SonicWall® Secure Mobile Access

Deployment Planning Guide

Contents

1

About this Guide

The *SonicWall™ Secure Mobile Access (SMA) Deployment Planning Guide* gives an overview of the features of the Secure Mobile Access SSL VPN appliance and some of the key concepts associated with planning, setting up, and operating a virtual private network.

For basic installation information, refer to the *SMA Getting Started Guide* for your model. For more 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 Appliance Management Console (AMC).

Organization of this Guide

About this Guide	Provides a summary of the contents of the guide and the conventions used.
About SonicWall SMA	Gives a broad overview of how to use the *SonicWall SMA Deployment Planning Guide*, which includes information on different methods of accessing WorkPlace and other resources, how to log in and out, using bookmarks, working with files and folders, and setting up and using Virtual Assistant. Also provided are sections on using a cache cleaner and troubleshooting.
Planning Your VPN	Covers all of the criteria and resources you need to consider when setting up your VPN.
Common VPN Configurations	Takes you through all of the configuration steps of a typical deployment.
SonicWall Support	Provides information about SonicWall Technical Support Resources.

Guide Conventions

Convention	Use
Bold	Highlights dialog, window, screen and button and icon names.
`Code`	Used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.

2

About SonicWall SMA

- About the SMA Appliance
- Key SSL VPN Concepts and SMA Features
- SonicWall SMA Components
- Managing Multiple Appliances

About the SMA Appliance

The SonicWall SMA appliance provides secure remote access to web applications, client/server applications, and file shares for employees, business partners, and customers.

All traffic is encrypted using Transport Layer Security (TLS) to protect it from unauthorized users.

This appliance makes secure remote access possible using different access methods on a wide range of platforms and mobile devices.

The SMA appliance can be used to:

- Create a remote access Virtual Private Network (VPN) that gives remote employees secure access to private company applications such as email.
- 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. The SMA appliance transparently and dynamically uses the access methods appropriate for those resources.

Key SSL VPN Concepts and SMA Features

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

Topics:

- Resources
- Users and Groups
- Authentication
- Communities
- Access Policy
- End Point Control (EPC)
- SSL and Encryption

- Single Sign-On
- Sharing Configuration Data
- Role-based Administration
- System Monitoring and Logging

Resources

The SonicWall SMA 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 makes use of that information to authenticate users.

Creating an authentication realm in AMC also involves specifying an authentication method (username/password or one-time password, token or smart card, or digital certificate).

The SMA appliance supports a broad range of authentication models including:

- Active Directory
- SAML 2.0
- LDAP
- RADIUS
- Kerberos
- Multi-factor authentication
- Federated SSO

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 (EPC) to prevent sensitive data from being left on a 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 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 **application access zone** is a set of attributes used to establish a trust relationship with a client iOS or Android device.
- 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.

SSL and Encryption

The SonicWall SMA appliance encrypts information using the Secure Sockets Layer (SSL) protocol. SSL protocol 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 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 appliance services use a certificate to secure user traffic.
- The Appliance 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 has not been signed by a commercial CA, and the associated private key data is encrypted using a password. AMC uses a self-signed certificate.

A self-signed certificate can also be a wildcard certificate, allowing it to be used by multiple servers which share the same IP address and certificate, but have different FQDNs. For example, a wildcard certificate such as `*.company.com` could be used for iPhone access at and for VPN access at `vpn.company.com`.

You can also configure an authentication server to trust an intermediate CA. For example, you could create a root certificate signing authority on a system that is not connected to the corporate network. You can then issue a set of trusted intermediate signing authority certificates to be deployed in various sectors of the network (often by department or organizational unit).

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. Or, add the self-signed certificate to the user's list of Trusted Root Certificate Authorities in the Web browser.

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.
- **Domain 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. Domain authentication forwarding passes a Windows domain name along with the user's authentication credentials.
- **RSA ClearTrust** is a third-party product that provides a centralized mechanism for administering authentication and single sign-on. You can configure the appliance to receive user authentication credentials and forward them to any back-end Web resources it is protecting.

Sharing Configuration Data

To keep settings matched up, you can replicate and distribute configuration data to a group of SonicWall appliances. For example, you might have 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 SonicWall 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.

If a user is experiencing trouble—for example, he is logged in but cannot establish a connection or is denied access to resources—you can view his session details to diagnose the problem. You can quickly see why a user’s device is classified into a particular zone, and what policy rules are applied, editing them as needed.

If you have an SNMP (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.

SonicWall SMA Components

Your SonicWall SMA appliance consists of several administrator and client components. For Web-based access, when a user logs in to 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 Connect Tunnel, can be provisioned from the appliance or distributed manually.

Topics:

- Client Components and Access Methods
- WorkPlace

Client Components and Access Methods

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

WorkPlace

The 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, 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 JavaScript and 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 would rather not install an agent or your users’ systems don’t support ActiveX, you can configure the appliance to provide Translated Web access.

- As an alternative to Translated Web access, which may have limitations with some Web applications such as AJAX, custom port mapping or custom FQDN mapping can be used. These methods involve mapping the backend resource either to a port on the EX-Series appliance, or to an external fully qualified domain name.

The SMA 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.

Topics:

- Network Explorer
- Connect Tunnel Client
- OnDemand Tunnel Agent
- Mobile Connect App
- Web Proxy Agent
- Translated Web Access
- Custom Port Mapping
- Custom FQDN Mapping
- End Point Control Components
- Virtual Administrator Components

Network Explorer

Network Explorer is a Web-based extension, accessible from 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

Connect Tunnel 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 IP-based type of application protocol and ICMP, and it will route VoIP (Voice Over Internet Protocol) over TCP/IP. Connect Tunnel is initially installed from the WorkPlace portal or from a separate installer package.

OnDemand Tunnel Agent

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

Mobile Connect App

SonicWall Mobile Connect provides fast, safe, easy-to-use secure mobile access to resources from a range of device platforms, including iOS, Android, Mac OS X, and Windows on both smart phones and tablets. Mobile Connect establishes encrypted SSL VPN connections to private networks that are protected by SonicWall SMA or other SonicWall security appliances. The Mobile Connect app is downloaded to a user's mobile device from the App Store, Google Play, Amazon Appstore, or Windows Store.

Web Proxy Agent

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

Translated Web Access

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

Custom Port Mapping

Custom port mapping provides Web-based access by mapping the backend resource or server to a port number at the SonicWall SMA or EX-Series appliance. Custom port mapping does not require installation of a client agent, and works with any Web browser.

Custom FQDN Mapping

Custom FQDN mapping provides Web-based access by mapping the backend resource or server to an external fully qualified domain name (host and domain). The FQDN name should be resolvable to an IP address in the public domain. Custom FQDN mapping does not require installation of a client agent, and works with any Web browser.

End Point Control Components

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, such as Cache Cleaner, 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 device profiles for clients running on Microsoft Windows and Mac OS X. Advanced EPC is included on the SMA 6200, SMA 7200, EX7000, and EX9000 appliance as well with the Virtual Appliance. The only optional purchases for these products are user licenses and support.

Virtual Administrator Components

This section highlights the key components that you'll use to set up and manage the SMA appliance and services.

