlace.

OnDemand has two modes of operation: Dynamic mode enables Windows users to access any network application, and mapped mode enables users to click a shortcut that is configured for a specific application. You can also disable OnDemand access entirely.

- **Dynamic mode.** In dynamic mode, OnDemand automatically redirects traffic for all network resources defined in AMC. In this mode, the user manually starts the desired application. Dynamic mode is supported on Windows only and requires administrator rights.
• **Mapped mode.** In mapped mode, OnDemand redirects traffic for specific network applications. Optionally, you can configure OnDemand to automatically launch a specified Web URL when users click a shortcut. This is useful for starting an application (such as a thin client application) when OnDemand runs. Note that you must manually create any shortcuts to specific applications. Mapped mode is supported on Windows, Macintosh, and Linux.

On Windows PCs, when a user logs in to ASAP WorkPlace for the first time, WorkPlace automatically downloads, installs, and launches OnDemand on the user’s computer. On subsequent WorkPlace logins, WorkPlace automatically starts OnDemand. However, you can disable this automatic startup and instead include a link that enables users to manually start OnDemand in dynamic mode.

## Activating OnDemand

By default, when Aventail OnDemand is enabled, OnDemand starts automatically when users log in to ASAP WorkPlace and runs within the WorkPlace window. Users must keep the WorkPlace window open while working with OnDemand in this embedded mode.

You can also configure OnDemand to run in stand-alone mode, which causes OnDemand to open in a separate window when a user clicks a link to start OnDemand; users can close the ASAP WorkPlace window without affecting OnDemand. The user can minimize the OnDemand window, but should not close it while working on the network—doing so will terminate any application connections and will log the user out of OnDemand. When the user has finished working, he or she can log out of OnDemand by closing the OnDemand window.

The following table summarizes the ways in which OnDemand can be activated.

<table>
<thead>
<tr>
<th>Activation mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded in ASAP WorkPlace</td>
<td>OnDemand runs transparently in the main WorkPlace window. The user must keep the WorkPlace window open while using OnDemand. Information about the OnDemand connection is displayed in the Connection status area.</td>
</tr>
<tr>
<td>Stand-alone agent</td>
<td>OnDemand runs in a separate window. The user can close the WorkPlace browser window and the OnDemand applet will continue to run. Information about the OnDemand connection is displayed in a separate Details window.</td>
</tr>
</tbody>
</table>

### Notes

- Users cannot start an application from the OnDemand window. Unless you configure a URL to launch automatically when users start OnDemand, users must manually start applications as they would normally.
- Users may need to configure their personal firewalls to allow OnDemand traffic.

## OnDemand Client Requirements

OnDemand requires a Web browser configured with a Java Virtual Machine (JVM). OnDemand supports the following client configurations.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web browser</th>
<th>Java Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP, Windows 2000 Professional, Windows 98 SE</td>
<td>Microsoft Internet Explorer 6.0 (Service Pack 1)</td>
<td>Microsoft VM for Java 5.0, Release 5.0.0.3810 (based on Sun JVM 1.1.4) Sun JVM 1.4.2_05 plug-in</td>
</tr>
<tr>
<td>Windows XP, Windows 2000 Professional, Windows Me, Windows 98 SE</td>
<td>Mozilla 1.7</td>
<td>Sun JVM 1.4.2_05 plug-in</td>
</tr>
</tbody>
</table>
When planning an OnDemand stand-alone deployment, consider the technology used for the client application. For example, an application based on Microsoft’s ActiveX technology won’t run on Macintosh or Linux systems, or on Netscape for Windows.

### How OnDemand Redirects Network Traffic

OnDemand uses the local loopback address to redirect and secure traffic through the appliance. This section provides an overview of loopback proxying and describes the various redirection methods.

#### Overview: Loopback Proxying

OnDemand uses local loopback proxying to securely submit application traffic through the Aventail client/server access service. For example, suppose a Windows user wants to connect to the appliance and run a Citrix application:

1. The user logs in to ASAP WorkPlace, and OnDemand automatically starts in dynamic mode.
2. OnDemand dynamically maps the local loopback address to the host name for the Citrix server.
3. The user runs the Citrix application, which attempts to connect to `citrix.example.com`.
   OnDemand resolves the Citrix host name to 127.0.0.1 and routes the traffic to the client/server access service.
4. OnDemand encrypts the Citrix traffic using SSL and securely routes it to the Aventail appliance, which in turn forwards it to the Citrix server.
5. The Citrix server responds, sending data back through the Aventail appliance.
6. The appliance forwards the response to OnDemand over SSL.
7. OnDemand forwards the information to the Citrix application.

OnDemand supports several redirection methods. The method you choose typically depends on the profile of your end users (including the operating systems in use and their local system privileges).

#### Dynamic Mode

On Windows systems, OnDemand can dynamically redirect traffic to any destination resources (such as a domain, host, or IP address) that are defined in AMC. When run in this mode, OnDemand inserts itself into the transport layer of the TCP/IP protocol and dynamically redirects traffic as needed.

Dynamic mode is automatically enabled for Windows users; you do not need to configure specific ports or loopback addresses for individual applications. This approach is convenient to administer and widely used in homogeneous Windows environments. For more information, see “Enabling OnDemand Dynamic Mode Access” on page 206.

Note that the user must have administrator privileges on the local computer to use OnDemand in dynamic mode.
Hosts File Redirection

Another option is to modify the hosts file on the user’s computer to redirect traffic to the destination server. This redirection method is supported on Windows, Macintosh, and Linux platforms.

Modifying the hosts file on an end-user’s system maps a destination server to a local loopback address. When an application attempts to resolve a host name, traffic is redirected to the loopback address on which OnDemand is listening.

The following example shows a typical hosts file, with host names mapped to IP addresses, followed by a hosts file modified for use by OnDemand. Notice that the OnDemand host names are mapped to the local loopback address, not the host’s IP address. For application-specific configurations, these loopback addresses would match the addresses you specify when configuring OnDemand in AMC; for more information, see “Configuring OnDemand to Access Specific Applications” on page 207.

<table>
<thead>
<tr>
<th>Typical Hosts File</th>
<th>OnDemand Hosts File</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.135 telnet.example.com telnet</td>
<td>127.0.0.1 telnet.example.com telnet</td>
</tr>
<tr>
<td>192.168.1.140 mailhost.example.com mail</td>
<td>127.0.0.1 mailhost.example.com mail</td>
</tr>
<tr>
<td>192.168.1.143 citrix.example.com citrix</td>
<td>127.0.0.1 citrix.example.com citrix</td>
</tr>
</tbody>
</table>

Note that the user must have administrator privileges on the local computer to rewrite the hosts file. This approach may not be practical for mobile users, because they need to switch between their original hosts file and OnDemand hosts file, depending on whether they’re working on the local network or from a remote location.

Managing the Local Hosts File

To use hosts file redirection, you will need to distribute a modified hosts file, or have users manually modify the hosts file themselves (which may not be practical for non-technical users). Use caution, because an invalid hosts file can cause connectivity problems. The hosts file location varies, depending on your operating system:

- **Windows** The hosts file—a text file named hosts, with no file extension—location varies depending on the version of Windows you’re using:
  - Windows XP Home c:\windows\system32\drivers\etc
  - Windows 2000 or Windows XP Pro c:\winnt\system32\drivers\etc
  - Windows 98 or Windows Me c:\windows

- **Macintosh** On OS X you can edit the /etc/hosts file in a text editor, or use the NetInfo Manager application to modify a local database of host entries.
  
  On Macintosh OS 9.x, hosts entries can be loaded through the TCP/IP Control Panel when in the Advanced User Mode. The format of the file differs from that shown in the previous example; Macintosh OS 9 requires the format hostname A address (for example, mailhost.example.com A 127.0.0.1).

- **Linux** The Linux hosts file information is in the /etc/hosts file.

Other Redirection Options

Most OnDemand deployments are managed using dynamic mode or by rewriting the local hosts file. However, if neither of these methods is feasible, there are other redirection alternatives:

- **Use split DNS.** With split DNS, you modify your public DNS to resolve a server’s FQDN to the loopback address, and leave your internal DNS unmodified (pointing to the FQDN). This approach provides the advantage of centralized control over application mappings. On the downside, however, it exposes private host names and may be difficult for you to manage if you don’t administer your company’s DNS. See “Using Split DNS” on page 320 for more information.
• **Access applications using the loopback address.** Instead of accessing an application using its host name or IP address, you can have the user run it by accessing the local loopback address. This approach is practical only for technically sophisticated users.

• **Modify the application configuration.** Here, you modify the client application configuration to point to the loopback interface instead of to the server host name or IP address. See “Configuring Client Applications” on page 321 for more information.

### Enabling OnDemand Dynamic Mode Access

For users running Windows, OnDemand automatically redirects all connections to destination addresses that match the network resources (domains, subnets, IP ranges, host names, or IP addresses) you define in AMC. You do not need to perform any application configuration—such as defining specific ports or loopback addresses—in AMC to use this dynamic mode.

**To enable OnDemand dynamic mode access**

- When configuring realm settings on the Configure Realm page, in the Access methods area, under **Client/server access with Aventail OnDemand**, select the **Enable Aventail OnDemand** and **Dynamically redirect connections** check boxes.

You can view a list of all defined network resources that users will be able to access through OnDemand in dynamic mode.
To view resources that users can access through OnDemand

- On the Configure OnDemand page, in the Dynamic mode area, click Show network redirection list. The Redirection List page appears and displays a list of all defined network resources that users will be able to access through OnDemand in dynamic mode.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM Application</td>
<td></td>
</tr>
</tbody>
</table>

Notes

- Dynamic mode is available only on Microsoft Windows operating systems, and is not supported on Macintosh or Linux.
- A user must have administrator privileges on his or her computer to use OnDemand in dynamic mode. If your users don’t have administrator privileges, you should configure OnDemand in mapped mode and choose a different method of redirection.
- It is not possible to configure dynamic mode to launch a Web page when OnDemand starts. To automatically start an application when OnDemand starts, you must configure OnDemand in mapped mode for a specific application.

Configuring OnDemand to Access Specific Applications

If you are deploying OnDemand to users on non-Windows platforms, or want to automatically use the launch URL feature to start a thin client application when users run OnDemand, you must define an application-specific configuration in AMC. This involves mapping the port numbers for the client and server, a process called "port mapping."

Overview: Port Mapping

To configure OnDemand to redirect traffic for a specific application, you need to know the port numbers the application uses for the client and server, and then map those ports in AMC. OnDemand listens for incoming requests on specific ports on the client and then proxies them to the appliance, which forwards the information to an IP address and port on the application server.

For example, you might configure an IP address and port on the client (such as 127.0.1.1:23) to the host or IP address and port on the destination server, such as telneta.example.com:23.
Some applications—such as e-mail—use multiple ports for different protocols. In this case, you must configure OnDemand to listen on several different ports. This configuration can also be useful for configuring OnDemand to work with several different applications. The following example shows OnDemand configured to work with three applications over five different ports.

In some situations, the process of port mapping may be more complicated:

- Macintosh operating systems enable only a single loopback address, 127.0.0.1. If you are deploying to Macintosh users, you must map all network services to the single localhost IP address of 127.0.0.1. If you have services running on different ports—for example, a telnet and an e-mail host—you could map both to 127.0.0.1 by specifying a different port number, like this:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1:23</td>
<td>telnet.example.com:23</td>
</tr>
<tr>
<td>127.0.0.1:110</td>
<td>mail.example.com:110</td>
</tr>
</tbody>
</table>

- On Macintosh OS X and Linux, mapping “well-known ports” (from port number 0 through 1023 inclusive) is a privileged operation that can be done only by users with administrator or root privileges. If you have Macintosh OS X or Linux users that do not have these privileges, you will need to use local loopback ports above 1023 to allow OnDemand to proxy traffic.

- You can have only one service listening on a given port number at any given time. For example, if you have two different telnet hosts on your network, OnDemand can have only one port listener for port 23 on 127.0.0.1. In this case, you would need to use different port numbers on the local loopback and the destination host:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1:2021</td>
<td>telneta.example.com:23</td>
</tr>
<tr>
<td>127.0.0.1:2023</td>
<td>telnetb.example.com:23</td>
</tr>
</tbody>
</table>

Notice that the destination port is mapped to ports 2021 and 2023, while the source ports are both mapped to port 23. This configuration would require you to perform additional configuration:

1. Modify the telnet applications on users’ computers to use the new mapped ports 2021 and 2023 for the telneta and telnetb hosts.

2. In AMC, configure the ports as you normally do (map the source address and port on the client to the destination server’s address and port).

Several entries will be added to the local hosts file. These entries map each destination server to the same loopback address:
• Each local address maps to a single destination address; you cannot map address ranges (although you can map a range of individual addresses one by one).

**Configuring an Application for Use With OnDemand**

If you are deploying OnDemand to users on non-Windows platforms, or want to provide a WorkPlace link that starts a thin client application, you must define an application-specific configuration in AMC. This involves mapping the port numbers for the client and server, a process called “port mapping.”

