Release Notes

Secure Remote Access

SonicWALL SRA 6.0.0.0

Contents

Platform Compatibility

The SONICWALL SRA 6.0 release is supported on the following platforms:

- **SonicWALL SRA 1200**
- **SonicWALL SRA 4200**
- **SonicWALL SRA Virtual Appliance**

Licensing on the SonicWALL SRA 4200/1200 and Virtual Appliance

The SonicWALL SRA 6.0 firmware provides for user-based licensing on the SonicWALL SRA 4200/1200 appliances and SRA Virtual Appliance. By default, the SRA 4200 comes with a 25-user license and the SRA 1200 and Virtual Appliance come with a 5-user license. On the SRA 4200, extra licenses are added in 10, 25, and 100 user denominations, up to a maximum that allows for 500 concurrent user sessions. On the SRA 1200 and Virtual Appliance, customers can add licenses in 5-user and 10-user denominations, up to a maximum of 50 concurrent user sessions.

Licensing is controlled by the SonicWALL license manager service, and customers can add licenses through their MySonicWALL accounts. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWALL.

License status is displayed in the SSL VPN management interface, on the Licenses & Registration section of the 'System > Status' page. The TSR, generated on the 'System > Diagnostics' page, displays both the total licenses and active user licenses currently available on the appliance.

If a user attempts to log in to the Virtual Office portal and no user licenses are available, the login page displays the error, “No more User Licenses available. Please contact your administrator.” The same error is displayed if a user launches the NetExtender client when all user licenses are in use. These login attempts are logged with a similar message in the log entries, displayed in the 'Log > View' page.

To activate licensing for your appliance or virtual appliance, perform the following steps:

1. Login as admin, and navigate to the System > Licenses page.
2. Click the **Activate, Upgrade or Renew services** link. The MySonicWALL login page is displayed.
3. Type your MySonicWALL account credentials into the fields to login to MySonicWALL. This must be the account to which the appliance is, or will be, registered.

   If the serial number is already registered through the MySonicWALL web interface, you will still need to login to update the license information on the appliance itself.
4. For the SRA 4200 or SRA 1200 appliance, MySonicWALL automatically retrieves the serial number and authentication code. For the virtual appliance, you will need to enter this information:
   - Type the serial number of the virtual appliance into the **Serial Number** field. The serial number and authentication code are provided when the software is purchased.
   - Type the authentication code into the **Authentication Code** field.
5. Type a descriptive name for the appliance or virtual appliance into the **Friendly Name** field, and then click **Submit**.
6. Click **Continue** after the registration confirmation is displayed.
7. Optionally upgrade or activate licenses to other services displayed on the System > Licenses page.
8. After activation, view the System > Licenses page to see a cached version of the active licenses.

Important Differences between the SRA Appliances

Although all SRA appliances support major SRA features, not all features are supported on all SRA appliances.

Similarities

The SonicWALL SRA 4200, SRA 1200, and SRA Virtual Appliance share all major SRA features, including:

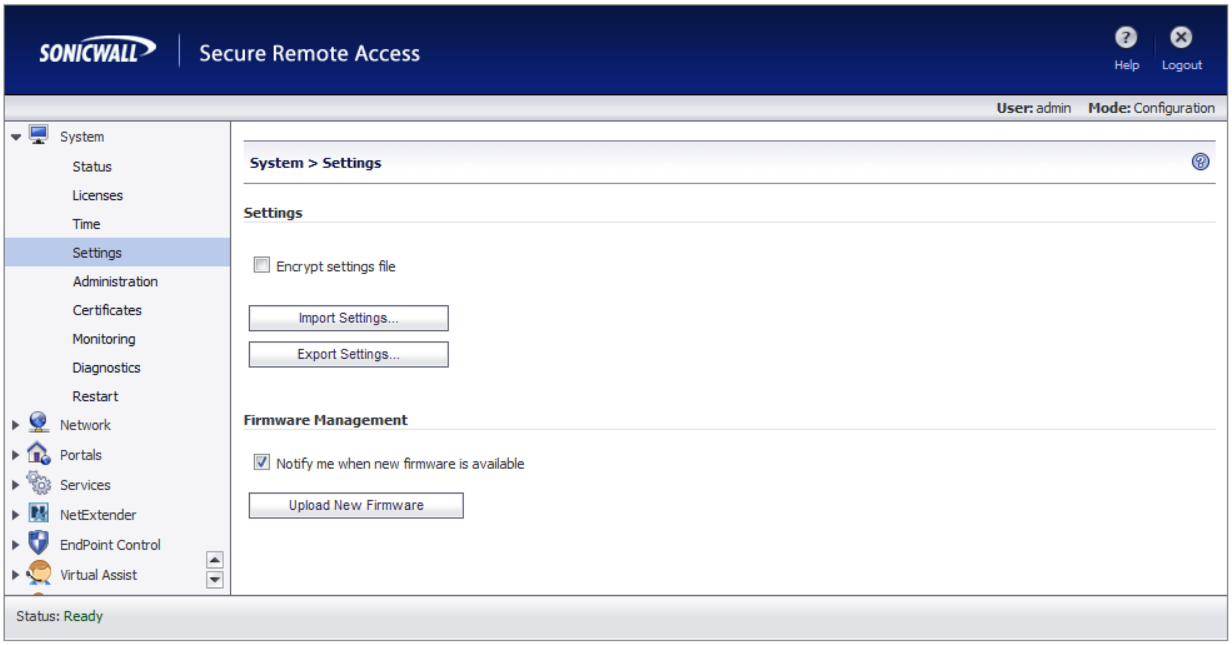
- Virtual Office
- NetExtender
- Virtual Assist
- Virtual Meeting
- Virtual Access
- Application Offloading
- Web Application Firewall

Differences

Important differences between the three SRA appliances are:

Differences	SRA 4200	SRA 1200	SRA Virtual Appliance
SSL Offloading	X		
Application Profiling	X		X
High Availability (HA)	X		
Virtual Meeting	X		X

Following are examples of the VA and SRA 4200/1200 System > Settings page:



System > Settings

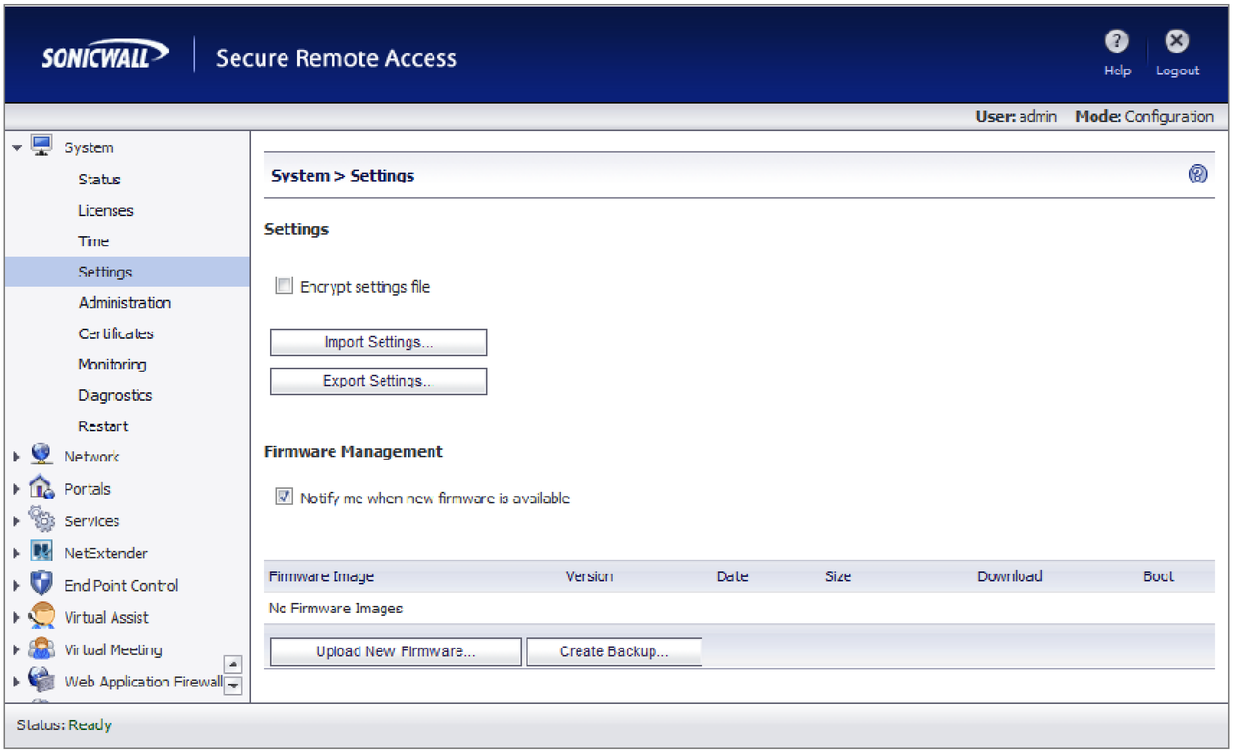
Settings

☐ Encrypt settings file

Firmware Management

☑ Notify me when new firmware is available

Figure 1 System > Settings page for SRA Virtual Appliance



System > Settings

Settings

☐ Encrypt settings file

Firmware Management

☑ Notify me when new firmware is available

Firmware Image	Version	Date	Size	Download	Boot
No Firmware Images					

Figure 2 System > Settings page for SRA 4200/1200

Feature Enhancements in SONICWALL SRA 6.0

The following enhancements and new features are introduced in the SONICWALL SRA 6.0 release:

End Point Control (EPC)

In traditional VPN solutions, accessing your network from an untrusted site like an employee-owned computer or a kiosk at an airport or hotel increases the risk to your network resources. The SonicWALL SRA appliance provides secure access from any Web-enabled system, including devices in untrusted environments.

The SRA appliance supports End Point Control (EPC), which verifies that the user's environment is secure before establishing a connection. EPC protects sensitive data and ensures that your network is not compromised when accessed from devices in untrusted environments. EPC also protects the network from threats originating from client devices participating in the SSL VPN.

The SonicWALL SRA appliance provides these end point security controls by performing host integrity checking and security protection mechanisms before a tunnel session is begun and periodically thereafter if desired. Host integrity checks help ensure that the client system is in compliance with your organization's security policy. SonicWALL end point security controls are tightly integrated with access control to analyze the Windows client system and apply access controls based on the results.

Currently, EPC only supports the Windows NetExtender client. EPC enhancements are supported on the SonicWALL SRA 1200, SRA 4200, and Virtual Appliance platforms.

Perform the following tasks to configure EPC:

1. Image the appliance with 6.0 firmware.
2. Configure the Device Profile (End Point Control > Device Profiles page).
3. Enable End Point Control (End Point Control > Settings page).
4. Add and configure global, group, and user End Point Control Allow/Deny profiles.
5. Configure groups to inherit global policy profiles.
6. Configure users to inherit their group profiles.
7. Configure when End Point Control checks will be performed (Users > Local Users > Edit Global Policies).
8. Connect to NetExtender and monitor the End Point Control logs.

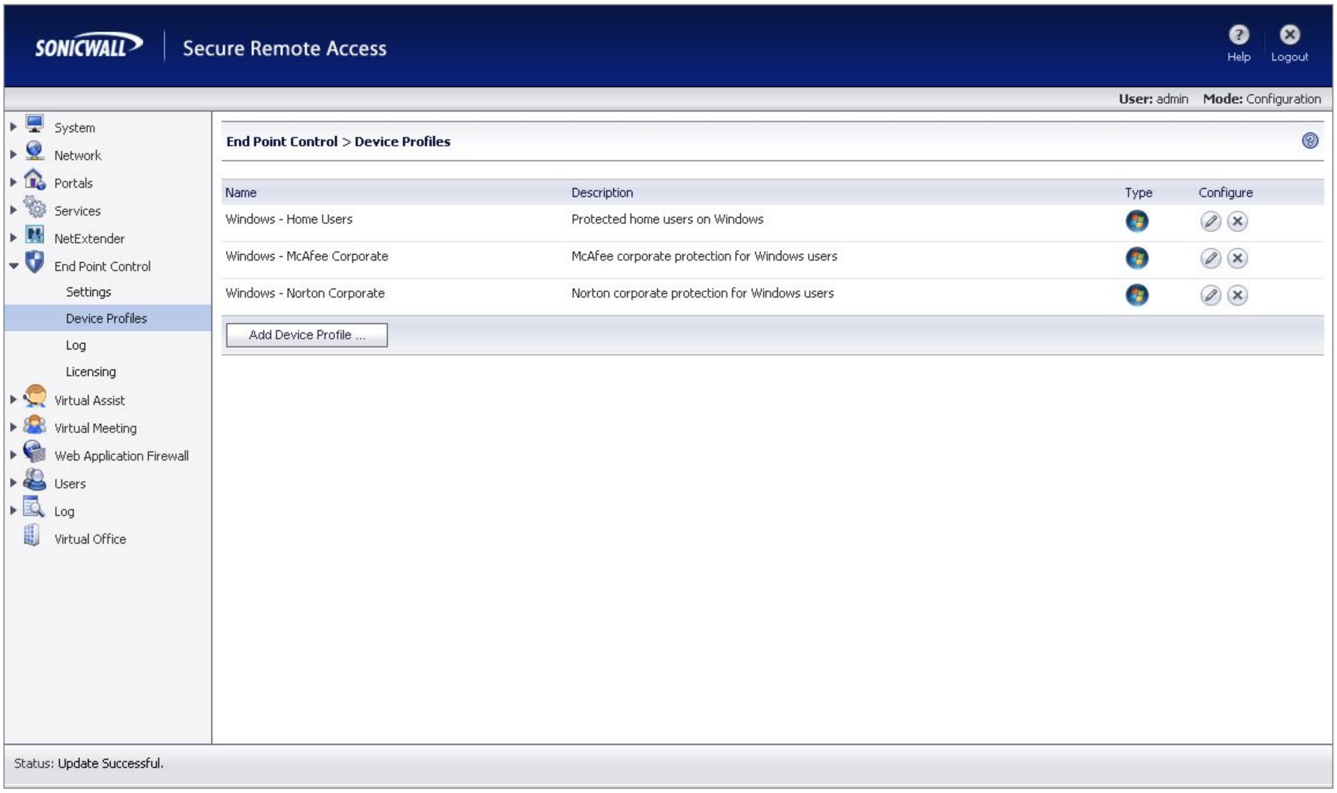
These tasks are explained in more detail in the following sections.