Topics:

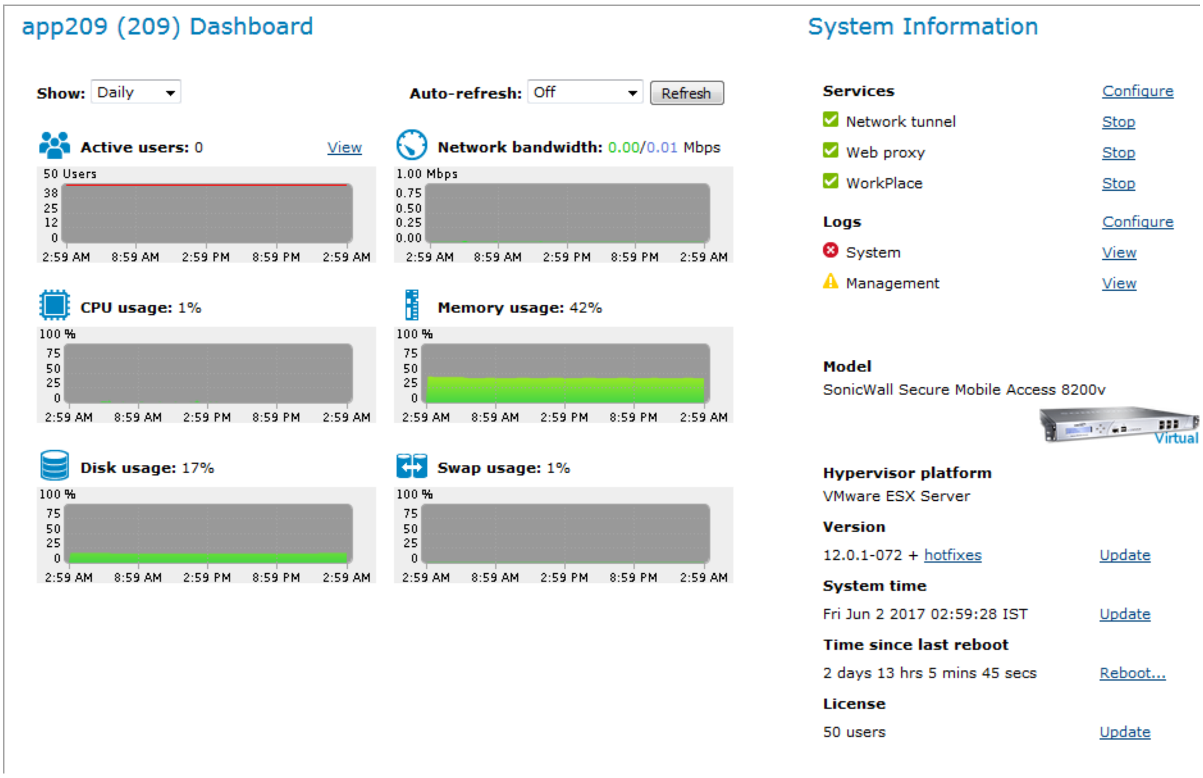
- Setup Wizard
- Appliance Management Console (AMC)
- Access Services

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 local users for testing purposes.

Appliance Management Console (AMC)

The 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.



app209 (209) Dashboard

Show: Daily

Auto-refresh: Off

Active users: 0

Network bandwidth: 0.00/0.01 Mbps

CPU usage: 1%

Memory usage: 42%

Disk usage: 17%

Swap usage: 1%

System Information

Services

☑ Network tunnel

☑ Web proxy

☑ WorkPlace

Logs

System

Management

Model

SonicWall Secure Mobile Access 8200v

Hypervisor platform

VMware ESX Server

Version

12.0.1-072 + hotfixes

System time

Fri Jun 2 2017 02:59:28 IST

Time since last reboot

2 days 13 hrs 5 mins 45 secs

License

50 users

Access Services

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

- **The 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 Connect Tunnel client and the OnDemand Tunnel agent to provide authenticated and encrypted access.
- **The Web proxy service** provides users with secure access to Web-based applications and servers from a Web browser, or Web-based applications and servers from a Windows Mobile-powered device using the Mobile Connect client. The Web proxy service contains a secure HTTP reverse proxy that brokers and encrypts access to Web-based resources.
- **The WorkPlace service** controls access to WorkPlace resources accessed from a Web browser. The 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.

Managing Multiple Appliances

SMA can also provide you with the tools and services to manage multiple network security appliances in your environment.

Topics:

- Central Management Server
- Global High Availability

Central Management Server

The SonicWall Central Management Server (CMS) with Global High Availability (GHA) is an add-on product for managing multiple SMA VPN appliances. It gives customers with multiple appliances a single administrative user interface from where they can manage all their VPN appliances. CMS reduces the total cost of operation and simplifies the management of multiple VPN appliances for organizations.

Global High Availability

Global High Availability (GHA) enables SMA appliances to scale performance by deploying multiple appliances under the same service name. GHA eliminates a single point of failure and provides resilience whether customers deploy 2 SMA appliances in the same data center or clusters of up to 100 physical and virtual appliances across multiple data centers around the globe. In the event of a fail-over, users get connected to another appliance in the service. Their experience is frictionless and productivity is not impacted.

3

Planning Your VPN

- Who Will Access Your VPN?
- Which Types of Resources Should Users Have Access To?
- Security Administration
- End Point Control
- Putting It All Together: Using Realms and Communities

About Designing 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.

Topics:

- Who Will Access Your VPN?
- Which Types of Resources Should Users Have Access To?
- How Will Users Access Your Resources?

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.** 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 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.

Which Types of Resources Should Users Have Access To?

The SonicWall SMA appliance manages a wide variety of corporate resources, which fall into the categories described in Types of user resources.

Types of user resources

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

Topics:

- How Will Users Access Your Resources?
- Tunnel, Proxy, or Web: Which Access Method is Best?

How Will Users Access Your Resources?

Users can access VPN resources secured by the 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?

The SMA 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 the levels of technical sophistication among your users.
- **Administrative resource**s available to manage and support a VPN.

Access method advantages summarizes the access methods and their advantages.

Access method advantages

Access Method	Provides Access to	Advantages
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 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 the 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.
Mobile Connect	Client/server applications, thin-client applications, and Web resources.	• Stand-alone, lightweight application that runs on Windows Mobile-powered devices.
ActiveSync	Email, calendar, contacts, tasks, and out-of-office functions available from the Exchange server.	• Convenient email and related functions access from Apple iPhones and iPads, smart phones running the Google Android operating system, and smart phones running the Symbian operating system
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 OnDemand Tunnel cannot run. • Minimal client configuration and administration tasks. • Users can access any network URL by typing the actual URL in the browser’s address field. • Broad Web-based access to enterprise applications. • Single sign-on.

Access method advantages

Access Method	Provides Access to	Advantages
Translated Web access Custom Port Mapped Web access Custom FQDN Mapped Web access	Any Web resource (including Web-based applications, Web portals, and Web servers). Translated Web on Windows operating systems also offers access to network shares. Custom Port Mapping provides access via a specific port defined by the administrator, which must be open on the external firewall. Custom FQDN Mapping provides access via DNS and requires new DNS entries and possibly a new SSL certificate and IP address.	Convenient access to Web and file system resources from any Web browser that supports SSL and has JavaScript enabled. 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. Custom Port Mapping and Custom FQDN Mapping handle Web programming technologies such as AJAX without the limitations of URL rewriting used in translation.

Security Administration

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

Topics:

- Defining Resources
- Managing Access Control with an Access Policy
- Access Control for Bi-Directional Connections
- Design Guidelines for Access Rules

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.