To configure an application, you’ll need to know the protocols it uses for each service and map the source address and port(s) on the client to those on the destination host. You also have the option of specifying a URL to open a Web page (useful for automatically starting an application) when the user runs OnDemand.

**To configure an application for use with OnDemand**

1. On the main navigation menu of AMC, click **Aventail OnDemand**. The **Configure OnDemand** page appears.
2. In the **Mapped mode** area, click the **New** button. The **Mapped Mode** page appears.

![Mapped Mode](image)

For each service used by the application, you must map the local host address to the destination resource and specify local and destination port numbers. Note that mapping a local port to a number less than 1024 is not supported on all operating systems.

3. In the **Application name** box, type the name to use for the application. This name is displayed to the user in ASAP WorkPlace. Use a short but descriptive name.

4. In the **Description** box, type a descriptive comment about the application.

5. Configure each service used by the application in the **Add mapping** area.
   a. Click the **Edit** button beside the **Destination resource** box, select the network resource you want to configure, and then click **Save**. Alternatively, you can create a new network resource by clicking the **New Resource** button in the **Resources** dialog box.
   b. If the IP address/port combination of the service conflicts with that of another service, you can modify the IP address displayed in the **Local host** box, or you can map the ports as described below. You can change the **Local host** value to any IP address in the 127.x.y.z address space.
   c. In the **Service type** box, click the type of service used by the application. Clicking a service type populates the **Destination/local ports** boxes with the well-known port for that service.
   d. Click **Add to Current Mapping**. This adds the mapping to the **Current mapping** list.

6. If the application uses multiple services, repeat step five to configure each one. Most applications use only one service, but applications that use multiple protocols (such as e-mail) have multiple services.
7. Select the **Create shortcut on ASAP WorkPlace** check box.

If you want OnDemand to open a Web page automatically (which is useful for automatically starting a thin client application), type the URL of the appropriate page in the **Start an application by launching this URL** box. Note that you must specify either an `http://` or an `https://` protocol identifier.

The URL you specify automatically opens in a new browser window after OnDemand loads.

**Notes**
- After you initially configure the **Create shortcut on ASAP WorkPlace** option, you can only view its setting on the **Mapped Mode** page; you cannot edit it on this page. After initially configuring this setting, shortcuts are managed from the **WorkPlace Shortcuts** page in AMC. For more information, see “Working with Shortcuts” on page 190.

**Configuring the OnDemand Activation Mode**

When OnDemand is embedded in ASAP WorkPlace, OnDemand runs transparently in the main WorkPlace window; no separate OnDemand window appears. The user must keep the WorkPlace window open while using OnDemand.

When you configure OnDemand as a stand-alone agent, OnDemand runs in a separate window. The user can close the WorkPlace browser window and the OnDemand applet will continue to run.

**To configure the OnDemand activation mode**

1. When configuring realm settings on the **Configure Realm** page, in the **Access methods** area, under **Client/server access with Aventail OnDemand**, select the **Enable Aventail OnDemand** check box.

2. To embed OnDemand in WorkPlace, select the **Embed Aventail OnDemand agent in WorkPlace** check box. To configure OnDemand as a stand-alone agent, clear this check box.
Chapter 10 - Configuring User Access Components

Configuring Advanced OnDemand Options

This section describes how to access the appliance using its external IP address and add debug messages to the OnDemand logs.

Accessing the Appliance Using Its External IP Address

By default, OnDemand accesses the appliance using the FQDN contained in the appliance's SSL certificate. This works fine in a production environment—where the FQDN is added to public DNS—but may be an issue in a test environment for one of two reasons:

- You have not added the FQDN for the appliance to DNS.
- The external IP address does not match the external network address on the appliance because your environment uses Network Address Translation (NAT).

In either case, you will need to configure OnDemand to use the IP address for the external network interface.

To configure OnDemand to use the appliance's external IP address

1. From the main navigation menu in AMC, click Aventail OnDemand, and then click to expand the Advanced area.
2. In the Appliance FQDN or IP address box, type the IP address for the external network interface.

Before moving the appliance into production, make sure this value contains the FQDN from the appliance's SSL certificate. Whenever you update the appliance's SSL certificate, AMC automatically inserts the FQDN in this field (overwriting any value you've previously specified).

The first time a user starts OnDemand, the Web browser displays a security warning asking the user to grant permissions to run the OnDemand applet. For information on configuring the browser, see "Suppressing the Java Security Warning" on page 322.

Adding Debug Messages to the OnDemand Logs

You can log debug messages to the OnDemand logs. Normally, the OnDemand logs show only information and warning messages. This should be used for troubleshooting purposes only.

To add debug messages to the OnDemand logs

1. On the main navigation menu in AMC, click Aventail OnDemand, and then click to expand the Advanced area.
2. Select the Enable debug OnDemand log messages check box.

Client Configuration

This section explains client-side configuration that may be useful for working with OnDemand.

Suppressing the Java Security Warning

When OnDemand starts, the Web browser displays a security warning asking the user to grant permissions to run the OnDemand applet. This warning will vary depending on the operating system and browser. The user must accept this certificate to run OnDemand.
OnDemand includes a Java code-signing certificate that ensures the validity of the applet. For Windows and Macintosh OS X, the certificate includes a Class 3 Digital ID from VeriSign (which is widely used by commercial software publishers). Because Macintosh OS 9.2 doesn’t support certificates signed by third-party organizations, OnDemand includes an Aventail-signed digital ID. This digital ID is signed as follows: Aventail, Java Object Signing Digital ID, APG, Aventail Corp., USA.

To prevent the security prompt from appearing each time OnDemand is started, users can configure their systems to trust the Aventail certificate. Once this is done, the browser trusts all subsequent software downloads from Aventail. The following table explains how the user can configure common browsers to trust the Aventail certificate:

<table>
<thead>
<tr>
<th>Web browser and platform</th>
<th>To configure the browser, the user should:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer for Windows (Microsoft JVM)</td>
<td>Select the <strong>Always trust content from Aventail Corporation</strong> check box and then click the <strong>Yes</strong> button.</td>
</tr>
<tr>
<td>Internet Explorer for Windows (Sun JVM)</td>
<td>Click the <strong>Grant Always</strong> button.</td>
</tr>
<tr>
<td>Netscape Navigator for Windows</td>
<td>Select the <strong>Remember this decision</strong> check box and then click the <strong>Grant</strong> button.</td>
</tr>
<tr>
<td>Internet Explorer for Macintosh OS X</td>
<td>Click the <strong>Grant Always</strong> button.</td>
</tr>
<tr>
<td>Internet Explorer for Macintosh OS 9.2</td>
<td>Select the <strong>Trust this signer always</strong> check box and then click the <strong>Yes</strong> button.</td>
</tr>
</tbody>
</table>

**Configuring a Proxy Server in the Web Browser**

When passing an outbound connection over a proxy server, OnDemand uses the Web browser’s settings to determine the proxy server address and port. This configuration requires the user to configure his or her Web browser, either by specifying the outbound proxy server address and port or by enabling automatic proxy detection.

If a user enables both automatic proxy detection and manual proxy identification, OnDemand checks for proxy server settings in this order:

1. **If the Automatically detect settings** option is enabled, OnDemand attempts to automatically detect the proxy server settings.
2. **If OnDemand is unable to automatically detect the proxy server settings,** it checks for an automatic configuration script if the browser’s **Use automatic configuration script** option is enabled.
3. If OnDemand is unable to detect the proxy server settings through the configuration script, it uses the proxy server settings that the user manually specified.

► To configure automatic proxy detection in Internet Explorer for Windows
   1. On the Tools menu, click Internet Options.
   2. On the Connections tab, click LAN Settings.
   3. Under Automatic Configuration, enable one or both of the options:
      - To automatically detect proxy-server settings, select the Automatically detect settings check box. (Note that this option is supported only for users running Internet Explorer with the Microsoft Virtual Machine.)
      - To use configuration information contained in a configuration file, select the Use automatic configuration script check box and then, in the Address box, type the URL or path for the configuration file.

► To manually specify proxy server settings in Internet Explorer for Windows
   1. On the Tools menu, click Internet Options.
   2. On the Connections tab, click LAN Settings.
   3. Under Proxy Server, select the Use a Proxy Server check box, and specify the IP address and port for the proxy server in the Address and Port boxes.
      Or, if a different proxy server is used for different protocols, click Advanced and specify the necessary information; be sure to specify proxy servers for both HTTP and Secure.

⚠️ CAUTION Enabling either of the automatic settings in the LAN Settings dialog box (the Automatically detect settings check box or the Use automatic configuration script check box) may override the proxy server settings; clear these two check boxes to ensure that proxy detection works correctly.
Chapter 11
Installing and Administering a Cluster

The Aventail appliance includes support for clustering two identical appliances behind one virtual IP address. An Aventail cluster provides high availability by including integrated load balancing, stateful user authentication failover, and centralized administration.

This section explains the capabilities of an Aventail cluster and describes the required procedures for installing, configuring, and maintaining a cluster.

Overview: An Aventail Cluster

A cluster is designed to prevent a single point of failure. When you deploy a cluster, you can distribute applications over more than one computer, which improves response time and avoids unnecessary downtime if a failure occurs. The cluster appears as a single system to users, applications, and the network, while providing a single point of control for administrators.

The Aventail appliance supports a two-node cluster, which provides support for up to 1,000 users in a high-availability configuration. This cluster supports an Active/Active configuration, meaning both nodes in the cluster are actively sharing the user load at any given time.

Cluster Architecture

There are two configurations in which you can deploy an Aventail cluster—a dual-interface configuration or a single-interface configuration. See "Network Architecture" on page 9 for details on these configurations. When deploying a cluster in either configuration, the two appliances must be connected to one another over the cluster network. Connecting the cluster interface of one appliance with the cluster interface of the other creates a private network over which the two cluster nodes can communicate (for state synchronization, credential sharing, and load balancing).

Regardless of the deployment scenario, the following connectivity requirements apply:

- To provide load-balancing redundancy, both nodes in the cluster must serve as load-balancing nodes. Thus, both nodes must be connected to the network switch facing the Internet.
- To communicate with internal resources, both nodes in the cluster must be connected to the network switch facing the intranet (this would be the same as the external switch in a single-interface configuration).
- As described above, both cluster nodes must be connected to each other via the cluster interface.
In a dual-interface configuration, the cluster architecture would look like this:

![Dual-Interface Configuration Diagram]

In a single-interface configuration, the cluster architecture would look like this:

![Single-Interface Configuration Diagram]

### The Load Balancing Service

The Aventail cluster contains integrated load balancing, eliminating the need for an external load balancer. This internal load-balancing service is responsible for two key functions:

- It distributes connections across the two nodes by sending an incoming request to the node that currently has the least number of connections.
- It contains an internal monitoring service that detects node failure and performs the failover of that node’s remote connections to the other node in the cluster. In the event of node failure, it directs all incoming requests to the other node until the failed node returns to service. It then continues distributing connections between the two nodes.

The load-balancing functionality exists on only one node at a time—the active load-balancing node. The other node serves as a redundant load balancer and takes over the load balancing responsibilities if the active load balancer goes down. This redundant node thus becomes the active load balancer, and remains so even after the failed node returns to service. The active load balancing node communicates with the standby load balancing node over the private cluster network (see “Cluster Architecture” on page 215).

### Stateful Failover

The cluster provides stateful user authentication failover (authentication credentials are shared in real time in a memory cache shared by all nodes). Because both nodes are synchronized, they are capable of handling the failover of connections initiated by the active load-balancing node without requiring the user to reauthenticate.

The cluster does not provide stateful application session failover. Disruption to users is dependent upon the TCP/IP disconnect tolerance of the applications that they are using at the time the failover occurs.
**Synchronized Cluster Administration**

You administer both nodes of an Aventail cluster from one master AMC. After installing the software on both nodes, you log in to AMC on one of the nodes and assign it as master. From that point on, this node controls the propagation and synchronization of policy and configuration across both nodes. If you log in to AMC on the slave node, its **Node Administration** page appears, displaying a message telling you that it is not the master node (it also displays status information about the services on the slave node).

Each node in the cluster hosts configuration and policy data stores. The master node, which communicates with the slave node via the cluster interface, synchronizes this data as follows:

- When you add a second node to a cluster, the master node provisions the new node with configuration data, after which the new node starts up its access services.
- When you apply a configuration change on the master node, AMC propagates the change to the slave node.

The slave node provides a redundant AMC, but it is not automatically assigned as master if the master node fails. Instead, you must log in to the slave node's AMC and manually assign it to be the master. When the original master node comes back online, it detects that the other node is now the master and it demotes itself to a slave node.

⚠️ **CAUTION** If you are upgrading the software on the master node, do not assign the slave node as master while the original master node is down. Doing so would prevent the upgraded node from running because it would be rejected by the other node (because of a version mismatch). Restoring the full cluster would require downtime for your users while you upgraded the second node.

For a step-by-step description of what happens when a master node fails, see "Master (AMC) Node Fails" on page 227. For detailed procedures on how to manage the cluster using the master AMC, see "Managing the Cluster" on page 222.