EPC Licensing

End Point Control is a default service available on all SRA appliances and is licensed by default.

Creating Device Profiles

Create Device Profiles to group users together based on various global, group, or user attributes. For example, you can select groups using an Antivirus program, users with a specific Windows version, and so on.



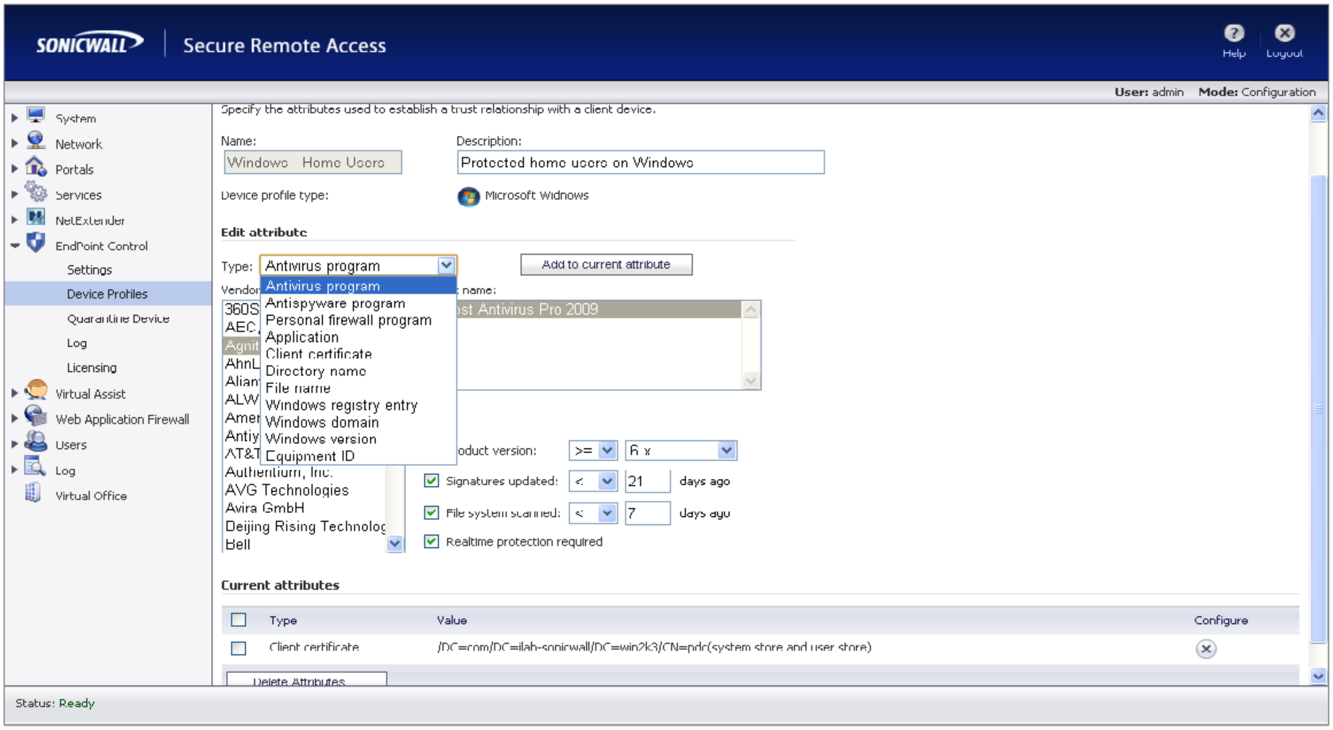
End Point Control > Device Profiles

Name	Description	Type	Configure
Windows - Home Users	Protected home users on Windows		
Windows - McAfee Corporate	McAfee corporate protection for Windows users		
Windows - Norton Corporate	Norton corporate protection for Windows users		

Status: Update Successful.

Figure 3 End Point Control > Device Profiles

Two kinds of profiles are available: Allow profiles and Deny profiles. Allow profiles identify attributes of the client's network that must be present before being authenticated, and Deny profiles identify attributes of the client's network that *cannot* be present. If multiple profiles are defined for a group or user, connection to the SRA appliance is granted only when a client's environment fulfills all Allow profiles for the group or user and does not fulfill any Deny profiles. Use the End Point Control > Device Profiles page to add and manage device profiles.



Specify the attributes used to establish a trust relationship with a client device.

Name: Windows Home Users

Description: Protected home users on Windows

Device profile type: Microsoft Widnows

Edit attribute

Type: Antivirus program

☑ Signatures updated: < 21 days ago

☑ File system scanned: < 7 days ago

☑ Realtime protection required

Current attributes

□	Type	Value	Configure
□	Client certificate	/DC=com/DC=ilab-sonicwall/DC=win2k3/CN=pdc(system store and user store)	⊗

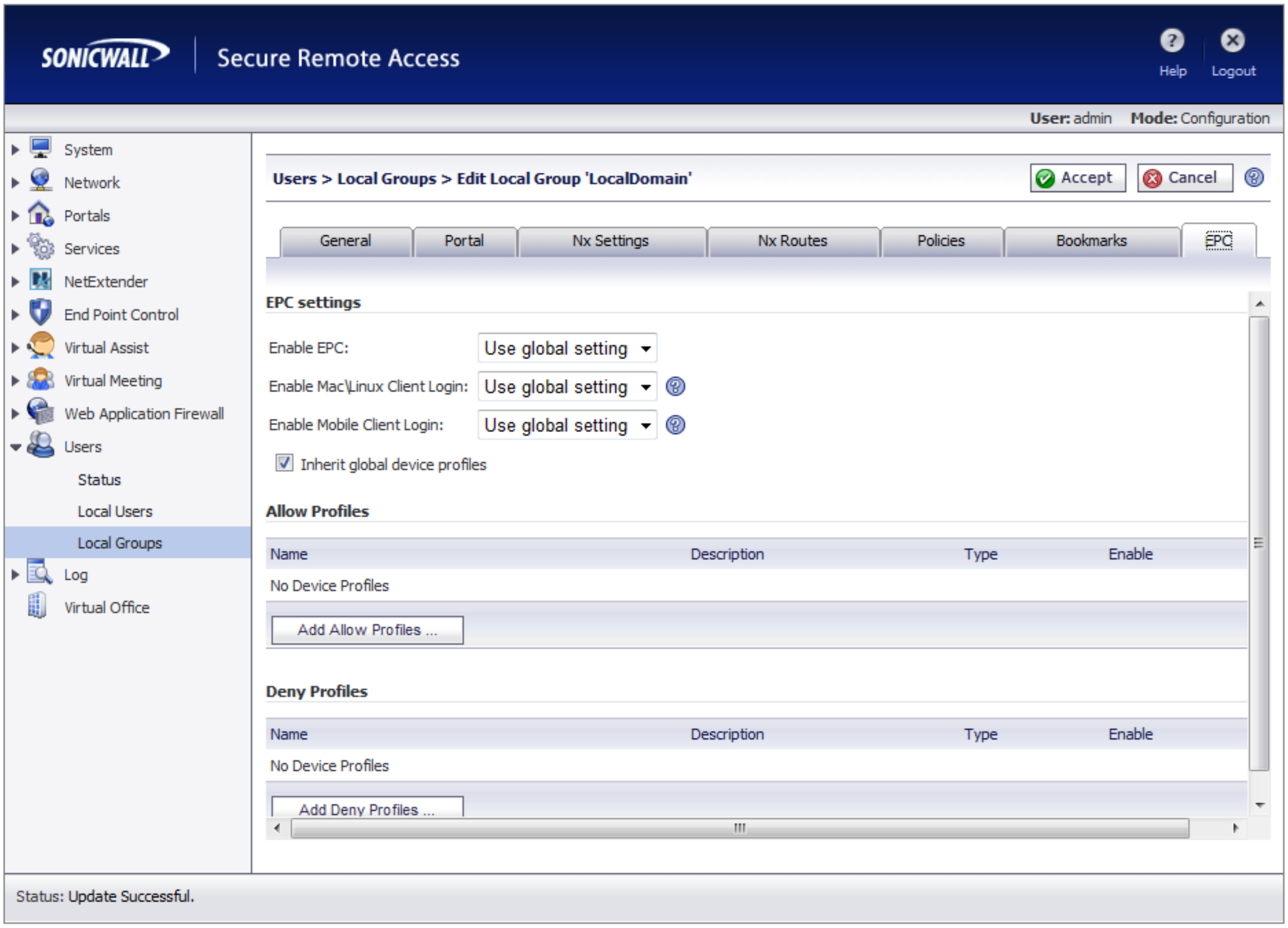
Status: Ready

Figure 4 End Point Control > Add Device Profile

Configuring Global/Group/User EPC Settings

Groups are configured to inherit global policy profiles, and users are configured to inherit group policy profiles. Allow profiles and Deny profiles are selected from device profiles. Therefore, users can disable NetExtender login from these platforms when EPC is enabled. Use the EPC tab on the Users > Local Groups > Add or Edit page to add and assign global or group profiles.

Note: *In SonicWALL SRA 6.0, EPC checking is not supported on Mac platforms, Linux platforms, or mobile devices.*



User: admin **Mode:** Configuration

Users > Local Groups > Edit Local Group 'LocalDomain'

EPC settings

Enable EPC: Use global setting

Enable Mac\Linux Client Login: Use global setting

Enable Mobile Client Login: Use global setting

☑ Inherit global device profiles

Allow Profiles

Name	Description	Type	Enable
No Device Profiles			

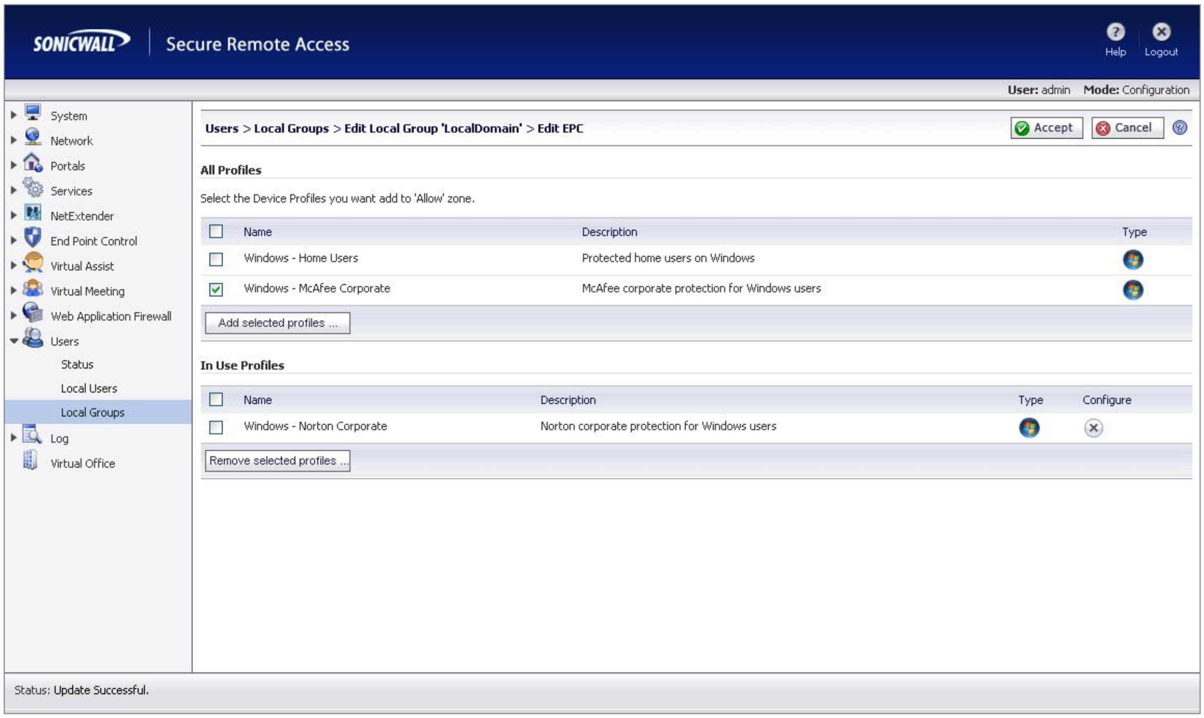
Deny Profiles

Name	Description	Type	Enable
No Device Profiles			

Status: Update Successful.

Figure 5 Users > End Point Control Settings for a Group

Once a group profile is created, it is assigned to one or more groups, as shown in Figure 8.



User: admin Mode: Configuration

Users > Local Groups > Edit Local Group 'LocalDomain' > Edit EPC

All Profiles

Select the Device Profiles you want add to 'Allow' zone.

☐	Name	Description	Type
☐	Windows - Home Users	Protected home users on Windows	
☑	Windows - McAfee Corporate	McAfee corporate protection for Windows users	

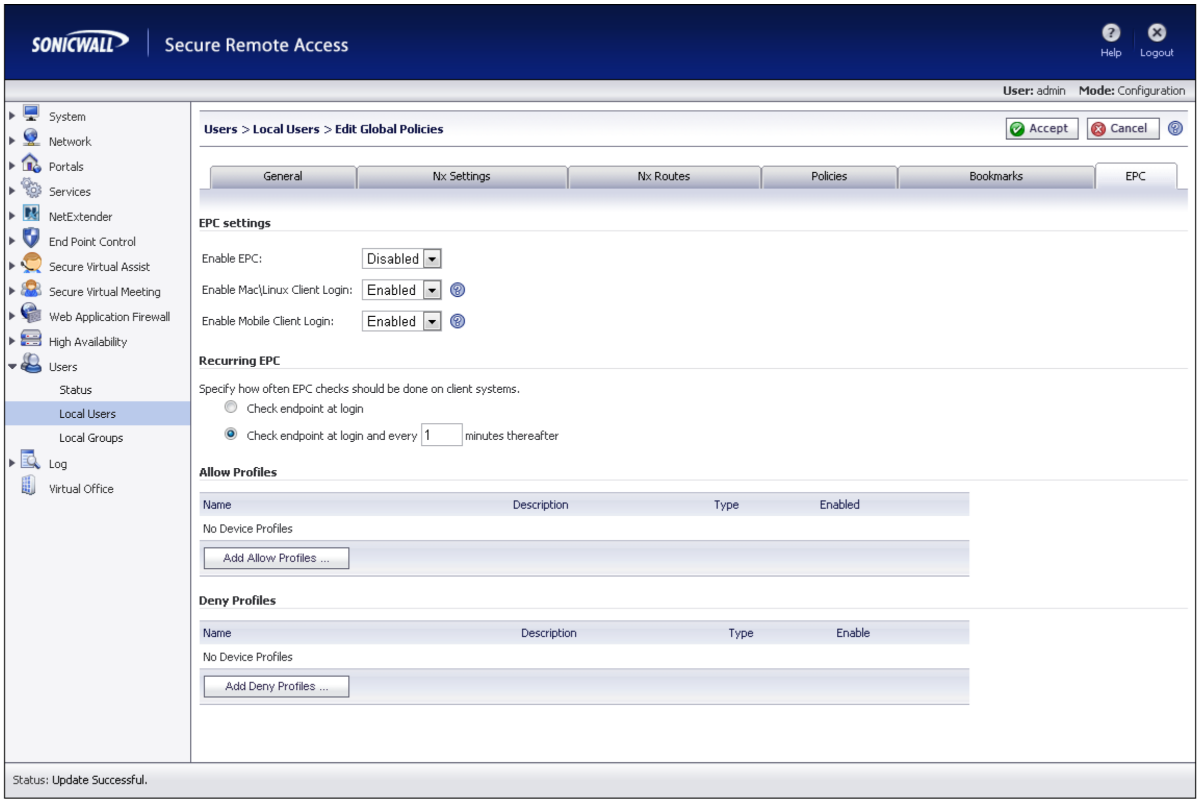
In Use Profiles

☐	Name	Description	Type	Configure
☐	Windows - Norton Corporate	Norton corporate protection for Windows users		⊗

Status: Update Successful.