Topics:

- Web Resources
- Client/Server Resources
- File Shares

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 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.

Web traffic is proxied through the 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 OnDemand or Connect Tunnel. (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 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 OnDemand or Connect Tunnel to get to those resources.

  On the downside, however, your users cannot access those resources from a shortcut on 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 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 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.

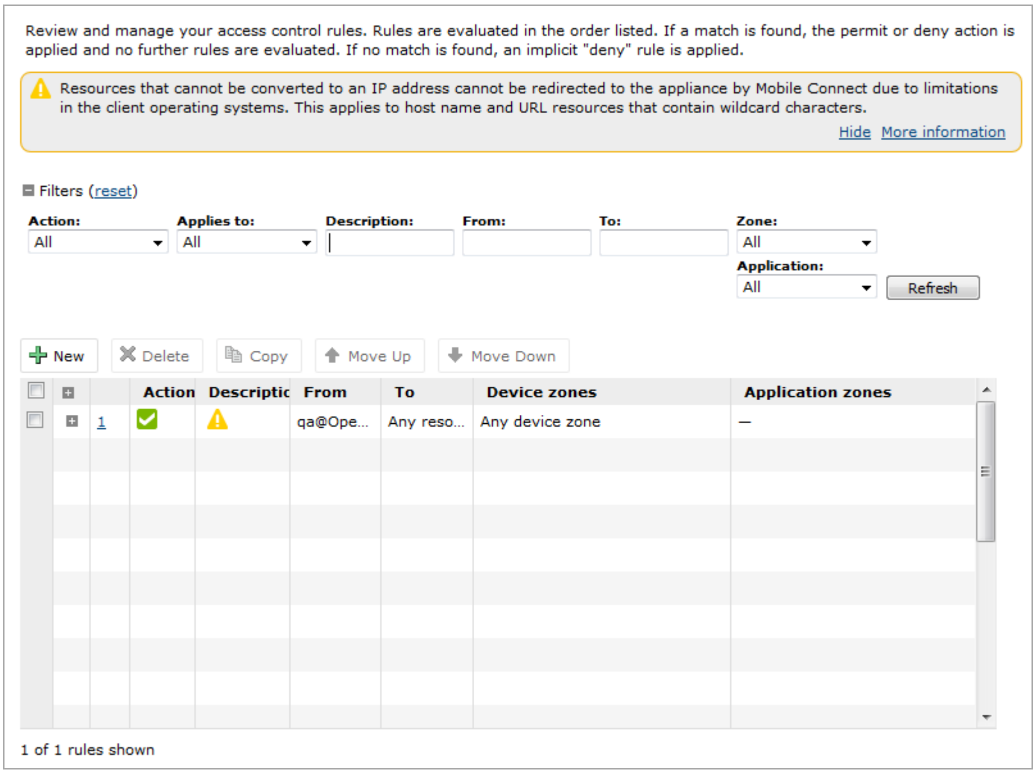
The various options for defining a file system resource provide you with the flexibility to create a granular policy that controls access at the server, share, or folder level, or to create a more open policy that provides access to an entire domain.

Managing Access Control with an Access Policy

After 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 (see Access Control rules).

Access Control rules



Review and manage your access control rules. Rules are evaluated in the order listed. If a match is found, the permit or deny action is applied and no further rules are evaluated. If no match is found, an implicit "deny" rule is applied.

⚠ Resources that cannot be converted to an IP address cannot be redirected to the appliance by Mobile Connect due to limitations in the client operating systems. This applies to host name and URL resources that contain wildcard characters.

Filters (reset)

Action: All
Applies to: All
Description:
From:
To:
Zone: All
Application: All

□	⊞		Action	Descriptic	From	To	Device zones	Application zones
□	⊞	1	✓	⚠	qa@Ope...	Any reso...	Any device zone	—

1 of 1 rules shown

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.)

In addition, you can control access based on several other criteria such as:

- **The EPC zone from which the connection request originates.** Suppose you want to require users accessing a sensitive financial application to run a browser cache cleaner after each session. If so, you could configure a rule that allows access only to systems in a trusted zone that are running a particular program.

  In Access Control rules, 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 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 as follows:

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 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 Secure Mobile Access VPN, bi-directional connections include 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 broader rules that grant more permissions 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. Refer to “Security Administration” in the *Installation and Administration Guide* for details on resolving incompatibility issues.

End Point Control

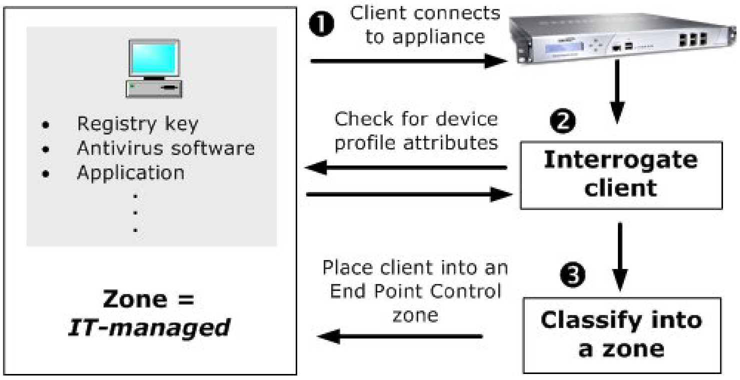
You can use End Point Control to classify devices as they attempt to connect to the appliance. When a device matches a profile that you have created, it is assigned to an EPC zone of trust, where the device is granted a certain amount of access, quarantined, or denied access altogether. In addition, once a device is classified into a given zone, you can keep checking it at a set interval to see if it meets your EPC requirements.

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.

EPC evaluation process illustrates the EPC evaluation process performed by the SMA appliance when a user connects to it.

EPC evaluation process



❶ Client connects to appliance
Check for device profile attributes
❷ Interrogate client
Place client into an End Point Control zone
❸ Classify into a zone
• Registry key
• Antivirus software
• Application
Zone = IT-managed

Advanced EPC

Advanced EPC provides an extended and detailed list of personal firewall, antivirus, and spyware programs to check for on a client. EPC can be done on Windows, OS X, Linux, Android and iOS.

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-user profiles, for example, check 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
- Device ID
- File name, size, or timestamp
- Personal firewall program
- Windows domain
- Windows registry entry
- Windows version

Putting It All Together: Using Realms and Communities

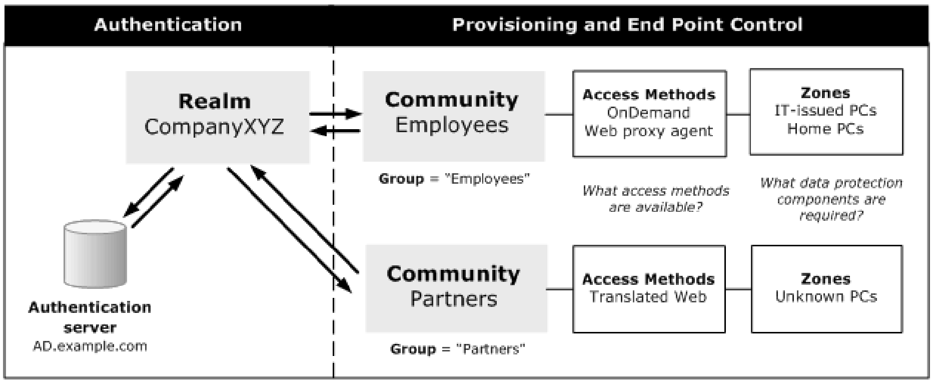
Realms are the top-level objects that tie together authentication, user management, access agent provisioning, and End Point Control restrictions.