**Installing and Configuring a Cluster**

Installing an Aventail cluster requires rack-mounting both appliances, connecting the cluster interface between the two appliances, running Setup Tool on each appliance, promoting one node to master, and then configuring the cluster's virtual IP address (VIP). The following diagram illustrates the workflow:

1. **Connect the nodes**: Connect the crossover cable to the “HA-3” NIC.

2. **Run Setup Tool on each node**: Specify the same cluster name, but unique node IDs.

3. **Assign one node as "master"**: Log in to AMC on the node you want to assign as master.

4. **Configure the cluster settings**: Configure the VIP and enable external interfaces (optional).

Before installing and configuring your Aventail cluster, it will be helpful to gather the following information:

**IP Addresses for a Dual-Homed Installation**

- Six IP addresses, one for each node's internal, external, and cluster interfaces.
- One virtual IP address (VIP) for the cluster. The VIP, which serves as the single external address for the entire cluster, must be on the same subnet as the external interface.
IP Addresses for a Single-Homed Installation

- Four IP addresses, one for each node’s internal and cluster interfaces.
- One virtual IP address (VIP) for the cluster. The VIP, which serves as the single external address for the entire cluster, must be on the same subnet as the internal interface.

Cluster and Node Names

- A unique alphanumeric name for the cluster (must begin with an alphabetical character)
- Two unique alphanumeric names, one for each node ID (must begin with an alphabetical character)

Step 1: Connect the Cluster Network

Before running Setup Tool, you must connect the cluster network between the two nodes of the cluster.

To connect the cluster network

1. Find the network crossover cable supplied with the appliance.
2. Use this cable to connect the cluster interface on one appliance with the cluster interface on the other appliance. See “Connecting the Appliance” on page 17.

Step 2: Run Setup Tool on Both Nodes of the Cluster

Setup Tool is a command-line utility that performs the initial network setup for an appliance. Details about running this tool in a single-node environment are explained in “Performing Initial Network Setup” on page 18. When installing a cluster, you should run Setup Tool on one appliance, and then repeat the process on the second appliance. You should also review “Tips for Working with Setup Tool” on page 18 before continuing.

To run Setup Tool in a clustered environment

1. Make a serial connection to one appliance in the cluster, confirm that the cluster network between the two nodes is connected, and then turn on one appliance using the power button on the front panel. Setup Tool automatically runs on the appliance (you can also invoke it by typing `setup_tool`).
2. When you’re prompted to log in, type “root” for the username.
3. The Aventail EULA appears. It scrolls over several screens; press ENTER to move to the next screen or press `q` to move to the end.
   Do you accept the terms of the license agreement? [n]:
   - If you accept the license agreement, type `y` and then press ENTER to continue.
4. You’re prompted to create a new root password for the system (it will also be used to access AMC).
   Password:
   - Your password must contain between eight and 20 characters, and is case-sensitive. We recommend that you create a “strong” password using a combination of uppercase and lowercase letters and numbers, and avoid using words found in a dictionary. Be sure to record your password somewhere and keep it secure. If you lose your password, Aventail Support cannot recover it. Press ENTER to continue.
   Confirm password:
   - Retype the root password exactly as entered previously (it is case-sensitive) and then press ENTER to continue.
5. Next, you’re asked to enter an IP address, subnet mask, and (optionally) a gateway for the internal interface. You’ll use this interface to connect to the appliance from a Web browser and continue setup using AMC.
   IP address:
• Type an IP address for the internal interface connected to your internal (or private) network and then press ENTER.

Subnet mask:
• Type a netmask for the internal network interface and then press ENTER.

Gateway:
• If the computer from which you’ll access AMC is on a different network than the appliance, you must specify a gateway. Type the IP address of the gateway used to route traffic to the appliance and then press ENTER.

If you’re accessing AMC from the same network on which the appliance is located, simply press ENTER.

6. Next, you’re prompted to review the information you provided. Press ENTER to accept the current value, or type a new value.

7. You are then asked if this node will be part of a cluster.

Install node in a cluster? [n]:
• Type y and then press ENTER to continue.

8. Next, you are asked to enter the cluster name. This name must be alphanumeric and must begin with an alphabetical character.

Cluster name:
• Type the cluster name for this cluster and then press ENTER.

CAUTION When entering the cluster name for the second node, make sure it is identical to the name entered for the first node. If these names differ, the cluster will not function as a cluster. Note that these names are case-sensitive.

9. Next, you are asked to enter a node ID for this appliance. Node ID names must also be alphanumeric and must begin with an alphabetical character. AMC uses this node ID to identify a specific appliance. You will see it displayed on several AMC pages.

Node ID:
• Type a unique node ID for this appliance and then press ENTER.

CAUTION When entering the node ID for the second node, make sure that it differs from the node ID for the first node. If these IDs are the same, the nodes will be unable to join in a cluster. Note that these names are case-sensitive.

10. Next, you are asked for the IP address and subnet mask of the cluster interface. This interface is used for communication between the two nodes of the cluster.

Cluster interface IP address:
• Type the cluster interface IP address for this appliance and then press ENTER.

Cluster interface subnet mask:
• Type the cluster interface subnet mask for this appliance and then press ENTER.

CAUTION When entering the cluster interface IP address for the second node, make sure that it differs from the cluster interface IP address for the first node. Each cluster interface IP address must be unique. Also, when entering the cluster interface IP address, make sure that the network range or subnet used for the cluster interface is not the same as any other interface’s network range. The cluster interface network range must be unique.

11. Next, you’re prompted to review the information you provided. Press ENTER to accept the current value, or type a new value.

12. Finally, you’re prompted to save and apply your changes.

Do you want to save and apply configuration changes [y]:
• Press ENTER to save your changes.

At this point, Setup Tool saves your changes and restarts the necessary services. It also generates Secure Shell (SSH) keys using the information you provided.
During this time, you will receive minimal feedback; be patient and do not assume that Setup Tool is not responding.

When the changes are complete, a message appears indicating that the initial setup is complete.

13. After running Setup Tool on the first node, repeat the process for the second node.

**Step 3: Assign the Master Node**

After running Setup Tool on both appliances, you need to assign one appliance to be the master node. You will use AMC on the master node to administer the cluster.

**CAUTION** Do not assign a node to be the master until you have run Setup Tool on both nodes, especially if you’re configuring dual-homed nodes. Both nodes must be configured with the same number of interfaces; otherwise the cluster will not function properly. So it is important that you avoid configuring interfaces via AMC until you have run Setup Tool on both nodes.

**To assign the master node**

1. Log in to AMC on the node that you want to be the master. For details on logging in, see “Logging In to AMC” on page 21. AMC automatically displays the Node Administration page.

```
Node Administration

Use this page to monitor and administer a node on an Aventail cluster.

Node name: space
Cluster name: mountains
Cluster last synchronized: N/A

No master is assigned for this cluster.
Once you assign a master, the cluster will be synchronized.

Node Status

Services
Client/server access service Running
Web access service Running
ASAP WorkPlace access service Running

System information
ASAP version: 8.0.0-69
Time since last reboot: 0 Days 1 Hours 59 Minutes 22 Seconds
System time: Thu Sep 28 23:00:04 GMT 2006
CPU usage: 0 %
Disk space utilization: 1 % of 8.16 GB
Swap space utilization: 0 % of 972 MB

Current connections
0 client/server (TCP/IP) connections
0 Web (HTTP/S) connections

Node management

If you want to manage the cluster from this node, you can assign it as the master of the cluster.

Assign as master
```

2. Under Node management, click Assign as master. You are then redirected to the AMC home page on this node.
Step 4: Configure the Cluster’s Virtual IP Address

The cluster’s virtual IP address serves as the single external address for the entire cluster.

To configure the cluster’s virtual IP address
1. From the main navigation page, click **Network Settings**.
2. On the **Network Settings** page, click the **General** tab.
3. In the **Cluster configuration** section, type the cluster’s **Virtual IP address**. This must be on the same subnet as the IP address for the interface connected to the Internet (internal interface in a single-homed configuration, external interface in a dual-homed configuration).

Step 5: Perform the Remaining Configuration Tasks

Now that the software is installed on both nodes and one AMC is serving as the master management console, you are ready to complete the remaining configuration tasks. There is little difference in configuring a single-node appliance and a cluster. The primary differences when configuring a cluster are as follows:

- Both nodes of the cluster appear on the **Network Settings** page of AMC. In a single-node environment, only one node appears here.
- The **Cluster interface settings** section that you used in the previous step appears. This section is not present in a single-node deployment.
- On the **Network Interface Configuration** page, you cannot edit the name of the appliance, which is actually the node ID. In a single-node deployment you can edit the appliance name.

Continue with your cluster configuration by turning to “Network and Authentication Configuration” on page 31, and then return to this procedure for the final step.

Notes

- If you plan to enable the external interfaces, you must enable them for both nodes at the same time (in other words, AMC prevents you from applying the configuration change until you have enabled the interface for both nodes).

Step 6: Configure the Managed Switch Connection (if applicable)

If you are using a switch connection that supports the 802.1d spanning-tree protocol, you must designate which interfaces should be monitored for failover. You must configure all your network interfaces before performing this step. See “Step 5: Perform the Remaining Configuration Tasks” on page 221.

This setting can provide more reliable failover capabilities, and should be enabled if supported in your network environment. In most test environments, you won’t need to enable this setting, but it is important that you do so whenever possible in a production environment. Note that this setting is disabled by default.

**CAUTION** Do not enable this setting unless you are using a managed switch that is enabled for the 802.1d spanning-tree protocol. If you erroneously enable this setting, the master node will be unable to detect the existence of the slave node.
To configure the managed switch connection

1. From the main navigation page, click Network Settings. The Network Settings page appears.
2. Click the General tab.
3. In the Cluster configuration section, select the appropriate setting for Check for managed switch connection on. This setting is disabled by default. To enable this setting, select the interfaces that are managed by the switch.

Managing the Cluster

You can perform most cluster management tasks from a single AMC—the AMC that has been designated as the master. The procedures in this section provide details on how to manage your cluster.

Viewing and Configuring Network Information for Each Node

From the master AMC, you can view and configure network interface settings for both nodes in the cluster.

To view network interface configuration settings

1. From the main navigation page, click Network Settings.
2. Click the General tab.
3. The table in the Network interfaces section displays information about each of the two nodes. Each node is identified by its node ID. The master node displays (master) under its
node ID. To view the network interface configuration page for a particular node, click its name to display the **Configure Network Interfaces** page for the node.

<table>
<thead>
<tr>
<th>Configure Network Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage configuration for a network interface.</td>
</tr>
<tr>
<td>Appliance name: NODE1</td>
</tr>
<tr>
<td><strong>Internal interface (adapter 2)</strong></td>
</tr>
<tr>
<td>IP address: 10.10.10.171</td>
</tr>
<tr>
<td>Subnet mask: 255.255.0.0</td>
</tr>
<tr>
<td>Interface speed: Auto</td>
</tr>
<tr>
<td><strong>External interface (adapter 1)</strong></td>
</tr>
<tr>
<td>Enable external interface</td>
</tr>
<tr>
<td>IP address: 192.168.156.46</td>
</tr>
<tr>
<td>Subnet mask: 255.255.255.0</td>
</tr>
<tr>
<td>Interface speed: Auto</td>
</tr>
<tr>
<td><strong>Cluster interface</strong></td>
</tr>
<tr>
<td>IP address: 172.20.20.3</td>
</tr>
<tr>
<td>Subnet mask: 255.255.255.0</td>
</tr>
<tr>
<td>Interface speed: Auto</td>
</tr>
</tbody>
</table>

From this page, you can make configuration changes for each interface. For details on configuring these network settings, see "Configuring Network Interfaces" on page 32.

**Powering up a Cluster**

When powering up both nodes in a cluster, it does not matter which node you power up first.

**Starting and Stopping Services**

You use the master node to start and stop services in a cluster environment. For details on how to stop and start services, see "Stopping and Starting the Aventail Services" on page 155. You cannot control a service on a single node of the cluster, however. When you start or stop a service, the service starts or stops on both nodes of the cluster. To stop services on a single node of the cluster, you have to power down the appliance itself.

**Notes**

- The **Status** column on the master **Services** page indicates the status of the services on the master node only. See "Monitoring a Cluster" on page 224 for more information on monitoring a slave node.
Monitoring a Cluster

From the master node, you can monitor the services running on the master node only. To view the status of services on the slave node, you must log in to AMC on the slave node.

► To view the status of services on the master node
1. From the main navigation menu, click Services.
2. In the Access services area, view the Status indicators for each service. The value in this column indicates the status of the service on the master node.

► To view the status of services on the slave node
1. Log in to AMC on the slave node. The Node Administration page appears.

Node Administration

Use this page to monitor and administer a node on an Aventail cluster.

