SonicWALL SSL VPN 4.0 HTTP(S) Reverse Proxy: Application Offloading and HTTP(S) Bookmarks

Document Scope

This document describes the implementation of HTTP(S) reverse proxy to provide access to offloaded Web-based applications and HTTP/HTTPS bookmark access to Microsoft Sharepoint, Microsoft Outlook Web Access (OWA) Premium and IBM Lotus Domino Web Access 7 on SonicWALL SRA and SSL-VPN appliances running 4.0 firmware.

This document contains the following sections:

Application Offloading and HTTP(S) Bookmarks Overview

This section provides an introduction to application offloading and HTTP(S) bookmarks. This section contains the following subsections:

- "What are Application Offloading and HTTP(S) Bookmarks?" section on page 2
- "Benefits of HTTP(S) Bookmarks" section on page 3
- "Benefits of Application Offloading" section on page 3
- "Supported Platforms" section on page 3
- "Software Prerequisites" section on page 4
- "Supported Application Configuration and Caveats" section on page 5

What are Application Offloading and HTTP(S) Bookmarks?

SonicWALL uses HTTP(S) bookmarks and application offloading on SonicWALL SSL VPN appliances to provide access to Web-based applications running on servers within the intranet. This includes Sharepoint 2007 and the enhanced versions of commonly-used Web mail interfaces, such as Microsoft OWA Premium and Domino Web Access 7.

Both application offloading and HTTP(S) bookmarks use an HTTP(S) reverse proxy. A reverse proxy is a proxy server that is deployed between a remote user outside an intranet and a target Web server within the intranet. The reverse proxy intercepts and forwards packets that originate from outside the intranet. An HTTP(S) reverse proxy specifically intercepts HTTP(S) requests and responses.

Application Offloading provides secure access to both internal and publicly hosted Web applications. An application offloading host is created as a special-purpose portal with an associated virtual host acting as a proxy for the backend Web application.

Unlike HTTP(S) bookmarks, access to offloaded applications is not limited to remote users. The administrator can enforce strong authentication and access policies for specific users or groups. For instance, in an organization certain guest users may need Two-factor or Client Certificate authentication to access Outlook Web Access (OWA), but are not allowed to access OWA public folders. If authentication is enabled, multiple layers of SonicWALL advanced authentication features such as One Time Password, Two-factor Authentication, Client Certificate Authentication and Single Sign-On can be applied on top of each other for the offloaded host.

The offloaded application portal must be configured as a virtual host with a suitable SSL VPN domain. It is possible to disable authentication and access policy enforcement for such an offloaded host.

Web transactions can be centrally monitored by viewing the logs. In addition, Web Application Firewall can protect offloaded application hosts from any unexpected intrusion, such as Cross-site scripting or SQL Injection.

Access to offloaded Web applications happens seamlessly as URLs in the proxied page are not rewritten in the manner used by HTTP or HTTPS bookmarks.

Benefits of HTTP(S) Bookmarks

By using HTTP(S) bookmarks, users can access the full-featured versions of Sharepoint 2007, Microsoft OWA Premium, and Domino Web Access 7 Web mail interfaces. These interfaces are easier to use and provide more enhanced features than their basic counterparts. For a full description of the application features supported using application offloading and HTTP(S) bookmarks, refer to the following sections:

- "Sharepoint Server 2007" section on page 6
- "Microsoft Outlook Web Access Premium" section on page 9
- "Lotus Domino Web Access 7 Support" section on page 13

Benefits of Application Offloading

An offloaded Web application has the following advantages over configuring the Web application as an HTTP(S) bookmark in SSL VPN:

- No URL rewriting is necessary, thereby improving throughput significantly.
- The functionality of the original Web application is retained almost completely, while an HTTP(S) bookmark is a best-effort solution.
- Application offloading extends SSL VPN security features to publicly hosted Web sites.

