Table of Contents

**Chapter 1**
- Introduction .............................................................................................................................................. 1
  - Introduction to the Aventail VPN ........................................................................................................ 1
- Key SSL VPN Concepts and Aventail Features
  - Resources ............................................................................................................................................... 2
  - Users and Groups .................................................................................................................................. 3
  - Authentication ......................................................................................................................................... 3
  - Communities .......................................................................................................................................... 4
  - Access Policy ....................................................................................................................................... 4
  - End Point Control (EPC) .......................................................................................................................... 5
  - SSL and Encryption ................................................................................................................................. 6
  - Single Sign-On ....................................................................................................................................... 6
  - Higher Availability and Capacity ........................................................................................................... 6
  - Sharing Configuration Data .................................................................................................................... 7
  - Role-Based Administration ..................................................................................................................... 8
  - System Monitoring and Logging ............................................................................................................ 8
- Aventail SSL VPN Components .............................................................................................................. 9
  - Client Components and Access Methods ............................................................................................ 9
  - End Point Control .................................................................................................................................. 13
  - Administrator Components ................................................................................................................... 13

**Chapter 2**
- Planning Your VPN .................................................................................................................................. 17
  - Who Will Access Your VPN? .................................................................................................................. 17
  - What Types of Resources Should Users Have Access To? ................................................................... 18
  - How Will Users Access Your Resources? ............................................................................................... 18
  - Security Administration .......................................................................................................................... 21
    - Defining Resources ............................................................................................................................... 21
    - Managing Access Control with an Access Policy .............................................................................. 23
  - End Point Control .................................................................................................................................. 26
    - Advanced EPC .................................................................................................................................... 27
  - Putting It All Together: Using Realms and Communities ....................................................................... 28

**Chapter 3**
- Preparing for Installation and Deployment ............................................................................................ 31
  - Installation ............................................................................................................................................. 31
    - Deployment Checklist ............................................................................................................................ 32
    - Verifying Your Firewall Policies .......................................................................................................... 34
    - Installation and Configuration Overview ............................................................................................. 35
  - Deployment ............................................................................................................................................ 36
    - Deploying Aventail WorkPlace ........................................................................................................... 36
Deploying the Aventail Access Methods .................................................. 37
Deploying End Point Control Agents ...................................................... 38

Chapter 4
Common VPN Configurations ................................................................. 41
Deployment Scenario: Remote Access for Employees and Partners .............. 41
   Establishing an Authentication Realm ................................................. 41
   Creating an Employee Community .................................................. 43
   Specifying Access Methods for the 'Employees' Community ................. 44
   End Point Control for the 'Employees' Community ............................ 46
   Creating a Partner Community ...................................................... 48
   Specifying Access Methods for the 'Partners' Community ..................... 48
   End Point Control for the 'Partners' Community ................................ 48
   Adding Resources ........................................................................... 50
   Access Control Lists ...................................................................... 51
   Testing the Deployment Scenario .................................................... 52
Other Remote Access VPN Scenarios ....................................................... 53
   Providing Access to Web Resources ............................................... 53
   Web-Based File Access to Entire Networks ....................................... 54
   Remote Access for Mobile Users .................................................... 55
Additional Partner VPN Scenarios .............................................................. 56
   Access to a Specific Web Resource Using an Alias ............................ 56
   Web-based Access to a Client/Server Application .............................. 56
End Point Control Scenarios ..................................................................... 56
   Aventail Cache Control for Employees on Untrusted Systems ............. 57
   Quarantining Employees on Untrusted Systems .................................. 57
   Aventail Secure Desktop for Partners .............................................. 58
   Denying Access .............................................................................. 58
Access Policy Scenarios ........................................................................... 58
Application-Specific Scenarios ................................................................. 59
   Providing Access to Outlook Web Access (OWA) ............................. 59
   Providing Access to Voice Over IP (VoIP) ........................................ 60
   Providing Access to Windows Terminal Services or Citrix Resources .... 60
Authentication Scenarios ......................................................................... 61
   Using Multiple Realms vs. a Single Realm ....................................... 61
Access Component Provisioning ................................................................. 61
   Deploying the Same Agents to All Users ........................................ 62
   Deploying Different Agents to Different Users .................................. 62
WorkPlace Scenarios ............................................................................... 63
   Creating Custom WorkPlace Sites .................................................. 63
   Configuring WorkPlace Features .................................................... 64
   Adding Shortcuts to WorkPlace ...................................................... 65
Chapter 1
Introduction

This chapter provides a brief overview of the features of the Aventail SSL VPN appliance and some of the key concepts associated with a virtual private network. For detailed information and step-by-step procedures describing how to install and configure the appliance, see the separate Installation and Administration Guide or online Help for the Aventail Management Console (AMC).

Introduction to the Aventail VPN

The Aventail SSL VPN appliance provides secure Internet access—with 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 appliance makes applications available using different access methods and devices on a wide range of platforms, including Windows, Macintosh, and Linux. You might use the appliance to:

- Create a remote access VPN that gives remote employees secure access to private company applications such as e-mail.
- Create a business partner VPN that provides designated suppliers with access to an internal supply chain application.
As the administrator, you determine the resources that users have access to, and the Aventail VPN transparently and dynamically uses the access methods appropriate for those resources.

The appliance’s access control enables you to define policy and control access in broad or very specific terms. To increase efficiency, the appliance is managed from a Web-based management console. With the Aventail Management Console (AMC), you can configure the appliance from a standard Web browser, and centrally manage and distribute policy.

Key SSL VPN Concepts and Aventail Features

This section describes the essential concepts that you should become familiar with before installing, configuring, and managing the Aventail SSL VPN appliance.

Resources

The appliance manages a wide variety of corporate resources in three main categories:

- **Web resources**—Applications or services that run over the HTTP or HTTPS protocol, such as Microsoft Outlook Web Access
- **Client/server resources**—Enterprise applications that run over TCP/IP, such as Citrix, and Voice over Internet Protocol (VoIP) telephony applications
- **File shares**—Network servers or computers containing shared folders and files
When specifying a resource type, keep the intended audience in mind. For example, you can give business partners narrow access to a Web application by defining a URL as a resource (and even “alias” the host name for an extra measure of security). To give remote employees broader access, you could define the network segment in which the Web application is located as a domain, IP range, or subnet resource. Employees would then have access to all of the Web resources in that domain.

Users and Groups

A user is an individual who needs access to resources on your network, and a group is a collection of users. After you’ve created users or user groups on the appliance that are mapped to an external authentication server, you can reference them in access control rules to permit or deny them access to resources. You can even form dynamic groups if you want to reference a user population that isn’t already defined in the external directory.

Authentication

Authentication is the process of verifying a user’s identity. To manage user authentication with the appliance, use AMC to define one or more external authentication servers (also known as directory servers or user stores) that contain the credentials for your user population. The actual management of the user information is still done on your authentication servers; the appliance simply makes use of that information to authenticate users.

Creating an authentication realm in AMC also involves specifying an authentication method (username/password, token or smart card, or digital certificate). The Aventail appliance supports the following directories and authentication methods:

- LDAP with username/password
- Microsoft Active Directory with username/password
- RADIUS with username/password or token-based authentication (such as SecurID or SoftID)
- Public Key Infrastructure (PKI) with digital certificate
- CA eTrust SiteMinder with credentials or RSA ClearTrust with credentials
- Local users with username and password (used primarily for testing purposes and not recommended in a production environment)

An authentication realm is what users log in to on the appliance to gain access to your resources. If your organization has only one authentication server, you would create one realm on the appliance. If you have several authentication servers, you can create a realm for each of them, or set up
pairs of servers for chained authentication. To take a more granular approach to deployment and security, you can further subdivide the user population of a realm into communities.

**Communities**

Communities are a cornerstone of the appliance’s approach to deployment and security. They are used to aggregate users and groups for the purpose of deploying access agents and controlling the end point, and can also be referenced in access control rules.

You can create communities for specific types of users, such as remote employees or business partners, or take a more granular approach and create communities of users in a particular department or location.

For example, employees who require broad access to resources and applications on your network could be assigned to a community that offers the network tunnel client as an access method. To make sure that they are using laptops managed by your IT department, specify which End Point Control zones are available to users in this community. You may have another group of users who require only limited access to resources because they’re logging in from public kiosks or other non-secure locations. To give these two different groups access to your network resources, you could create separate communities, each configured to deploy the appropriate access agents, and (in the case of users with non-secure devices) use End Point Control to prevent sensitive data from being left on the device.

**Access Policy**

An access policy is a set of rules that defines the applications or network resources that users or groups are given access to through the appliance.

Access to a resource can be based on several criteria. Most rules control access based on who the user is—that is, the user’s name or group membership—and the destination resource. You can use other criteria in access control rules, such as the access method for a resource, the user’s network address, the zone of trust, or the date and time of the connection request.

The appliance gives you wide latitude in creating access control rules, depending on whether your organization’s security policy is relatively permissive or demands stringent control. For example, if your VPN is accessed only by highly trusted employees who are using computers...
managed by your IT department, you could create an open access policy that defines your entire network domain as a resource and grants broad access to your employees.

Conversely, if you are providing access to a diverse group of users with varying degrees of access privileges, or who connect from less-secure devices such as public kiosks, you might use an access policy that defines individual resources and establishes more granular access requirements.

As the network changes over time, so should your access control rules.

**End Point Control (EPC)**

Traditional VPN solutions typically provide access only from the relative safety of an IT-managed device. 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 the additional risk of computers in untrusted environments, such as a kiosk at an airport or hotel, or an employee-owned computer.