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 based on the identity supplied during login. By default, all users are assigned to a default community, but you can sort users into different groups based on individual identity or group memberships. In turn, the community defines a default set of access methods and the set of end point restrictions placed on client devices. The community can also determine the appearance of WorkPlace: the layout and style of WorkPlace pages can be tailored to a particular community.

Authenticating with realms and communities 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.

Authenticating with realms and communities



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 Employee community and Business partner community tables contrast the access agents that are made available to these two groups, and how EPC is used to secure their connections. By creating different WorkPlace styles and layouts you also can determine how WorkPlace looks to members of these two communities.

Employee community

Access Agent	EPC
A tunnel client, enabling them to access Web, network, and file share resources.	EPC is used to detect whether employees' computers are running an antivirus program and firewall before placing them in a trusted zone.
Users connect from trusted computing environments (such as laptops provided by your IT department) and require broad access to your network resources.	

Business partner community

Access Agent	EPC
Limited, Web-only access	Business partners are assigned to a less-trusted zone where they are provisioned with Cache Cleaner.
Partners connect through unsecured computing environments and require access only to specific, limited resources.	

4

Common VPN Configurations

About the Configurations

The following sections take you through the configuration steps of a typical deployment: relatively open, remote access for employees, and more restricted access for partners. As part of this exercise, we also make WorkPlace appear different, depending on which of the two communities the user belongs to. Following these steps will introduce you to the Appliance Management Console (AMC) and how its configuration elements interact.

The sample deployment, Testing the Deployment Scenario, 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, go through the steps in this section to set up relatively open access for employees, and more restricted remote access for a less trusted group, partners. The assumption in this scenario is that you have Advanced EPC, which is included in an evaluation license and with the SMA 6200, SMA 7200, EX6000, EX7000, and EX9000 appliances, and is otherwise licensed separately.

First, we'll lay the foundation for this sample VPN, configuring the items that you'll make use of later when you set up access for the two communities; see VPN building blocks and their descriptions.

VPN building blocks and their descriptions

VPN Building Blocks	Description
Create an authentication realm	Set up a Microsoft Active Directory (AD) authentication server. See Establishing an Authentication Realm.
Identify users	Add a few test users with names that match ones on your AD server. For this test scenario, we will identify two of them as employees, and two of them as partners. See Identifying Users.
Add resources	Define just a few resources. See Adding Resources.
End Point Control	Create two Standard zones of trust: a trusted one for members of the *Employees* community, and a less trusted one for *Partners*. Also, create a quarantine zone for devices that don’t fit into either community.
Create WorkPlace styles and layouts	Change how WorkPlace looks on a per-community basis. Though optional, this produces a more polished and customized look. We will modify the default style and layout and use it for the employees community, and then create a different look for the partner community. See Customizing WorkPlace.

The next step is to put it all together, using the VPN building blocks you created, and configure two communities, an employee community and a partner community. The steps for configuring either community are the same:

Setting up communities and their description

Setting Up Communities	Description
Members	Identify the members for each community.
Access methods	Define what access methods are available.
End Point Control	Create zones of trust: a trusted one for members of the *Employees* community, and a less trusted one for *Partners*.
WorkPlace appearance	Use different WorkPlace styles and layouts for the two communities.
Access control rule	Create rules for what resources can be accessed by which users. See Access Control Lists.

Throughout these procedures, remember to click **Pending Changes** in the upper-right corner in AMC, and then click **Apply Changes** to save your configuration changes.

Topics:

- Establishing an Authentication Realm
- Identifying Users
- Adding Resources
- Creating Zones of Trust

Establishing an Authentication Realm

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

To define an authentication realm:

1 From the main navigation menu, click **Realms**.

2 Click **New realm**.

3 Enter a realm name in the **Name** field. For example, `Company XYZ`.

4 Click **New** next to the **Authentication server** drop-down menu.

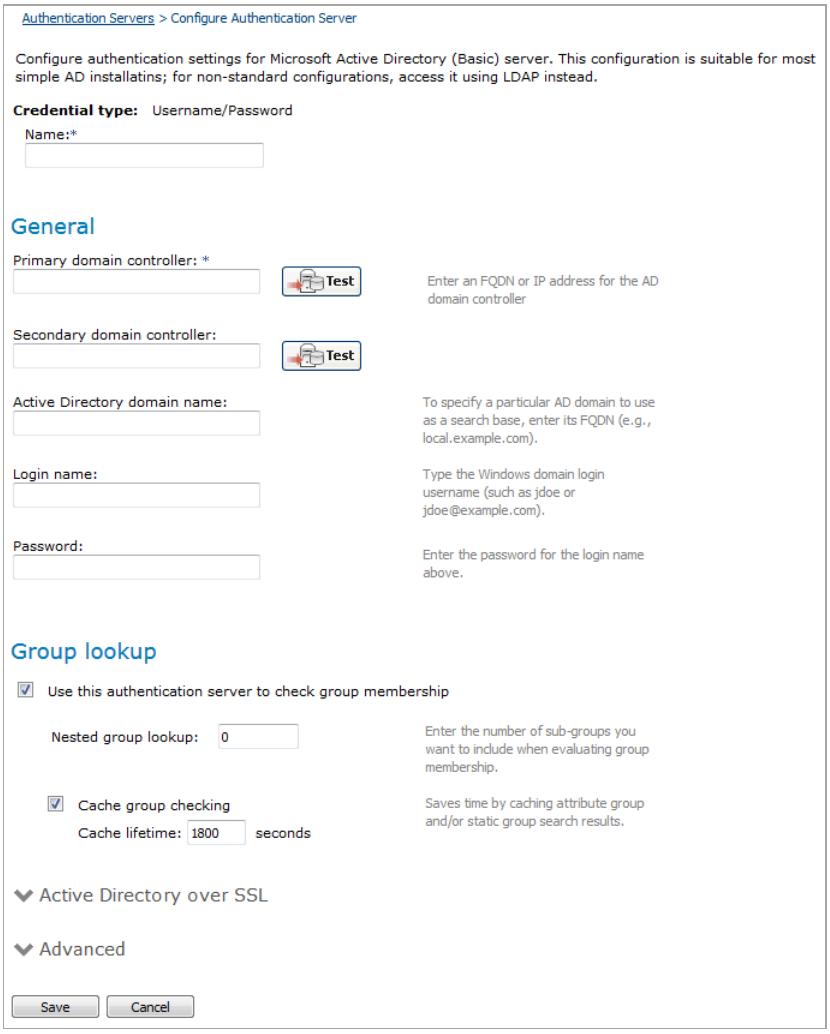
5 Select **Microsoft Active Directory**.

6 Click **Continue**.

7 Enter a name for the credential type in the **Name** field. For example, `Company Directory`.

> **TIP:** Resources sometimes require NTLM credentials to be forwarded to back-end Web servers; Outlook is often set up this way.

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



Authentication Servers > Configure Authentication Server

Configure authentication settings for Microsoft Active Directory (Basic) server. This configuration is suitable for most simple AD installatins; for non-standard configurations, access it using LDAP instead.