Application offloading can be used in any of the following scenarios:

- To function as an SSL offloader and add HTTPS support to the offloaded Web application, using the integrated SSL accelerator hardware of the SSL-VPN appliance.
- In conjunction with the Web Application Firewall subscription service to provide the offloaded Web application continuous protection from malicious Web attacks.
- To add strong or stacked authentication to the offloaded Web application, including Two-factor authentication, One Time Passwords and Client Certificate authentication.
- To control granular access to the offloaded Web application using global, group or user based access policies.
- To support Web applications not currently supported by HTTP/HTTPS bookmarks. Application Offloading does not require URL rewriting, thereby delivering complete application functionality without compromising throughput.

Supported Platforms

Appliance Platforms

Application offloading and HTTP(S) bookmarks are supported on the following SonicWALL SRA and SSL-VPN series appliances running firmware version 4.0:

- SRA 4200
- SRA 1200
- SSL-VPN 4000
- SSL-VPN 2000

HTTP(S) bookmarks are also supported on the SonicWALL SSL-VPN 200 appliance.

Note Application Offloading is only supported on SonicWALL SRA 1200/4200 and SSL-VPN 2000/4000 appliances.

HTTP Versions

HTTP(S) bookmarks and application offloading portals support both HTTP/1.0 and HTTP/1.1.

Certain performance optimization features, such as caching, compression, SSL hardware acceleration, HTTP connection persistence, TCP connection multiplexing and transfer-chunk encoding for proxies are automatically enabled depending on the usage.

Applications

The following applications are supported for use with application offloading and HTTP(S) bookmarks:

- **Sharepoint Server 2007**
- **Novell Groupwise 7.0 Webmail**
- **Microsoft Outlook Web Access 2010**
- **Microsoft Outlook Web Access Premium, Web client for Outlook 2003/2007** – Supported on the SonicWALL SRA 4200/1200 and SSL-VPN 2000/4000 platforms.
- **Lotus Domino Web Access 7** – Supported on the SonicWALL SRA 4200/1200 and SSL-VPN 2000/4000 platforms.
- **Exchange ActiveSync** – Supported on the Apple iPhone and iPad, and on Windows Mobile 6.5 based phones. Microsoft Exchange 2010, 2007, and 2003 are supported for use with Exchange ActiveSync.

Authentication Schemes

The following authentication schemes are supported for use with application offloading and HTTP(S) bookmarks:

- **Basic** – Collects credentials in the form of a username and password
- **NTLM (Microsoft NT LAN Manager)** – Automatic authentication between Active Directory aware applications
- **Forms-based authentication** – Uses a Web form to collect credentials

Software Prerequisites

The following end-user requirements must be met in order to access the complete set of application offloading and HTTP(S) bookmarks features:

- Internet Explorer 6.0 or later
- Windows 2000, Windows XP, or Windows Server 2003

Supported Application Configuration and Caveats

When using application offloading or HTTP(S) bookmarks to access applications for Web-based clients, full feature sets are accessible to users. SonicWALL SSL VPN 4.0 application offloading and HTTP(S) bookmarks provide enhanced application support for the following software applications:

- Sharepoint Server 2007, page 6
- Microsoft Outlook Web Access Premium, page 9
- Lotus Domino Web Access 7 Support, page 13

Note Feature support varies based on your hardware and installation, see the respective sections for more detailed information about specific applicaton support.

Tip If you are using the correct Web browser and operating system, and a supported application does not work, delete the browser session cookies, close and reopen all instances of your browser, clear the browser cache, and then try again.