The appliance’s EPC configuration options give you granular control over VPN access using device profiles and zones to protect sensitive data and ensure that your network is not compromised:

- **A device profile** is a set of attributes that characterize the device requesting the connection, such as a Windows domain name, the presence of a certain software program, a registry entry, or other unique characteristics.

- **An End Point Control zone** classifies a connection request based on the presence or absence of a device profile. The zone in which a device is then placed controls the provisioning of data protection components and can be used to determine which resources are available. A device can be placed in a Standard zone, a Quarantine zone (with instructions on installing the required security programs), or in a Deny zone, where the user is denied access to the network.

The appliance also supports integration with third-party client integrity controls that automatically check for malware on the client system before the user authenticates to the appliance.
SSL and Encryption

The Aventail appliance encrypts information using the Secure Sockets Layer (SSL) protocol. SSL is an authentication and encryption protocol that uses a key exchange method to establish a secure environment in which all data exchanged is encrypted to protect it from eavesdropping and alteration.

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

- The Aventail services use a certificate to secure user traffic.
- The Aventail Management Console (AMC) uses a certificate to secure management traffic.

There are two types of certificates: self-signed and commercial. With a self-signed SSL certificate, the appliance identifies itself with a certificate that hasn’t been signed by a commercial CA, and 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 secure user traffic with a certificate from a commercial certificate authority (CA), such as VeriSign.

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 users are not prompted to accept a self-signed certificate each time they connect.

Single Sign-On

Single sign-on (SSO) is an option that controls whether user credentials are forwarded to back-end Web resources. Configuring the appliance to use SSO 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 supports several types of Web-based 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 unique authentication credentials, or “static” credentials (that is, the same credentials for all users). Basic authentication forwarding is configured within a Web application profile, which is assigned to one or more application resources in AMC.

- **NTLM authentication forwarding** provides a secure method for sending Windows network credentials to a Microsoft IIS (Internet Information Services) Web server. NTLM (Windows NT LAN Manager, also known as Windows NT challenge/response authentication) 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.

- **CA eTrust SiteMinder** and **RSA ClearTrust** are third-party products that provide a centralized mechanism for administering authentication and single sign-on. You can configure the appliance to receive user authentication credentials from one of these servers and forward the credentials to any back-end Web resources it is protecting.

### Higher Availability and Capacity

A high-availability cluster of Aventail appliances is designed to prevent a single point of failure by providing integrated load balancing, stateful user authentication failover, and centralized administration. The cluster is administered from a single point and appears as a single appliance to users, applications, and the network.

The Aventail EX-1600 appliance supports a two-node cluster for up to 250 users. In a similar two-node configuration with internal load-balancing, the Aventail EX-2500 can handle up to 2,000 users. These clusters support an Active/Active configuration, meaning that both nodes in the cluster are actively sharing the user load at any given time.

To increase capacity and support more users, the Aventail EX-2500 appliance supports the clustering of up to eight appliances using an external load balancer.
Chapter 1 - Introduction

Sharing Configuration Data

To keep settings matched up, you can replicate and distribute configuration data to a group of Aventail appliances. For example, you might have appliances behind an external load-balancer supporting thousands of users, or appliances in different locations that must share configurations. This is not a merging of data: some of the settings on the receiving appliances are overwritten (security policy and CA certificates, for example), and others are not (network settings).

When you define a collection of appliances that will share settings, the nodes in the collection communicate over the internal interface using SSL. They operate in peer-to-peer mode: replication can be initiated from any system that knows the shared secret for a collection. This is in contrast to the synchronization that occurs in a high-availability cluster of Aventail appliances, in which one node is designated the master.

Role-Based Administration

Permission to manage the appliance and perform specific administration functions using AMC is assigned in AMC. The primary administrator defines the roles and identities of all secondary administrators, setting the permission levels for each administrative role, and creating a password-protected account for each administrator.

System Monitoring and Logging

System monitoring and logging features allow administrators to view both real-time and historical data about the performance of the appliance and its access services, as well as user activity.

The AMC home page displays a graphical summary of the current number of active users, network bandwidth, disk space usage, and CPU usage. More detailed views of this graphical data are available in hourly, daily, weekly, and monthly increments.

You can use AMC to view the total number of active users at any given time and search the list of active sessions by user name. User monitoring also lets you terminate a user’s session, even if the user has multiple active connections on different services or nodes.

If you have an SMTP (Simple Network Management Protocol) tool, you can use it to monitor the appliance as an SNMP agent. The appliance provides a variety of management data in MIB (Management Information Base) format.
The AMC log viewer provides a detailed view of appliance, user access, and other activities contained in a series of log files. The viewer allows you to customize the display of log message data using sorting, searching, and filtering options. If you need to perform additional analysis of the log message data, or display the data differently than how it appears in the log viewer, you can export data to comma-separated values (.csv) files for use by another application, such as Microsoft Excel.

Aventail SSL VPN Components

Your Aventail SSL VPN appliance consists of several administrator and client components. For Web-based access, when a user logs in to Aventail WorkPlace for the first time, the appliance automatically provisions the agent that will provide the broadest range of access based on the user's privileges, operating system, browser configuration, and any other constraints on the user's system. Stand-alone clients, such as the Aventail Connect tunnel, can be provisioned from the appliance or distributed manually.

Client Components and Access Methods

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

Aventail WorkPlace

The Aventail WorkPlace portal provides your users with access to Web-based resources. You can create customized WorkPlace sites, each with a unique URL and appearance (colors, logo, and greeting text). This enables you to configure and deploy unique portals for different audiences, such as partners and employees.

For Windows users, Aventail Access Manager takes care of installing agents and clients through the browser, and client installation log files make the process easy to troubleshoot. Once Access Manager is installed on a user device, most users will be able to receive client updates without requiring administrator privileges.

After a user logs in to WorkPlace, a Web page presents an administrator-defined list of shortcuts. These shortcuts reference the Web-based resources, Windows file system resources, and terminal servers to which the user has access privileges. Users can also add their own WorkPlace bookmarks to Web sites or network shares. The means of access to these resources depends on the user's 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 Web proxy agent) on Microsoft Windows systems running Internet Explorer. The Web proxy agent proxies Web content directly through the appliance.

For users running other browsers, the appliance automatically provides 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 appliance also supports Web-based access to Windows Terminal Services (WTS) and Citrix hosts. These hosts are accessed by Web-based terminal agents that use proprietary protocols to communicate with the terminal server.
Network Explorer

Network Explorer is a Web-based extension, accessible from Aventail WorkPlace, that provides access to any Windows file system resources that the user has permission to use (even from desktop browsers on non-Windows platforms). These resources can include servers, computers, workgroups, folders, and files.

Connect Tunnel Client

The Aventail Connect tunnel client is an application that provides broad access to network resources from devices running a Windows, Macintosh, or Linux operating system. It provides access to any type of application or protocol, including non-TCP protocols such as VoIP (Voice Over Internet Protocol), ICMP, and multicast. The Connect tunnel client is initially installed from the Aventail WorkPlace portal or from a separate installer package.
OnDemand Tunnel Agent

The Aventail OnDemand tunnel agent is lightweight, Web-based, and provides the same broad access to applications and protocols as the Connect tunnel client. It is similar in all respects to the Connect tunnel client except that it is activated each time a user logs in to the Aventail WorkPlace portal from an ActiveX or Java-enabled device.

Connect Mobile Client

The Aventail Connect Mobile client is a lightweight application for Windows Mobile-powered devices. It provides access to a broad range of resources, including client/server applications, thin-client applications, file servers, and Web resources. The Connect Mobile client is installed using a Windows setup program that extracts the application files and then copies the files to the user's mobile device using ActiveSync.

OnDemand Proxy Agent

The Aventail OnDemand proxy agent provides access to network resources protected by the Aventail Web proxy service. It runs as an applet in Java-enabled browsers and as an ActiveX control in Internet Explorer on Windows.

Web Proxy Agent

The Aventail Web proxy agent provides access through Aventail WorkPlace to any Web resource, including Web-based applications, Web portals, and Web servers, as well as Windows network shares. Web proxy access eliminates the need for Web content translation and provides broad access to enterprise Web applications for users running Microsoft Windows, and Internet Explorer with ActiveX enabled.

Translated Web Agent

The translated Web agent provides access to Web resources and Windows network shares. It is available from any Web browser that supports SSL and has JavaScript enabled.

Connect Proxy Client

The Aventail Connect proxy client is a Windows application that provides access to a broad range of resources, including traditional client/server applications, thin-client applications, file servers, and Web resources. Installed on the user's computer, the Aventail Connect proxy client can
provide additional end-point security by requiring personal firewalls and antivirus applications. Aventail Connect supports Microsoft single sign-on and provides seamless access to network share resources from Network Neighborhood.

**End Point Control**

End Point Control (EPC) components ensure that your network is not compromised when accessed from PCs in untrusted environments. As devices attempt to connect to the appliance, EPC “interrogates” them to determine whether they are running the programs that you require. You can also use EPC to specify that a data protection agent—Aventail Cache Control—automatically removes session data from the PC. **Advanced EPC** provides an extended and detailed list of personal firewall, antivirus, and spyware programs to check for in a device profile for clients running on Microsoft Windows, and provides additional session-related security with Aventail Secure Desktop. Advanced EPC is included with the EX-2500 appliance and licensed separately for the EX-750 and EX-1600.

The appliance also supports integration with third-party client integrity controls that automatically check for malware on the client system before allowing access.

**Administrator Components**

This section highlights the key components that you’ll use to manage the Aventail appliance and services.