Figure 6 Add Device Profiles to Group

Use the EPC tab on the Users > Local Users > Add or Edit page to configure EPC and add/assign user profiles.



User: admin Mode: Configuration

Users > Local Users > Edit Global Policies

EPC settings

Enable EPC: Disabled

Enable Mac\Linux Client Login: Enabled

Enable Mobile Client Login: Enabled

Recurring EPC

Specify how often EPC checks should be done on client systems.

○ Check endpoint at login

● Check endpoint at login and every 1 minutes thereafter

Allow Profiles

Name	Description	Type	Enabled
No Device Profiles			

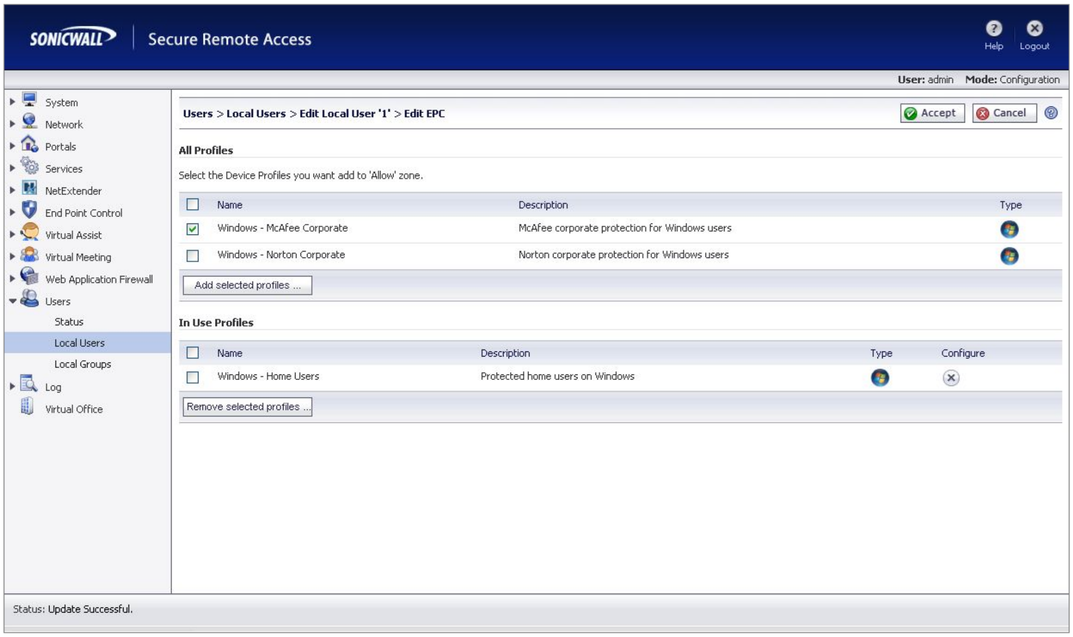
Deny Profiles

Name	Description	Type	Enable
No Device Profiles			

Status: Update Successful.

Figure 7 End Point Control Settings for a User

Once a user profile is created, it is assigned to one or more users, as shown in Figure 10.



Users > Local Users > Edit Local User '1' > Edit EPC

All Profiles

Select the Device Profiles you want add to 'Allow' zone.

□	Name	Description	Type
☑	Windows - McAfee Corporate	McAfee corporate protection for Windows users	
□	Windows - Norton Corporate	Norton corporate protection for Windows users	

In Use Profiles

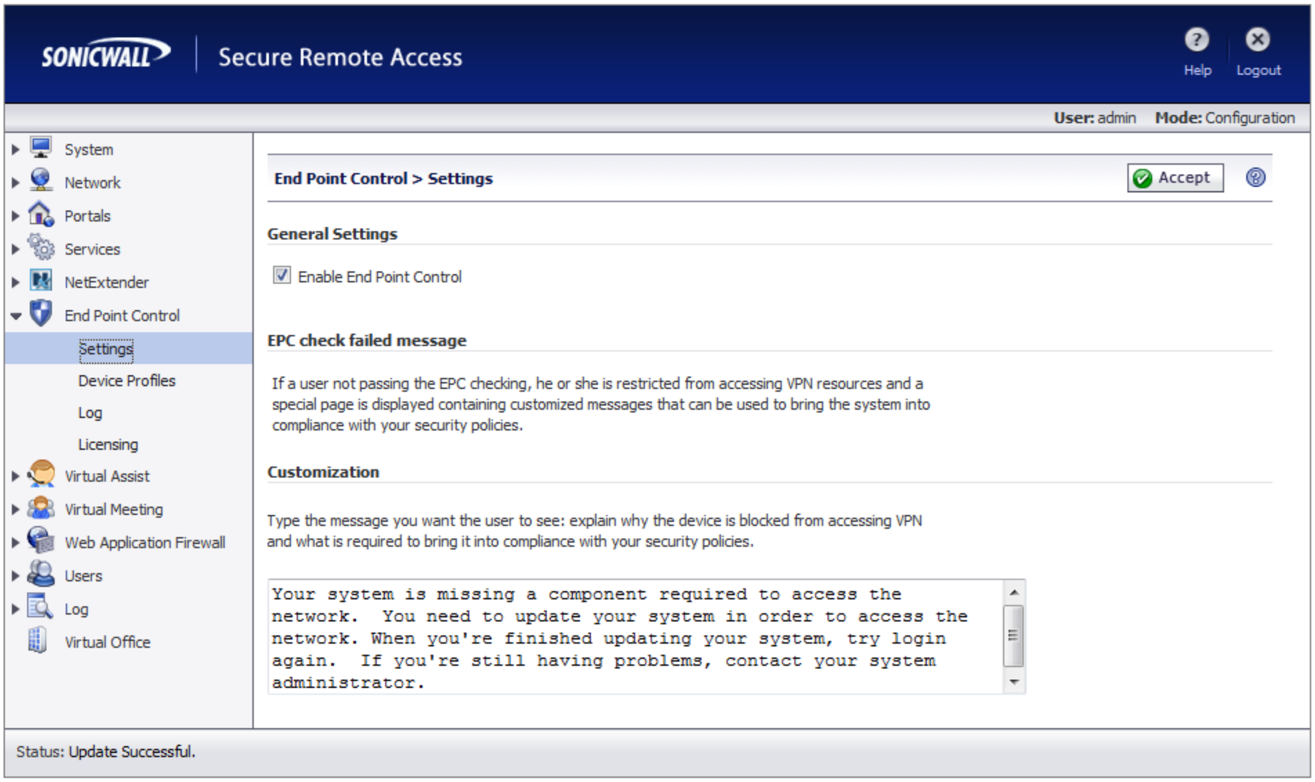
□	Name	Description	Type	Configure
□	Windows - Home Users	Protected home users on Windows		⊗

Status: Update Successful.

Figure 8 Apply Device Profiles to User

Global Settings

EPC is globally enabled or disabled on the End Point Control > Settings page. The Settings page also is used to customize the message displayed when a NetExtender client login fails EPC security checking.



General Settings

☑ Enable End Point Control

EPC check failed message

If a user not passing the EPC checking, he or she is restricted from accessing VPN resources and a special page is displayed containing customized messages that can be used to bring the system into compliance with your security policies.

Customization

Type the message you want the user to see: explain why the device is blocked from accessing VPN and what is required to bring it into compliance with your security policies.

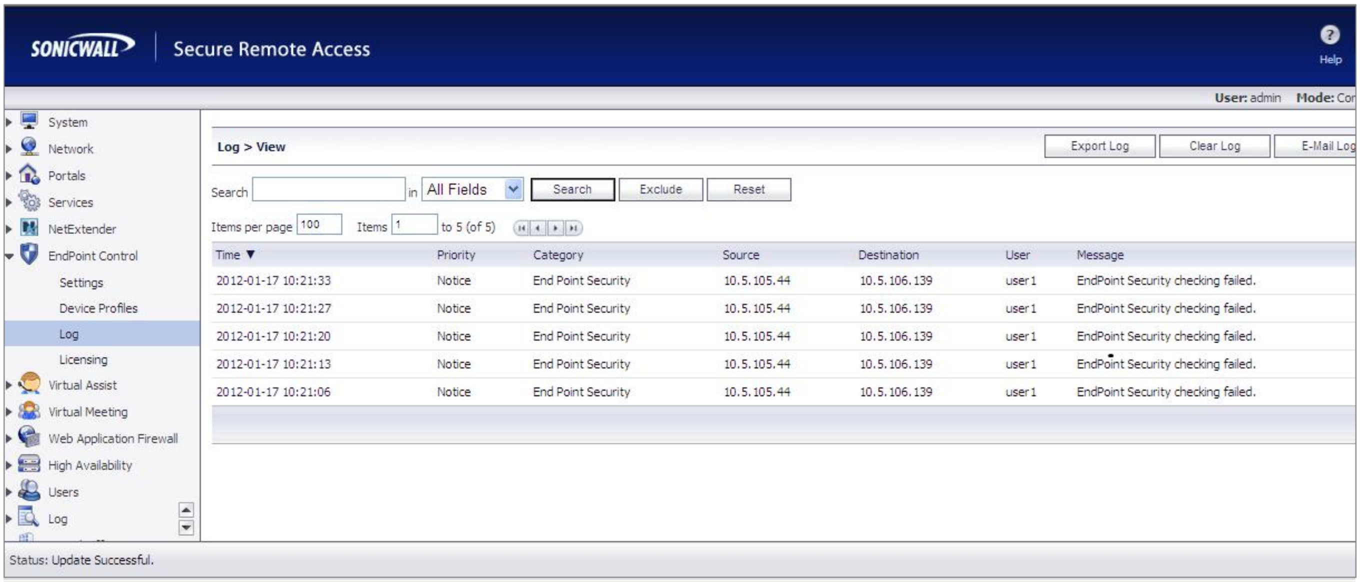
```
Your system is missing a component required to access the
network.  You need to update your system in order to access the
network. When you're finished updating your system, try login
again.  If you're still having problems, contact your system
administrator.
```

Status: Update Successful.

Figure 9 End Point Control > Settings

EPC Log

The End Point Control > Log page lists all client logins blocked by EPC. This log can be searched, filtered, emailed, and exported.



Time ▼	Priority	Category	Source	Destination	User	Message
2012-01-17 10:21:33	Notice	End Point Security	10.5.105.44	10.5.106.139	user1	EndPoint Security checking failed.
2012-01-17 10:21:27	Notice	End Point Security	10.5.105.44	10.5.106.139	user1	EndPoint Security checking failed.
2012-01-17 10:21:20	Notice	End Point Security	10.5.105.44	10.5.106.139	user1	EndPoint Security checking failed.
2012-01-17 10:21:13	Notice	End Point Security	10.5.105.44	10.5.106.139	user1	EndPoint Security checking failed.
2012-01-17 10:21:06	Notice	End Point Security	10.5.105.44	10.5.106.139	user1	EndPoint Security checking failed.

Status: Update Successful.

Figure 10 End Point Control > Log

Performance

When the EPC feature is active other features may run slower due to the increased traffic handled by the appliance.

Secure Virtual Meeting

SonicWALL SRA 6.0 introduces Secure Virtual Meeting for the SRA 4200 and Virtual Appliance. The Secure Virtual Meeting allows multiple users to view a desktop and interactively participate in a meeting from virtually anywhere with an Internet connection. Virtual Meeting is similar to the one-to-one desktop sharing provided by Virtual Assist except multiple users can share a desktop.

Note: *When the Secure Virtual Meeting feature* is active other features may run slower due to the increased traffic handled by the appliance.

Licensing

Virtual Meeting is part of the Virtual Assist package. Multiple Virtual Meetings and Virtual Assist sessions can occur simultaneously. However, a Virtual Assist technician license is required for every three active Virtual Meeting users. For example, your company has 5 Virtual Assist technician licenses and 2 of them are being used for Virtual Assist technicians. Any number of Virtual Meetings can occur concurrently, but the number of concurrent users in the lobby is limited to 9 (5-2=3 licenses available, 3x3=9 licenses for meeting users available).

Licenses are assigned on a first come, first served basis. Virtual Meeting licenses are considered in use when an attendee is in the lobby. Virtual Assist/Access licenses are considered in use when the connection is active and screen sharing is occurring.

User Types

Secure Virtual Meeting has several user types:

- Coordinator (Owner of the meeting)
  The Coordinator must be a SonicWALL SRA user with Virtual Meeting privileges on the appliance. The Coordinator schedules, sets up, and controls the meeting. In addition, the Coordinator has the sole power to promote a Participant to the Assistant.