Supported Application Caveats

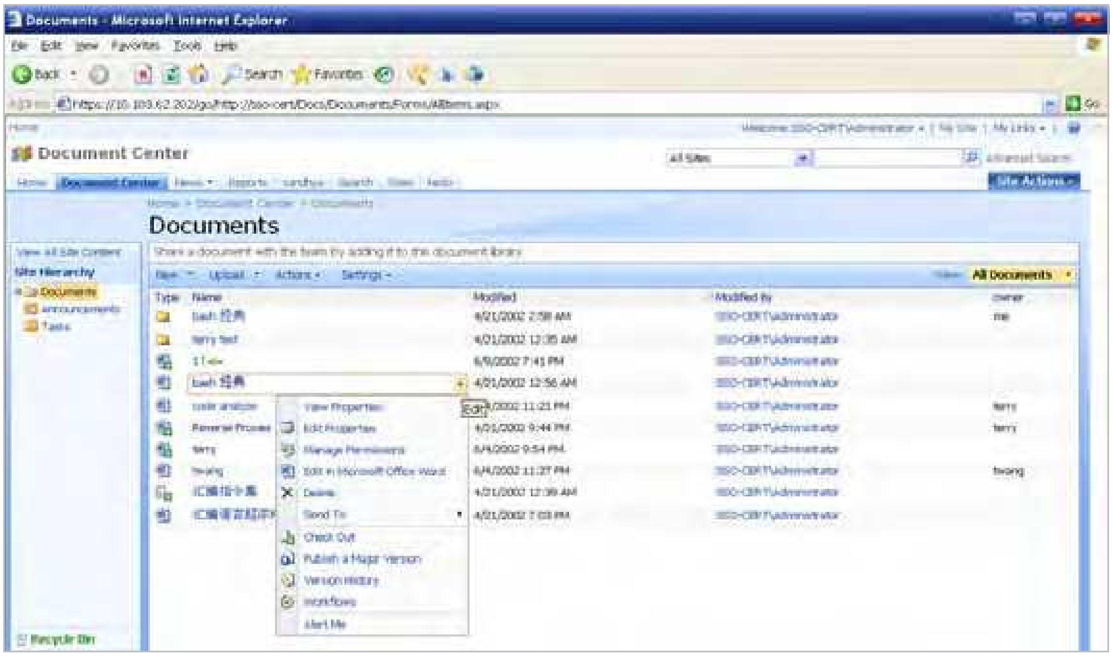
Be aware of these installation and general feature caveats when using application offloading and HTTP(S) bookmarks with the following software applications:

- **Sharepoint**
  - For features that rely on Windows Sharepoint Services-compatible client programs, SSL VPN 4.0 application offloading and HTTP(S) bookmarks do not support client integration capabilities on Internet Explorer.
  - Only forms-based authentication and basic authentication schemes are supported.
  - Single Sign-On is supported only for basic authentication.
- **Microsoft OWA**
  - S/MIME support and bi-directional layout support for Arabic and Hebrew in Microsoft OWA Premium are only available using Internet Explorer 6 SP1 and later. Gzip compression supported by Microsoft OWA Premium is not supported through the reverse proxy.
- **Domino Web Access**
  - This technology uses ActiveX controls for access using Internet Explorer 5.0 and later. Single Sign-On is not supported for Domino Web Access 7 through the reverse proxy.

Sharepoint Server 2007

Sharepoint is a Web portal management tool that lets users share information including spreadsheets, presentations, photographs, and more. Sharepoint facilitates creating a site for each project and managing the relevant data, allowing management with nothing more than a browser.

Figure 1 Sharepoint Web User Interface



Sharepoint utilizes distributed authoring to make additions and edits easy. Users can collaboratively create Wiki-style entries including events, contact information, documents, and news groups. Customized views can also be set up for diverse teams requiring multiple views and secured access to information.

This section contains the following sub-sections:

- Supported Sharepoint Features, page 6
- Enabling Basic Authentication for Sharepoint Server, page 7
- Enabling Basic Authentication for a Web Application Zone, page 8
- Disabling Client Integration on a Web Application Zone, page 8

Supported Sharepoint Features

The following features are supported in the SSL VPN 4.0 Reverse Proxy feature:

- **Using Site Templates to Collaborate or Manage Meetings** - The site templates in the Collaboration group are designed to help teams within an organization work on projects and collaborate on documents. The templates in this group support everything from basic meetings to decision-focused meetings or even social events.
- **Sharing Documents, Contacts, Tasks, and Calendars** - Synchronize your Office SharePoint Server 2007 calendar with Office Outlook 2007, enter all-day events and specify more types of repeating, or recurring events. Track team projects more effectively with visual day and month views.