Node name:  egl500_2
Cluster name:  N/A
Cluster last synchronized:  Thu Oct 16 22:10:50

Node status

Services
Web access service  Running
Client/Server access service  Running
Aventail Workplace access service  Running

System information
Time since last rebuild  47 Days 23 Hours 29 Minutes 50 Seconds
System time  Thu Oct 16 22:12:50 GMT 2003
CPU usage  0%
Disk space utilization  52% of 814 GB
Swap space utilization  15% of 444 MB

Current connections
04 client/server (TOP/IP) connections
92 Web (HTTP/3) connections

2. In the Node status area, view Services, System information, and Current connections. This page also provides the timestamp of the last cluster synchronization.

3. To see the most current statistics, click the Refresh button.

Backing up a Cluster

To back up configuration data for a cluster, you run Backup Tool on the master node only. This will back up configuration data for both nodes. For details on running Backup Tool, see “Backing up the Current Configuration Using Backup Tool” on page 147.

Performing Maintenance on a Cluster

To perform maintenance on one or both nodes of a cluster, you must stop services on both nodes. You should plan all maintenance activities during a time that will be least disruptive to users. See “Starting and Stopping Services” on page 223 for details.

Upgrading a Cluster

To update the Aventail software in a cluster environment, you must run Update Tool on each node of the cluster. The order in which you update the nodes in the cluster is very important. There may be minimal disruption to service when performing the upgrade, so you should schedule it during a maintenance window.

► To upgrade a cluster
1. Run Update Tool on the master node first. For details on running Update Tool, see “Installing a System Update from the Command Line” on page 152. While the master node is updating, the slave node will continue servicing requests.
2. When the update to the master node completes and the master comes back online, it will notice that the slave node’s version differs from its own. It will stop the services on the slave node and will service all incoming requests itself.

3. Run Update Tool on the slave node.

4. When the update to the slave node completes and the slave node comes back online, it rejoins the cluster and is synchronized with the master node, and the load balancer becomes aware that both nodes are now available to service requests.

Notes

- After performing an upgrade, users may need to reauthenticate. New connections will not be affected, however.
- It’s recommended that you run Config Backup Tool before performing an upgrade. See “Backing up the Current Configuration Using Backup Tool” on page 147 for details.
- If you want to roll back a cluster version, follow the same procedure as for an upgrade.
- When changing cluster versions, it is very important that you begin the process with the master node. It is also important that you perform the procedure on both nodes of the cluster.

Upgrading a Single Appliance to a Cluster Configuration

If you have an appliance running as a single node and you want to upgrade it to be part of a cluster, you must run Cluster Tool. This tool allows you to reconfigure the appliance so that it is cluster-aware. Running the tool does not interrupt existing connections.

To run Cluster Tool

1. On the command line of the appliance, type `cluster_tool`.

2. You are asked to enter the cluster name. This name must be alphanumeric and must begin with an alphabetical character.

   Cluster name:
   - Type the cluster name for this cluster and then press ENTER, or if you want to keep the same cluster name, simply press ENTER.

   **CAUTION** Be sure to enter this name correctly. The cluster name must be identical on both nodes of the cluster; otherwise the nodes will not function as a cluster.

3. Next, you are asked to enter a node ID for this appliance. Node ID names must also be alphanumeric and must begin with an alphabetical character. AMC uses this node ID to identify a specific node. You will see it displayed on several AMC pages.

   Node ID:
   - Type a unique node ID for this appliance and then press ENTER.

4. Next, you are asked for the IP address and subnet mask of the cluster interface. This interface is used for communication between the two nodes of the cluster.

   Cluster interface IP address:
   - Type the cluster interface IP address for this appliance and then press ENTER.

   Cluster interface subnet mask:
   - Type the cluster interface subnet mask for this appliance and then press ENTER.

   **CAUTION** The cluster interface IP address of each cluster node must be unique.

5. Next, you’re prompted to review the information you provided. Press ENTER to accept the current value, or type a new value and then press ENTER.

6. Finally, you’re prompted to save and apply your changes.

   Do you want to save and apply configuration changes [y]:
   - Press ENTER to save your changes.
At this point, Cluster Tool saves your changes and restarts the necessary services. When the changes are complete, a message appears indicating that the appliance has been configured to be part of a cluster.

**Troubleshooting a Cluster**

This section explains how to troubleshoot various situations that may occur in a cluster environment.

**Avoiding Delays in Service if a Failover Occurs**

When a node transitions from STANDBY to ACTIVE or vice versa, its interfaces are briefly disabled as the switch checks to see if its ports are connected to another switch. You can configure your switch to skip these checks by enabling spanning-tree fast port negotiation. On Cisco switches, this functionality is known as *PortFast*.

**Cluster Error Messages**

When configuring a cluster, one or more of the following messages may appear in AMC if the associated error condition is encountered.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You are trying to cluster too many nodes (your system supports a maximum of two nodes).</td>
<td>A cluster can contain only two nodes. If you are configuring multiple clusters, confirm that the cluster names are unique.</td>
</tr>
<tr>
<td>Invalid configuration. Each node in the cluster must use the same number of network interfaces.</td>
<td>Both nodes in the cluster must be configured identically. If one node is dual-homed and the other node is single-homed, this message is displayed on the <em>Network Settings</em> page. If you try to apply changes without fixing this problem, the same message is displayed on the <em>Apply Changes</em> page and the button for applying changes is disabled.</td>
</tr>
<tr>
<td>You have specified a duplicate cluster IP address. Re-run Setup Tool and assign a different one.</td>
<td>The IP address of a node’s cluster interface must be unique.</td>
</tr>
<tr>
<td>You have specified a duplicate node ID. Re-run Setup Tool and assign a different one.</td>
<td>For the cluster to function properly, each node must have a unique ID.</td>
</tr>
<tr>
<td>The version of the software running on this node is incompatible with the master. Compare the version numbers and upgrade the appropriate node.</td>
<td>For the cluster to function properly, each node must be running the same version of the software. See “Upgrading a Cluster” on page 224 for more information.</td>
</tr>
</tbody>
</table>

**Cluster Scenarios**

This section provides a step-by-step view of how the cluster responds to various situations.

**Normal Flow of Traffic**

If both nodes are functioning properly, traffic flows through a cluster as follows:

1. An incoming request is routed to the cluster’s virtual IP address.
2. The active load balancer, which is monitoring the nodes in the cluster, determines that all nodes are available.
3. The load balancer checks to see which service currently has the least number of connections and routes the request to that service.

**Node Failure**

The following scenarios detail what happens if a cluster node fails. In most failure situations, the appliance will not require users to reauthenticate and existing user connections will continue operating normally. Service may be interrupted, however, if a particular application requires a user to reauthenticate.

**Active Load Balancer Fails**

If the active load balancer fails, the standby load balancer takes over as follows:

1. The active load balancer fails.
2. The standby load balancer, which is monitoring the cluster network, detects that the active load balancer has failed.
3. The standby load balancer resumes the active load balancing duties. It also routes all incoming requests to the single node that is available.
4. When the original active load balancer comes online, it becomes the standby load balancer.
5. The new active load balancer detects that the second node is online and begins distributing incoming requests to both nodes.

**Standby Load Balancer Fails**

1. The standby load balancer fails.
2. The active load balancer, which is monitoring the cluster network, detects that the standby load balancer has failed.
3. The active load balancer routes all incoming requests to the single node that is available.
4. When the standby load balancer comes online, the active load balancer begins distributing incoming requests to both nodes.

**Master (AMC) Node Fails**

These scenarios describe what happens with regards to AMC when the master node fails. In the first scenario, the original master remains the master. In the second scenario, the original master is demoted to slave.

**Original master remains master**

1. The master node fails.
2. The slave node continues functioning normally and the administrator does not assign the slave node to be the master.
3. The master node comes back online and recognizes that it is the master node.
4. The master synchronizes its state with the slave node’s state.
5. The master continues functioning as the master (with respect to administration, configuration, and synchronization).

**Slave node becomes master node**

1. The master node fails.
2. The administrator logs in to the AMC on the slave node and assigns it to be the master.
3. The original master comes back online, communicates with the other node, and determines that the other node is now master. The original master demotes itself to slave.
4. The new master synchronizes its state with the new slave node’s state.
Cluster Network Fails

If the cluster network fails, the two nodes of the cluster are no longer able to communicate with each other.

1. The active load balancer detects that the cluster network is down. It sends all incoming requests to the node on which it resides.
2. The master AMC detects that the cluster network is down. It can no longer communicate with the slave node.

Notes

- A symptom of a failed cluster network is if the slave node is running but the master node cannot communicate with it.
Appendix A
Troubleshooting

This section provides general troubleshooting instructions and discusses the troubleshooting tools available in ASAP Management Console (AMC). Note that failure in core networking services (such as DHCP, DNS, or WINS) will cause unpredictable failures.

General Networking Issues

- Check all network cables to be sure you don’t have a bad cable.

- If you’re using Network Address Translation (NAT), you might be blocked by a firewall. Temporarily bypass the firewall by connecting a laptop to the appliance on the physical interface using a crossover cable, and then verify network connectivity.

  If this type of connection is impractical, try placing your laptop on the same network segment as the external interface of the appliance (to get as close to the appliance as possible).

- Ping the external interface to verify the network connection. If you can ping a host’s IP address but not its fully qualified domain name, you probably have a name resolution problem. You can issue the ping command from the command line or from within AMC (see “Ping Command” on page 234).

- If you’ve recently assigned a new IP address to the appliance, be sure to clear the local Address Resolution Protocol (ARP) cache from network devices such as firewalls or routers. This ensures that these network devices are not using an old IP-to-MAC address mapping.

- Run a packet trace on the external interface and verify that traffic is reaching the appliance and being returned. This is commonly done using the tcpdump utility. For example, typing tcpdump -i -n eth1:1 port 80 or 443 will check for traffic over ports 80 and 443 on the eth1:1 interface.

- If traffic is not reaching its destination, verify that it’s not being filtered by iptables, a firewall running on the appliance. Examine the contents of the log file /var/log/kern.iptables and look for dropped packets. To review the iptables ruleset, run the iptables -L -n -v command. (Note that log messages indicating traffic filtered by iptables will not be forwarded to an external syslog server.)

- If you can’t connect to the external network, ping the default gateway and verify that you have Internet connectivity. You can issue the ping command from the command line or from within AMC. See “Ping Command” on page 234.

- If you experience network latency, such as slow scp file copy performance or slow performance by the Web access and client/server access services, the problem may be due to configuration differences between the appliance interface settings and the switch port(s) to which the appliance is connected. It’s possible for a switch to improperly detect duplex mode settings (for example, the appliance is configured at full duplex but the switch detects half duplex). Cisco has documented such problems with its switches. This can adversely affect the appliance’s performance.

To resolve this problem, it is recommended that you not use autonegotiate. Instead, you should configure the switch port to statically assign settings that match the appliance. Note
that you must check both switch ports and both appliance interface settings (internal and external, if applicable). If even one interface/switch port is mismatched, there will be a negative impact on performance.

If you are experiencing network latency but your appliance/switch ports are configured correctly, the problem is somewhere else in the network. It could also be an application-level issue (such as slow name resolution on the DNS server being accessed by the Web access and client/server access services).

**AMC Issues**

- If you can't access AMC, connect a crossover cable to the internal network interface on the appliance and verify that you can access AMC without any network. If this type of connection is impractical, put the laptop on the same network segment as the internal interface (to get as close to the appliance as possible).
- If you still can't access AMC, make sure your URL includes the https:// protocol identifier. Also verify that you've included the port number 8443 in the URL.
- If your configuration changes are not taking effect, make sure you click **Apply Changes** in AMC to restart the services and apply your changes.
- If you lose the password for the primary administrator, you'll need to log in to the appliance as "root" and modify /usr/local/app/mgmt-server/sysconf/pending/avconfig.xml. Locate the `<credentials>` block for the primary administrator and replace the `<password>` element with the following password (encrypted using an MD5 hash):
  
  $1$h/Vql8b.$G8FZroTP0ainA4w78uZga.

  Restart AMC, and your password will be reset to "password" (of course, you should then use AMC to change it to something more secure).

  If you are a secondary administrator and lose your password, ask the primary administrator to reset it for you.

**Authentication Issues**

- Verify that you can access the external authentication server. This is commonly done using the tcpdump utility. For example, typing `tcpdump -i eth0 udp port 1645` would verify that you can access a RADIUS authentication server on port 1645.
- Verify that AMC contains the proper credentials needed to access your external server. For LDAP, check the **Login DN** and **Password** settings; for RADIUS, check the **Shared secret** setting.
- Review the authentication server logs. Make sure you're not entering invalid credentials or having connectivity problems.