- Assistant (Coordinator-designated Assistant)
  The Coordinator selects an Assistant from the list of available Participants and assigns the Assistant privileges. Possible Assistant privileges are:

  Start/End Meeting
  Set Host
  Open Polling
  Set/Unset View Only
  Invite Participants
  Kick out Participants
  Reschedule Meeting

  When the Coordinator exits the meeting, the Assistant automatically becomes the Coordinator. A meeting may have multiple Assistants, each with the same or a different set of privileges. An Assistant need not be a user of the SSL-VPN appliance.

- Host
  The Host is a Participant who shares their desktop with all Participants in the meeting.
  When a meeting begins, the Host's desktop is shown to all Participants. The Host can be changed by the Coordinator during the meeting by selecting any available Participant. If a Host is not explicitly set when the meeting starts, the Coordinator becomes the Host. Only one Participant is designated as the Host at any one time.

  Only the Host can control the Host System, unless the Host grants permission when a Participant requests control. The Host may also give control to any Participant by selecting the Participant from the Meeting Members list. Only one Participant can control the Host System at any one time. When a Participant takes control of the Host System, he loses control as soon as the Host moves his mouse pointer on the screen. The meeting control permission state is visible to all Participants while in the lobby.

- Participant (User with credentials to join the meeting)
  A Participant must enter a meeting code before they can join a meeting. The code required to join the meeting is determined by the Coordinator prior to the meeting. After joining a meeting, the Participant can view the shared desktop and chat with another attendee privately or type a message in the Chat window that is visible to all attendees. A Participant becomes the Assistant if selected by the Coordinator or by an Assistant who has the required privilege.

- View-only Participant (User with limited meeting capabilities)
  The Coordinator may designate any Participant as a View-only Participant. A View-only Participant cannot be assigned any privileges nor become an Assistant or Host.

Roles are switched before or during a meeting. Except when the Host permits a Participant to become the Host, only the Coordinator can switch the roles of those attending a meeting. A Participant wishing to change roles can send a request to the Coordinator.

SonicWALL SRA Server Setup

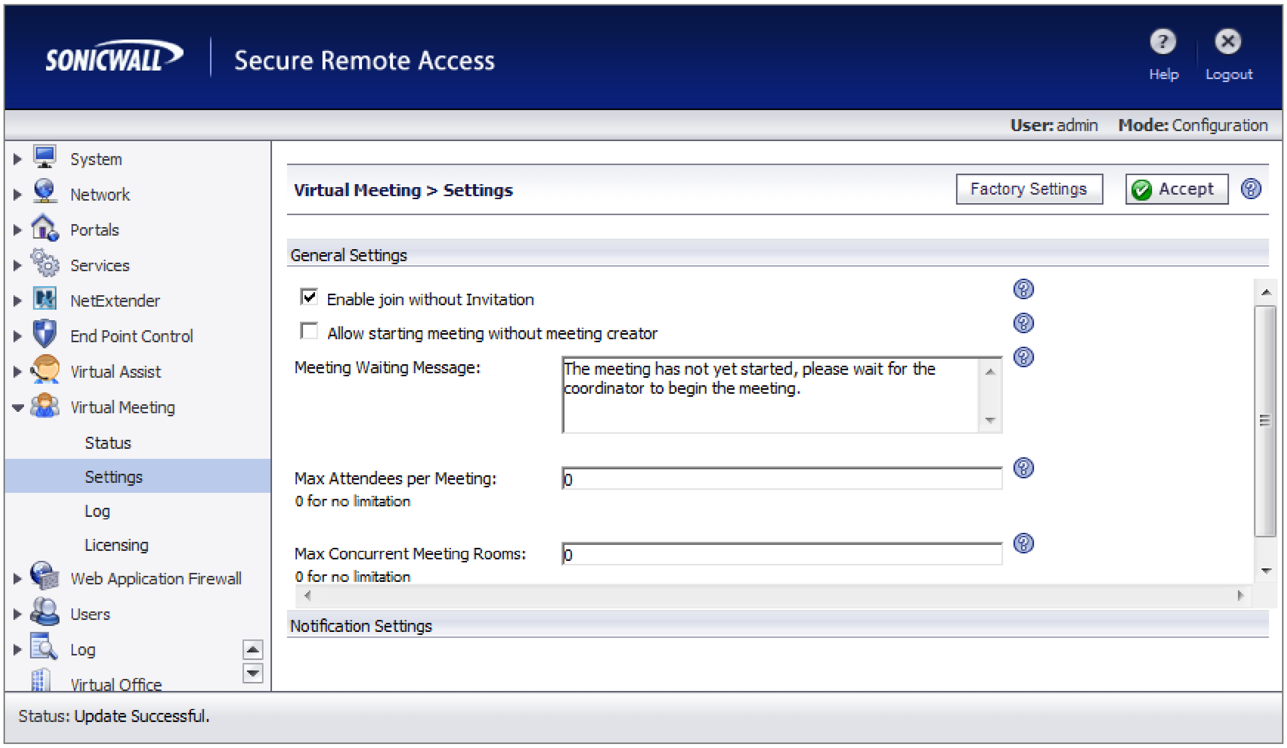
Several Secure Virtual Meeting settings are configurable.

- Enable join without Invitation

This option allows Participants to join the meeting without being required to go through the invite link from the e-mail. Participants would run the Virtual Meeting client and join the meeting directly with meeting code set by the Coordinator.

- Allow starting meeting without meeting creator
  This option allows a meeting to start without the coordinator present. If enabled and a scheduled meeting has no coordinator in the meeting room at the scheduled start time, a participant will be selected to become the coordinator and begin the meeting.
- Meeting Waiting Message
  This sets the message to be displayed to Participants awaiting the start of the meeting.
- Max Attendees per Meeting
  This sets the maximum systems that may join any given meeting.
- Max Concurrent Meeting Rooms
  This sets the maximum number of concurrent meetings that may take place.
- Subject of Invitation
  This sets the Subject for the e-mail invitation for Virtual Meeting to be sent to participants.
- Invitation Message
  This allows you to customize the body of the Virtual Meeting invite.

Use the General Settings page to configure general Virtual Meeting settings.



User: admin Mode: Configuration

Virtual Meeting > Settings

General Settings

☑ Enable join without Invitation

□ Allow starting meeting without meeting creator

Meeting Waiting Message: The meeting has not yet started, please wait for the coordinator to begin the meeting.

Max Attendees per Meeting: 0
0 for no limitation

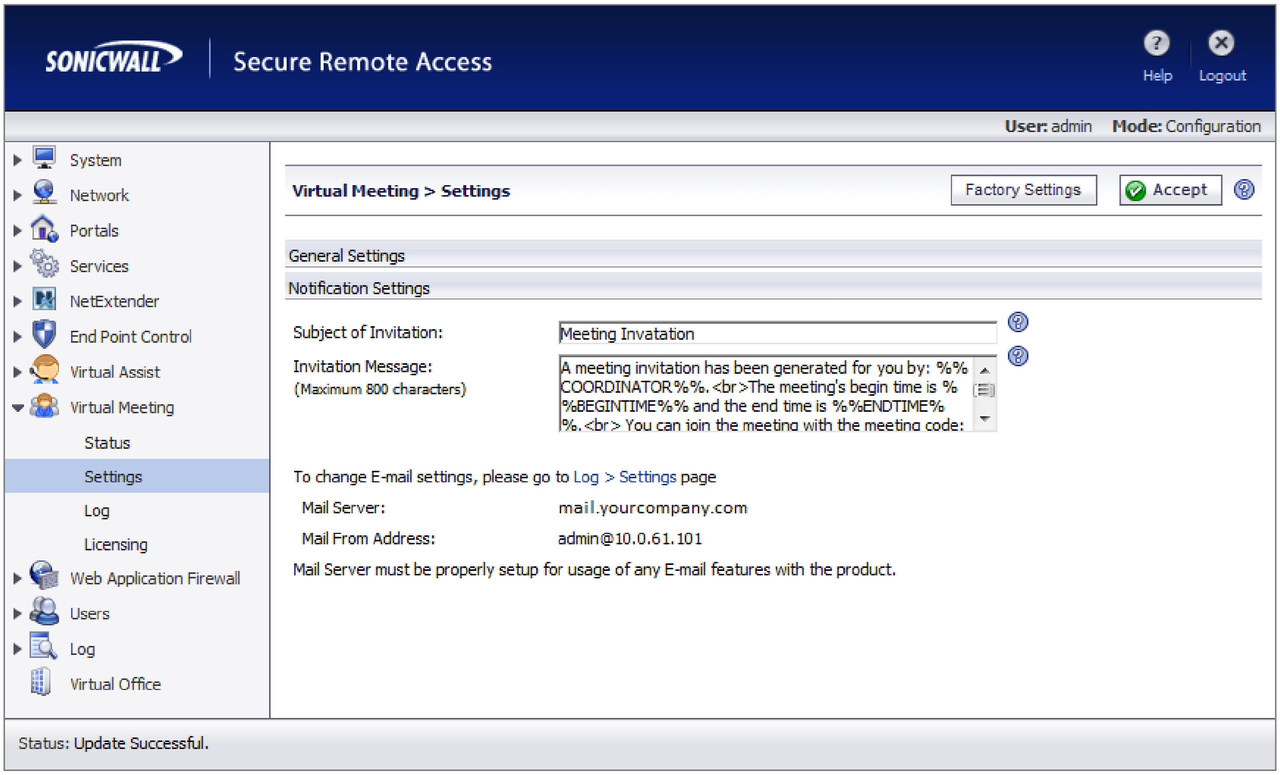
Max Concurrent Meeting Rooms: 0
0 for no limitation

Notification Settings

Status: Update Successful.

Figure 11 Virtual Meeting > Settings > General Settings

Use the Notification Settings page to configure Virtual Meeting settings used for notifications.



Subject of Invitation: Meeting Invatation

Invitation Message: (Maximum 800 characters) A meeting invitation has been generated for you by: %%COORDINATOR%%.
The meeting's begin time is %%BEGINTIME%% and the end time is %%ENDTIME%%.
 You can join the meeting with the meeting code:

To change E-mail settings, please go to Log > Settings page

Mail Server: mail.yourcompany.com

Mail From Address: admin@10.0.61.101

Mail Server must be properly setup for usage of any E-mail features with the product.

Status: Update Successful.

Figure 12 Virtual Meeting > Settings > Notification Settings

Installation and Setup

The Virtual Meeting executable, which includes both Host and Client software, is downloaded and installed by users with the proper credentials. After downloading and installing Virtual Meeting, the user logs into the system using the provided credentials (or automatically, if possible).

Prior to starting a meeting, the Coordinator can set certain preferences and options. The Coordinator loads the meeting settings and controls when the meeting starts.

Features

Once Virtual Meeting is installed and set up, the following events can occur:

- Scheduling a meeting
- Logging In
- Starting a meeting
- Chatting
- Polling
- Ending a meeting

These events are described in this section. Instructions to perform these functions are provided in the *SonicWALL SRA Virtual Meeting User Guide*, available on MySonicWALL.

- Scheduling
  The Coordinator must schedule a meeting by setting up the required parameters before a meeting can start. A meeting is scheduled to start at any future time or immediately. The scheduled time can be changed any

time before the meeting starts. A reminder to start the meeting will be sent to the Coordinator if he is in the meeting lobby but has not started the meeting at the scheduled time

- Logging In

  Participants join a meeting by clicking the link in the meeting invite email and entering the meeting code, which is also identified in the meeting invite email. After joining a meeting, Participants wait in the lobby until the Host System screen is shared.
- Starting the Meeting
  Once a meeting is set up, the Coordinator can start the meeting at any time. A scheduled meeting is started with or without the Coordinator, depending on the setting on the Virtual Meeting > Settings page. Depending on who has joined the meeting by the start time and whether this setting allows a meeting to start without the Coordinator, the following may happen when a meeting starts:

  - If the setting allows a meeting to start without the Coordinator and the Coordinator does not join the meeting by the scheduled start time, Virtual Meeting randomly chooses a Participant to become the Coordinator.
  - If the setting forbids a meeting to start without the Coordinator and the Coordinator does not join the meeting by the scheduled start time, all Participants in the meeting room are kept waiting until the meeting end time and notified when the meeting ends.

    If Participants are in multiple time zones, the appliance server automatically compensates for time differences, so users join the meeting at the same time.
  - When nobody joins the meeting at the scheduled time, the meeting is removed from the meeting room list after the end time.
- Using the Meeting Features

  Virtual Meeting has several features that are used during a meeting:

  - Invite Participants
    The Coordinator can invite Participants to join a meeting during the meeting. The Participants, who are sent an e-mail invitation automatically, can use the link in the e-mail to join the meeting immediately. The Participant is not required to enter a meeting code to join the meeting.
  - Managing Roles
    The Assistant and Host are set up before or during the meeting. A Participant can request to become the Host. If the Host approves the request, the Participant's screen becomes the Host System. Additionally, a Participant can control the Host System remotely if the Control option is enabled and the Host grants permission to the Participant.
  - Sharing the Host System
    The Host can share the Host System screen with Participants and stop screen sharing at any time. The entire desktop is displayed to all Participants except for the Virtual Meeting control panel, which is always hidden from Participant view.
  - Chatting
    Two types of text chat are possible during a meeting: private chats between two or more Participants and chat room chats for all Participants. Text chat is initiated by anyone at any time before or during the meeting and chat room chats are allowed only during the meeting and are initiated by the Coordinator only.
  - Polling
    Polling may be started by the Coordinator or Assistant. Polls may be created and saved before the meeting and then loaded during the meeting. Polling can occur before or during the meeting, and the poll initiator may end the poll at any time. Once started, all Participants except View-Only Participants receive the poll and may respond. The poll initiator receives all poll feedback. Polling questions and results are saved and then loaded into a poll and reviewed by the poll initiator.
  - Kick out Attendee
    This feature lets the Coordinator instantly remove any person from the meeting room.

- Ending a Meeting
  Only the Coordinator or Assistant (if given sufficient privileges) can end a meeting. Ending the meeting automatically returns all Participants to the meeting selection room. For a scheduled meeting, the Coordinator is responsible for ending the meeting once the meeting starts. If the meeting has not started and the Coordinator is present, the Coordinator receives a notification to end or reschedule the meeting. If the meeting has not started and the Coordinator is not present, the meeting is ended silently; and all Participants in the meeting are notified that the meeting has ended.

Virtual Assist Enhancements

Virtual Assist is a remote support tool that allows a technician to service a customer by controlling the customer's PC from virtually anywhere in the world. SonicWALL SRA 6.0 includes the following Virtual Assist enhancements for the SRA 1200, SRA 4200, and Virtual Appliance platforms.