- **Brainstorm Easily with Wiki Sites -** Collaborate on a team design, build an encyclopedia of knowledge, or just gather routine information in a format that is easy to create and modify. Your team members can contribute to wikis from their browsers — they don't need a word processor or special technical knowledge.
- **Share Ideas with Blogs** - With just a few clicks, easily publish customized short posts that are displayed in order, starting with the most recent post.
- **Receive updates to lists and libraries with RSS** - Automatically update members of your workgroup about changes to content using Really Simple Syndication (RSS) technology.
- **Manage Projects** - Create a Project Tasks list, which includes a Gantt chart for a visual overview of project tasks to monitor dates and progress of team tasks.
- **Get Mobile Access to Content** - View portals, team sites, and lists on a mobile device to help you stay current on team projects and tasks when you are travelling.
- **Store and Share Information on Your Own “My Site”** - Each user can store content, links, and contacts on their personal My Site. Your My Site also serves as a point of contact for others to find information about you such as your skills and roles, your colleagues and managers, the groups and distribution lists that you belong to, and the documents that you are working on. Each site contains stringent privacy control and security mechanisms so that you can choose how much information to present and to whom.
- **Search from the Search Center** - A central location for initiating queries and browsing search results to locate users with specific skill sets, documents, information about projects, and even data in enterprise applications such as SAP and Siebel.
- **Manage Documents in the Document Center** - Create large-scale document management sites that support highly structured document management scenarios with strong content control: Check-out, major and minor version control, multiple content types, and auditing to track content changes over time.
- **Manage Document Translation** - Create, store, and manage translated documents to facilitate the manual document translation process.
- **Web Content Management** - Office SharePoint Server 2007 includes many features that are useful for designing, deploying, and managing enterprise intranet portals, corporate Internet presence Web sites, and divisional portal sites.
- **Streamline Processes with Workflows** - Collaborate on documents and manage project tasks by implementing specific business processes on documents and items on an Office SharePoint Server 2007 site.
- **Store Reports in a Report Center** - Link to business applications such as SAP, Siebel, and Microsoft SQL Server 2005 to easily publish reports, lists, and key performance indicators (KPIs). The Report Center site provides a central location for storing reports that are common to a group.

Enabling Basic Authentication for Sharepoint Server

To enable basic authentication for Web application zone:

1. Navigate to **Administrative Tools** panel, open the **SharePoint Central Administration** website application. The Central Administration home page displays.
2. Navigate to **Application Management > Authentication Providers**. The Authentication Providers page displays.
3. On the **Authentication Providers** page in the Site Actions section, select the application you want to configure by choosing **Change Web Application** from the **Web Application** drop-down list.
4. In the **Select Web Application** dialog box, choose the Web application that you want to configure.
5. On the **Authentication Providers** page, click the **zone** of the Web application on which you want to enable authentication. The zones that are configured for the selected Web application are listed on the Authentication Providers page.

6. On the **Edit Authentication** page, in the **IIS Authentication** section, clear the **Integrated Windows authenticatio**n and **Digest authentication** check boxes.
7. Click **Save** to commit your changes.

Note The reverse proxy supports only forms-based authentication and basic authentication. Single-Sign-On is supported only for basic authentication.

Enabling Basic Authentication for a Web Application Zone

Follow the steps below to enable basic authentication on the Sharepoint server.

To enable authentication for a zone of a Web application:

Step 1 From **Administrative Tools**, open the SharePoint Central Administration Web site application.

Step 2 On the Central Administration home page, click **Application Management**.

Step 3 On the Application Management page, in the Application Security section, click **Authentication Providers**.

Step 4 On the Authentication Providers page, make sure the Web application that is listed in the **Web Application** box (under Site Actions) is the one that you want to configure. If the listed Web application is not the one that you want to configure, click the drop-down arrow to the right of the Web Application drop-down list box and select **Change Web Application**.

Step 5 In the Select Web Application dialog box, click the Web application that you want to configure.

Step 6 On the Authentication Providers page, click the **zone** of the Web application on which you want to enable authentication. The zones that are configured for the selected Web application are listed on this page.

Step 7 On the Edit Authentication page, in the **IIS Authentication** section, clear the **Integrated Windows authentication** and **Digest authentication** check boxes, and then click **Save**.

The reverse proxy does not support client integration capability on Internet Explorer. These are a set of features built into Sharepoint that work exclusively on IE and not on other browsers.

Note The Sharepoint administrator should consider disabling client integration on the Sharepoint server. Having these features appear on the UI and not supporting them through the HTTP bookmarks could confuse some users. Without client-integration, the Sharepoint features look the same between IE and non-IE browsers.