**Aventail Services**

**Web Access Service Issues**

- Temporarily increase the server log level in AMC to **Verbose** (don't forget to go to the **Apply Changes** page to restart the appliance).
- View the Web access service log in real time as you make a connection. This is done using the `tail` command by typing `tail -f /var/log/aventail/access_servers.log`. Verify that your connection request appears in the log.
- Verify that your DNS server can resolve the Web access service **Server name** setting in AMC to the IP address of the Web access service interface. You can use the lookup tool within AMC (see "DNS Lookup" on page 235) or you can issue the `nslookup` or `dig` commands from the command line.
- If your network uses NAT to translate IP addresses, make sure that the Web access service **Server name** setting contains the IP address of the outside (or public) IP address that is being substituted using NAT.
Standard Web Mode Access Agent Issues

The standard (non-translated) Web mode access agent provides access to any URL resources only on Windows XP and Windows 2000 with Internet Explorer 6.0 or later. ASAP Workplace indicates that standard Web mode is active on a client by displaying “Agent: Standard Web” in the Connection Status area. If you need to troubleshoot whether the standard Web mode agent is running properly on a client machine, you can take the following steps:

1. On the client machine, press CTRL+ALT+DELETE and then click Task Manager.
2. Look in Windows Task Manager’s Processes list for the process ewpca.exe. If that file is present, it indicates that the standard Web mode access agent is running, although it may not be receiving network traffic.
3. To confirm that the standard Web mode access agent is receiving traffic, in Internet Explorer select Internet Options from the Tools menu, then on the Connections tab, click LAN Settings or Settings for the dial-up/VPN connection you are using to connect to the appliance.
4. In the appropriate Settings dialog box for your connection type, verify that the Use automatic configuration script check box is selected and that the Address box contains the following address:
   http://127.0.0.1:<portnumber>/redirect.pac
   Internet Explorer uses the redirect.pac file to determine which connections to send to the standard Web mode access agent.
5. To view the resource addresses that are redirected by the redirect.pac file, open the file in a text editor. The file is located on the client machine in the folder:
   \Documents and Settings\<username>\Application Data\Aventail\ewpca
   The //Redirection Rules// section of the redirect.pac lists the addresses defined as destinations that are sent through the standard Web mode access agent. These addresses come from the list of network and URL resources defined in AMC.

Client/Server Access Service Issues

- Temporarily increase the server log level in AMC to Verbose (don’t forget to go to the Apply Changes page to restart the appliance).
- View the client/server service log in real time as you make a connection. This is done using the tail command by typing
  tail -f /var/log/aventail/access_servers.log. Verify that your connection request appears in the log.

Aventail OnDemand Issues

This section describes how to troubleshoot general and specific OnDemand problems.

General OnDemand Issues

If OnDemand fails to work properly, perform the following diagnostics.

Testing OnDemand

Test OnDemand by connecting to the appropriate URLs to start the applet, and then running the supported applications.

When testing, make sure that:
- OnDemand can communicate with required Aventail client/server access services.
- Aventail client/server access service authentication and access control are working.
- OnDemand automatically redirects connections properly.
- OnDemand creates connections for each configured application.
- OnDemand starts any thin-client applications configured to start automatically.
Viewing OnDemand Log Files

For users running Windows, when OnDemand starts it creates log files containing useful troubleshooting messages. The location of the log files (named `od.log` and `odapp.log`) varies depending on which operating system the user is running:

- Windows 2000 and Windows XP:
  `%SystemRoot%\Documents and Settings\<username>\Application Data\Logfiles\`
- Windows 98 SE and Windows Me:
  `%SystemRoot%\Windows\Application data\Aventail\Logfiles\`

Detecting the JVM Version

If OnDemand is not working properly, ensure that the user is running one of the JVMs supported by OnDemand. For a list of supported JVMs, see “OnDemand Client Requirements” on page 203. In addition, make sure the user has enabled Java in the browser; see “Enabling Java in the Browser” on page 232.

To determine the JVM version running on a client computer, use the instructions in this section.

- **To detect the JVM version**
  - Internet Explorer for Windows: You can open the browser’s Java Console to view information on your JVM; see “Viewing the Java Console” on page 233.
  - Internet Explorer for Macintosh OS X: In the Applications folder, open the Utilities folder, and then open the Java folder. Run the Java Plugin Settings program, and go to the About tab to see information about the JVM version.
  - Internet Explorer for Macintosh OS 9.2: In the Applications folder, open the Apple Extras folder, and then open the Apple Mac OS Runtime folder. Open the About MRJ document to see information about the JVM version.
  - Netscape Navigator 7.x for Windows: On the browser’s Tools menu, point to Web Development, and then click Java Console. The Java Console opens; the first two lines of this window show the JVM version.

**Notes**

- Some versions of Windows may not include a JVM; in this case, you will get an error message stating `jview.exe must exist in \path or you need to set JAVA_HOME`. If you are getting this message but you know that you have a JVM on your Windows computer, set the path to the JVM directory as `JAVA_HOME` in the Environment Variables dialog box; see the Windows Help for information. Otherwise, you will need to either install a JVM on your Windows computer or use a different computer.

Enabling Java in the Browser

Java must be enabled in the user’s browser for the OnDemand applet to run. In Internet Explorer and Netscape Navigator, Java is enabled by default. If OnDemand doesn’t run, and you suspect the defaults have been changed, enable them as described here. Instructions shown are for the most recent versions of the browsers; for earlier versions, see the browser documentation.

- **To enable Java in Internet Explorer 5.5 for Windows**
  1. On the Tools menu, click Internet Options.
  2. On the Security tab, click Custom Level.
  3. Under Microsoft VM, verify that in the Java Permissions section, anything other than Disable Java is selected.
  4. Scroll down further to Scripting, and verify that in the Active Scripting section, anything other than Disable is selected.
EX-1500 Installation and Administration Guide | 233

To enable Java in Internet Explorer for Macintosh
1. On the Explorer or Edit menu, click Preferences.
2. Under Web Browser, click Java.
3. Click the Enable Java check box.

To enable JavaScript in Netscape Navigator 7.x for Windows
1. On the Edit menu, select Preferences.
2. Under Advanced/Scripts & Plugins, be sure that the Enable JavaScript for Navigator check box is selected.

Viewing the Java Console
If the OnDemand applet doesn’t start, you might need to have the user open the Java Console to view technical messages about OnDemand.

To open the Java Console
- Internet Explorer for Windows: On the Tools menu, select Internet Options and then click the Advanced tab. Under Microsoft VM, select the Java Console enabled and Java logging enabled check boxes, and then click OK. Close the browser and then reopen it. Then, click Java Console on the View menu.
- Internet Explorer for Macintosh OS X: In the Applications folder, open the Utilities folder, and then run the Console program.
- Internet Explorer for Macintosh OS 9.2: On the View menu, click Java Messages. If this doesn’t work, ensure that Java logging is on: On the Edit menu, click Preferences. Under Web Browser, click Java, and then select the check boxes for Java message logging.
- Netscape Navigator 7.x: On the browser’s Tools menu, point to Web Development, and then click Java Console.
- When using the Sun Java Plug-In on Windows, users can access the Java Console by double-clicking the Sun Java icon in the taskbar notification area.

Specific OnDemand Issues
Following are some troubleshooting tips for specific situations you may encounter when using OnDemand.

OnDemand does not start
First, verify that Java or JavaScript is enabled in the Web browser on the computer trying to run OnDemand. For instructions on enabling Java, see “Enabling Java in the Browser” on page 232.

If Java is enabled in the browser, also verify that the browser is using a Java Virtual Machine (JVM) version that is supported by OnDemand; for a list of supported JVMs, see “OnDemand Client Requirements” on page 203.

If both of these options are enabled, and OnDemand still doesn’t start, open the Java Console on the user’s computer to see Java messages that may be helpful when getting technical support; see “Viewing the Java Console” on page 233.

An application does not run correctly over OnDemand
Have the user check the OnDemand Details page and verify whether the application name is active or inactive. One potential issue is that more than one application is configured to use the same local IP address and port. To see more details about the problem, ask the user to copy the log messages from the OnDemand Details page and e-mail them to you.

The server certificate Accept button is unavailable
Under some circumstances, OnDemand may present the user with a server certificate that he or she cannot accept. If the Accept button on the certificate page is unavailable, OnDemand detects a problem with the server certificate. The most common causes of this problem are:
• Date/time mismatches between client computer and server. Verify that the client computer and the Aventail client/server access service have the correct date and time.
• The certificate has expired or is not yet valid.
• The certificate information does not match the server information.
• The certificate chain is invalid.

Troubleshooting Tools in AMC

Several basic network troubleshooting tools are included in AMC, including ping, traceroute, DNS lookup, and the ability to view the current routing table.

When running a troubleshooting tool, keep in mind that it may take a couple of minutes to execute the command. Please be patient and don’t browse to another page in AMC until the command is finished.

Ping Command

Use the ping command to verify a network connection. When you issue the ping command, it sends an ICMP ECHO_REQUEST packet to a target host and waits to see if the host answers.

To issue a ping command
1. From the main navigation menu, click Troubleshooting.
2. Click the Ping tab.
3. In the Address box, type the IP address or host name of the machine you want to ping.
4. Click Go. AMC issues the ping command. After about five seconds, the results appear in the large box at the bottom of the page. A successful connection returns results similar to the following:

If the ping command is unable to reach the host, it returns results resembling the following:

Traceroute Command

Use the traceroute command to see the sequence of gateways through which an IP packet travels to reach its destination. This can help you find a network failure point.
To issue a traceroute

1. From the main navigation menu, click Troubleshooting.
2. Click the Ping tab.
3. In the Address box, type the IP address or hostname of the machine against which you want to issue the traceroute command.
4. Select the Use traceroute check box.
5. Click Go. AMC issues the traceroute command. The results appear in the large box at the bottom of the page. Traceroute returns a list of hosts, starting with the first gateway and ending at the destination.

---

DNS Lookup

You can use AMC’s Lookup tool to find out how DNS is resolving an IP address or a host name. This tool is useful for troubleshooting various DNS problems, including determining if your DNS server is running.

The Lookup tool expects either a fully qualified domain name or an IP address. You can enter a non-qualified host name as long as you have defined one or more default search domains on the Name Resolution tab (in Network Settings). For details on configuring name resolution, see “Configuring Name Resolution” on page 36.

To find out how DNS is resolving an IP address or host name

1. From the main navigation menu, click Troubleshooting.
2. Click the Lookup tab.
3. In the Address box, type the IP address or hostname of the machine against which you want to issue the command.
4. Click **Go**. The results appear in the large box at the bottom of the page.

![Image](image.png)

**Viewing the Current Routing Table**

You can view the current routing table, including both dynamic and static routes, from within AMC.

- **To view the current routing table**
  1. From the main navigation menu, click **Troubleshooting**.
  2. Click the **Routes** tab.
  3. Click **Go**. The results, which include both dynamic routes and static routes, appear in the large box at the bottom of the page and resemble the following:

![Image](image.png)

**UNIX Command Reference**

We assume that you are an experienced network or system administrator familiar with managing network security devices. This document also assumes that you have some experience with UNIX (or Linux), including basic commands, working with files and directories, and editing text files with vi. If you are new to UNIX, the Web contains a wealth of information that can help you get started. A few sites worth visiting are:

- [Linux Installation and Getting Started Guide](http://www.tldp.org/LDP/gs/gs.html)
- [Linux Online Documentation](http://www.linux.org/docs/index.html)
- [Introduction to Vi](http://docs.freebsd.org/44doc/usd/12.vi/paper.html)

If you’re a PC user new to UNIX, the following table provides a quick reference of DOS commands and their equivalent UNIX commands.

<table>
<thead>
<tr>
<th>DOS command</th>
<th>UNIX command</th>
<th>Command description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cd</code></td>
<td><code>cd</code></td>
<td>Change directory</td>
</tr>
</tbody>
</table>
When working with log files, you may need the following UNIX commands:

<table>
<thead>
<tr>
<th>UNIX command</th>
<th>Command description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat</td>
<td>Look at a file or combine contents of multiple files</td>
</tr>
<tr>
<td>tail</td>
<td>Prints the end of a file</td>
</tr>
</tbody>
</table>

The system supports local users (stored in `/etc/password`) for use in testing the appliance. You cannot create local user accounts in AMC; instead, use the standard UNIX commands within a command shell to manage local user accounts:

<table>
<thead>
<tr>
<th>UNIX command</th>
<th>Command description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adduser</td>
<td>Add a local user</td>
</tr>
<tr>
<td>usermod</td>
<td>Modify a local user account</td>
</tr>
<tr>
<td>userdel</td>
<td>Delete a local user account</td>
</tr>
<tr>
<td>passwd</td>
<td>Change a user’s password</td>
</tr>
</tbody>
</table>

See [http://www.yolinux.com/TUTORIALS/unix_for_dos_users.html](http://www.yolinux.com/TUTORIALS/unix_for_dos_users.html) for a more comprehensive list.
Appendix B
Best Practices for Securing the Appliance

This section provides tips for ensuring maximum security for the Aventail appliance.

Network Configuration

- **Configure the appliance to use dual interfaces.**
  The Aventail appliance optimizes firewall settings when it has external and internal interfaces. Services are split between the interfaces so that management services, such as the Aventail ASAP Management Console (AMC), only listen internally and public services, such as the Aventail access services, only listen externally.

- **Protect both appliance interfaces with firewalls.**
  Allow traffic on only ports 80 and 443 from the Internet. Allow the appliance to access only the necessary resources on the customer network. Allow only trusted IP addresses from the customer network to access AMC.