**Setup Wizard**

Setup Wizard streamlines the initial configuration of the appliance. It guides you through the process of selecting basic network settings, configuring appliance options, defining resources, creating a basic access policy, and creating local users for testing purposes.
Aventail Management Console

AMC is a Web-based administrative tool for managing the appliance. It provides centralized access for managing security policies, configuring the system (including networking and certificate configuration), distributing configuration data, monitoring, troubleshooting, and setting up administrator accounts.

Aventail Access Services

The appliance uses four access services to manage the access clients and agents that users employ to connect to your network resources:

- **The Aventail network tunnel service** is a network routing technology that provides secure network tunnel access to a wide range of applications and protocols, including non-TCP protocols such as VoIP (Voice over IP) and ICMP, reverse-connection protocols like SMS, and bi-directional protocols such as FTP. It works in conjunction with the Aventail Connect tunnel client and the Aventail OnDemand tunnel agent to provide authenticated and encrypted access.

- **The Aventail network proxy service** provides a secure proxy for accessing standard client/server applications. It works in conjunction with the Aventail Connect proxy client to provide authenticated and...
encrypted access over the Internet. The network proxy service is based on the SOCKS v5 protocol, and it brokers and encrypts access to internal applications and networks. Its proxy-based architecture and use of SSL enable the network proxy service to traverse firewalls, NAT devices, and other proxy servers that can interfere with traditional VPN devices.

- **The Aventail Web proxy service** provides users with secure access to Web-based applications and Web servers from a Web browser, or Web-based applications and Web servers from a Windows Mobile-powered device using the Aventail Connect Mobile client. The Web proxy service contains a secure HTTP reverse proxy that brokers and encrypts access to Web-based resources. It also proxies TCP/IP client/server connections for the Aventail OnDemand proxy agent.

- **The Aventail WorkPlace service** controls access to WorkPlace resources accessed from a Web browser. The Aventail 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.
Chapter 2
Planning Your VPN

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

Who Will Access Your VPN?

A key consideration in planning your VPN is identifying the users who need to access your network resources. Your user community will have a major impact on how you design and administer your VPN.

Most VPN users generally fall into one of two major categories: remote employees or business partners.

- **Remote employees.** When serving remote and mobile employees, you'll probably give them 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 the Aventail Connect tunnel client—on the desktop.

- **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 open access privileges, you'll often need to define specific host resources and manage a more complex access policy. When defining a Web resource you may also 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 computers outside the control of your IT organization, a Web-based access method is often best for business partners.

What Types of Resources Should Users Have Access To?

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

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Examples</th>
<th>Planning considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>● Microsoft Outlook Web Access</td>
<td>● When specifying URLs to Web resources, include the <code>http://</code> or <code>https://</code> prefix.</td>
</tr>
<tr>
<td></td>
<td>● Web-based applications</td>
<td>● Use aliases to obscure host names on private networks.</td>
</tr>
<tr>
<td></td>
<td>● Web portals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Web servers</td>
<td></td>
</tr>
<tr>
<td>Client/server</td>
<td>● Terminal servers (such as Citrix or WTS)</td>
<td>● Identify resources by host name, IP address or IP range, subnet IP address, or domain name.</td>
</tr>
<tr>
<td></td>
<td>● Microsoft Outlook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Lotus Notes</td>
<td></td>
</tr>
<tr>
<td>File shares</td>
<td>● Network folders</td>
<td>● A specific file system resource can be an entire server (for example, <code>\ginkgo</code>), a shared folder (<code>\john\public</code>), or a network folder (<code>\ginkgo\news</code>).</td>
</tr>
<tr>
<td></td>
<td>● Shared folders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Network browsing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Windows domains</td>
<td></td>
</tr>
</tbody>
</table>

How Will Users Access Your Resources?

Users can access VPN resources secured by the Aventail appliance using a variety of agents and clients. Your deployment options can range anywhere from “managed” desktops controlled by your IT department, to systems outside of your control, including employees’ home computers, partner desktops, and other systems such as kiosks or handheld devices.

How users gain access to your network resources depends on what those resources are. The Connect tunnel client, for example, is installed on the user’s device and provides the broadest network access and support, and greatest ease of administration. The OnDemand agent also provides broad cross-platform support, but does not handle bi-directional applications like VoIP.
Tunnel, Proxy, or Web: Which Access Method is Best?

Aventail’s access services and clients offer a wide array of methods with different degrees of capability for reaching your organization’s resources. Use the table below to determine which ones are best for you and your users.

Other factors to consider, aside from technical requirements, are:
- **Security requirements**, such as the safeguards you want to put in place on the desktop.
- **User profiles**, including users’ level of technical sophistication.
- **Administrative resources** available to manage and support a VPN.

The following table summarizes the access methods and their advantages.

<table>
<thead>
<tr>
<th>Access method</th>
<th>Provides access to</th>
<th>Advantages</th>
</tr>
</thead>
</table>
| Connect tunnel    | Full network access to client/server applications, Web resources, network shares, and bi-directional applications such as VoIP, SMS, and FTP. | - Stand-alone client installed from Aventail WorkPlace portal or from custom installer package, with no rebooting required.  
                   |                                                                                 | • Enhanced security options including split tunneling, and redirection of all traffic or only local traffic.  
                   |                                                                                 | • Local printing support.  
                   |                                                                                 | • 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.  
                   |                                                                                 | **Note:** Administrator rights are required for installation. |
| OnDemand tunnel   | Full network access to client/server applications, Web resources, network shares, and bi-directional applications such as VoIP, SMS, and FTP. | • Activated from Aventail WorkPlace portal.  
                   |                                                                                 | • Enhanced security options including split tunneling, and redirection of all or only local traffic.  
                   |                                                                                 | • Local printing support.  
                   |                                                                                 | • Auto-updating (Windows client only).  
                   |                                                                                 | **Note:** Administrator rights are required for installation. |
## Chapter 2 - Planning Your VPN

### Access method

<table>
<thead>
<tr>
<th>Provides access to</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Mobile Client/server applications, thin-client applications, and Web resources.</td>
<td>- Stand-alone, lightweight application that runs on Windows Mobile-powered devices.</td>
</tr>
</tbody>
</table>
| OnDemand proxy Client/server applications and Web resources from any Java-enabled or ActiveX platform. | - Broad cross-platform support.  
- Lightweight and easy to administer and deploy.  
**Note:** On Windows, administrator rights are required for dynamic redirection mode. |
| Web proxy agent (Internet Explorer) Any Web resource (including Web-based applications, Web portals, and Web servers) and Windows network shares. | - Convenient access from Internet Explorer with ActiveX enabled.  
- Used as a fallback if other agents—OnDemand proxy, OnDemand tunnel, or Web proxy—can’t run.  
- Minimal client configuration and administration tasks.  
- Users can access any network URL by typing the actual URL in the browser’s address box.  
- Broad Web-based access to enterprise applications.  
- Single sign-on. |
| Translated Web Any Web resource (including Web-based applications, Web portals, and Web servers). Translated Web on Windows operating systems also offers access to network shares. | - Conventional access to Web and file system resources from any Web browser that supports SSL.  
- 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.  
- A good option for providing business partner access, because it does not require any client configuration or administration. |
Security Administration

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

Defining Resources

You have some flexibility when you specify a resource type for a given object on your network. For example, you might define a Web application narrowly as a URL resource for business partners; employees, on the other hand, might be given access to an entire domain, including the Web application.

Web 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). Examples include Microsoft Outlook Web Access and other Web-based e-mail programs, Web portals, corporate intranets, and standard Web servers.

Defining a Web resource as a URL provides several advantages:

- You can create a Web shortcut on Aventail WorkPlace to give users quick access.
- 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.
- You can block attachments from being downloaded to untrusted devices, or prevent a Web-based application from displaying restricted data to untrusted devices.
Chapter 2 - Planning Your VPN

Web traffic is proxied through the Aventail Web proxy service, a secure gateway through which users can access private Web resources from the Internet.

Client/Server Resources

Client/server resources encompass applications, file servers, and multiple Web resources and are specified in AMC using either a domain, subnet, IP range, host name, or IP address:

- **Client/server applications** include "traditional" applications developed for a particular operating system, or thin-client applications that are Web-based.

- **Network shares** include Windows file servers or file shares. Network shares are accessible using either Aventail OnDemand or Aventail Connect. (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 on the location from which the request originates. For example, you might permit connections only from a particular domain, or permit them only from a specific IP address.

- **Graphical terminal agents** can be added to Aventail WorkPlace as shortcuts that provide access to a terminal server (or Citrix server farm) using a Windows Terminal Services or Citrix client.  

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

  On the downside, however, your users cannot access those resources from a shortcut on Aventail WorkPlace; instead, they must know the internal host name of the resource. If the Web proxy agent is running, they can enter any URL directly in the 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 resources. Broad resource definitions simplify your job as system 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 requires 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 Shares**

File shares include Windows network servers or computers containing shared folders and files that users can access through Aventail Workplace.

You can define a specific file system resource by typing a UNC path, or you can define an entire Windows domain:

- A specific file system resource can be an entire server, a shared folder, or a network folder.
- A file system resource can also reference a user’s personal folder on the network. This feature allows you to create a single shortcut on Aventail Workplace that dynamically references a personal folder for the current user.
- Defining an entire Windows domain gives authorized users access to all the network file resources within the domain.

The various options for defining a file system resource provide you with the flexibility to create a granular policy that controls access at the server, share, or folder level, or to create a more open policy that provides access to an entire domain.

**Managing Access Control with an Access Policy**

Once you’ve defined your VPN resources, you control which ones are available to users by creating an access policy.
After a user successfully authenticates (that is, his or her identity is verified), the appliance evaluates the rules that control access to specific resources. Rules appear on the Access Control page:

Access control rules are displayed as an ordered list in AMC. When the appliance evaluates a connection request, it begins at the top of the list and works its way down 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.