Disabling Client Integration on a Web Application Zone

Disabling client integration on the Sharepoint server is an option to consider if users might be confused when client integration is not supported through HTTP bookmarks. Without client-integration, the Sharepoint features look the same between IE and non-IE browsers.

Follow the steps below to disable Client Integration support on the Sharepoint server:

Step 1 From **Administrative Tools**, open the SharePoint Central Administration Web site application.

Step 2 On the Central Administration home page, click **Application Management**.

Step 3 On the Application Management page, in the Application Security section, click **Authentication providers**.

Step 4 On the Authentication Providers page, make sure the Web application that is listed in the **Web Application** box (under Site Actions) is the one that you want to configure. If the listed Web application is not the one that you want to configure, click the drop-down arrow to the right of the Web Application drop-down list box and select Change Web Application.

Step 5 In the Select Web Application dialog box, click the Web application that you want to configure.

Step 6 On the Authentication Providers page, click the **zone** of the Web application on which you want to disable client integration. The zones that are configured for the selected Web application are listed on this page.

Step 7 Clear all of the **client integration** check boxes, and then click **Save**.

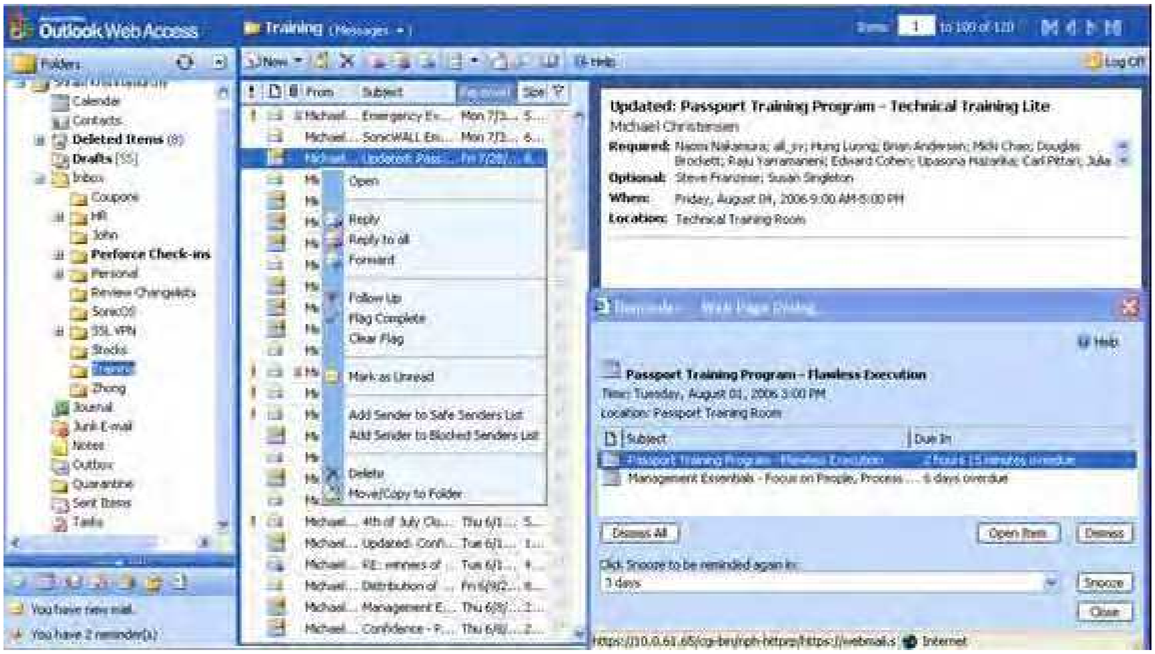
Microsoft Outlook Web Access Premium

Microsoft OWA Premium mode is a Web client for Microsoft Outlook 2003/2007 that simulates the Microsoft Outlook interface and provides more features than basic OWA. Microsoft OWA Premium includes features such as spell check, creation and modification of server-side rules, Web beacon blocking, support for tasks, auto-signature support, and address book enhancements.

Note The SonicWALL SSL VPN 200 supports OWA 2007 light version only. Because of this, some of the features listed in this document may not apply to the SSL VPN 200 platform.