Credential type: Username/Password

Name:*

General

Primary domain controller: * — Enter an FQDN or IP address for the AD domain controller

Secondary domain controller:

Active Directory domain name: — To specify a particular AD domain to use as a search base, enter its FQDN (e.g., local.example.com).

Login name: — Type the Windows domain login username (such as jdoe or jdoe@example.com).

Password: — Enter the password for the login name above.

Group lookup

☑ Use this authentication server to check group membership

Nested group lookup: 0 — Enter the number of sub-groups you want to include when evaluating group membership.

☑ Cache group checking — Saves time by caching attribute group and/or static group search results.

Cache lifetime: 1800 seconds

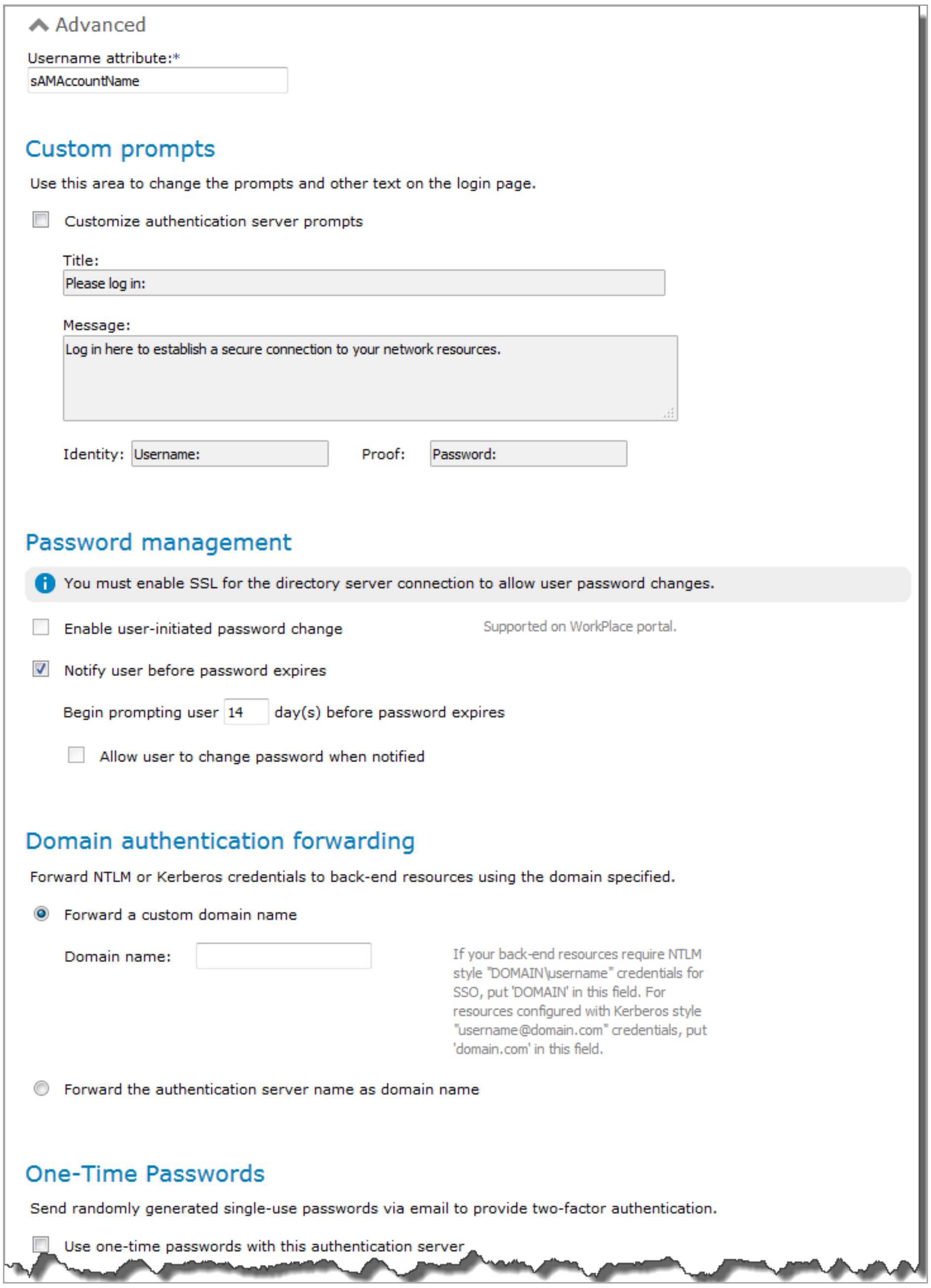
9 To perform Active Directory searches, the appliance must be able to log on to the authentication server. In the **General** section:

   a In the **Login name** field, type the Active Directory login name.

   b In the **Password** field, type the password that corresponds with the login name.

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

11 Expand the **Advanced** settings area.



Advanced

Username attribute:* sAMAccountName

Custom prompts

Use this area to change the prompts and other text on the login page.

□ Customize authentication server prompts

Title: Please log in:

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

Identity: Username: Proof: Password:

Password management

You must enable SSL for the directory server connection to allow user password changes.

□ Enable user-initiated password change Supported on WorkPlace portal.

☑ Notify user before password expires

Begin prompting user 14 day(s) before password expires

□ Allow user to change password when notified

Domain authentication forwarding

Forward NTLM or Kerberos credentials to back-end resources using the domain specified.

● Forward a custom domain name

Domain name:

If your back-end resources require NTLM style "DOMAIN\username" credentials for SSO, put 'DOMAIN' in this field. For resources configured with Kerberos style "username@domain.com" credentials, put 'domain.com' in this field.

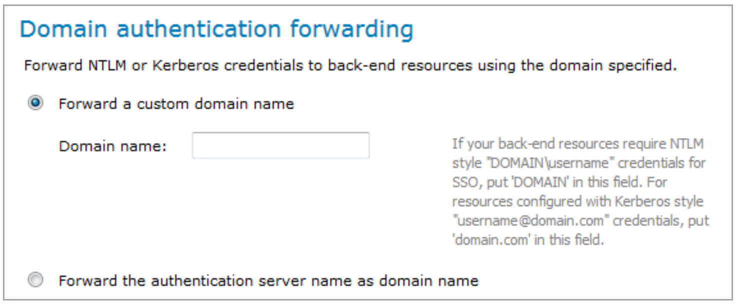
○ Forward the authentication server name as domain name

One-Time Passwords

Send randomly generated single-use passwords via email to provide two-factor authentication.

□ Use one-time passwords with this authentication server

12 Scroll down to the **Domain authentication forwarding** area to specify how the domain name portion of the credentials will be forwarded.



Domain authentication forwarding

Forward NTLM or Kerberos credentials to back-end resources using the domain specified.

● Forward a custom domain name

Domain name:

If your back-end resources require NTLM style "DOMAIN\username" credentials for SSO, put 'DOMAIN' in this field. For resources configured with Kerberos style "username@domain.com" credentials, put 'domain.com' in this field.

○ Forward the authentication server name as domain name

13 In the **Domain authentication section**, select either:

- **Forward a custom domain name**, the default, and enter the domain name in either NILM or Kerberos style.
- **Forward the authentication server name as the domain name**.