Access to a resource can be based on several criteria. Most rules control access based on who the user is—that is, the user's name or group membership—and the destination resource. (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 EPC 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 that allows access only to systems in a "trusted" zone running Aventail Secure Desktop.
In the previous illustration, access to *Remote office desktops* is restricted to users in the *Remote* group who have device profiles that place them in the *Trusted laptop zone.*

- **The address from which the connection request originates.** You might want to control access to a resource based on the names of any source networks you want evaluated in the rule.
- **The access method used to reach the resource.** You might want to enable broad access to resources within an internal domain from the network tunnel or proxy agents, but prevent browser-based access to Web servers within the domain.
- **The encryption strength of the connection.** You might require connections to a particularly sensitive resource to use strong, 128-bit encryption.
- **The day or time of the request.** For example, you might give business partners access to a particular application on weekdays from only 9:00 A.M. to 5:00 P.M.

A connection request can be summarized like this:

1. A user is authenticated and initiates a connection.
2. The appliance analyzes the connection request to identify its attributes (including user and group information, the destination being requested, the 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 and 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, an implicit *Deny* rule is applied.

### Access Control for Bi-Directional Connections

VPN connections typically involve what are called forward connections, which are initiated by a user to a network resource. However, if you deploy Aventail’s network tunnel clients (Connect tunnel or OnDemand tunnel) to your users, bi-directional connections are enabled. Examples of bi-directional connections include an FTP server that downloads files to or uploads files from a VPN user, and remote Help Desk applications.
Within the Aventail VPN, bi-directional connections encompass the following:

- Forward connections from a VPN user to a network resource.
- Reverse connections from a network resource to a VPN user. An example of a reverse connection is an SMS server that “pushes” a software update to a user’s machine.
- Cross-connections refer specifically to VoIP (Voice over IP) applications that enable one VPN user to telephone another. This kind of connection requires a pair of access control rules: one for the forward connection and one for the reverse connection.

**Design Guidelines for Access Rules**

Because the appliance processes your access control rules sequentially, the order in which you organize them is significant 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 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, carefully consider its impact on policy rules.

- **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. AMC validates your rule and notifies you of potential problems when you save it. See "Security Administration" in the Aventail Installation and Administration Guide for details on resolving incompatibility issues.

**End Point Control**

You can use End Point Control to classify devices as they attempt to connect to the appliance. When a device matches a profile that you have created, it is assigned to an EPC “zone of trust,” where the device is granted a certain amount of access, quarantined, or denied access altogether.
An EPC zone can reference one or more device profiles. Multiple device profiles are useful if users with similar VPN access needs use different computer platforms. For example, you could configure an EPC zone that references a device profile for Windows computers, and another zone for Macintosh computers.

Zones are in turn referenced in a community, which determines what data protection agents are deployed. (Optionally, you can reference a zone in an access control rule to determine which resources are available to users in that zone.)

The following diagram illustrates the EPC evaluation process performed by the appliance when a user connects to the appliance:

**Advanced EPC**

Advanced EPC provides an extended and detailed list of personal firewall, antivirus, and spyware programs to check for in a device profile for clients running on Microsoft Windows. It also provides additional session-related security (beyond cache cleaning) with Aventail Secure Desktop.

There are a few device profiles to help you get started: you can use them as is or modify them to suit your access policy and resource requirements. The *Home Users* profile, for example, checks for a wide variety of antivirus and personal firewall programs, while a series of corporate profiles check for programs from particular vendors.
If the preconfigured device profiles don’t address your specific security needs or computing environment, you can create additional profiles that the appliance will use to detect the presence of specified attributes on users’ devices. The types of device profile attributes available are:

- Antivirus software
- Antispyware software
- Application
- Client certificate
- Directory name
- File name, size, or timestamp
- Personal firewall program
- Windows domain
- Windows registry entry
- Windows version

**Putting It All Together: Using Realms and Communities**

Realms are the top-level objects that tie together authentication, user management, access agent provisioning, and End Point Control restrictions.

A realm references one authentication server or a pair of them (for chained authentication). Authentication servers must first be defined in AMC, and they are then referenced by a realm that users log in to.

After users log in to the appliance, they are assigned to a community, which is a user population with similar access and security requirements, or one that is based on user identity or group membership. A community determines which access methods are provided to its member users, and whether any restrictions are placed on their end point devices.
The following illustration shows how a realm authenticates users, assigns them to communities to provision access agents and, with End Point Control enabled, assigns community members to different zones based on the trustworthiness of their computers.

If your network uses a single authentication server to store user information, you’ll probably need to create only one realm in AMC. That realm could then reference the global community that is configured by default in AMC. This would be useful if you have a homogenous user population with identical access requirements.

Using only one realm doesn’t limit your ability to configure more granular levels of user access and End Point Control. AMC allows you to create communities of users within a realm based on their access needs or other security considerations. A community can consist of all the users in a realm, or only selected users or groups.

For example, you might have two distinct groups of users—employees and business partners—requiring different forms of VPN access. The following tables contrast the access agents that are made available to these two groups, and how EPC is used to secure their connections.
Chapter 2 - Planning Your VPN

Employee community

Users connect from trusted computing environments (such as laptops provided by your IT department) and require broad access to your network resources.

<table>
<thead>
<tr>
<th>Access agent</th>
<th>EPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A tunnel client, enabling them to access Web, network, and file share resources.</td>
<td>EPC is used to detect whether employees’ computers are running an antivirus program and firewall before placing them in a trusted zone.</td>
</tr>
</tbody>
</table>

Business partner community

Partners connect through unsecured computing environments and require access only to specific, limited resources.

<table>
<thead>
<tr>
<th>Access agent</th>
<th>EPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited, Web-only access</td>
<td>Business partners are assigned to a less-trusted zone where they are provisioned with Aventail Cache Control.</td>
</tr>
</tbody>
</table>
Chapter 3
Preparing for Installation and Deployment

This chapter provides an overview of the basic steps involved and the information you’ll need in order to install and configure your Aventail appliance and deploy resources to users.

Installation

Use a Web browser to run Setup Wizard and let it guide you through the process of configuring basic network settings and other options. Using the wizard is typically easier for first-time administrators of the appliance.

Setup Wizard also enables you to import your license file, configure an SSL certificate (which is required to proxy traffic), and set the date and time. You can use it to create test users on the appliance and set up some basic resources and access control rules for testing the appliance when you’re done setting it up.

If you prefer using a command-line utility, or if the default IP address for the appliance is already in use on your network, you can configure the appliance by running Setup Tool from a serial connection using a laptop computer or terminal. For more information, see “Appliance Command-Line Tools” in the Installation and Administration Guide.
Deployment Checklist

Before configuring the appliance, you’ll need to gather the information outlined in this section. You’ll provide some of this information when you run Setup Wizard.

The AMC home page includes a Setup Checklist that you can use to track your progress. As each configuration item is completed, a check mark is added:

- **Setup Checklist**
  - Follow these links to set up the appliance:
    - System configuration
      - Configure network settings
      - Configure an SSL certificate
      - Upload license file
      - Define an authentication realm
      - Define an IP address pool
    - Access policy
      - Create application resources
      - Define users and groups
      - Create access control rules
      - Configure Aventail WorkPlace (optional)
      - Configure End Point Control (optional)

To complete the setup checklist you’ll need the following information:

**Root password and appliance name**
- The root password you’ll use to administer the appliance.
- The name for the appliance (optional; the default is AventailSSLVPN). Because this name will be used only in log files, you don’t need to add it to DNS.

**Network interface addressing**
- The IP address, subnet mask, and interface speed for both the internal and the external interfaces (a dual-homed configuration), or just the internal interface (a single-homed configuration).

**Routing information**
- Determine the routing mode for the appliance, which is based in part on whether you are using a dual- or single-homed configuration.
• Network gateway options are also based on your network architecture and whether your appliance is dual-homed or single-homed. Enter the addresses of one or two routers that serve as your access point to another network.
• IP address, netmask, and gateway information for static routes.

**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 (these are required to browse files on a Windows network using Aventail WorkPlace, but otherwise optional).

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

**Authentication information**
• Server name and login information for your authentication servers (Microsoft Active Directory, RADIUS, LDAP, CA eTrust SiteMinder, or RSA ClearTrust).

**Virtual address pool information**
• If you are planning to deploy a network tunnel client (Connect tunnel or OnDemand tunnel), you must either allocate IP addresses for one or more address pools, or use a DHCP server (the appliance sends broadcast requests to locate DHCP servers, or you can specify one).

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

**Clusters**
- If you’re installing a high-availability or high-capacity cluster, you need additional information. See the *Installation and Administration Guide* for more details.

### 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 to enable the appliance to access the following services:

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Port/protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft networking</td>
<td>138/tcp and 138/udp, 137/tcp and 137/udp, 139/udp, 162/snmp, 445/smb</td>
<td>Used by Aventail WorkPlace to perform WINS name resolution, browse requests, and access file shares</td>
</tr>
<tr>
<td>LDAP (unencrypted)</td>
<td>389/tcp</td>
<td>Communicate with an LDAP directory or Microsoft Active Directory</td>
</tr>
</tbody>
</table>
Installation and Configuration Overview

The installation process is composed of several basic steps that are outlined here. For more detailed information, see the Installation and Administration Guide.