Figure 2 provides a view of the Microsoft OWA Premium interface using SonicWALL SSL VPN 4.0 HTTP(S) reverse proxy.

Figure 2 Microsoft OWA Premium



Michael... Emergency Ev... Mon 7/3... 5...
Michael... SonicWALL En... Mon 7/3... 6...
Michael... Updated: Pass... Fri 7/28/... 8...
Michael... 4th of July Clo... Thu 6/1... 5...
Michael... Updated: Conf... Tue 6/1... 1...
Michael... RE: winners of ... Tue 6/1... 4...
Michael... Distribution of ... Fri 6/9/2... 8...
Michael... Management E... Thu 6/8/... 1...
Michael... Confidence - P... Thu 6/8/... 2...

Updated: Passport Training Program - Technical Training Lite
Michael Christensen
Required: Naomi Nakamura; all_sv; Hung Luong; Brian Anderson; Nikki Chao; Douglas Brockett; Raju Yarramaneni; Edward Cohen; Upasona Hazarika; Carl Pittari; Julie
Optional: Steve Franzese; Susan Singleton
When: Friday, August 04, 2006 9:00 AM-5:00 PM
Location: Technical Training Room

Passport Training Program - Flawless Execution
Time: Tuesday, August 01, 2006 3:00 PM
Location: Passport Training Room

Subject	Due In
Passport Training Program - Flawless Execution	2 hours 15 minutes overdue
Management Essentials - Focus on People, Process ...	6 days overdue

Click Snooze to be reminded again in:
3 days

https://10.0.61.65/cgi-bin/nph-httprp/https://webmail.s

This section contains the following sub-sections:

- Application and Feature Support, page 10
- Premium and Basic Modes, page 11

Application and Feature Support

SonicWALL SSL VPN HTTP(S) reverse proxy application support for Microsoft OWA Premium, using Internet Explorer 5.0 or higher, provides users with full functionality of the following features:

- Access to email, calendar, and tasks
- New Outlook look-and-feel, including right-click functionality
- Ability to mark an email as unread
- Server-side spelling checker (limited to six languages)
- Forms-based authentication (session time-out)
- S/MIME support

Note S/MIME support for Microsoft OWA Premium is only available on Internet Explorer 6 SP1.

- Two-line view
- Context menus
- Improved keyboard shortcuts
- Ability to forward meeting requests
- Notifications on navigation pane
- Ability to add to contacts
- Ability to pick names from address book
- Ability to set maximum number of messages displayed in views
- Support for bi-directional layout for Arabic and Hebrew

Note Bi-directional layout support for Arabic and Hebrew for Microsoft OWA Premium is only available on Internet Explorer 6 SP1.

- Option to set message status “mark as read” when using the reading pane
- Public folders display in their own browser window
- Access to GAL property sheets within an email message or meeting request
- Message sensitivity settings on information bar
- Attendee reminder option for meeting request
- Ability to launch the calendar in its own window
- User interface to set common server-side rules
- Outlook style Quick Flags
- Support for message signatures
- Search folders (must be created in Outlook online mode)
- Deferred search for new messages after delete
- Attachment blocking
- Web beacon blocking to make it more difficult for senders of spam to confirm email addresses
- Protection of private information when a user clicks a hyperlink in the body of an email message

Tip For better performance, it is recommended that the Exchange administrator configure OWA to list at the most 40 items in any page. This can be done in the Outlook Web Access Administration Web-based utility provided part of the Exchange installation. Navigate to **Server Settings > Administration > View Settings**. On the View Settings page, the **Maximum View Rows** attribute defines the maximum row count of items visible in any view. From the drop-down menu, select 40 or less and click **OK**.