Mac OS X Lion (10.7) Customer Client Support
Expanded Plug-in Support
Server Certificate Verification

Note: *Virtual Assist enhancements may cause other features to run slower due to increased traffic that will be handled by the appliance*.

Mac OS X Lion (10.7) Customer Client Support

SonicWALL SRA 5.5 and 6.0 firmware now support the Mac OS X Lion operating system (10.7). When customers enter the queue on a Mac Lion they are able to receive service.

Expanded Plug-in Support

The VAX.cab plug-in software has been updated to allow installation on systems that previously could not install or run the SonicWALL ActiveX control.

Server Certificate Verification

SonicWALL SRA 6.0 firmware now verifies the server certificate, which provides a safer environment for the appliance. If the certificate is not issued by an authorized organization, an alert message is displayed to notify the user of the risk. The user can view detailed information about the server certificate and choose to continue or end the connection.

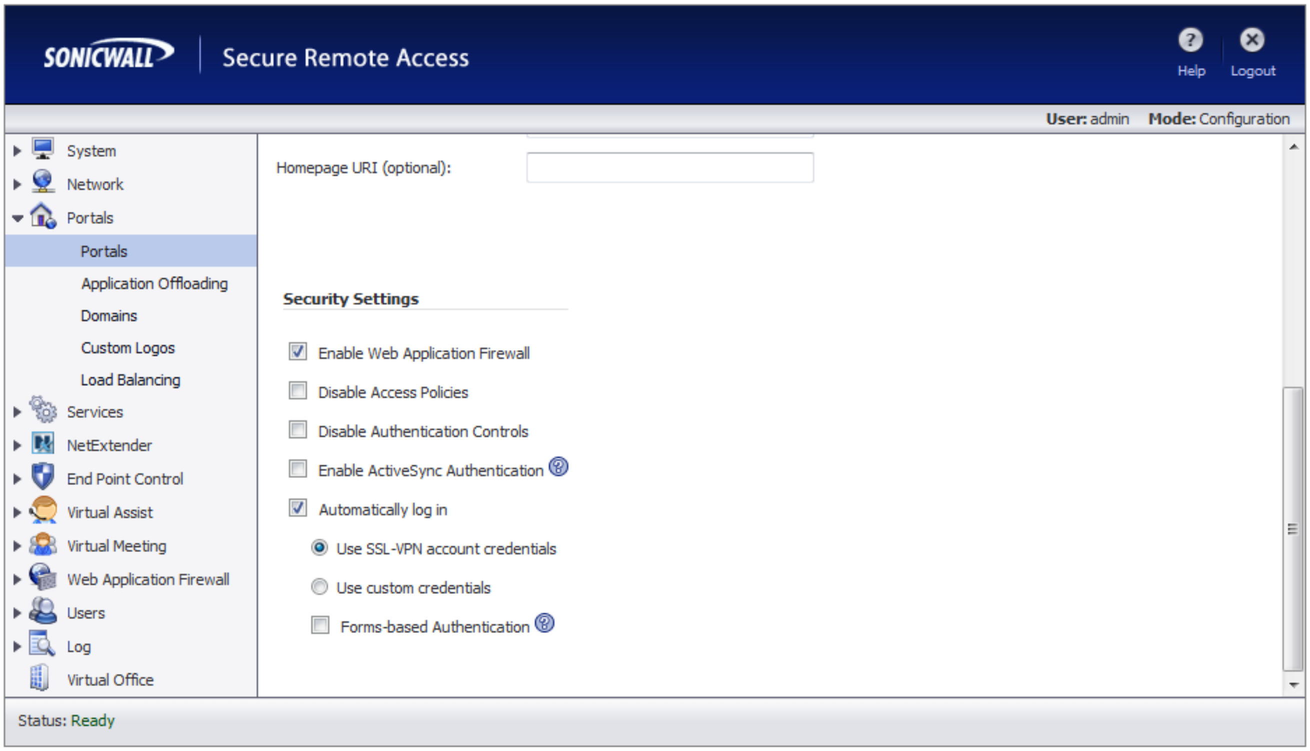
Application Offloading Enhancements

Application Offloading technology delivers Web applications using Virtual Hosting and Reverse Proxy. Users still need to authenticate with the SonicWALL SRA before accessing the backend Web application. However, the proxy avoids URL rewriting in order to deliver the Web applications seamlessly.

ActiveSync authentication

Application Offloading now supports authentication for ActiveSync. ActiveSync is a protocol used by a mobile phone's email client to synchronize with an Exchange server. The Administrator can create an offloading portal and set the application server host to the backend Exchange server. Then, a user can use the new virtual host name in a mobile phone's email client, and synchronize with the backend Exchange server through the SRA appliance. Before SonicWALL SRA 6.0, users had to disable authentication for ActiveSync offloading portals, because ActiveSync requests are different from requests sent from the browser.

ActiveSync is managed through the Portals > Offloading > Security Settings page:



Homepage URI (optional):

Security Settings

☑ Enable Web Application Firewall

□ Disable Access Policies

□ Disable Authentication Controls

□ Enable ActiveSync Authentication

☑ Automatically log in

● Use SSL-VPN account credentials

○ Use custom credentials

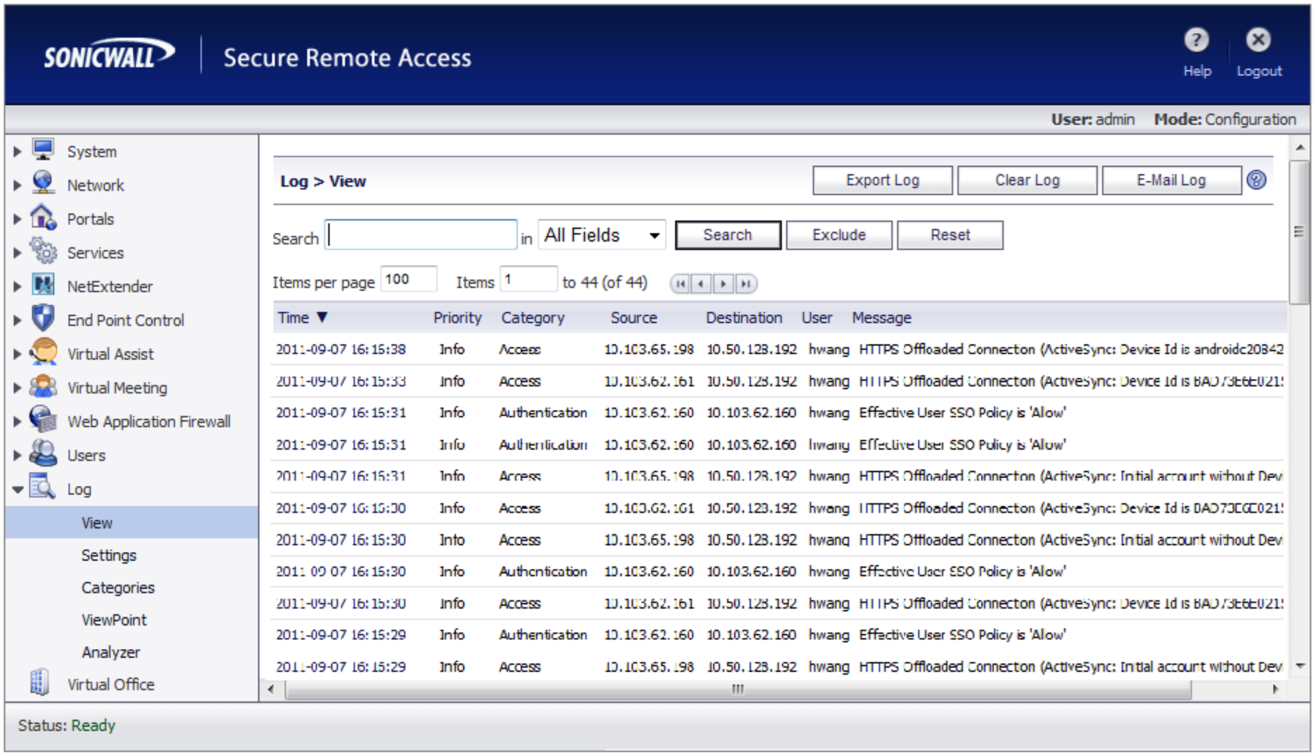
□ Forms-based Authentication

Figure 13 Portals > Portals > Offload Web Application > Offloading

To configure ActiveSync authentication, clear the **Disable Authentication Controls** checkbox to display the authentication fields. Select the **Enable ActiveSync authentication** checkbox and then type the default domain name. The default domain name will not be used when the domain name is set in the email client’s setting.

ActiveSync Log Entries

The Log > View page is updated when a Web application is offloaded:



Search in All Fields

Items per page 100 Items 1 to 44 (of 44)

Time ▼	Priority	Category	Source	Destination	User	Message
2011-09-07 16:15:38	Info	Access	10.103.65.198	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Device Id is androidc20842
2011-09-07 16:15:33	Info	Access	10.103.62.161	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Device Id is BAD73E6E021
2011-09-07 16:15:31	Info	Authentication	10.103.62.160	10.103.62.160	hwang	Effective User SSO Policy is 'Allow'
2011-09-07 16:15:31	Info	Authentication	10.103.62.160	10.103.62.160	hwang	Effective User SSO Policy is 'Allow'
2011-09-07 16:15:31	Info	Access	10.103.65.198	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Intial account without Dev
2011-09-07 16:15:30	Info	Access	10.103.62.161	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Device Id is BAD73E6E021
2011-09-07 16:15:30	Info	Access	10.103.65.198	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Intial account without Dev
2011-09-07 16:15:30	Info	Authentication	10.103.62.160	10.103.62.160	hwang	Effective User SSO Policy is 'Allow'
2011-09-07 16:15:30	Info	Access	10.103.62.161	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Device Id is BAD73E6E021
2011-09-07 16:15:29	Info	Authentication	10.103.62.160	10.103.62.160	hwang	Effective User SSO Policy is 'Allow'
2011-09-07 16:15:29	Info	Access	10.103.65.198	10.50.128.192	hwang	HTTPS Offloaded Connecton (ActiveSync: Intial account without Dev

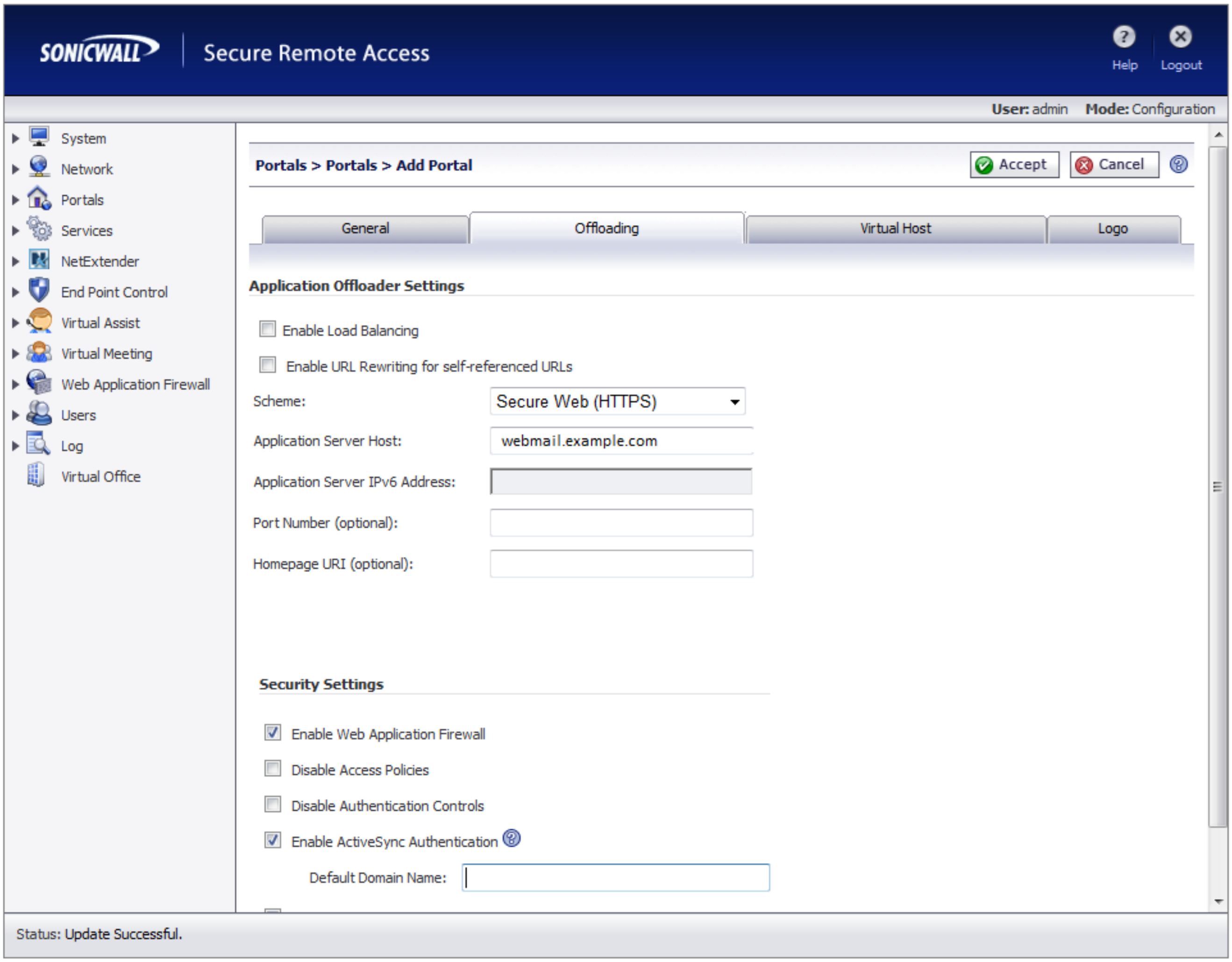
Figure 14 Security Settings Log

Most mobile systems (iPhone, Android, Windows Mobile, etc.) support ActiveSync. The SRA log shown in Figure 16 contains two ActiveSync entries (Android and Windows Mobile), each identifying when the client began to use ActiveSync through the offloading portal. The ActiveSync message identifies the device ID (ActiveSync: Device Id is…) for an ActiveSync request unless a client sets up the account and the request does not contain a device ID. The ActiveSync label is not used in log entries for anonymous users who use ActiveSync.