1. Rack-mount the appliance, connect the cables, and power it on.
2. Type the static URL for Setup Wizard (192.168.0.10) in the Web browser’s address bar. If this IP address is in use by another device on your network, you must access Setup Wizard from a private network (for example, connect to the appliance using a local hub).
3. Run Setup Wizard to configure the basic network settings, and optionally set up some basic resources, access rules, and test users. (You can alternatively run Setup Tool from the command line.)
4. Log in to AMC to complete the network configuration.
   In your Web browser, type the URL https://<ip>:8443/console, where <ip> matches the address you specified for the internal interface when you ran Setup Wizard. Enter a username of admin and type the root password you created.
5. Configure a server certificate (either a self-signed certificate using AMC, or one obtained from a commercial certificate authority).
6. Define one or more authentication servers.
7. Define a realm containing one or more communities to deploy access agents and optionally provision End Point Control tools.
8. Define application resources.
9. Define users and groups.

### Traffic type | Port/protocol | Usage
---|---|---
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 a RADIUS authentication server
NTP | 123/udp | 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
10. Create access control rules.
11. Configure Web, network, and graphical terminal shortcuts for Aventail WorkPlace.
12. Apply your changes.
13. Test system accessibility.

**Deployment**

After you've defined your resources and access policy, it's time to make those resources available to users. Using AMC, you can make Web resources, file shares, and terminal server resources available to users in Aventail WorkPlace using the clients and agents you specify for them.

- See “How Will Users Access Your Resources?” on page 18 for a complete list of access methods and the advantages of each.
- See “Deploying the Aventail Access Methods” on page 37 for a summary of how access methods are deployed to users.

**Deploying Aventail WorkPlace**

Aventail WorkPlace is a Web portal that provides users with dynamically personalized access to your network. It's an easy way for you to deploy resources directly from the appliance and give users access to the major components of your VPN:

- **Web shortcuts** provide your users with quick access to Web resources. **Network shortcuts** give them access to file system resources, and **Graphical terminal shortcuts** give them Web-based access to resources that are available through Windows Terminal Services or Citrix hosts.
- The **Network Explorer** page provides Web-based access to 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 Aventail WorkPlace, or disable access to file shares entirely.
- Users can create and manage personal **Bookmarks** that point to URLs and other resources that are protected by the Aventail appliance. These personal links are stored on the appliance, so users have access to them whenever (and however) they are logged in to WorkPlace.
The **Intranet Address** box enables users to type a URL or UNC path name for access to resources for which you have not yet created specific shortcuts. For example, a user could type the host name of a Web server, or a specific folder on a Windows share.

You can create multiple WorkPlace sites for different user populations. Each site can have a unique appearance, including logo, heading, greeting text, and FQDN (external URL).

WorkPlace also provides support for a variety of small form factor devices, including PDAs, smartphones, WAP-compatible phones, and i-mode phones. When a user logs into WorkPlace from a small form factor device, WorkPlace detects the device type and automatically transforms to best match the capabilities of the client device.

For complete information on configuring Aventail WorkPlace, see the Aventail *Installation and Administration Guide*.

### Deploying the Aventail Access Methods

This section offers a brief description of how the Aventail access clients and agents are deployed to users. For detailed information, see the Aventail *Installation and Administration Guide*.

<table>
<thead>
<tr>
<th>Access method</th>
<th>Deployment options</th>
</tr>
</thead>
</table>
| Connect tunnel client       | - Users can download and install the client for Windows, Macintosh, or Linux in Aventail WorkPlace.  
- Administrators can create a custom installer package of the Connect tunnel client components and make it available for users to install from another network location (without requiring them to log in to Aventail WorkPlace), or distribute the client as a disk image. |
| OnDemand tunnel agent       | - The agent is automatically activated each time a user logs in to Aventail WorkPlace and authenticates using a Web browser.                      |
| OnDemand proxy agent        | - In embedded mode, OnDemand automatically starts when a user connects to Aventail WorkPlace.  
- In stand-alone mode, the user manually starts OnDemand by clicking a shortcut on WorkPlace. OnDemand appears in a separate browser window. |
| Connect Mobile client       | - The client is installed using a Windows setup program that extracts the application files and then copies the files to the user's Windows Mobile-powered device. |
Deploying End Point Control Agents

This section offers a brief description of how End Point Control components are deployed to users. Both the Aventail and third-party EPC tools are configured on the Agent Configuration page in AMC. For detailed information, see the Installation and Administration Guide.

<table>
<thead>
<tr>
<th>Access method</th>
<th>Deployment options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web proxy agent</td>
<td>• The agent is automatically activated each time a user logs in to Aventail WorkPlace and authenticates using Internet Explorer.</td>
</tr>
<tr>
<td>Translated Web agent</td>
<td>• The translated Web agent provides access through the Aventail WorkPlace portal as a fallback for systems that do not support the Web proxy agent.</td>
</tr>
</tbody>
</table>
| Connect proxy client      | • The client is configured using a separate Windows program called the Aventail Connect Configuration Tool.  
                              • You can customize Connect setup packages using the Aventail Connect Customizer Tool. |

<table>
<thead>
<tr>
<th>EPC component</th>
<th>Deployment steps</th>
</tr>
</thead>
</table>
| Aventail Cache Control    | • Enabled and configured on the Configure Data Protection page.  
                              • EPC must also be enabled on the End Point Control Zones page.  
                              • Deployed on a per-realm basis. |
| Aventail Secure Desktop   | • Upload Aventail Secure Desktop license to the appliance from the Manage Licenses page (requires separate purchase of Advanced EPC for EX-750 and EX-1600 appliances, and is included with the EX-2500 appliance).  
                              • Enabled and configured on the Configure Data Protection page.  
                              • EPC must also be enabled on the End Point Control Zones page.  
                              • Deployed on a per-realm basis. |
| Sygate On-Demand          | • Requires a separate purchase and upload.  
                              • Enabled on the Configure Data Protection page.  
                              • Deployed globally. |
| ZoneLabs Integrity Clientless Security | • Requires a separate purchase and upload.  
                              • Enabled on the Configure Client Integrity page.  
                              • Deployed globally. |
### Deployment steps

<table>
<thead>
<tr>
<th>EPC component</th>
<th>Deployment steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>WholeSecurity Confidence Online</td>
<td>- Requires a separate purchase.</td>
</tr>
<tr>
<td></td>
<td>- A URL pointing to where the WholeSecurity agent must be specified on the Configure Client Integrity page.</td>
</tr>
<tr>
<td></td>
<td>- Deployed globally.</td>
</tr>
</tbody>
</table>
Chapter 4
Common VPN Configurations

This chapter walks you through the configuration steps of a typical deployment: relatively open, remote access for employees, and more restricted access for another group of users, partners. These steps will introduce you to the Aventail Management Console (AMC) and how its configuration elements interact. Even if you used the Web-based Setup Wizard to configure the basic system and establish a security policy, the tutorial is helpful if you are new to the Aventail appliance.

The sample deployment is followed by brief descriptions of other scenarios for configuring and deploying VPN access for your users.

Deployment Scenario: Remote Access for Employees and Partners

To better understand how to deploy a remote access VPN, walk through the steps in this section to set up relatively open access for employees. We’ll set up a Microsoft Active Directory (AD) authentication server, define the community of employees, determine what remote access methods they will use, and define some resources for them. Later, in “Creating a Partner Community” on page 48, we’ll set up remote access for a less trusted group of users. The assumption in this scenario is that you have Advanced EPC, which is included in an evaluation license and with the EX-2500 appliance, and is otherwise licensed separately.

Establishing an Authentication Realm

In order to authenticate your users, you must first define an authentication realm, which is the combination of an existing company directory and an authentication method.

1. From the main navigation menu, click Realms, and then click New.
2. Enter a name for the realm in the Name box. For example, Company XYZ.
3. Click **New** next to the **Authentication server** drop-down list.

4. Select **Microsoft Active Directory**, and then click **Continue**.

5. Enter a name for the authentication server in the **Name** box. For example, **Company Directory**.

6. In the **Primary domain controller** box, type the host name (assuming you’ve already configured DNS) or IP address for the authentication server.

7. To perform Active Directory searches, the appliance must be able to log on to the authentication server. In the **Login name** box, type the Active Directory login name. In the **Password** box, type the password that corresponds with the login name.

8. Click the **Test** button to validate that the connection is properly configured and that the authentication server is accessible from the appliance.

9. Click **Save**. You will be returned to the **Configure Realm** page.
10. From the **Authentication server** drop-down list, select the authentication server you just configured (*Company Directory*).

11. Click **Next** to create a community within the *Company XYZ* realm.

**Creating an Employee Community**

You must now create a new community for your employees. Normally you would set this broadly (to include all employees or a group of them). We’ll add just two users for now.

▶ **Create a community for your employees**

1. You should be on the **Configure Realm - Company XYZ** page in AMC. (If you’re not, click **Realms** in the main navigation menu, click **Company XYZ**, and then click **Communities**.)

2. Click the **Create new** button. The **Configure Community** page appears.

3. Enter a name for the community in the **Name** box. For example, Employees.

4. To add users as members of the community, click **Edit**. The **Users and Groups** window is displayed.
5. In our sample deployment, we’re going to add just two users, one in the sales department and one in human resources (later you’ll see how to control access to resources on the Access Control page). Click New User to create a user mapping:
   a. From the Realm name list, select Company XYZ.
   b. In the Username box, enter a username as it appears in your AD server, and then click Save.
   c. Click New User again and add a second user, and then click Save.

6. Select the check box for each of the two users you just added:

   ![Users and Groups Table]

   Select which users and groups you want referenced. To define a new user or group, click one of the New buttons.

   ![Users and Groups Table]

   Click Save. The Users and Groups window closes and the users are now displayed in the Members list.

7. Click Next.

**Specifying Access Methods for the ‘Employees’ Community**

For each community of users, you can configure which access methods are available: Smart Tunnel Access (IP Protocol), Web-based proxy access (TCP Protocol), or Web access (HTTP).