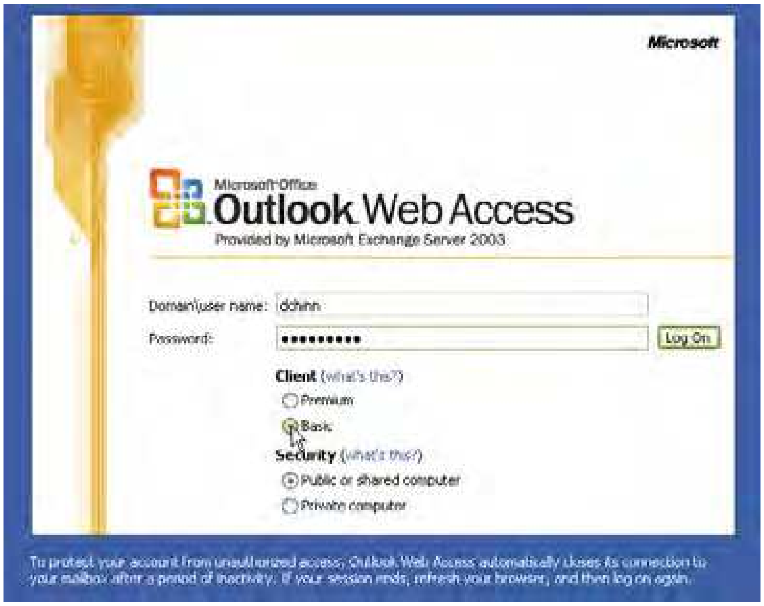
Note GZip compression supported by Microsoft OWA Premium is not supported through the reverse proxy.

Premium and Basic Modes

Microsoft Internet Explorer defaults to loading OWA Premium, but in some cases clients may prefer to run Microsoft OWA in Basic mode for speed and accessability reasons. There are two solutions for users wishing to use OWA basic:

1. Use a browser that is <u>not</u> Microsoft Internet Explorer. All browsers that are HTML 3.2 compliant (Mozilla Firefox, Apple Safari, etc...) are compatible with OWA, although they are forced to load in Basic mode.
2. Give your clients the option of loading Basic or Premium mode at the OWA login screen shown in Figure 3. Accomplish this by setting the Microsoft Exchange server to use forms-based Authentication (FBA).

Figure 3 OWA login screen with Forms-Based Authentication enabled



Domain\user name: dchinn

Password: ●●●●●●●●●

Client (what's this?)

○ Premium

● Basic

Security (what's this?)

● Public or shared computer

○ Private computer

To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.

Configurin Forms-Based Authentication in Exchange

To use the Exchange Management Console to configure forms-based authentication for Outlook Web Access, perform the following steps:

Step 1 In the **Exchange Management Console**, locate the virtual directory that you want to configure to use forms-based authentication by using the information in step 2 or step 3.

Step 2 If you are running the Mailbox server role on the computer that is running the Client Access server role, do one of the following:

- **a.** To modify an Exchange 2007 virtual directory, select **Server Configuration**, select **Client Access**, and then click the **Outlook Web Access** tab. The default Exchange 2007 virtual directory is /owa.
- **b.** To modify a legacy virtual directory, select **Server Configuration**, select Mailbox, and then click the **WebDAV** tab. The default legacy virtual directories are as follows: /Public, /Exchweb, /Exchange, and /Exadmin.

Step 3 If you are not running the Mailbox server role on the computer that is running the Client Access server role, select **Server Configuration**, select **Client Access**, and then click the **Outlook Web Access** tab.

Step 4 In the work pane, select the virtual directory that you want to configure to use forms-based authentication, and then click **Properties**.

Step 5 Click the **Authentication** tab.

Step 6 Select **Use forms-based authentication**.

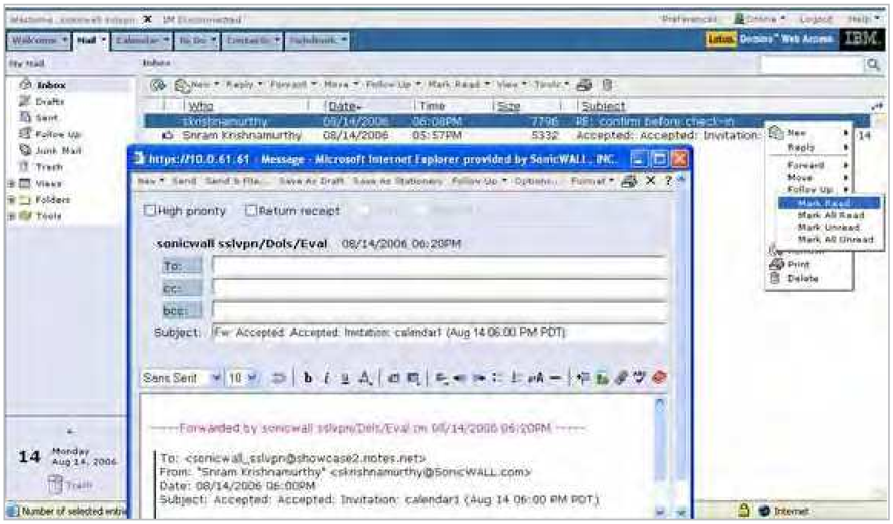
Step 7 Select the **logon format** that you want to use.