- **Enable strict IP address restrictions for the SSH service.**
  If both network interfaces are enabled, Secure Shell (SSH) will listen on both interfaces. Be sure to restrict SSH service access to the IP addresses of trusted management workstations or, at a minimum, the address range of the internal network.

- **Enable strict IP address restrictions for the SNMP service.**
  If both network interfaces are enabled, Simple Network Management Protocol (SNMP) will listen on both interfaces. Be sure to restrict SNMP service access to the IP addresses of trusted management workstations or, at a minimum, the address range of the internal network.

- **Use a secure passphrase for the SNMP community string.**
  By default, in AMC the SNMP configuration sets the string your network management tool uses to query the Aventail appliance in the Community string box to public. Be sure to change the community string to a secure passphrase.

- **Disable or suppress ICMP traffic.**
  If both network interfaces are enabled, enabling Internet Control Message Protocol (ICMP) will make it possible to discover the appliance from the Internet. The most secure approach is to disable ICMP. If you do enable ICMP, you should suppress ICMP Echo Request traffic using a firewall or other network device.

- **Use an NTP server.**
  Synchronize with an external Network Time Protocol (NTP) server to ensure accurate timestamps in the system logs.
Appendix B - Best Practices for Securing the Appliance

- **Protect the server certificate that the appliance is configured to use.**
  Don’t leave the appliance server certificate where others can access it, and always make sure the key is encrypted with a strong password. If attackers obtain it, it will tell them which host it goes with and will allow them to decrypt private data.

**Appliance Configuration**

- **Keep the software image on the appliance updated.**
  Be sure to use the Update page to apply patches and upgrade files promptly because they often contain security fixes.

- **Make regular configuration backups.**
  Use the Export option Import/Export page or the command-line utilities to periodically back up your current configuration.

**Administrator Accounts**

- **Use a strong root password.**
  Your root password should be at least eight characters long and should contain punctuation characters, uppercase letters, lowercase letters, and numbers.

- **Change the AMC administrator password.**
  By default, the AMC administrator password is set to the same value as the root password during the initial installation. You should change the AMC administrator password to a different value, subject to the same composition criteria as the root password. It is good practice to change the AMC administrator password because it is transmitted in an SSL tunnel between the Web browser and the AMC server.

- **Change the root and administrator passwords often.**

- **Don’t share the root or administrator passwords.**
  It is good practice to not share passwords with anyone unless necessary. If you need to enable access for other administrators, create individual administrative accounts. It is not recommended that you create a second root account. One person should own the root account, and the password should be kept in escrow or some other safe place.

- **Limit the number of administrative accounts you create and only assign administrative privileges to trusted individuals.**

**Access Policy**

- **Follow the principle of “least privilege.”**
  The most secure approach to policy design is to specifically list the resources to which you want to permit access. Anything not accounted for in the “permit” rules is denied by the appliance. This approach follows one of the fundamental design principles of computer security: that access rights should be explicitly required, rather than given to users by default.

  An alternate approach is to create “deny” rules for restricted resources, but permit access to everything else by default. Here, anything not accounted for in the “deny” rules is accessible, until the final “deny” rule is processed. This method may be easier to set up, but is more error-prone and thus not as secure.

  Of course, you can also use a combination of permit and deny rules. In this case, users are permitted access to some resources, but denied access to others.

- **Pay close attention to rule order.**
  Because the appliance processes your access control rules sequentially, the order in which you organize them has great significance in terms of whether access is permitted or denied. The appliance stops reading the rules as soon as it finds a match. Carefully review your security policy settings to avoid inadvertently placing rules in the wrong order.
• **Put your most specific rules at the top of the list.**
  Putting the least restrictive rules at the top of the list may cause the appliance to find a match before it has a chance to process your more restrictive rules. It is usually best to put your most specific rules at the top of the list.

• **Carefully audit rules containing “any.”**
  If you create a rule that does not restrict access to a particular user or destination resource, the word “any” appears in the access control list.
  Carefully consider the impact of “any” in your policy rules. For a “permit” rule, too many “any” criteria could expose a security hole. On the other hand, too many “any” criteria in a “deny” rule could unnecessarily restrict network access.

**SSL Ciphers**

• **Disable low-strength symmetric ciphers.**
  • From the main AMC navigation menu, click **SSL Settings**, and then click the **SSL Encryption** tab.
  • Under **Web access ciphers** and **Client/server access ciphers**, clear the check boxes next to all 40-bit and 56-bit ciphers.

• **Never use NULL ciphers.**
  Never enable any of the Null ciphers on the **SSL Encryption** page; these ciphers do not encrypt data. Null authentication can be useful in testing situations, but should always be disabled for normal production use.

**Client Access**

• **Change timeout settings**
  On the **General Settings** page, set the **Maximum session length** to force users to reauthenticate periodically. This setting is applied to both the client/server access service and the Web access service.
  On the **Configure Client/Service Access** page, configure the **Timeout value** settings for **SSL timeout**, **Default connection timeout**, and **Authentication timeout** to force users to reauthenticate periodically.

• **Deploy End Point Control components**
  Aventail’s End Point Control components help protect sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments. Note that both Aventail Cache Control and Aventail Secure Desktop provide an inactivity timer that will terminate user connections after a specified period of inactivity.

• **Use strong two-factor authentication mechanisms, such as SecurID.**

• **Configure the Aventail Connect client with the following SSL settings:**
  • Set the maximum certificate chain length to 2.
  • Use a trusted roots file. Place only the signer certificate of the appliance’s SSL certificate in the roots file.
  • In Aventail Connect’s **SSL Options** dialog box, under **If a Server Certificate is Suspect**, click **Show me the certificate, but reject the connection.**
Glossary

access control
A means of limiting access based on a user’s identity or credentials. Typically used to control user access to network resources. An access policy is the set of rules that defines the privileges of users on the system. These rules define applications or network resources that users or user groups are allowed to access.

alias
An alternative label or name for an object such as a network, host computer, or network resource. Aliases have special meaning for the Web access service; they mask the URLs of the internal network. Because all requests are directed to the Web access service, the user sees only the incoming URL that contains the alias. The Web access service matches the alias to a list defined in AMC, and then translates the URL. Aliasing is available only with translated Web access.

authentication
The practice of validating a user’s identification or credentials in order to allow access to resources. Credentials are typically compared to some type of permissions list. There is a variety of authentication methods that dictate what type of credentials the user must have and when authentication should take place.

authentication server
External authentication servers store user identification or credentials, and are referenced by the realms you set up for users to log in to the appliance. The appliance supports LDAP, Microsoft Active Directory, and RADIUS authentication servers.

authorization
Permission granted to a user to use a system and the data stored on it. Authorization specifies access rights after a user has authenticated.

Aventail ASAP Management Console (AMC)
A Web-based administrative tool used to manage the appliance. It provides centralized access to managing security policies, configuring the system (including networking and certificate configuration), and monitoring. AMC is accessible from any Web browser.

Aventail ASAP WorkPlace
A dynamically personalized user access component that provides access to Web-based resources and Windows network shares from any Web browser.

Aventail Connect
A configurable 32-bit Windows client that can connect to the Aventail client/server access service to provide authenticated and encrypted access to network resources. Aventail Connect is installed on the user’s computer.

Aventail OnDemand
A secure, lightweight Java applet that can connect to the Aventail client/server access service to provide authenticated and encrypted access to network resources. By default, OnDemand starts automatically when the user logs in to ASAP WorkPlace. Alternatively, you can configure OnDemand so that the user clicks a link on ASAP WorkPlace to start OnDemand.

back-end
In a client/server application or system, the part of the program that runs on the server. (Note: Servers can also have front and back ends).

CA (certificate authority)
A trusted third-party organization that issues, renews, and revokes certificates. The CA guarantees that the individual granted a unique certificate is, in fact, who that individual claims to be (according to the CA’s individual policies). A root CA typically issues certificates to intermediate CAs, which in turn issue certificates to users. Certificates are validated by following this hierarchy of trust up the certificate chain to the root.
certificate
A digital certificate that serves to verify a server’s or client’s identity and binds it to an RSA keypair that can be used to encrypt and sign digital information. A certificate is signed by a CA that vouches for the identity of the individual.

certificate chain
A sequence of certificates that includes the user’s certificate (or “leaf”) at the bottom, certificates for intermediate CAs (if any) in the middle, and the “root” certificate of the primary CA at the top.

cipher
A type of cryptographic algorithm that uses a key to convert plaintext to ciphertext, and vice versa.

client
The client component of a client/server architecture. It is used to send commands to and receive information from the corresponding server component that carries out the requests.

client/server access service
A service providing secure, anywhere access to TCP/IP applications on your network, including enterprise client/server applications. Formerly known as the Aventail Anywhere VPN server, the client/server access service is based on the SOCKS v5 protocol.

cluster
A group of two identical appliances that reside behind one virtual IP address. An Aventail cluster prevents a single point of failure and provides high availability by including integrated load balancing, stateful user authentication failover, and centralized administration.

credentials
The specific information validating a user’s permission to access a resource, such as the specific password used to authenticate or the actual information contained in a certificate.

CSR (certificate signing request)
An application to a CA to issue a certificate that contains the user’s name and cryptographic keys. The CSR does not contain information that allows the CA to authenticate the user; this is handled separately per the CA’s due-diligence policies. The file name for a request usually ends with .req.

DES (Data Encryption Standard)
A popular standardized cipher for encrypting data. A common 56-bit key is used to encrypt and decrypt the data. Because 56 bits is inadequate for modern security standards, a common variant is to use DES three times with different keys (Triple DES).

device profile
A group of unique attributes defined in AMC that are used by the appliance to identify a client device, assess its level of trustworthiness, and assign it to an End Point Control zone.

DMZ
The “demilitarized zone” situated between the Internet and a network’s firewall. Typically, the DMZ is used to host resources accessible via the Internet while maintaining security to the private network.

DN (distinguished name)
A name made up of a list of attributes and corresponding values that identify a user or group. DNs are used to represent names in certificates, and to look up entries in directory servers. Aventail generally uses the RFC 2253 guidelines when representing DNs.

DNS (domain name system)
The Internet utility that translates alphabetic domain names into numeric IP addresses. Each time a domain name is used, a DNS server must translate it. If one DNS server does not know how to translate a given domain name, it asks another server and so on until the domain name is correctly translated.

DNS server
A computer that answers domain name system (DNS) queries. A DNS server maintains a database of host computers and domain names, and their corresponding IP addresses. When presented with the domain name, it returns the matching IP address.
domain
A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

downstream Web server
A private server on your internal network that is secured behind the Aventail Web access service. The Web access service uses aliases to obscure the URLs on downstream servers. Because all requests are directed to the Web access service, the user sees only the incoming URL that contains the alias. The Web access service matches the alias to a list defined in AMC, and then translates the URL.

dynamic redirection
An Aventail OnDemand redirection mode that, for users running Windows, enables OnDemand to dynamically redirect connections to any destination domains or IP addresses that are defined in AMC. Dynamic redirection is automatically enabled for Windows users; you do not need to configure specific ports or loopback addresses for individual applications.

encryption
The use of a cipher to generate the ciphertext, given the plaintext and a key. Encryption protects data from eavesdropping.

End Point Control
Components that protect sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments.

file system resource
A domain, server, share, or folder on a Windows network. You can make file system resources available to your users through Aventail ASAP WorkPlace, which can be used on any standard Web browser.

Filter-ID
A RADIUS attribute used to indicate a group to which the user belongs. Through its use, authorization rules may then specify group names, rather than usernames, in setting policy.

firewall
A system that can be implemented in software or hardware and prevents unauthorized access to a network. A firewall examines each message that attempts to pass through and obstructs those that do not meet specified criteria. There are several types of firewall techniques, and it is common to use two techniques together. Firewalls are considered the first line of defense in a security-based architecture.

fully qualified
May also be referred to as “full” or “FQDN” (fully qualified domain name). Used to describe the entire name, address, or path of a computer, host, domain, or file. It refers to a listing of all the components of a hierarchical system that lead to the specific file, IP address, host, or domain. A name, address, or path that is not fully qualified may contain an alias or may be a shortened version.

gateway
A combination of hardware and software that connects two networks using different communications protocols. It converts data exchanged between the networks so that each network can read what has been received from the other.

hash
Also referred to as a “hash value.” A number generated by applying a formula to a string of text so that it is unlikely that another string could produce the same number. The hash is always much smaller than the text itself.

host
A computer connected to a TCP/IP network (which includes the Internet) that runs the server programs supplying resources and services to the Internet. Each host has a unique IP address.

host name
The non-numeric name for a specific computer that can be found via the Internet. An example of a host name is private.aventail.com. The host name refers to both the left-most portion of the name (private) and the name in its entirety (private.aventail.com). The remaining two portions are the domain name (aventail) and top-level domain (com).

HTTPS
A commonly used method of securing the HTTP protocol by layering it inside SSL.
**IP (Internet Protocol)**
The basic data transfer protocol used for the Internet. Information such as the address of the sender and the recipient is inserted into an electronic "packet" and then transmitted. For more information, refer to RFC 791.