For the Employees community, it’s likely that you will want to grant open access so that a user can establish remote access using whatever method is appropriate for his or her device. By contrast, the Partners community, in this example, will have only Web access.

Aventail Smart Tunneling gives users an "in-office" experience, with full VPN access to their applications. In the following steps you’ll grant Employees the ability to use OnDemand Tunnel, and set up an IP address pool for the client.
1. In the **Smart tunnel access (IP Protocol)** section, select the **Network tunnel client** check box. A warning is displayed:

<table>
<thead>
<tr>
<th>Access method (IP protocol)</th>
<th>Platform</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel access will not be available until you define an IP address pool. See Help for more information.</td>
<td>Admin privileges</td>
<td>Configure</td>
</tr>
<tr>
<td>Network tunnel client</td>
<td>Internet Explorer, Firefox or Safari with SSL enabled or Address</td>
<td></td>
</tr>
<tr>
<td>Auto-activate from Aventail Workplace (OnDemand Tunnel)</td>
<td>Automatically starts the agent when the user connects to Aventail Workplace</td>
<td></td>
</tr>
</tbody>
</table>

2. Click **Configure**. The **Network Tunnel Client Settings** page is displayed.

3. Click **Edit** next to **Address pools**.

4. On the **Address Pools** page, click **New**.

5. In the **Name** box, enter a label for the IP address pool that will be used to allocate addresses to the network tunnel clients.

6. There are three ways to specify an address pool. If you’re not sure which one to choose, select **Translated address pool (Secure NAT)** so that the appliance will assign non-routable IP addresses to clients and use Secure NAT to translate them to a single address. The drawback is that applications that require reverse connections, such as VoIP or active-mode FTP, may not function properly.

7. Click **Save**. The address pool appears in the **Address Pools** list.

8. Select the check box next to the address pool you just configured and click **Save**.

9. Click **OK**. You should now be back on the **Configure Community - Access Methods** page.

10. Click **Finish**, and then (on the **Configure Realm - Communities** page), click **Finish** again.

11. Click **Pending Changes** in the upper-right corner, and then click **Apply Changes**.
End Point Control for the ‘Employees’ Community

Aventail’s End Point Control (EPC) provides extensive protection to ensure that your users’ access devices are secure. To keep things simple in this example, we will assume that your appliance has a license for Advanced EPC, and we will create two Standard zones: a trusted one for members of the Employees community, and a less trusted one for Partners. We’ll also set up a Quarantine zone for users (employees or partners) whose devices fail to match the profiles that we specify.

Creating a zone is simply a way of setting one or more conditions that users must meet before they are granted access to the SSL VPN. In our example, the user will be classified into the Trusted zone if a certain antivirus program is running (Norton AntiVirus Corporate Edition is used in this example, but you can substitute another program). If the program is not running, the user is classified into the Untrusted zone.

The conditions you set in a real deployment will of course be different—this is just a demonstration of how EPC works.

► Create a Standard zone named Trusted for employees

1. From the main navigation menu in AMC, click End Point Control.
2. Click New and then select Standard zone from the menu. The Zone Definition - Standard Zone page appears.
3. In the Name box, type Trusted.
4. In the All Profiles list, select the check box next to Windows antivirus, and then click the right arrows (>>) to add it to the In Use list. To see the attributes in this built-in profile, click its name:

   ![Current attributes table](image)

   - Delete
   - Value

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus program</td>
<td>Norton AntiVirus</td>
</tr>
<tr>
<td></td>
<td>McAfee VirusScan</td>
</tr>
</tbody>
</table>

5. At the bottom of the Zone Definition page you can specify whether a Data protection agent is required. Skip this step for now.
6. When you are finished configuring the zone, click **Save**. The Standard zone named **Trusted** is now displayed in the list of End Point Control zones. In order to match this profile, a user's device must be running the security programs you specified in step 4.

7. Make sure that EPC is enabled:
   a. From the main AMC navigation menu, click **End Point Control**.
   b. If the link next to **End Point Control** is **Disabled**, click the link and select the **End Point Control** check box on the **Configure General Appliance Options** page.

In this example, we will classify devices that do not match the Standard zone we created into a Quarantine zone named **Untrusted**. A user with a device that is classified as **Untrusted** will see an explanation that you write.

- **Create a Quarantine zone named Untrusted**
  1. From the main AMC navigation menu, click **End Point Control**.
  2. Click **New** and then select **Quarantine zone**.
  3. Enter a name for the Quarantine zone. For example, **Untrusted**.
  4. In the **Customization** area, enter the text a user will see if he or she does not meet the criteria for any of the Standard zones. For example, **You are not running an antivirus product from the approved list.**
  5. Click **Save**. Click **Pending Changes** in the upper-right corner, and then click **Apply Changes**.

Now you need to make the new Quarantine zone the "fallback" for devices that do not meet the requirements of the **Trusted** zone.

- **Quarantine any devices that are not a match for Trusted**
  1. From the main AMC navigation menu, click **Realms**.
  2. Click **Company XYZ**, and then go to the **Communities** page.
  3. In the **Employees** community, click **Edit** next to **End Point Control**.
  4. Under **Zone fallback options**, click **Place into quarantine zone** and then select **Untrusted** from the drop-down list.
  5. Click **OK**, and then click **Save**. Click **Pending Changes** in the upper-right corner, and then click **Apply Changes**.
Creating a Partner Community

1. From the main navigation menu in AMC, click Realms, and then click Company XYZ.
2. On the Configure Realm page, click the Communities link at the top; you’ll see the Employees and Default communities. Click the Create new button.
3. Enter a name for the new community in the Name box. For example, Partners.
4. To add users to the Partners community, click Edit. The Users and Groups window is displayed.
5. You’ll see the two users you added in “Creating an Employee Community” on page 43. Click New User to create a user mapping for a third user:
   a. From the Realm name list, select Company XYZ.
   b. In the Username box, enter a username as it appears in your AD server, and then click Save. The Users and Groups window closes and the user is now displayed in the Members list.
6. Click Next.

Specifying Access Methods for the ‘Partners’ Community

The Partners community in this example should be configured for Web access only, which is the default setting. Click Finish, and then click Save on the Configure Realm page. To save the realm settings before moving on to End Point Control, click Pending Changes in the upper-right corner, and then click Apply Changes.

End Point Control for the ‘Partners’ Community

This section walks you through the steps for creating a Standard zone for partners. In order to be granted VPN access, the partner community member must meet the set of conditions (in other words, match the device profiles) for the Standard zone, otherwise he or she is classified into the Quarantine zone.

You could create a device profile, for example, named Symantec AV that requires one of three Symantec antivirus programs to be running. When this End Point Control policy is in place, a device that matches the profile is placed in a “zone of trust” named Partner zone.
Create a Standard zone named Partner zone for partners

1. From the main navigation menu in AMC, click End Point Control.
2. Click New and then select Standard zone from the menu.
3. In the Name box, type Partner zone.
4. To create a device profile, click New and then select a platform from the shortcut menu (for example, Microsoft Windows).
5. Enter a name for the device profile in the Name box. For example, Symantec AV.
6. Select Antivirus program from the list of attribute types, and then select a series of antivirus programs. For a match, the client device you plan to use for testing should have one of these products. For example, select Symantec Corp. as the vendor, and then select the first three products in the Product name list, clicking Add to Current Attributes after each one.

The Current attributes list at the bottom of the AMC page now looks like this:

```
Current attributes
The following attributes on the client device will be used to match this profile.

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus program</td>
<td>Norton Antivirus, version = 14.x</td>
</tr>
<tr>
<td></td>
<td>Norton Antivirus 2002, version = 8.06.58.x</td>
</tr>
<tr>
<td></td>
<td>Norton Antivirus 2002 Professional, version = 5.x</td>
</tr>
</tbody>
</table>
```

7. Click Save.
8. In the All Profiles list, select the check box for Symantec AV, and then click the right arrow (>) button.
9. At the bottom of the Zone Definition page select Aventail Cache Control from the Required data protection tool list. ACC removes data left on the client after a user’s session, such as the browser cache.
10. When you are finished configuring the zone, click Save. The Standard zone named Partner zone is now displayed in the list of End Point Control zones. Click Pending Changes in the upper-right corner, and then click Apply Changes.
11. From the main AMC navigation menu, click Realms.
12. Click Company XYZ, and then go to the Communities page.
13. In the Partners community, click Edit next to End Point Control.

14. From the Standard zones list, select the check box of the device profile that was just created (Symantec AV) and then click the right arrow (>>) button. The device profile is now displayed in the In use list.

We now want to classify devices that do not match the Standard zone into the Quarantine zone named Untrusted. (This is the same zone that you created for the Employees community.)

► Quarantine any devices that are not a match for Partner zone
1. Under Zone fallback options, click Place into quarantine zone and then select Untrusted from the drop-down list.
2. Click OK, and then click Save. Click Pending Changes in the upper-right corner, and then click Apply Changes.

Adding Resources

The Aventail appliance can manage a wide variety of corporate resources, which are described in “Defining Resources” on page 21. For our sample scenario we will just define a few:

- A network share with marketing materials (intended for business partners and visible to employees)
- Access to Microsoft Outlook on the Web (intended solely for employees)

► Define two corporate resources
1. Click Resources in the main navigation menu in AMC, and then click New and select Network share.
2. Enter a name for the resource in the Name box. This is the only resource in our sample deployment to which partners will have access. Name it VAR marketing collateral.
3. Using UNC syntax, enter the path for the resource in the Network share box. For example, \company_xyz\var\marketing.
4. Select Create shortcut on Aventail WorkPlace so that a link to the resource will be visible to users.
5. Click Save. VAR marketing collateral is now added to your list of resources.
6. Add a second resource: click New and select URL.
7. In the **Name** box, enter *Outlook Web Access*. This resource is intended for employees only.