Note: *A user's credential in the Exchange server must be the same as the one in the SRA. Many authentication types are available for each domain in the SRA. If using the Local User Database, make sure the user name and password is the same as the one for the Exchange server. Fortunately, other authentication types like Active Directory can share credentials for both the Exchange server and SonicWALL SRA. However, authentication using authentication types that share credentials may take longer and the first ActiveSync request may time out. Once authentication succeeds, a session is created and other requests won't need to be authenticated again.*

The following example shows how to set up ActiveSync to check SonicWALL emails with an Android. Be sure to replace entries shown in the example with entries for your environment, and be careful to input the correct password. Otherwise, the account will be blocked.

1. In the SRA, create an offloading portal with the name **webmail**:
2. Set the **Scheme** to **Secure Web (HTTPS).**
3. Set the **Application Server Host** to your Exchange server, for example *webmail.example.com*.



Application Offloader Settings

□ Enable Load Balancing

□ Enable URL Rewriting for self-referenced URLs

Scheme:	Secure Web (HTTPS)
Application Server Host:	webmail.example.com
Application Server IPv6 Address:	
Port Number (optional):	
Homepage URI (optional):	

Security Settings

☑ Enable Web Application Firewall

□ Disable Access Policies

□ Disable Authentication Controls

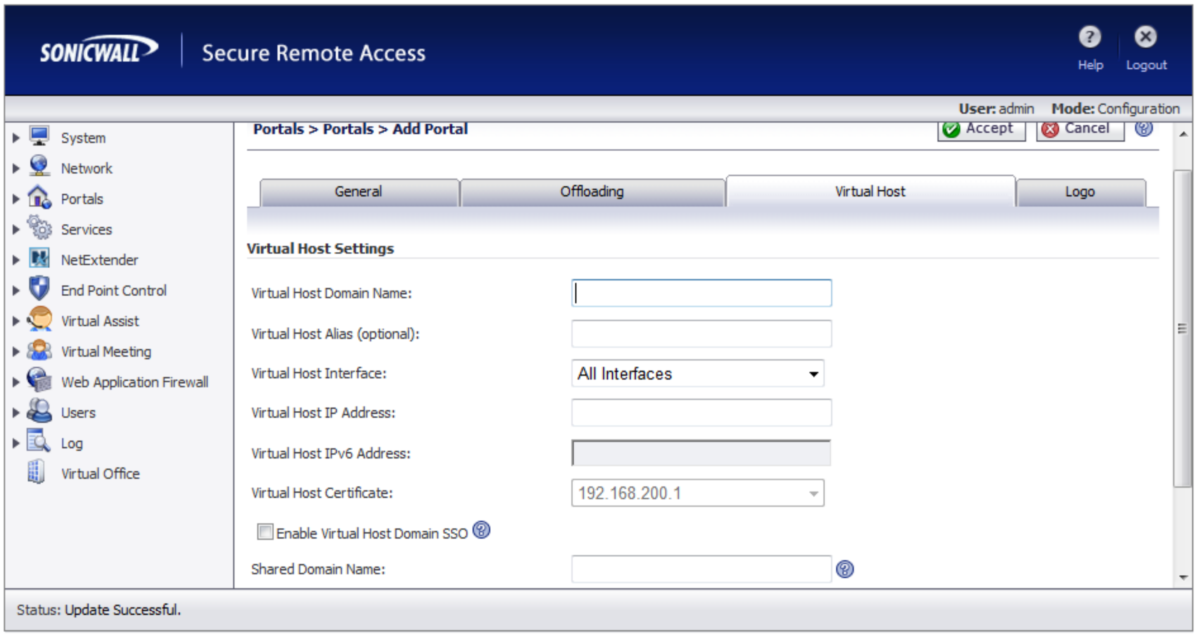
☑ Enable ActiveSync Authentication

Default Domain Name:

Status: Update Successful.

Figure 15 Portals > Portals > Add > Offloading

4. Set the virtual host name, for example, *webmail.example.com*. The virtual host name should be resolved by the DNS server. Otherwise, modify the hosts file in the Android phone.



Virtual Host Settings

Virtual Host Domain Name:

Virtual Host Alias (optional):

Virtual Host Interface: All Interfaces

Virtual Host IP Address:

Virtual Host IPv6 Address:

Virtual Host Certificate: 192.168.200.1

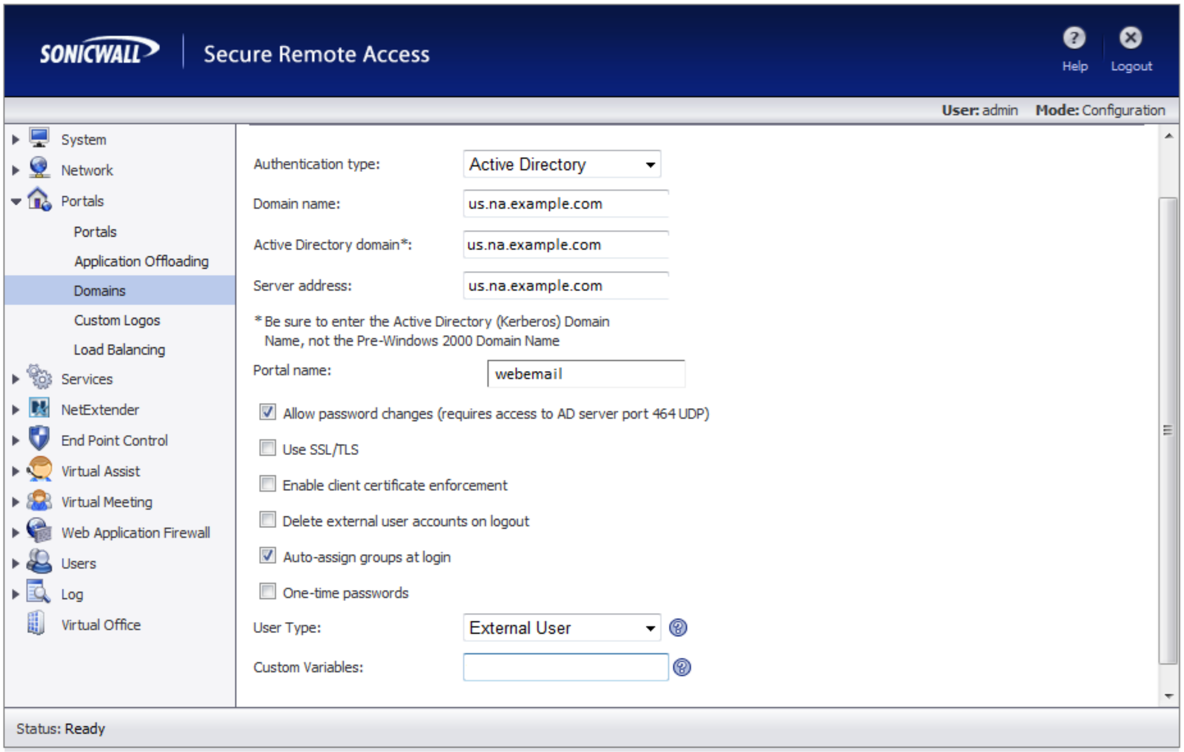
☐ Enable Virtual Host Domain SSO

Shared Domain Name:

Status: Update Successful.

Figure 16 Portals > Portals >Add > Virtual Host

5. Select the **Enable ActiveSync Authentication** checkbox, as shown in Figure 17. Leave the default domain name blank or input **webmail.example.com.**
6. Create a **Domain name** of webmail.example.com. Set the **Active Directory domain** and **Server address** to webmail.example.com. Set the **Portal name** to webmail.



Authentication type: Active Directory

Domain name: us.na.example.com

Active Directory domain*: us.na.example.com

Server address: us.na.example.com

* Be sure to enter the Active Directory (Kerberos) Domain Name, not the Pre-Windows 2000 Domain Name

Portal name: webemail

☑ Allow password changes (requires access to AD server port 464 UDP)

☐ Use SSL/TLS

☐ Enable client certificate enforcement

☐ Delete external user accounts on logout

☑ Auto-assign groups at login

☐ One-time passwords

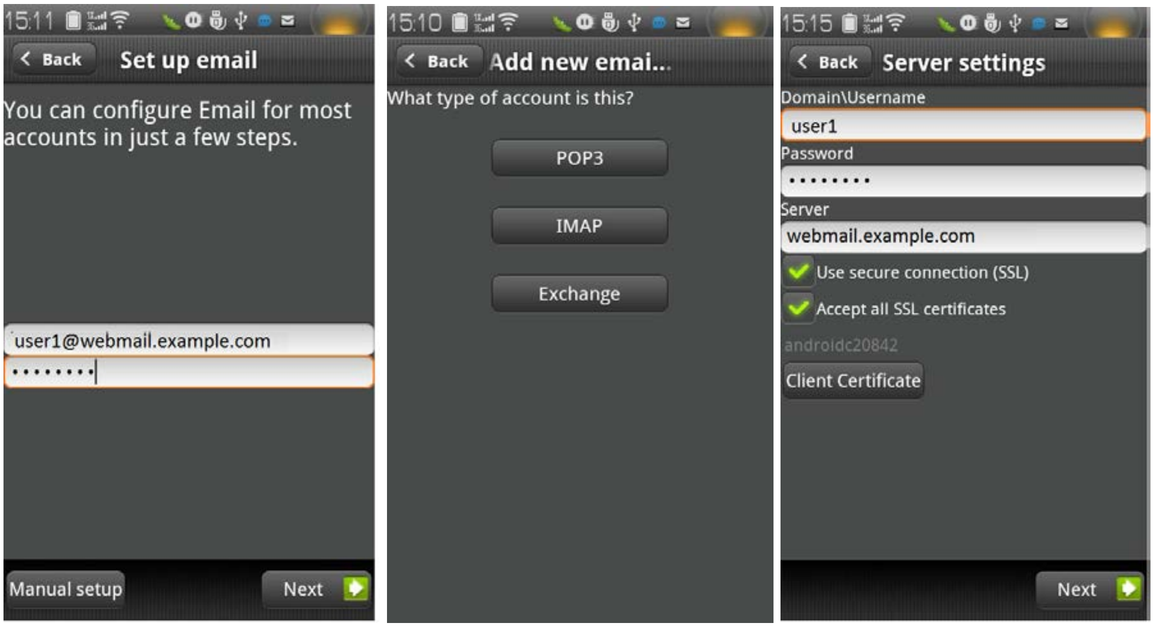
User Type: External User

Custom Variables:

Status: Ready

Figure 17 Add Domain

7. Turn on the Android phone, open the Email application, and type your email address and password. Click **Next**.
8. Choose **Exchange.**
9. Input your **Domain\Username**, **Password**, and **Server**. No domain name is displayed, so use the default domain name specified in the offloading portal's setting. Select **Accept all SSL certificates** and click **Next**.



You can configure Email for most accounts in just a few steps.

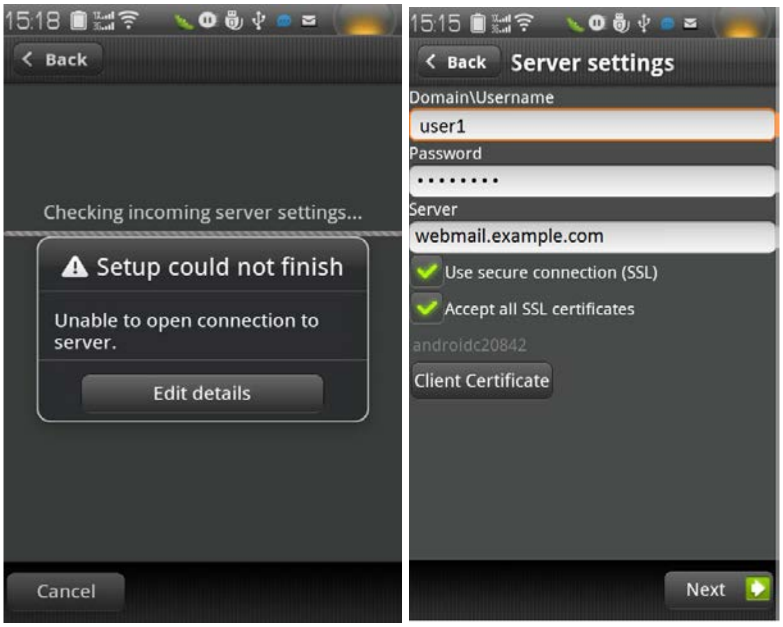
user1@webmail.example.com
••••••••

What type of account is this?

Domain\Username: user1
Password: ••••••••
Server: webmail.example.com
☑ Use secure connection (SSL)
☑ Accept all SSL certificates
androidc20842

Figure 18 Add Email Account to Android

10. If the AD authentication times out, the **Setup could not finish** message is displayed. Wait about 20 seconds and try again. You can also check the SRA log to see if the user logged in successfully. You may not encounter this problem if the AD authentication is fast.



Checking incoming server settings...

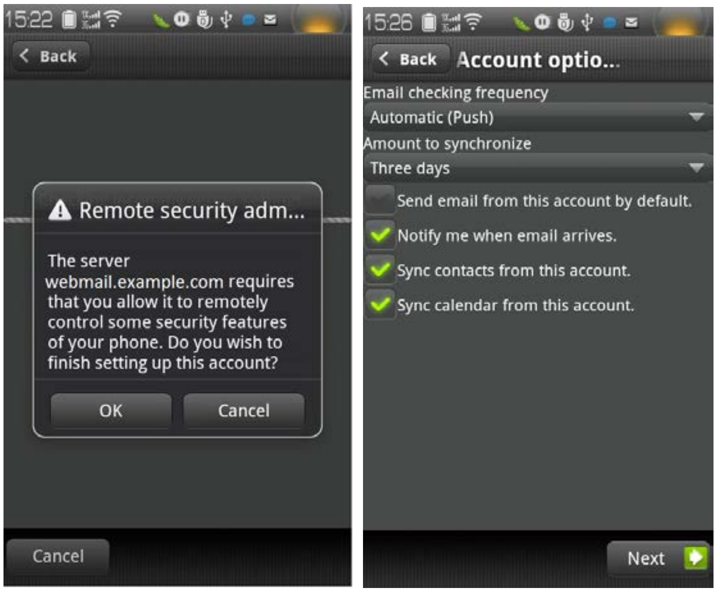
Setup could not finish

Unable to open connection to server.