**IP address**
A unique ID number that identifies each individual computer on the Internet. Each 32-bit address is represented as four sets of 8-bit numbers, ranging from 0 to 255, separated by periods. A hierarchy from left to right represents a rough organization of the entire Internet, so that some networks can contain other networks. The last number on the right identifies the individual host computer.

**key**
A piece of information necessary for performing certain cryptographic operations. Keys may be generated randomly, or may be derived from user-friendly representations (such as passwords).

**key length**
The size of a key, generally measured in bits. When all other things are equal, a longer key length means a more secure but possibly slower algorithm.

**key pair**
The matching pair of public and private keys used by public-key cryptographic algorithms (for example, RSA). The public and private keys are used for opposing operations (encrypt a message with the public key; decrypt it with the private key).

**LAN (local area network)**
A network that connects workstations, computers, and other devices within a relatively small area (usually a single building). A LAN allows users to access data on other computers and to share devices such as printers. Multiple LANs can be linked together to create a WAN.

**LDAP (Lightweight Directory Access Protocol)**
A simplified version of the X.500 directory access protocol (DAP). For more information, refer to RFC 2251.

**master node**
In an Aventail cluster, the node that controls the propagation and synchronization of policy and configuration across the cluster. All configuration is performed on the master node; the master node then passes any configuration changes to the slave node.

**MD5**
A specific message digest algorithm. MD5 is less secure than SHA-1 but is much faster and is often considered "secure enough."

**multi-homed**
A machine that has more than one NIC (network interface card) and is attached to more than one network.

**NAS (Network Access Server)**
A server that provides managed connectivity to a set of resources, such as a terminal server handling dial-in modems. A RADIUS client is generally called a NAS.

**NAT (Network Address Translation)**
An Internet standard that translates internal IP addresses into one external IP address, allowing organizations to present just one IP address to the Internet. NAT hides internal addresses, and also conserves IP addresses by reducing the number of addresses an organization needs.

**Network Explorer page**
A page in ASAP WorkPlace that displays any Windows file system resources that the user has permission to access; these resources can include servers, computers, workgroups, folders, and files.

**network resource**
A client/server (TCP/IP) resource on a network. Examples include thin-client applications such as Citrix; full client/server applications such as Microsoft Outlook, Lotus Notes, or SAP; or terminal servers. A network resource can be defined by host name, IP address, IP address range, subnet IP address, or DNS domain.
network share
On a Windows network, a workgroup, computer, or folder whose contents can be accessed by authorized users. You can make network shares available to your users through Aventail ASAP WorkPlace, which can be used on any standard Web browser.

network shortcut
A link in ASAP WorkPlace that provides access to a file system resource on your network. Network shortcuts can be defined for Windows servers, computers, workgroups, or folders.

NIC (network interface card)
A printed circuit board or card installed in clients and servers in a network that enables the computers to exchange data. Also called a network adapter.

ping
A diagnostic tool used to determine connectivity. To “ping” a remote host means to send ICMP ECHO_REQUEST packets and wait for a response. If there is no response, the remote host is down or unreachable; if there is a response, the time delay for the response can be used to determine the Round Trip Time (RTT) necessary for the exchange of data with that host.

plaintext
The unencrypted, readable text of a message.

ports and port numbers
In reference to TCP/IP and UDP networks, a logical channel or channel endpoint. Port numbers are assigned to application programs, and are used to link incoming data to the correct service. Well-known ports are standard port numbers commonly used for certain types of traffic. For instance, port 80 is typically used for HTTP (Web) traffic, while port 20 is typically assigned to FTP transfer.

private key
One half of a key pair used in public-key cryptographic algorithms, known to its owner and never shared. The public key is the other half of the key pair.

protocol
Rules and procedures used to exchange information between networks in computer systems.

proxy server
A firewall component that manages Internet traffic to and from a LAN, serving as a proxy or intermediary between internal resources and external requests for those resources. Proxy servers hide true network addresses (preventing IP addresses from being spoofed or mapped), and secure and manage all application communication. With a proxy server, there is never a direct connection between an outside user and an internal resource. All traffic to and from internal resources is proxied by the proxy server. The Aventail client/server access service is a SOCKS v5 proxy server.

public key
One half of a key pair used in public-key cryptographic algorithms, known by anybody and included in the user's certificate. The private key is the other half of the key pair.

public-key encryption
A cryptographic algorithm that uses two different keys for encrypting and decrypting data (as opposed to a conventional cipher, which uses the same key for both). Such systems allow key pairs (with one half made public and one half kept private) to be generated and used for digital signatures and key exchanges. Public key systems can be extremely secure and allow communication without the exchange of keys in advance, which facilitates communication among large numbers of unrelated parties (as over the Internet). The idea was invented by Diffie and Hellman, and the most commonly used public key algorithm is RSA.

RADIUS (Remote Authentication Dial-In User Service)
A protocol for communicating with a back-end authentication database. Useful for Username/Password, CHAP, and CRAM authentication mechanisms. The user sends credentials to the Network Access Server or NAS (for example, the Aventail client/server access service), which then sends them to a RADIUS server. The RADIUS server performs the checking of the password, and tells the NAS whether to consider the authentication valid. For more information, refer to RFC 2138.
realm
A user community defined in AMC that checks user identities or credentials against an external authentication server and provisions access agents to users who are allowed to log in to the realm.

RIP (Routing Information Protocol)
A protocol that enables routers to dynamically share routing table information with one another.

RSA (Rivest-Shamir-Adelman) encryption
The most widely used public-key algorithm today, RSA is named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adelman, who developed it at MIT in 1978. PGP, SSL, and S/MIME are generally used with RSA for key exchanges and digital signatures. RSA was patented in the United States, which limited use, but the patent expired in September of 2000.

SecurID
A two-factor user authentication system developed by RSA Security. The system is based on something you know (a PIN), and something you have (a hardware token). These factors are combined to form a dynamic passcode that the user types in via the authentication mechanism.

server
A networked computer that shares resources with other computers. Servers “serve up” information to clients.

single sign-on
An option that controls whether and how a user’s login credentials are forwarded to downstream Web applications. Forwarding a user’s credentials prevents the user from needing to log in multiple times.

slave node
In an Aventail cluster, the secondary node that is controlled by the master node. All configuration is performed on the master node; the master node then passes any configuration changes to the slave node.

SOCKS v5
A security protocol for handling TCP traffic through a proxy server. SOCKS is the IETF standard for authenticated firewall traversal and can be used with virtually any TCP application. It acts as a proxy mechanism that manages the flow and security of data traffic to and from a LAN, intranet, or extranet. SOCKS uses sockets to represent and track individual connections. There are two main versions of SOCKS—SOCKS v4 and SOCKS v5. SOCKS v5 provides an authentication mechanism, while SOCKS v4 does not. For more information, refer to RFC 1928.

SSL (Secure Sockets Layer)
An authentication and encryption protocol developed by Netscape Communications to secure application protocols such as HTTP over the Internet. SSL uses a key exchange method (RSA is most common) to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. The IETF has generated a successor of SSL, a network standard called Transport Layer Security (TLS). SSL is the most widely deployed security protocol on the Internet today. For more information, refer to RFC 2246.

standard Web access
The default access method that enables users to access any URL from WorkPlace. Standard Web access eliminates the need for Web content translation and provides broader access to enterprise Web applications. Standard Web access is automatically provisioned to users and requires no special configuration.

subnet
A segment of a network. Networks are divided into subnets (or subnetworks) for performance and security reasons. Subnets share a common network address with other parts of the network, even though they may be physically independent. Subnets are distinguished by subnet numbers and are bridged by routers. IP networks are divided using a subnet mask.

subnet mask
The method used to divide IP networks into smaller segments, or subnets. A subnet mask identifies the subnet to which an IP address belongs. Network administrators can divide the host portion of an IP address into two or more subnets. Part of the host address is then reserved to identify the particular subnet.

syslog
The UNIX system log to which logging information can be output.
TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic protocol suite of the Internet, of which TCP and IP are the foundation. TCP is the transport layer of the suite and correlates to OSI Layer 4, which regulates traffic. IP is the network layer of the suite and correlates to OSI Layer 3, which handles addressing. (TCP/IP uses four layers, in contrast to the OSI networking model’s seven layers.) TCP ensures the reliable delivery of packets to their intended destinations, while IP ensures that packets are addressed properly. Other protocols in the TCP/IP suite include SNMP (Simple Network Management Protocol), PPP (Point-to-Point Protocol), SMTP (Simple Mail Transfer Protocol), and UDP (User Datagram Protocol). The TCP/IP protocol suite was developed by the Department of Defense for communications between computers. It has become the de facto standard for data transmission over networks, including the Internet. For more information, refer to RFC 793.

Token

A small security device used to generate dynamic passwords. Some tokens display a number that frequently changes; the number is a password that is valid for a short period of time. Others include keypads for typing in a challenge, and compute the appropriate response that will allow successful authentication. Tokens are sometimes called “first-generation smart cards.”

trusted roots file

A list of the root certificates an administrator chooses to trust. Every certificate chain ends with a root certificate. There is no “higher” CA to validate the root, so that root must either be trusted or not (if not, the whole chain is untrusted and should be rejected).

UDP (User Datagram Protocol)

A means of sending data over the Internet without guaranteed delivery. Also known as a connectionless protocol. UDP is part of the TCP/IP protocol suite and corresponds to Layer 4 in the OSI networking model (the transport layer). UDP converts data messages generated by an application into packets to be sent over an IP network, but does not guarantee that all of the packets will be delivered or will be in the proper order when they reach their destination. Unlike TCP, UDP provides no error-recovery services and is used primarily for the exchange of very small data units (datagrams) that require little message reassembly. For more information, refer to RFC 768.

URL resource

A Web-based application or service that is accessed using HTTP or HTTPS. Examples include Web portals, standard Web servers, and Web-based e-mail programs such as Microsoft Outlook Web Access.

virtual private network (VPN)

A secure channel used to access a private network over a public network (such as the Internet). There are two main types of VPNs: remote access VPNs provide remote employees with secure access to e-mail, file servers, and other network resources, and extranet VPNs provide business partners (such as suppliers or vendors) with secure access to a variety of applications, such as supply chain management (scm) programs.

Web access service

A secure gateway through which users can access Web applications and files, making secure, clientless access available from any Internet browser. The Aventail Web access service was formerly known as the Aventail ExtraWeb server. The Web access service provides two access modes: standard Web mode and translated mode.

Web shortcut

A link on ASAP WorkPlace that provides access to a Web-based application or service on your network.

wildcard

A special symbol that represents one or more characters. Wildcards can be used to identify files and directories, allowing users to select many files with a single specification. In the Windows operating system, for example, the asterisk is a wildcard that represents any combination of letters, so * refers to all files that begin with n, and *.doc refers to all files that start with n and end with .doc.

X.500

A set of standards developed by the ITU (International Telecommunication Union) and ISO (International Organization for Standardization) in the mid-1980s that defines how global directories should be structured. The X.509 system of authentication (based on public and private key pairs) and LDAP evolved from the X.500 effort.

X.509

An ITU recommendation used to define digital certificates. The standard has not been officially approved and thus is implemented in different ways by different companies. Virtually all certificates in use today (SSL, S/MIME) are X.509 certificates.
zone

An End Point Control feature that defines “zones of trust” used to provide different levels of access depending on the degree of trust at the user’s end point. Connection requests are compared against the device profiles you set up in AMC and then assigned to the appropriate zone.
Index

A
ACC. See Aventail Cache Control
access control rules
  adding 97
  best practices 240
  configuring 95
  copying 102
  deleting 102
  disabling 96
  editing 102
  enabling 96
  managing 95
  moving 103
  overview 78, 95
  reordering 103
  viewing 96
access logs 124, 132
accessing
  AMC 21
  ASAP WorkPlace 198
  OnDemand 202
accounts, administrator 24, 240
Active Directory 58, 59, 62
active nodes 216
adding
  access control rules 97
  administrator accounts 25
  authentication servers 52
  CA certificates 48
  device profiles 171
  realms 110
  resource groups 90
  resources 86, 87, 89, 101
  roots certificates 46, 48, 49
  shortcuts 191, 192
  user groups 101, 115, 118
  users 101, 115, 118
  Web application profiles 92
  zones 169, 173, 174, 175, 176
administrator accounts
  adding 25
  best practices 240
  deleting 26
  editing 25
  managing 25
  overview 24
administrator sessions 26
aliases 62, 76, 88
AMC
  accessing 21
  accounts 24
  applying changes 27
  configuration data 27
  getting help 24
  interface 22
  logging in to 21
  logging out of 22, 27
  overview 3, 21
  saving changes 23, 27
  timeout 27
  version number 136
appliance. See Aventail appliance
applying configuration changes 27, 155
architecture, network 9
ASAP Management Console. See AMC
ASAP WorkPlace
  accessing 198
  client requirements 188
  configuring 190, 194
  customizing 189, 194, 195
  deploying 15, 81, 198
  End Point Control and 199
  logging in 183
  overview 3, 79, 183
  realms 107
  starting service 155
  stopping service 155
  supported platforms 188
  templates 195
ASD. See Aventail Secure Desktop
authentication
  Active Directory 58
  configuring 51, 108
  digital certificates 56
  group affinity checking 114
  LDAP 53
  local users 67
  Netegrity SiteMinder 70
  NTLM 69
  overview 51
  RADIUS 63
  realms 51, 105
  single sign-on 69, 70
  smart cards 65
  tokens 65
  username/password 53, 59, 64
authentication servers
  defining 52
  LDAP authentication 53
  multiple 52
  overview 51
  referencing in realms 52
  types of 51
Aventail appliance
  architecture 9
  clusters 215
  configuring 13
  connecting 17
  controls 16
  indicators 16
  installing 13, 15
  managing 12
  monitoring activity 124, 224
  moving into production 14
  overview 1
  powering down 17
index

powering up 17
restarting 17
security best practices 239
setup 18
shutting down 17
troubleshooting 229
Aventail ASAP WorkPlace. See ASAP WorkPlace
Aventail Cache Control 177
Aventail Connect client 5, 15, 82, 107, 172, 200
Aventail Management Console. See AMC
Aventail OnDemand. See OnDemand
Aventail Secure Desktop
  configuring 179
  enabling 179
  overview 178