8. In the **URL** box, enter *https://mail.company_xyz.com*.

9. Select **Create shortcut on Aventail Workplace**.

10. Click **Save**. You should now see two items in your resource list:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Outlook Web Access</em></td>
<td>URL</td>
</tr>
<tr>
<td></td>
<td><em>VAR marketing collateral</em></td>
<td>Network share</td>
</tr>
</tbody>
</table>

11. Click **Pending Changes** in the upper-right corner, and then click **Apply Changes**.

### Access Control Lists

Broadly speaking, access rules define which resources can be accessed by which users. They can be defined very broadly (all the users in *Group X* have access to any corporate resource), or very narrowly (the users in *Group Y* have Web-only access to a single resource).

In our example we’ll keep it simple and give the *Partners* community access to the resource named *VAR marketing collateral*, and give *Employees* access to all of the resources. The appliance evaluates the rules in numbered order. If a match is found, the permit or deny action is applied and no further rules are evaluated.

**Add a rule that gives partners access to VAR marketing collateral**

1. Click **Access Control** from the AMC navigation menu, and then click **New**.

2. Type a name for the rule (for example, *Partner materials*) and leave the **Action** as *Permit*.

3. Next to the **From** box, click the **Edit** button, and then select the check box next to the *Partners* community.

4. Click the **Edit** button next to the **To** box, and then select the check box next to *VAR marketing collateral* in the **Resources** list.

5. Click **Save and Add Another**.
Add a rule that gives employees access to all resources

1. Type a name for the second rule (FT employees only) and leave the Action as Permit.
2. Next to the From box, click the Edit button, and then select the check box next to the Employees community.
3. Click Save. Your access control list now looks like this (Default Workplace permit all rule is present by default in an “open policy”):

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>From</th>
<th>To</th>
<th>Method</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partner materials</td>
<td>Partners</td>
<td>VAR marketing</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>FT employees only</td>
<td>Employees</td>
<td>Any resource</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>Default Workplace permit all</td>
<td>Any user</td>
<td>Aventail Workplace</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

Testing the Deployment Scenario

To test out the scenario you have configured, log in to WorkPlace as an employee, and then (in a separate session) as a partner.

To get to WorkPlace, click Home in the upper-right corner of any AMC page, and then click the link for WorkPlace, just under the appliance image.

Log in as an employee

In “Creating an Employee Community” on page 43, you set up two users who belong to the Employees community. Log in using the credentials of one of those users. If you are in the Trusted zone (that is, your device has the attributes specified in the Windows antivirus device
profile), you should see the two resources you set up in “Adding Resources” on page 50:

Log in as a partner

In “Creating a Partner Community” on page 48, you set up a user who belongs to the Partners community. Log in using the credentials of that user. If you are in the Partners zone—meaning that your device has the attributes specified in the Symantec AV device profile—you should see a single resource (VAR marketing collateral). This is because the appliance found a match for you in the first access control rule; once a match is found, no further rules are evaluated.

Other Remote Access VPN Scenarios

To better understand how to deploy a remote access VPN, here is an overview of some common scenarios.

Providing Access to Web Resources

Web resources are applications or services that run over the HTTP or HTTPS protocols, such as Microsoft Outlook Web Access or a corporate intranet. There are several ways to give users access to these resources—choose the method that is appropriate for your various audiences. For example, you can give business partners narrow access to a Web application by specifying a particular URL in your resource definition. Employees are granted broader access if you define the domain in which that Web application is located as a resource.
Defining Specific Web Resources

To provide user access to a specific Web application or other Web resource:

1. Define a URL resource on the **Add/Edit Resource** page.
2. Create an access control rule referencing the URL on the **Add/Edit Access Rule** page.
3. Add a Web shortcut to WorkPlace on the **WorkPlace Shortcuts** page.

Web Resources on a Portion of Your Network

To provide user access to any Web resource on a given portion of your network:

1. Define a resource (such as a subnet or IP address range) for the portion of the network containing the Web resources on the **Add/Edit Resource** page.
2. Create a rule referencing the network object on the **Add/Edit Access Rule** page.
3. Instruct your users to type the host name or URL for any Web resources in the **Intranet Address** box on WorkPlace.

All Web Resources on Your Network

To provide user access to all the Web resources on your network:

1. Define a resource (such as a domain) for all internal DNS domains on the **Add/Edit Resource** page.
2. Create a rule referencing the network object on the **Add/Edit Access Rule** page.
3. Instruct users to type the host name or URL for any Web resources in the **Intranet Address** box on WorkPlace.

Web-Based File Access to Entire Networks

To provide Web-based access to all the file system resources within a domain:

1. Define a resource referencing your Windows domain on the **Add/Edit Resource** page.
2. Create a rule referencing the domain on the **Add/Edit Access Rule** page.
3. Add a network shortcut referencing the domain on the WorkPlace Shortcuts page.

4. Make sure WorkPlace’s Network Explorer tab is enabled (this is the default state).

5. Instruct your users to click the appropriate link to the file system resource in Network Explorer.

**Broad Access to Network Resources**

To give users comprehensive access to your network resources from devices that are owned and managed by your organization, you can distribute the Aventail Connect clients. These clients run on a wide variety of devices:

- Connect tunnel clients run on Windows, Macintosh, and Linux devices
- The Connect Mobile client gives users with Windows Mobile-powered devices access to both Web and client/server applications

To allow broad, “in-office” access to your network:

1. Define a resource referencing your DNS domain on the Add/Edit Resource page.

2. Create a rule referencing the domain on the Add/Edit Access Rule page.

3. Configure and distribute the network tunnel clients to your users.

**Remote Access for Mobile Users**

Aventail has two remote access solutions for mobile device users:

**WorkPlace Mobile** is a Web portal that provides access to Web-based applications from virtually any mobile device with a functional Web browser. For detailed information on this solution, see the “WorkPlace and Small Form Factor Devices” section of the Installation and Administration Guide or the AMC online Help.

**Aventail Connect Mobile** is a proxy client for Windows Mobile-powered devices that gives users access to a broad range of Web and client/server applications. Connect Mobile users can reach secure, intranet resources that are not available using traditional Web-only access. A link in an e-mail message, for example, to a confidential Word document located on an internal server can be opened just as if the recipient were in the office.
Chapter 4 - Common VPN Configurations

Connect Mobile can also be used with any client/server application that is supported by the mobile device. A salesperson, for example, can use inventory management and CRM applications to send and receive account and supply information securely from any location where there is Internet access. Instead of synchronizing data at the end of the day, opportunities and sales-related activities can be tracked in real-time.

Additional Partner VPN Scenarios

Here are examples of common steps for deploying a VPN to business partners. These scenarios could also be useful in providing VPN access to contractors or other third-party users who require access to your network resources.

Access to a Specific Web Resource Using an Alias

To provide access to a specific Web resource, using an alias to prevent users from seeing its internal host name:

1. Define a URL resource on the Add/Edit Resource page, and then specify an alias for the resource in the page’s Advanced section.
2. Create a rule referencing the URL on the Add/Edit Access Rule page.
3. Add a Web shortcut to WorkPlace on the WorkPlace Shortcuts page.

Web-based Access to a Client/Server Application

To provide Web access to a client/server application, such as a CRM system:

1. Define a network resource on the Add/Edit Resource page, referencing the application’s host name or IP address.
2. Create a rule on the Add/Edit Access Rule page referencing the network resource.
3. Configure the OnDemand tunnel or OnDemand proxy client.
4. Add a Web shortcut on the WorkPlace Shortcuts page.

End Point Control Scenarios

Here are some basic examples of how to deploy End Point Control to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments.
Aventail Cache Control for Employees on Untrusted Systems

Follow these configuration steps to deploy Aventail Cache Control to employees who are connecting from untrusted environments. This configuration uses the global Default EPC zone as a fail-safe for employees who are connecting from devices that don’t match your device profiles.

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 communities used by your employees.

4. Configure the global Default zone to require Aventail Cache Control. Connection requests from devices that don’t match the trusted profile are automatically assigned to the Default zone. Aventail Cache Control then removes history, temporary files, passwords, and cookies from users’ systems after each Web session.

Quarantining Employees on Untrusted Systems

Follow these configuration steps to quarantine an employee who logs in using a device that doesn’t match any of your device profiles. The only resources available will be those that you set up. You could, for example, display a customized page with links to Web resources for bringing the user’s system into compliance with your security policies:

1. Define a device profile on the Device Profile Definition page with an attribute referencing an application or other attribute that is unique to your organization.

2. Configure a Standard zone that references the device profile in step 1.

3. Configure a Quarantine zone that displays a custom Web page with links to resources for bringing a user’s system into compliance.

4. Create a community that references the Standard zone you created, and identify the Quarantine zone as your fallback option. Connection requests from devices that don’t match the trusted profile are automatically assigned to the Quarantine zone.
Aventail Secure Desktop for Partners

To deploy Aventail Secure Desktop (which is part of Advanced EPC) to business partners who are connecting from their company domain:

1. Enable Aventail Secure Desktop on the Agent Configuration page in AMC.
2. Define a device profile with an attribute referencing the partner’s Windows domain name.
3. Reference the device profile in a zone, and configure the zone to require Aventail Secure Desktop.
4. Reference the zone in the community used by your partners.
5. Configure the Default zone to block VPN access (this will prevent unknown systems from accessing the network).