14 In the **One-Time Passwords** section, select the **Use one-time passwords with this authentication server** checkbox to enable a one-time password. This is enabled by default.

a Enter the length of the password in the **Passwords contain** field; the default is 8 characters.

b Select the type of acceptable characters, such as **Alphabetic**, **Numeric** from the **characters** drop-down menu.

c In the **From address** field, enter the email address from which email is sent to the user.

d Optionally, if the primary email address attribute exists on the authentication server, enter it in the **Primary email address attribute** field.

e Optionally, if the secondary email address attribute exists on the authentication server, enter it in the **Secondary email address attribute** field.

f Enter the subject for the email sent to the user in the **Subject** field; the default is **One time password**.

g Enter the message to be sent to the user in the **Body** field; the default is **Hi *{username}*, Your one time password is: *{password}***.

15 To test the message, enter an email address in the **Email Address** field and click the **Send test message** button.

16 Click **Save**. You are returned to the **Configure Realm** page.

17 From the **Authentication server** drop-down menu, select the authentication server you just configured (*Company Directory*).

18 Click **Finish** (we will create communities within the *Company XYZ* realm later in this process).

Identifying Users

Using the AD store associated with the *Company XYZ* realm, add two employees and two partners.

To add users:

1 Click **Users & Groups** in the main navigation menu, and then click the **Users** tab.

2 In our sample deployment, we're going to add just four users (later you'll see how to control access to resources based on the user on the **Access Control** page). Click **New**, and then select **Manual entry**.

3 Create four user mappings:

   a From the **Realm name** list, select *Company XYZ*.

   b In the **Username** field, enter a username as it appears in your AD server.

   c Click **Save and add another**.

   d Continue to add three more users.

   e Click **Save**.

Adding Resources

The SonicWall appliance can manage a wide variety of corporate resources, which are described in Defining Resources. 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).

To define two corporate resources:

1 Click **Resources** in the main navigation menu in AMC.

2 Click **New**, and select **Network share**.

3 Enter a name for the resource in the **Name** field. This is the only resource in our sample deployment to which partners will have access. Name it VAR `marketing collateral`.

4 Using UNC syntax, enter the path for the resource in the **Network share** field. For example, `\\company_xyz\var\marketing`.

5 Select **Create shortcut on WorkPlace** so that a link to the resource will be visible to users.

6 Click **Save**. *VAR marketing collateral* is now added to your default resources.

7 Add a second resource:

   a Click **New**.

   b Select *URL*.

8 In the **Name** field, enter `Outlook Web Access`. This resource is intended for employees only.

9 In the **URL** field, enter `https://mail.company_xyz.com`.

10 Select **Create shortcut on WorkPlace**.

11 Click **Save**. You should now see two new items in your resource list.

There are some built-in resources, to make setting up a WorkPlace portal easier; they cannot be deleted. The **Used** column indicates whether a resource is in use (as part of a WorkPlace shortcut or layout, for example). To see where a resource is used, expand its icon. A resource cannot be deleted until it is no longer used by other configuration elements.

Creating Zones of Trust

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 secure, remote access to resources. In our example, the user will be classified into the *Trusted* zone if a certain antivirus program is running (*Norton AntiVirus* 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.

Topics:

- Creating a Standard Zone for Trusted Users
- Creating a Standard Zone for Partners
- Creating a Quarantine Zone for Untrusted Users

Creating a Standard Zone for Trusted Users

To create a Standard zone named Trusted for employees:

1. From the main navigation menu in AMC, click **End Point Control**.
2. If the link next to **End Point Control** is **Disabled**, click the link and select the **Enable End Point Control** checkbox on the **Configure General Appliance Options** page.
3. Click **New,** and then select **Standard zone** from the menu. The **Zone Definition - Standard Zone** page appears.
4. In the **Name** field, type `Trusted`.
5. In the **All Profiles** list, select the checkbox 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.
6. The client device will be checked at login to see if it is running either Norton Antivirus or MacAfee VirusScan. If you want this check to reoccur during a given session, set the interval in minutes in the **Recurring EPC** area.
7. 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. To match this profile, a user's device must be running the security programs you specified in Step 5.

In this example, we will classify devices that do not match the Standard zone we created into a Quarantine zone named *Untrusted*; see Creating a Quarantine Zone for Untrusted Users

Creating a Standard Zone for Partners

To 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** field, 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** field. 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.

7 Click **Save**.

8 In the **All Profiles** list, select the checkbox for **Symantec AV**, and then click the right arrow (**>>**) button.

9 The client device will be checked at login to see if it is running one of the antivirus programs identified in the **Symantec AV** device profile. If you want to this check to reoccur during a given session, set the interval in minutes in the **Recurring EPC** area.

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.

Creating a Quarantine Zone for Untrusted Users

To 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 his or her device 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**.

Customizing WorkPlace

You can alter the appearance of WorkPlace on a per-community basis by creating different styles and layouts:

- Styles are used to customize the look and feel of the WorkPlace login and portal pages. They contain information about fonts, colors, and images that will be displayed on the WorkPlace site.
- WorkPlace layouts are used to customize page content in terms of links, groups, navigation, columns, and personal bookmarks. Creating additional layouts is useful if you find that your access policies don't completely define what you want each user to see.

Both styles and layouts are created independent of communities and can be reused.

In our example we'll modify the default style and layout slightly for the *Employees* community, and then create a different look for the *Partners* community.

Topics:

- Modifying the Default Style and Layout
- Creating a New WorkPlace Style and Layout

Modifying the Default Style and Layout

In our example we'll modify the default style and layout slightly for the *Employees* community, and then create a different look for the *Partners* community.

To modify the default WorkPlace layout and style:

1 Click **WorkPlace** in the main navigation menu, and then click the **Appearance** tab.

2 Click **Default Style** in the **Styles** area.

3 The default look for WorkPlace is intended for employees in our scenario. For now, just change the banner that employees will see. Type `WorkPlace` in the **Title** field.

4 Click **Save**, and then click **Default Layout** in the **Layouts** area.

5 Again, we'll keep changes to a minimum: on the **General** page, select **Display the Personal Bookmarks group**. This automatically displays the content in two columns. Click **Save**.

Creating a New WorkPlace Style and Layout

The appearance of WorkPlace for the *Employees* community in this sample deployment has a few changes (the title is different, and personal bookmarks are included in a two-column page layout). Now we'll create a different look for the partner community.

Topics:

- Creating a WorkPlace Style
- Creating a Workplace Layout

Creating a WorkPlace Style

To create a WorkPlace style for partners:

1 On the main navigation menu, click **WorkPlace**, and then click the **Appearance** tab.

2 In the **Styles** area, click **New**.

3 In the **Name** field, type a unique name for the WorkPlace style. For example, `Partners style`.

4 In the **Font family** list, select the type of font you want to use. (In general, a sans-serif font is easier to read online.)

5 In the **Color scheme** list, click the name of the color scheme you want to use.

6 To replace the SonicWall logo that is displayed in WorkPlace with a different image, use the **Replace with** field to enter or browse for the `.gif` or `.jpg` file you want to use.

7 When **Display gradient background behind logo** is selected, the accent color of your **Color scheme** is displayed at the top of each WorkPlace page, gradually going from dark (at the top of the page) to light. Any heading (**Title**) that you have appears in white.

8 On small form factor devices, the logo specified in the **Images** area is resized by default. The logo is automatically omitted from WAP and i-mode devices, so this setting does not affect the display on those devices.

9 In the **Title** field, type `WorkPlace for Partners`.

10 In the **Greeting** field, type the introductory text that should appear below the title. If you have multiple pages in WorkPlace, the same text appears on all of them.