Domain\Username: user1
Password: ••••••••
Server: webmail.example.com
☑ Use secure connection (SSL)
☑ Accept all SSL certificates
androidc20842

Figure 19 Authentication on Android

11. When the authentication finishes, a security warning appears. Click **OK** to continue, modify your account settings, and click **Next**.



Remote security adm...

The server webmail.example.com requires that you allow it to remotely control some security features of your phone. Do you wish to finish setting up this account?

OK Cancel

Account optio...

Email checking frequency
Automatic (Push)

Amount to synchronize
Three days

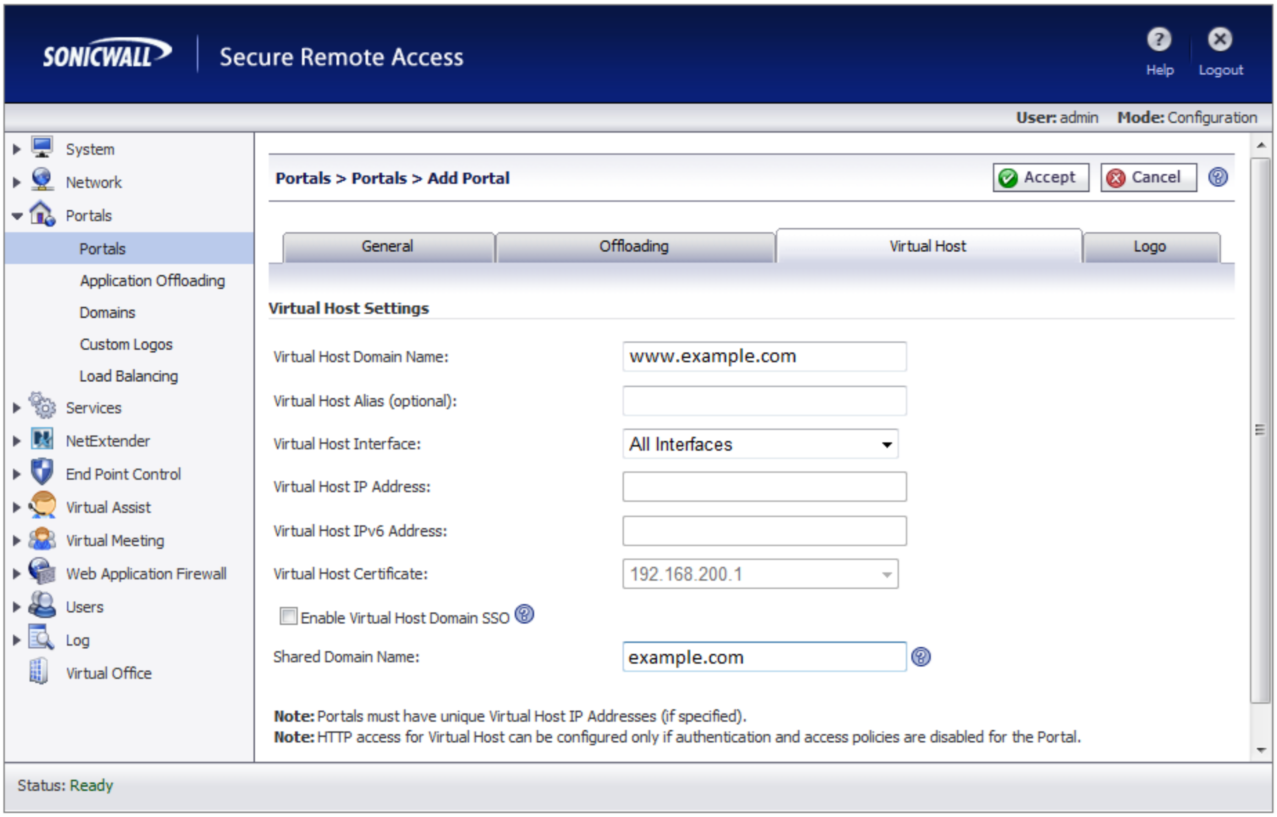
□ Send email from this account by default.
☑ Notify me when email arrives.
☑ Sync contacts from this account.
☑ Sync calendar from this account.

Figure 20 Authentication Complete on Android

12. Try to send and receive emails, and ensure that ActiveSync entries are included in the SRA log, as shown in Figure 16.

Cross Domain Single Sign-On (SSO)

External Website Bookmarks can be created for application offloading portals to achieve a single point of access for users. In previous releases, users had to login twice – once for the regular portal and once for the application offloading portal after External Website Bookmark redirection. The Cross Domain SSO feature allows users to automatically sign into application offloading portals after logging into the main portal.
Cross Domain SSO shares the credentials for all portals in the same shared domain. Use the Portals->Virtual Host page to configure settings for these portals. Then, check the **Enable Virtual Host Domain SSO** checkbox to enable cross domain SSO.



Portals > Portals > Add Portal

Virtual Host Settings

Virtual Host Domain Name: www.example.com
Virtual Host Alias (optional):
Virtual Host Interface: All Interfaces
Virtual Host IP Address:
Virtual Host IPv6 Address:
Virtual Host Certificate: 192.168.200.1
□ Enable Virtual Host Domain SSO
Shared Domain Name: example.com

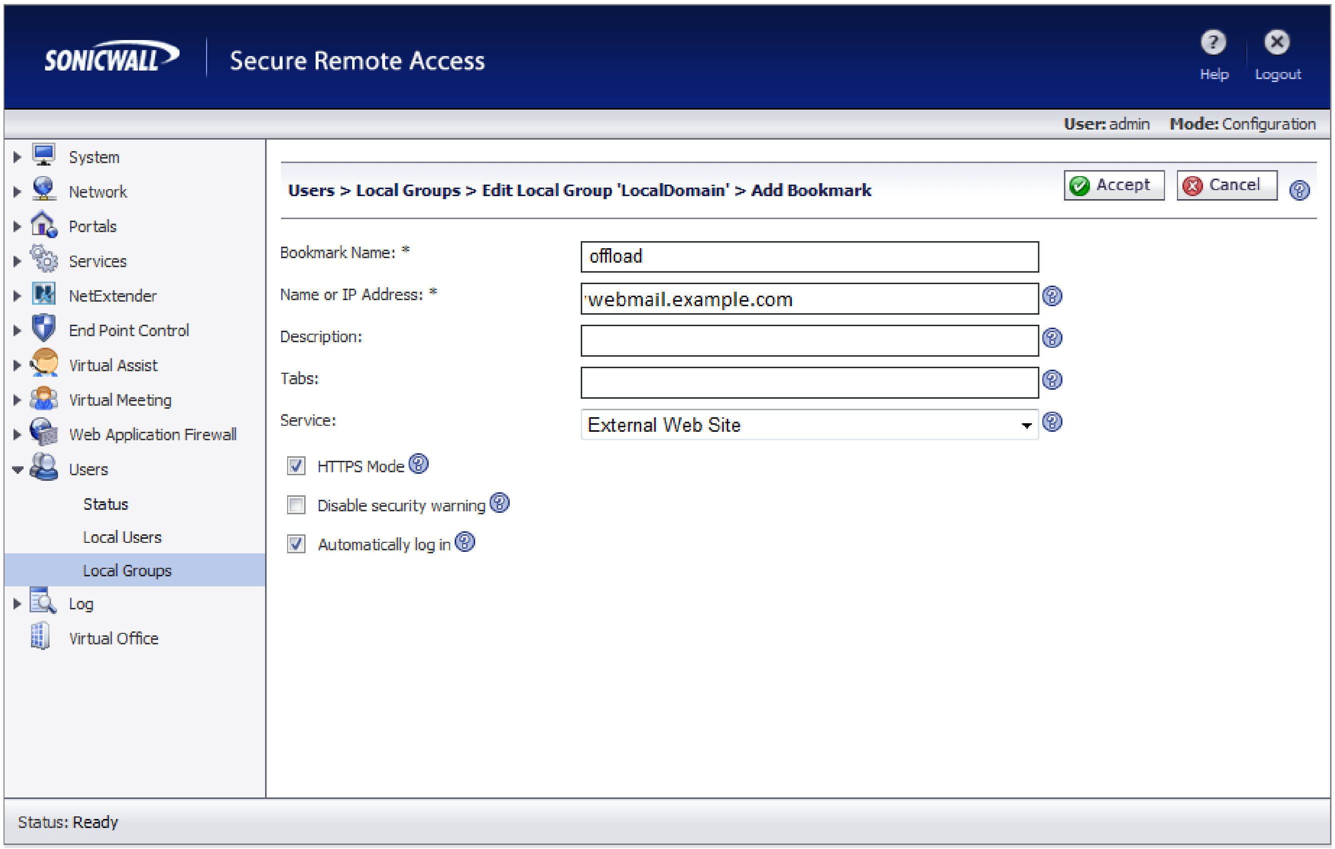
Note: Portals must have unique Virtual Host IP Addresses (if specified).
Note: HTTP access for Virtual Host can be configured only if authentication and access policies are disabled for the Portal.

Figure 21 Portals > Virtual Host Settings for Cross Domain SSO

The input box below shows the **Shared Domain Name** that is generated from the **Virtual Host Domain Name** as one level up. For example

Intranet.eng.example.com→ .eng.example.com
webmail.example.com → .example.com
portalabc→""(empty)

Next, set the bookmarks (Users > Local Groups > Edit > Bookmarks).



Users > Local Groups > Edit Local Group 'LocalDomain' > Add Bookmark

Bookmark Name: * offload

Name or IP Address: * 'webmail.example.com

Description:

Tabs:

Service: External Web Site

☑ HTTPS Mode

☐ Disable security warning

☑ Automatically log in

Figure 22 Portals > Virtual Host Settings > Bookmark Settings

To use Cross Domain SSO, first create two or more portals with the same shared domain (from Virtual Host Domain name) and that need authentication. One portal should be a regular portal. These portals are also in the same SRA appliance’s domain so that a user can log in to both of them with the same credentials. Once the portals are created:

1. Log in the portal and create a bookmark.
2. Set the service to **External Web Site**.
3. Enable **Automatically log in**., which enables Cross Domain SSO for this bookmark.
4. Specify a Host, which is a portal with the same shared domain name.
5. Save the bookmark and launch it. The new portal is logged in automatically without any credential.

The shared domain names don’t need to be identical; a sub-domain also works. For example, one portal is a regular portal whose virtual host domain name is “www.example.com” and its shared domain name is “.example.com”. The other portal’s virtual host domain name is “intranet.eng.example.com” and the shared domain name is “.eng.example.com”. If a bookmark to xyz.eng.example.com is created in the www.example.com portal, Cross Domain SSO works because “.eng.example.com” is a sub-domain of “.example.com”.

Web Application Firewall Enhancements

The following Application Profiling enhancements have been added to the Web Application Firewall, which thwarts zero-day attacks and reduces false positives while performing intrusion scanning:

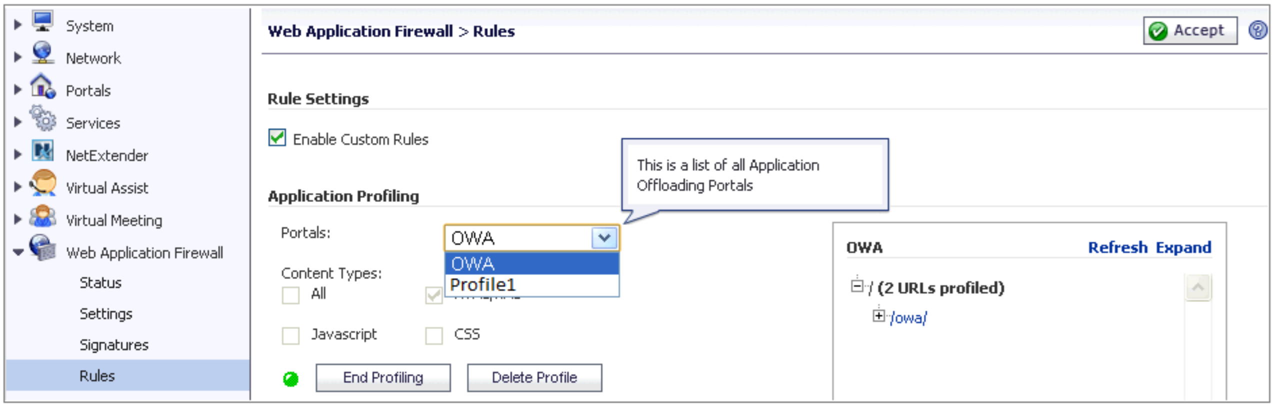
- Simultaneous Profiling for Multiple Applications
- Filtering Rule Chains by Applications

The rules generated during Application Profiling correspond to the parameters saved in the URL Profiles.

Note: *The Application Profiling feature is available only for the SonicWALL SRA 4200 and SRA Virtual Appliance, even though the Web Application Firewall feature is available for the SonicWALL SRA 1200, SRA 4200, and Virtual Appliance.*

Simultaneous Profiling for Multiple Applications

Use the Application Offloading Portals to profile multiple applications at the same time. In addition, you may also save changes to content types for applications being profiled.