Denying Access

There may be situations in which you want to deny access to an employee using a device that has an unacceptable profile. Follow these configuration steps to deny access to an employee who logs in using a device that is running Google Desktop:

1. Define a device profile with an attribute referencing the Google Desktop application.
2. Reference the device profile in a Deny zone.
3. Reference the Deny zone in the community used by your employees.
4. The Aventail appliance determines that the device is running Google Desktop, making it a match for a Deny zone. Deny zones are always evaluated first: if Google Desktop is running, no other zones are evaluated, the access request is denied, and the user is logged out.

Access Policy Scenarios

Access control rules determine what resources are available to users or groups. Rules can be defined broadly to provide access from any Aventail access method, or defined narrowly so that only a specific access method is permitted.
VPN connections typically involve what are called forward connections—these are initiated by a user to a network resource. All Aventail access methods support forward connections. However, if you are running the Aventail network tunnel service and deploy Aventail’s network tunnel clients to your users, you can also create access control rules for bi-directional connections.

For the Aventail VPN, bi-directional connections encompass:

- **Reverse connections** from a network resource to a VPN user, such as an SMS server that “pushes” a software update to users’ computers.
- **Cross-connections** using Voice over Internet Protocol (VoIP) applications that enable one VPN user to telephone another VPN user. These connections require a pair of access control rules: one for the forward connection and one for the reverse connection. For information on VoIP scenarios, see “Providing Access to Voice Over IP (VoIP)” on page 60.
- Other types of bi-directional connections include FTP servers that download files to or upload files from a VPN user, and remote Help Desk applications.

**Application-Specific Scenarios**

Here are some examples of how to configure the appliance to permit remote users to access some commonly used applications, such as Microsoft Outlook Web Access and Citrix.

**Providing Access to Outlook Web Access (OWA)**

For convenience, AMC includes a pre-configured Web application profile for Microsoft Outlook Web Access (OWA). To provide user access to OWA:

2. Select OWA/Single Sign-On as the Web application profile on the Add/Edit Resource page. This automatically configures single sign-on and content translation for OWA.
3. Create an access control rule referencing the OWA server resource on the Add/Edit Access Rule page.
4. Add a Web shortcut to OWA for Aventail WorkPlace users on the Add/Edit Web Shortcut page.
5. Use the Start page box on the Add/Edit Web Shortcut page to append more specific information to the URL for OWA. For example, if you want the shortcut to point to a directory or file other than the root, type a relative path in the Start page box. If the selected URL for
Outlook Web Access is owa.company_xyz.com, for example, you could set the start page to /mail/root.asp. The resulting URL would be https://owa.company_xyz.com/mail/root.asp.

You can also create a resource that will block e-mail attachments; see the description of the Matching URL resource type in the AMC help.

**Providing Access to Voice Over IP (VoIP)**

To permit users running an Aventail network tunnel client to call each other using a Voice over IP (VoIP) telephony application, follow the steps outlined next.

1. Ensure that the network tunnel service is running on the appliance; you can do this on the AMC home page or Services page.
2. Create an IP address pool for the network tunnel clients (Connect tunnel or OnDemand tunnel) on the Configure Network Tunnel Service page.
3. Ensure that the users who will access the VoIP application belong to a community that is configured to deploy one of the network tunnel clients to their computers. This is done on the Access Methods tab of the Configure Community page.
4. Create an access control rule from the VoIP users to the address pool that will be used for the VoIP application on the Add/Edit Access Rule page.
5. Create a second access control rule from the address pool for the VoIP application to the VoIP users the Add/Edit Access Rule page.

**Providing Access to Windows Terminal Services or Citrix Resources**

To give users access to an individual Windows Terminal Services or Citrix host, or a Citrix server farm, follow the steps outlined here:

1. Install or update the Windows Terminal Services agent or the Citrix agent on the Configure Graphical Terminal Agents page.
2. Define a resource on the Add/Edit Resource page for the Windows Terminal Services or Citrix host, or the Citrix server farm.
3. Create a rule on the Add/Edit Access Rule page referencing the terminal-server resource.
4. Create a WorkPlace shortcut for accessing the Windows Terminal Services host or Citrix resource on the Add/Edit Terminal Shortcut page.
Authentication Scenarios

Realms are used by the appliance for the following key purposes:

- Referencing external authentication servers
- Provisioning access agents to VPN users, based on community membership
- Determining which End Point Control restrictions are imposed on users’ devices
- Controlling the user’s login experience at a WorkPlace portal

Using Multiple Realms vs. a Single Realm

If your organization uses only one authentication server, you'll probably need to configure only one realm in AMC. There are other situations in which multiple authentication servers are required:

- **Multiple user repositories**—If your users are stored in multiple directories, you must create a separate realm for each one. For example, if your employees are stored on an LDAP server, while your business partners are stored on an Active Directory server, you would create a separate realm for each directory server.

- **Chained authentication**—For increased security, you can require users to authenticate to a single realm using two different authentication methods. For example, you could set up RADIUS or a digital certificate as the first authentication method, and LDAP or Active Directory as the second one. To make the login experience for your users a one-step process you can configure AMC such that users see only one set of prompts.

Access Component Provisioning

All of the Aventail user access components are provisioned or activated through the Aventail WorkPlace portal with the exception of the Aventail Connect proxy client.

Optionally, you can make the Aventail Connect tunnel client components available for users to download and install from another network location (such as a Web server, FTP server, or file server), without requiring them to log in to Aventail WorkPlace.

User access agents are deployed on a per-community basis. When configuring a user community, you can specify which access methods will be available to community members to connect to resources on your network.
When a user logs in to Aventail WorkPlace for the first time, WorkPlace automatically provisions and installs the appropriate user access agent based on the user’s community settings. The agent that is deployed will be installed on the user’s computer; on subsequent connections from the same computer with the same Web browser, that same agent is automatically deployed.

**Deploying the Same Agents to All Users**

When you create an authentication realm in AMC, a default community associated with the realm is also automatically created. This single community may be sufficient if you have a homogenous group of users whose resource needs and access methods are identical.

The configuration steps involved in creating a single community are as follows:

1. Create a realm on the **General** section of the **Configure Realm** page that references an external authentication server. AMC automatically creates a default community that is referenced by the realm. The default community settings are global and apply to any realms that reference it.
2. Configure the community by selecting the users or groups who belong to it, the access methods they’ll use to connect to the VPN, and optionally any End Point Control options.

If you have a diverse group of remote users, you’ll probably want to create multiple communities, as described next.

**Deploying Different Agents to Different Users**

Multiple communities give you the flexibility to provision different access agents to different populations of users, and to deploy different End Point Control configurations. Even if your users are stored on a single external authentication server, you may want to segment them by function in your organization, by the types of resources to which they need access, or for security reasons.

For example, you may want to create a community for those employees who use IT-managed laptops for remote access, and provision them with the Connect tunnel client to allow them extensive access to your network resources. For your business partners, you may want to create a community that restricts them to Web access and assigns them to an End Point Control zone that provisions a data protection tool to remove all session data after they log off.
The configuration steps involved in creating multiple communities are as follows:

1. Create a realm that references an external authentication server on the Configure Realm page.
2. Create two or more communities whose membership includes your selected users or groups.
3. Configure the access agents available to each community.
4. Optionally configure an End Point Control zone and device to deploy pre- or post-authentication data integrity tools.
5. Attach the EPC zone to the community.

**WorkPlace Scenarios**

Here are some examples of how to use WorkPlace to create a customized portal that gives users access to your network resources.

**Creating Custom WorkPlace Sites**

You can create multiple WorkPlace sites for different user populations. Each custom WorkPlace site can have its own, unique external URL and appearance.

To create custom WorkPlace sites:

1. Create a WorkPlace site on the Configure WorkPlace Site page.
   - Enter a name for the site and its fully qualified domain name on the General tab, and specify the realm users will log in to.
   - Customize the font, color scheme, logo, and other visual attributes of the site on the Appearance tab.
   - Specify a fully qualified domain for the WorkPlace site. You can have the site share the appliance domain name, or (if you associate the site with a unique SSL certificate) give it a custom host and domain name.
     
     Users will type this name, prefixed with http://, to access WorkPlace. Note that you must communicate this external FQDN to users so they know how to access WorkPlace. You must also add this FQDN to your public DNS.

2. Define the resources you want the users to be able to access on the Add/Edit Resource page.
3. Create the appropriate shortcuts to the resources on the WorkPlace Shortcuts page.
Configuring WorkPlace Features

You can specify whether certain features in the WorkPlace portal are enabled for users. These are global settings (they cannot be configured on a site-by-site basis).

Choose between shortcuts that redirect through a network agent, or that use Web content

Enable/disable personal links

Enable/disable access to Web resources and terminal servers when WorkPlace is running in translated mode

Enable/disable access to file system resources

These settings are configured on the Services page in AMC (click the Configure link under Aventail WorkPlace):

- Personal links: Users can manage a personal list of links that point to resources protected by the Aventail appliance. These are available whenever they log in to WorkPlace.
Web shortcut access: Determine whether URL resources are redirected through a network agent, or Web content translation is used.

Network Explorer: Gives users Web-based access to file system resources.

Intranet address box: When WorkPlace is running in translated mode, users can access a resource just by typing its name.

Adding Shortcuts to WorkPlace

If you don’t want to create customized WorkPlace sites, you can make modifications to the preconfigured default WorkPlace site. Shortcuts, which appear on the WorkPlace home page, provide your users with quick access to Web, network file system, and other resources. They do not require that users know specific URLs, hosts, or file system paths.

To configure shortcuts in WorkPlace:

1. Define the resources (Web, network, or graphical terminal) you want users to be able to access. This is done on the Add/Edit Resource page.

2. Select the type of shortcut you want to create on the WorkPlace Shortcuts page.

3. Configure the relevant shortcut options.