B
back-end servers, verifying roots file 46, 48
backing up
  clusters 224
  configurations 143, 147
backup files 147, 148, 150
branding in ASAP WorkPlace 194
browsers
  determining JVM version 232
  enabling Java in 232
  requirements for OnDemand 203
  requirements for Workplace 188
  viewing Java console 233

C
CA certificates 48
Cache Control. See Aventail Cache Control
caching DNS settings 157, 158
certificate signing requests
  generating 41
  importing responses 44
  overview 41
  submitting 43
certificates
  adding 46, 48, 49
  authenticating with 56
  client 46, 49
  configuring 38, 46, 49
  exporting 47
  FAQ 50
  generating CSRs 41
  importing 45, 48
  importing CSR responses 44
  managing 46
  obtaining third-party 41
  overview 38
  self-signed 38
  server 38, 53
  submitting CSRs 43
  trusted roots files and 39, 45
  viewing details 46
changing passwords 25
checklists
  initial setup 10
  moving appliance into production 14
client access, best practices for 241
client certificates 46, 49
client requirements
  ASAP Workplace 188
  OnDemand 203
client/server access service
  access logs 124, 132
  Aventail Connect client and 200
  configuring 157
  OnDemand and 201
  overview 2, 79
  starting 155
  stopping 155
clusters
  architecture 215
  assigning master node 220
  backing up 224
  configuring 217, 222
  connecting networks 218
  failover 216
  installing 217
  managed switch connections 221
  managing 222
  monitoring 224
  overview 215
  stateful failover 216
  troubleshooting 226
  upgrading 224
  viewing network information 222
  virtual IP addresses 221
commercial CA, obtaining certificates from 41
comparing configurations 150
Config Backup Tool 147
Config Compare Tool 150
Config Reset Tool 149
Config Restore Tool 148
configuration data in AMC 27
configurations
  backing up 143, 147
  comparing 150
  file conflicts, avoiding 26
  importing and exporting 144
  resetting 149
  restoring 143, 148
  saving 23
  updating 143
configuring
  access control rules 95
  ASAP Workplace 190, 194
  authentication 51, 108
  Aventail Cache Control 177
  Aventail Connect client 200
  Aventail Secure Desktop 179
  certificates 38, 46, 49
  client/server access service settings 157
  clusters 217
  DNS 36
  IP addresses 32
  LDAP authentication 53
  local user authentication 67
  logging settings 133
  network information for clusters 222
  network settings 31

Aventail
overview 13
RADIUS authentication 63
realms 110
services 155
shortcuts 190
single sign-on 68
SNMP 137
SSH 121
SSL encryption settings 159
time settings 123
user access components 3, 183
username/password authentication 53, 64
Web access service settings 156

Connect client. See Aventail Connect client
connecting cluster networks 218
connecting the appliance 17
connections, serial 17
Console. See AMC
cookies, translating 93
copying
access control rules 102
realms 113
zones 172
credential forwarding 92, 93
customizing ASAP WorkPlace 189, 194, 195
D
debug messages, in OnDemand 212
default factory settings 149
default gateway 33
default realms 106, 112
default zones 173
deleting
access control rules 102
administrator accounts 26
device profiles 173
referenced objects 29
resource groups 91
resources 90
shortcuts 193
user groups 120
users 120
Web application profiles 95
zones 173
deployment
appliance checklist for 10
ASAP WorkPlace 15, 81, 198
Aventail Connect client 15, 82, 200
OnDemand 15, 81
overview 81
Web resources 81
designing a VPN 73
device profiles
defining 171
deleting 173
overview 164
viewing 168
disabling
access control rules 96
active user sessions 137
End Point Control 168
realms 112
DNS caching 157, 158
DNS, configuring 36
domain name, specifying 31
downloading system updates 151
downstream Web servers 156
dual interfaces 215
dynamic mode 202, 206
dynamic routing 34
E
editing
access control rules 102
administrator accounts 25
objects in AMC 22
realms 113
resource groups 91
resources 90
shortcuts 193
user groups 119
users 119
Web application profiles 95
enabling
access control rules 96
Aventail Cache Control 177
Aventail Secure Desktop 179
End Point Control 168
realms 112
Sygate On-Demand 180
WholeSecurity 181
Zone Labs Integrity 181
encryption
client/server access service 159
Web access service 159
End Point Control
ASAP WorkPlace and 199
Aventail Cache Control 177
Aventail Secure Desktop 179
device profiles 164, 167
disabling 168
enabling 168
overview 80, 163
scenarios 165
Sygate On-Demand 180
WholeSecurity 181
Zone Labs Integrity 181
zones 164, 167
exporting
certificates 47
configuration files 144
F
failover, stateful 216
file system resources 77, 89
files
backup 147, 148, 150
comparing 150
configuration 26, 143
log 124, 134
trusted roots 39, 45, 53, 58
update 151
firewall policies 11
forwarding, authentication 92, 93
front-panel indicators 16

G
gateway, default 33
group affinity checking 114
groups
  managing 90
  mapping names 105
  resource 90
  user 105

H
hardware installation 15
hidden realms 106, 112
high availability 215
hosts file redirection 205

I
ICMP, enabling 123
importing
  certificates 45, 48
  configuration files 144
installation
Aventail appliance 15
Aventail Connect client 200
clusters 217
hardware 15
overview 13
interfaces
  configuring speed 32
  network 9, 32
IP addresses, configuring 32

J
Java console, viewing 233
Java security warning, suppressing 212
Java, enabling in the browser 232
JVM, determining version of 232

L
LDAP authentication
  Active Directory 62
digital certificates 56
  overview 53
  servers 53
  SSL and 53
  username/password 53
licenses
  base 160
  components 160
  managing 161
  overview 160
  viewing details 161
limbo life, maximum 158
Linux support in OnDemand 207
load balancing 215
local user authentication 67
logging
  configuring settings 133
  file formats 124
  file locations 134
  levels of 133

OnDemand 212
  overview 124
  syslog servers and 134
  viewing messages 132
logging in to AMC 21
logging in to ASAP WorkPlace 183
logging in to OnDemand 202
logging out of AMC 22
logos in ASAP WorkPlace 194
loopback addresses 207

M
Macintosh support in OnDemand 207
managed switch connections 221
Management Console. See AMC
management
  access control rules 95
  administrator accounts 25
  Aventail appliance 12
  certificates 46
  clusters 222
  End Point Control 167
  realms 108
  resource groups 90
  resources 85
  user groups 115
mapping
  group names 105
  ports in OnDemand 207
  user names 105
master nodes 217, 220
maximum limbo life 158
maximum user session length 155
monitoring
  active users 136
  appliance activity 124, 135
  ending active user sessions 136
moving
  access control rules 103
  individual shortcuts 194
  multiple shortcuts 193

N
name resolution, configuring 36, 37
Netegrity SiteMinder 70
network configuration 239
network interfaces 9, 32
network resources 76, 86
network settings
  default gateway 33
  DNS 36
  ICMP 123
  network interfaces 32
  NTP 123
  overview 31
  server certificates 38
  SSH 121
  system identity 31
  Windows name resolution 37
network shortcuts 192
nodes
  active 216
dual 215
master 217
redundant 216
NTLM authentication forwarding 69
NTP 123

O
OnDemand
client requirements 203
cross-platform support 207, 209
debug messages 212
deploying 15, 81
dynamic mode 202, 206
genral network access 206
logging 212
loopback addresses 207
mapped mode 202
overview 4, 201
proxy detection 213
redirection 205
running 202
status window 202
supported applications 202
supported platforms 203
testing 231
Windows support 206
online Help 24
outbound proxy server support 213

P
passwords, changing 25
personal folders, shortcuts to 192
ping command 123
planning process 73
port mapping 207
portals, Web 198
powering down 17
powering up 17
production, moving appliance into 14
proxy server identification 213

R
rack installation 15
RADIUS authentication
overview 63
realms 63
smart cards 65
tokens 65
username/password 64
realms
Active Directory 58
adding 110
ASAP WorkPlace 107
Aventail Connect client 107
best practices 109
copying 113
default 106, 112
deleting 113
disabling 112
ing 113
enabling 112
group affinity checking 114
hidden 106, 112
managing 108
overview 105
RADIUS 63
referencing authentication servers 52
restricting user or group membership 113
searching 115
viewing 109
visible 106, 112
redirecting to another site 198
redundant nodes 216
referenced objects, deleting 29
reordering
access control rules 103
shortcuts 193, 194
resetting configurations 149
resource groups
adding 90
deleting 91
ing 91
managing 90
viewing 85
resources
adding 86, 87, 101
deleting 90
ing 90
file system 77, 89
managing 85
network 76, 86
overview 75
URL 76
viewing 85
Web 76, 87
Web application profiles 92
restarting the appliance 17
restoring
configurations 148
factory settings 149
Rollback Tool 154
roots files, verifying 46, 48
routing 33
running OnDemand 202

S
saving changes 23, 27
scp 12
searching realms 115
Secure Desktop. See Aventail Secure Desktop
secure LDAP authentication 53
securing the appliance 239
self-signed certificates 38
serial connections 17
server certificates 38, 53, 56
servers
authentication 51
downstream Web 156
syslog 134
services
configuring 155
overview 79, 155
starting 155
stopping 155
sessions
active user 136
administrator 26
maximum user length 155
Setup Tool 18, 218
shortcuts
adding 191, 192
configuring 190
deleting 193
editing 193
moving 193, 194
overview 183
personal folders 192
reordering 193, 194
viewing 190
shutting down 17
single interfaces 215
single sign-on 68, 69, 70, 92, 93
smart card authentication 65
SNMP
Aventail MIB data 140
configuring 137
downloading Aventail MIB 139
overview 137
retrieving data using 139
SSH access 12, 121
SSL encryption
best practices 241
client/server access service 159
LDAP connections and 53
Web access service 159
starting services 155
stateful failover 216
static routes 35
status window, OnDemand 202
stopping services 155
Sygate On-Demand 180
syslog servers 134
system
backing up 143
backup files 150
logging 124
restoring 143
updating 143, 151
viewing status 135
T
templates, ASAP WorkPlace 195
testing OnDemand 231
time settings 123
token authentication 65
tools
Config Backup Tool 147
Config Compare Tool 150
Config Reset Tool 149
Config Restore Tool 148
Rollback Tool 154
Setup Tool 18, 218
translation
content 93
cookie 93
troubleshooting
clusters 226
overview 229
trusted roots files 39, 45, 53, 58
U
undoing system updates 154
update files 151
upgrading, system 143, 151
upgrading clusters 224
URL resources 76
user access components 3, 183
user access, best practices for 241
user groups
adding 101, 115, 118
deleting 120
editing 119
managing 115
mapping names 105
overview 105
user sessions, disabling 137
username/password authentication 53, 59, 64
users
adding 101, 115, 118
deleting 120
editing 119
ending active sessions 136
mapping names 105
maximum session length 155
monitoring 136
overview 73, 105
V
version number, AMC 136
viewing
access control rules 96
certificate details 46
device profiles 168
log messages 132
network information for clusters 222
resource groups 85
resources 85
shortcuts 190
system status 135
zones 168
virtual IP addresses in clusters 221
visible realms 106, 112
VPNs
designing 73
overview 1
planning 73
W
Web access service
access logs 124, 132
configuring 156
overview 2, 79
SSL encryption 159
starting 155
stopping 155
Web application profiles
adding 92
deleting 95
editing 95
overview 68
viewing 92
Web portals 198
Web resources 76, 81, 87
Web servers, downstream 156
Web shortcuts 191
WholeSecurity Confidence Online 181
Windows name resolution, configuring 37

Z
Zone Labs Integrity 181
zones
  Aventail Connect and 172
  copying 172
  default zones 173
  defining 169, 174, 175, 176
  deleting 173
  device profiles 164, 167
  for special situations 173
  overview 164
  viewing 168