11 To further assist the user, you could specify a custom **Help file** that provides more detailed information about the resources available on your VPN, or describe how to get technical support.

12 Click **Save** to save *Partners style*.

Creating a Workplace Layout

To create a WorkPlace layout for partners:

1. On the main navigation menu, click **WorkPlace**, and then click the **Appearance** tab.
2. In the **Layouts** area, click **New**.
3. In the **Name** field, type a unique name for the WorkPlace layout. For example, `Partners layout`.
4. In the **Initial content** area, either:
   - Select a layout for any shortcuts and shortcut groups that you've defined.
   - Choose to set up an initial structure for your content and add WorkPlace resources later.

   ⓘ **TIP:** No matter how you decide to lay out your initial content, you can change it later by adding, removing, or rearranging pages and page content.
5. In the **Page navigation** area, specify the kind of navigation controls that will be displayed if your content requires more than one page.
6. Specify whether the **Intranet Address** field will be displayed when this layout is used. It gives users access to resources by typing a resource name (a UNC path, URL, or both).
7. Click **Next**.
8. Click the **Edit page properties** link to change the basic properties of this WorkPlace page. Change its name to *Partner resources*, and then click **Save**.
9. Use the page, column, and shortcut controls to add pages, content, and rearrange the elements on each page (click **Help** in AMC for details on using these controls). Rearranging items in a layout or deleting them from a layout does not affect the resource itself, just its appearance in WorkPlace.
10. Click **Next** to move to the **Device Preview** page to see how the layout will look on devices with different display capabilities. On a mobile device, for example, the **Intranet Address** field cannot be displayed, even if it is configured to be part of a layout.
11. Click **Finish**.

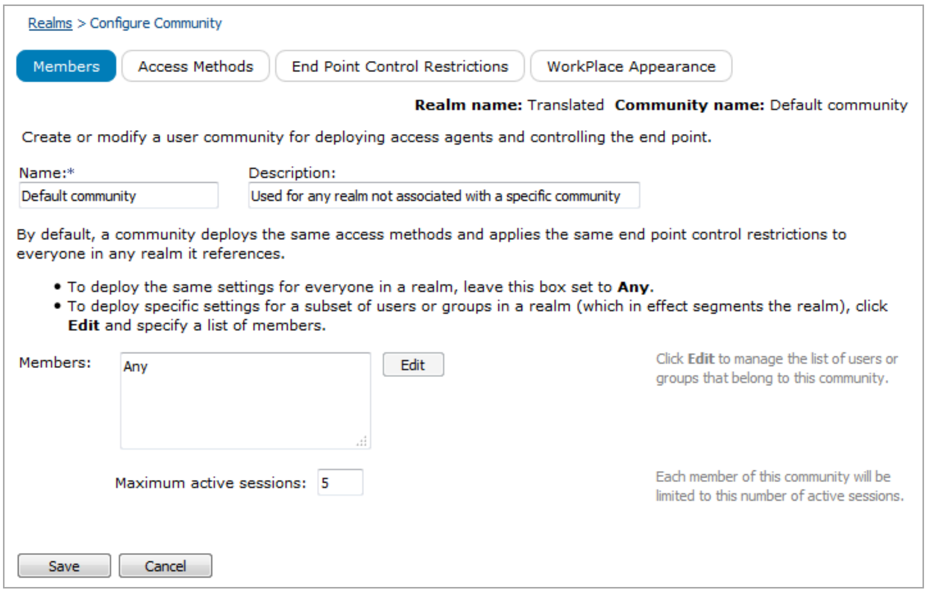
Creating an Employee Community

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

To create a community for your employees:

1. Click **Realms** in the main navigation menu, click **Company XYZ**, and then click the **Communities** page.

2 Click **New**: the **Configure Community** page appears.



Realms > Configure Community

Realm name: Translated **Community name:** Default community

Create or modify a user community for deploying access agents and controlling the end point.

Name:* Default community

Description: Used for any realm not associated with a specific community

By default, a community deploys the same access methods and applies the same end point control restrictions to everyone in any realm it references.

- To deploy the same settings for everyone in a realm, leave this box set to **Any**.
- To deploy specific settings for a subset of users or groups in a realm (which in effect segments the realm), click **Edit** and specify a list of members.

Members: Any

Click **Edit** to manage the list of users or groups that belong to this community.

Maximum active sessions: 5

Each member of this community will be limited to this number of active sessions.

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

4 To add users as members of the community, click **Edit**. The **Users and Groups** dialog is displayed.

5 Select the checkbox next to two of the users you added.

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

7 Click **Next** to configure the access methods allowed for the *Employees* community.

Specifying Access Methods for Employees

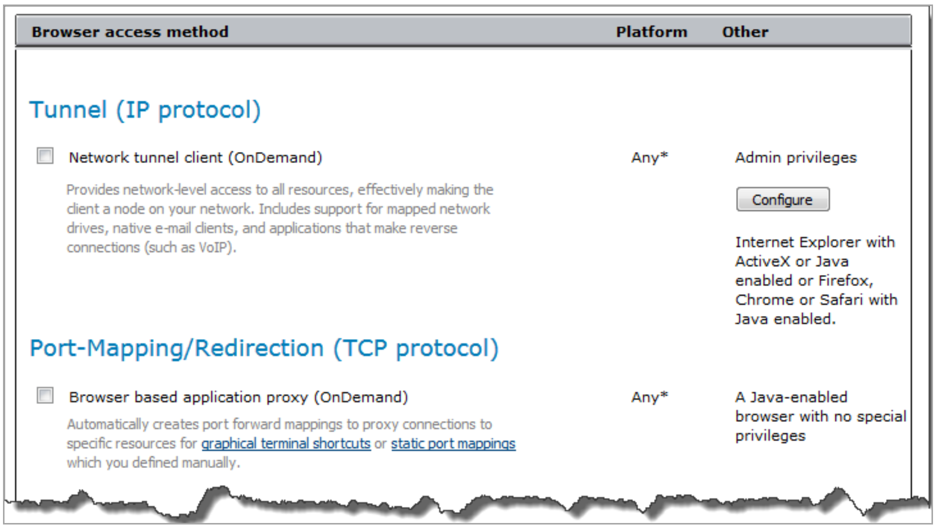
For each community of users, you can configure which access methods are available: Smart Tunnel Access (IP Protocol), Web-based proxy access (TCP Protocol), or Web access (HTTP).

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.

The tunnel clients give 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.

To specify open, tunnel access for employees:

1 In the **Tunnel (IP Protocol)** section, select the **Network tunnel client** checkbox. If you don’t have an IP address pool configured yet, a warning is displayed:



Browser access method	Platform	Other
Tunnel (IP protocol)		
□ Network tunnel client (OnDemand) Provides network-level access to all resources, effectively making the client a node on your network. Includes support for mapped network drives, native e-mail clients, and applications that make reverse connections (such as VoIP).	Any*	Admin privileges Configure Internet Explorer with ActiveX or Java enabled or Firefox, Chrome or Safari with Java enabled.
Port-Mapping/Redirection (TCP protocol)		
□ Browser based application proxy (OnDemand) Automatically creates port forward mappings to proxy connections to specific resources for graphical terminal shortcuts or static port mappings which you defined manually.	Any*	A Java-enabled browser with no special privileges

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

6 There are several ways to specify an address pool. If you're not sure which one to choose, select **Translated address pool (Source NAT)** so that the appliance will assign non-routable IP addresses to clients and use Source 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 checkbox next to the address pool you just configured.