☑ Enable Custom Rules

This is a list of all Application Offloading Portals

Portals: OWA

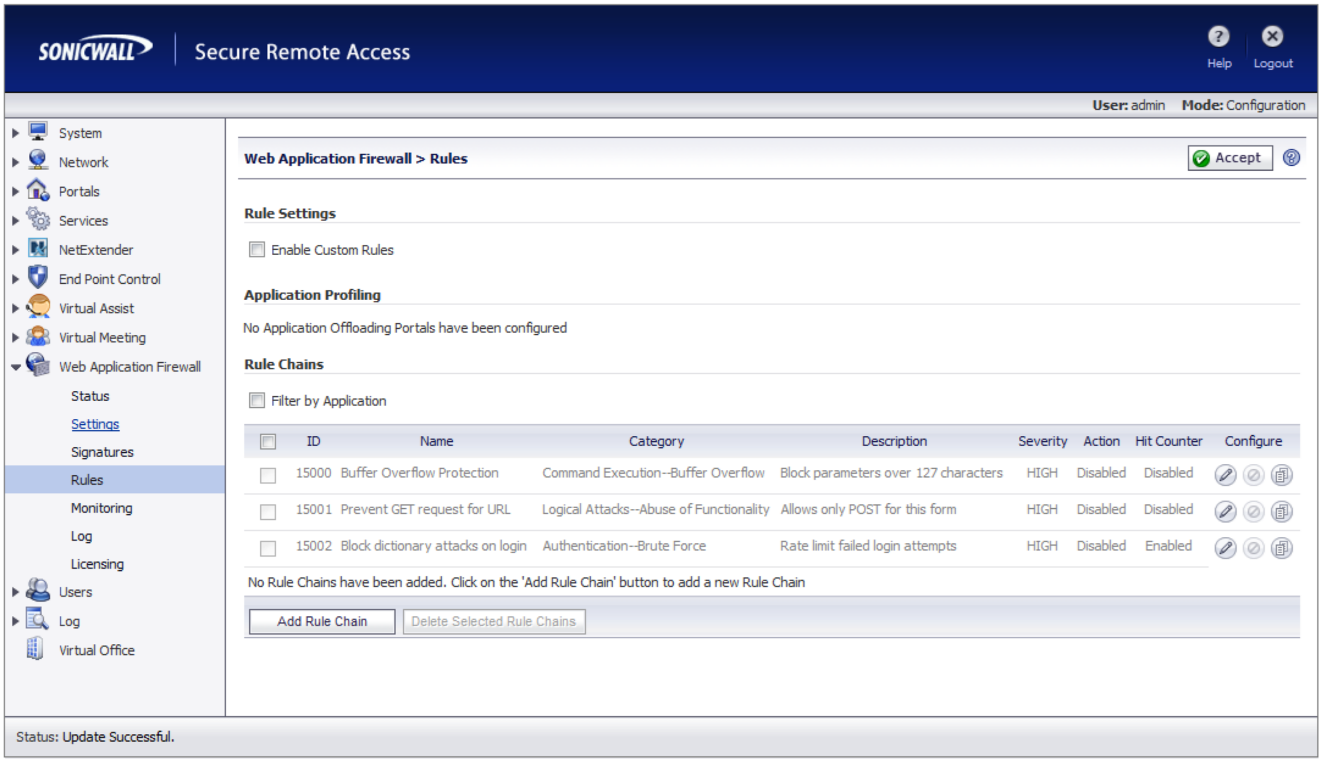
Content Types: □ All ☑ HTML/XML □ Javascript □ CSS

Figure 23 Web Application Firewall > Rules

In previous releases, only one application could be profiled at any time. This limitation increases the amount of learning time if a Web Application Firewall is protecting multiple applications. It is also a management issue to individually turn on/off Profiling for multiple applications. The 6.0 firmware introduces Simultaneous Profiling for Multiple Applications as a solution to address this issue.

Filtering Rule Chains by Applications

Rule Chains generated from Application Profiles can be filtered on the Web Application Firewall > Rules page. This improves viewing and modification of Rules for an application. The **Add Rule Chain** button is hidden because an add operation is unnecessary here. Modification, cloning, and deletion of auto-generated Rule Chains are allowed.



User: admin Mode: Configuration

Web Application Firewall > Rules

Rule Settings

□ Enable Custom Rules

Application Profiling

No Application Offloading Portals have been configured

Rule Chains

□ Filter by Application

□	ID	Name	Category	Description	Severity	Action	Hit Counter	Configure
□	15000	Buffer Overflow Protection	Command Execution--Buffer Overflow	Block parameters over 127 characters	HIGH	Disabled	Disabled	
□	15001	Prevent GET request for URL	Logical Attacks--Abuse of Functionality	Allows only POST for this form	HIGH	Disabled	Disabled	
□	15002	Block dictionary attacks on login	Authentication--Brute Force	Rate limit failed login attempts	HIGH	Disabled	Enabled	

No Rule Chains have been added. Click on the 'Add Rule Chain' button to add a new Rule Chain

Status: Update Successful.

Figure 24 Web Application Firewall > Rule Chains

Known Issues

This section contains known issues in the SonicWALL SRA 6.0 release:

Symptom	Condition / Workaround	Issue
Java applet for the Terminal Session broker stops responding	Occurs when login connection is redirected to a server other than the server name resolved by the appliance.	109486
Java client experiences “Print Redirect” error messages.	Occurs when 64-bit operating systems (OS) run 32-bit JVM.	92481
Nothing happens when user requests virtual assistance directly through a stand-alone client.	Occurs when a Mac user requests assistance from an appliance with a valid certificate.	115503
Password changes are failing for users who belong to multiple groups.	Occurs when using MIT Kerberos version 1.4.4. **Workaround**: Check the 'Do not require Kerberos pre-authentication, which allows the password to be changed.	112904

Resolved Issues

The following issues are resolved in the SonicWALL SRA 6.0 release:

End Point Control

Symptom	Condition / Workaround	Issue
Unassigning one EPC device profile for a local user unassigns all device profiles for the user.	Occurs when the **Remove selected profiles** button on the Edit Local Users page is used to unassign a single EPC device profile.	115321
Local users do not inherit EPC device profiles from the group.	Occurs when the **Inherit Group Device Profile** button on the Edit Local Users page is used.	115269

NetExtender

Symptom	Condition / Workaround	Issue
Linus NetExtender client fails to connect to the appliance.	Occurs when using OpenJDK to connect to an appliance with an invalid certificate.	115254
Connection profiles are not saved. Instead, only the last login credentials are saved.	Occurs when attempting to save connection profiles on a Mac or Linux NetExtender client.	111389

System

Symptom	Condition / Workaround	Issue
OTP %AD:mobile% value is not resolved	Occurs when the OTP %AD:mobile% value is inserted only in the subject.	111447
RDP bookmarks are unreliable (do not open, force close, etc.)	Occurs when using RDP bookmarks with Safari 5.1.	106456
Unable to control portal help link	Occurs when opening portal help link	109322
Unable to configure custom variable in an appliance tied to an LDAP attribute	Occurs when configuring a custom variable in an appliance tied to a LDAP attribute.	102659

Virtual Assist/Virtual Meeting

Symptom	Condition / Workaround	Issue
URL is not pre-configured for Virtual Assist MSI	Occurs when installing Virtual Assist MSI.	106505
Unable to reverse screen sharing in Virtual Meeting.	Occurs when the Host screen is shared during a Virtual Meeting.	64696
During a Virtual Assist session, the Technician side crashes after the Technician selects the System Info tab control.	Occurs when the Virtual Assist Technician attempts to retrieve system information from a Linux client.	115003

Upgrading SonicWALL SRA Firmware

The following procedures are for upgrading an existing SonicWALL SRA firmware image or Virtual Appliance software image to a newer version:

Obtaining the Latest SRA Image Version

1. To obtain a new SRA image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <http://www.mysonicwall.com>.

   Note: *If you have already registered your SonicWALL SSL VPN appliance, and you selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.*

2. Copy the new SRA image file to a directory on your management station.

   For the SonicWALL SRA 4200 or 1200 appliance, this is a file such as:
   sw_sslvpnsra4200_eng_6.0.0.0_tip_8sv_381693.sig

   For the SonicWALL Virtual Appliance, this is a file such as:
   sw_sslvpnsra-vm_eng_6.0.0.0_tip_8sv_381693.sig

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SonicWALL SSL VPN appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SonicWALL SSL VPN appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. The default settings file is named *sslvpnSettings.zip*.

   Tip: To more easily restore settings in the future, rename the .zip file to include the version of the SonicWALL SSL VPN image from which you are exporting the settings.

Uploading a New SRA Image

Note: *SonicWALL SSL VPN appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a SonicWALL SRA image, you must select **Uploaded Firmware with Factory Defaults – New!** . You can then import a settings file saved from the previous version or reconfigure manually.*

1. Download the SRA image file from www.mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the **System > Settings** page. Browse to the location where you saved the SRA image file, select the file, and click the **Upload** button. The upload process can take up to one minute.

When the upload is complete, you are ready to reboot your SonicWALL SSL VPN appliance with the new SRA image. Do one of the following:

- To reboot the image with current preference, click the boot icon for the following entry: **Uploaded Firmware – New!** ☞
- To reboot the image with factory default settings, click the boot icon for the following entry: **Uploaded Firmware with Factory Defaults – New!** ☞

Note: *Be sure to save a backup of your current configuration settings to your local machine before rebooting the SonicWALL SSL VPN appliance with factory default settings, as described in the previous "Saving a Backup Copy of Your Configuration Settings" section.*

3. A warning message dialog is displayed saying **Are you sure you wish to boot this firmware? Click OK to proceed**. After clicking **OK**, do not power off the device while the image is being uploaded to the flash memory.
4. After successfully uploading the image to your SonicWALL SSL VPN appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

Resetting the SonicWALL SRA 4200/1200 Using SafeMode

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.

   Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

2. Use a narrow, straight object, like a straightened paper clip or a pen tip, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is on the front panel in a small hole to the right of the USB connectors.

   💡**Tip**: *If this procedure does not work while the power is on, turn the unit off and on while holding the **Reset** button until the Test light starts blinking.*

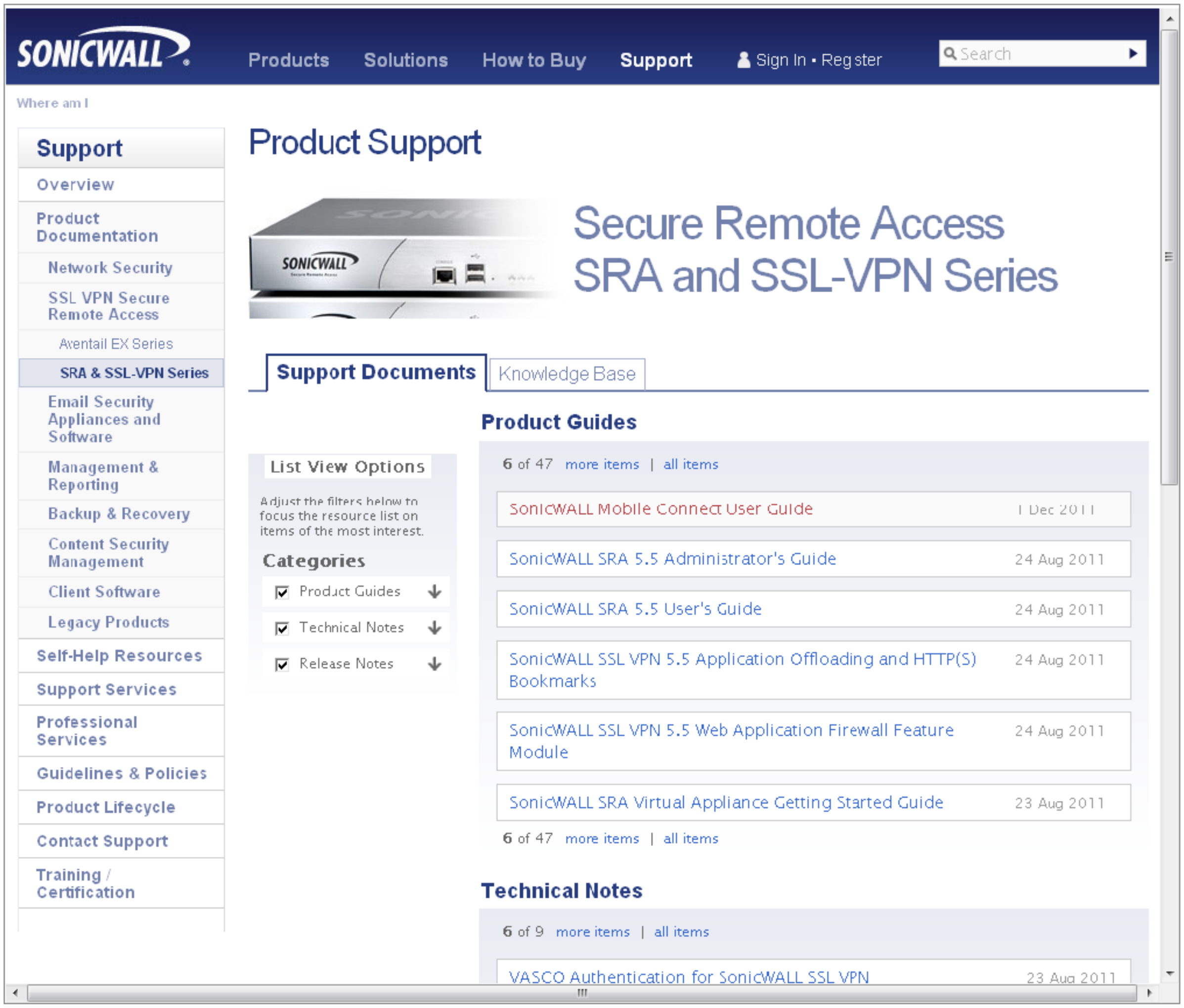
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

3. Connect to the management interface by pointing the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.
4. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon ☞ in the same line with **Current Firmware**.
5. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again. In SafeMode, restart the SRA image with the factory default settings. Click the boot icon in the same line with **Current Firmware with Factory Default Settings**.

Related Technical Documentation

This section contains a list of technical documentation available on the SonicWALL Technical Documentation Online Library located at:

http://www.sonicwall.com/us/Support.html



Adjust the filters below to focus the resource list on items of the most interest.

Categories

☑ Product Guides
☑ Technical Notes
☑ Release Notes

Product Guides

6 of 47 more items | all items

SonicWALL Mobile Connect User Guide	1 Dec 2011
SonicWALL SRA 5.5 Administrator's Guide	24 Aug 2011
SonicWALL SRA 5.5 User's Guide	24 Aug 2011
SonicWALL SSL VPN 5.5 Application Offloading and HTTP(S) Bookmarks	24 Aug 2011
SonicWALL SSL VPN 5.5 Web Application Firewall Feature Module	24 Aug 2011
SonicWALL SRA Virtual Appliance Getting Started Guide	23 Aug 2011

6 of 47 more items | all items

Technical Notes

6 of 9 more items | all items

VASCO Authentication for SonicWALL SSL VPN	23 Aug 2011

Figure 25 SonicWALL Technical Documentation Online Library

Information about SONICWALL SRA is found in the many reference guides available on the Web site, including the following:

- *SonicWALL SRA Administrator's Guide*
- *SonicWALL SRA User's Guide*
- *SonicWALL SRA NetExtender Feature Module*
- *SonicWALL SRA Citrix Access Feature Module*
- *SonicWALL SRA Web Application Firewall Feature Module*
- *SonicWALL SRA Application Offloading and HTTP(S) Bookmarks Feature Module*

Last updated: 4/17/2012