9 Click **Save**.

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

11 Click **Next** to define the zone of trust for employees. Go to Creating Zones of Trust.

Configuring End Point Control for Employees

Configure the *Employees* community to use the zone of trust you configured in Creating a Standard Zone for Trusted Users. (The conditions you set in a real deployment will of course be different—this is just a demonstration of how EPC works.)

To specify the Trusted zone for Employees:

1 In the **Standard zones** list, select the checkbox next to *Trusted* and then click the right arrow (**>>**) button. It is now in the **In use** list.

2 Under **Zone fallback options**, click **Place into quarantine zone** and then select *Untrusted* from the drop-down menu.

3 Click **Next** to select WorkPlace appearance settings for employees.

WorkPlace Appearance for Employees

Configure the *Employees* community to use the WorkPlace look you defined earlier (Modifying the Default Style and Layout).

To specify the Default style and layout for Employees:

1. In the **Style** list, select *Partners style*.
2. In the **Layout** list, select *Partners layout*.
3. On smaller devices, the layout for this community is automatically changed to accommodate them; for example, the Intranet Address field (if it is part of the layout) will be displayed on an advanced mobile device, but not a basic one.
4. Click **Finish**.

Creating a Partner Community

To give remote access to partners—a less trusted group of users—create a separate community.

To create a community for partners:

1. From the main navigation menu in AMC, click **Realms**.
2. Click **Company XYZ**.
3. On the **Configure Realm** page, click the **Communities** link at the top; you'll see the *Employees* and *Default* communities. Click **New**.
4. Enter a name for the new community in the **Name** field. For example, `Partners`.
5. To add users to the *Partners* community, click **Edit**. The **Users and Groups** dialog is displayed.
6. You'll see the users you added in Identifying Users. Click the checkbox next to one or two of them.
7. Click **Next** to configure the access methods allowed for partners.

Specifying an Access Method for Partners

The *Partners* community should be configured for Web access only.

To specify Web access for partners:

1. Clear the **Network tunnel client (OnDemand)** checkbox; only **Web proxy agent** should be selected.
2. Click **Next** to define the zone of trust for partners.

End Point Control for Partners

Configure the *Partners* community to use the zone of trust you configured earlier (Creating a Standard Zone for Partners).

To specify the Partner zone for partners:

1. In the **Standard zones** list, select the checkbox next to *Partner zone*, and then click the right arrow (**>>**) button to put it in the **In use** list.

2. Under **Zone fallback options**, click **Place into quarantine zone** and then select *Untrusted* from the drop-down menu.
3. Click **Next** to select WorkPlace appearance settings for partners.

WorkPlace Appearance for Partners

Configure the *Partners* community to use the WorkPlace look you defined earlier (Creating a New WorkPlace Style and Layout).

To specify the new style and layout for the partners community:

1. In the **Style** list, select *Partners style*, and in the **Layout** list, select *Partners layout*.
2. On smaller devices, the layout for this community is automatically changed to accommodate them; for example, the Intranet Address field (if it is part of the layout) will be displayed on an advanced mobile device, but not a basic one.
3. Click **Finish**.

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.

Topics:

- Adding a Rule for Limited Resources
- Adding an Unrestricted Rule

Adding a Rule for Limited Resources

To add a rule that gives partners access to VAR marketing collateral:

1. Click **Access Control** from the AMC navigation menu.
2. Click **New**.
3. Type a name for the rule (for example, `Partner materials`).
4. Leave the **Action** as **Permit**.
5. Next to the **From** field, click the **Edit** button.
6. Select the checkbox next to the *Partners* community.
7. Click the **Edit** button next to the **To** field.
8. Select the checkbox next to *VAR marketing collateral* in the **Resources** list.
9. Click **Finish and Add Another**.

Adding an Unrestricted Rule

To add a rule that gives employees access to all resources:

1. Type a name for the second rule (`FT employees only`).
2. Leave the **Action** as *Permit*.
3. Next to the **From** field, click the **Edit** button.
4. Select the checkbox next to the *Employees* community.
5. Click **Finish**.

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:

1. Click **Home** in the upper-right corner of any AMC page.
2. Click the link for **WorkPlace**, just under the appliance image.

Logging In as an Employee

In Creating an Employee Community, 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), among the resources you should see will be the two you set up in Adding Resources.

Logging In as a Partner

In Creating a Partner Community, you set up at least one 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—among the resources you should see will be *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.

Topics:

- Providing Access to Web Resources
- Web-Based File Access to Entire Networks
- Broad Access to Network Resources
- Remote Access for Mobile Users

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.

Topics:

- Defining Specific Web Resources
- Web Resources on a Portion of Your Network
- All Web Resources on Your Network

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, distribute the following clients, which run on a wide variety of devices:

- Connect Tunnel clients run on Windows, Macintosh, and Linux devices.
- The Mobile Connect 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

There are 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. You also have the option of customizing the appearance of the portal for mobile devices. 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.
- **SonicWall Mobile Connect** provides fast, safe, easy-to-use secure mobile access to resources from a range of device platforms, including iOS, Android, Mac OS X, and Windows on both smart phones and tablets. Mobile Connect establishes encrypted SSL VPN connections to private networks that are protected by SonicWall SMA or other SonicWall security appliances. The Mobile Connect app is downloaded to a user's mobile device from the App Store, Google Play, Amazon Appstore, or Windows Store.

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.

Topics:

- Access to a Specific Web Resource Using an Alias
- Web-Based Access to a Client/Server Application

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.
2. Specify an alias for the resource in the page's **Advanced** section.
3. Create a rule referencing the URL on the **Add/Edit Access Rule** page.
4. 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 and Tunnel 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.

Topics:

- Quarantining Employees on Untrusted Systems
- Denying Access

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:

To quarantine an employee on Untrusted systems:

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.

Denying Access

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

To deny access:

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 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 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 access methods support forward connections. However, if you are running the network tunnel service and you deploy the network tunnel clients to your users, you can also create access control rules for *bi-directional connections*.

Access control rules for the Secure Mobile Access VPN, bi-directional connections encompass the following:

- **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).
- 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.

Topics:

- Providing Access to Outlook Web Access (OWA)
- Providing Access to Voice Over IP (VoIP)
- Providing Access to Windows Terminal Services or Citrix Resources

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:

1. Define a URL resource for the Outlook Web Access server on the **Add/Edit Resource** page.
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 WorkPlace users on the **Add/Edit Web Shortcut** page.
5. Use the **Start page** field 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** field. 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 one of the network tunnel clients to call each other using a Voice over IP (VoIP) telephony application, follow the steps outlined next.

To provide access to VoIP users:

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:

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, 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 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, configure AMC such that users see only one set of prompts.

Access Component Provisioning

All of the user access components are provisioned or activated through the WorkPlace portal.

Optionally, you can make the 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 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 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.

Topics:

- Deploying the Same Agents to All Users
- Deploying Different Agents to Different Users

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.

To configure a single community:

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.

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 described in Deployment Scenario: Remote Access for Employees and Partners.

5

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SMA Connect Tunnel Deployment Planning Guide
Updated - November 2017
Software Version - 12.1
232-004071-00 RevA

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of US 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
5455 Great America Parkway
Santa Clara, CA 95054