Note For more information about configuring FBA for Microsoft Exchange Server, visit the Microsoft TechNet Library at http://technet.microsoft.com/en-us/library/ and perform a search for “forms-based authentication”.

Lotus Domino Web Access 7 Support

Lotus Domino Web Access 7 is a Web client for IBM Lotus Domino server with an easy-to-use interface. It provides features such as advanced Web messaging and rich-text messages, scheduling meetings, managing tasks, collaboration, and managing personal information. Domino Web Access 7 also provides increased server capability and reduced CPU usage to boost performance and response time. Figure 4 provides a view of the Lotus Domino Web Access 7 interface using SonicWALL SSL VPN 4.0 HTTP(S) reverse proxy.

Figure 4 Lotus Domino Web Access 7



Who	Date	Time	Size	Subject
skrishnamurthy	08/14/2006	06:08PM	7796	RE: confirm before check-in
Sriram Krishnamurthy	08/14/2006	05:57PM	5332	Accepted: Accepted: Invitation:

https://10.0.61.61 - Message - Microsoft Internet Explorer provided by SonicWALL, INC.

sonicwall sslvpn/Dols/Eval 08/14/2006 06:20PM

Subject: Fw: Accepted: Accepted: Invitation: calendar1 (Aug 14 06:00 PM PDT)

-----Forwarded by sonicwall sslvpn/Dols/Eval on 08/14/2006 06:20PM -----

To: <sonicwall_sslvpn@showcase2.notes.net>
From: "Sriram Krishnamurthy" <skrishnamurthy@SonicWALL.com>
Date: 08/14/2006 06:00PM
Subject: Accepted: Accepted: Invitation: calendar1 (Aug 14 06:00 PM PDT)

Note Domino Web Access 7 uses ActiveX controls for access using Internet Explorer 5.0 and later.

SonicWALL SSL VPN HTTP(S) reverse proxy application support for Domino Web Access 7, using Internet Explorer 5.0 or higher, provides users with full functionality of the following features:

- **Email**
  - Send and receive email
  - Send and receive attachments
  - Delete messages
  - Open attachment from reading and preview panes
  - Spell check
  - Quick Flags and message flags
  - Set message importance
  - Send and receive HTML mail
  - Mark messages as read or unread
- **Navigation**
  - Navigate folder hierarchy in navigation pane
  - Sort message list by standard fields

  - Search capabilities
  - Logout
- **Calendar**
  - Calendar views of different time periods
  - Create a meeting
  - Check schedule
  - Use address book to pick attendees
  - Search for resource
  - Change invitee list
  - Delete meeting
- **Folders and Storage**
  - Create a folder
  - Move messages using drag and drop
  - Recover from trash
  - Empty trash
- **Contacts**
  - View by options
  - Add and edit contacts
  - Delete contact
- **Tasks and Options**
  - Create a to-do list
  - View to-do list
  - Use notebook to create a new note.
  - Delegation
  - Change password
  - Display options
  - Change notes ID
  - Out of office settings
- **Rules**
  - Create new mail and quick rules
  - Delete rules
  - Test created rules

Note Single sign-on is not supported for Domino Web Access 7.

Configuring Offloaded Applications and HTTP(S) Bookmarks

The SSL VPN administrator can configure Web (HTTP) or Secure Web (HTTPS) offloaded applications or bookmarks to allow user access to Web-based resources and applications such as Sharepoint 2007, Microsoft OWA Premium, or Domino Web Access 7. When user or group bookmarks are defined, the user or group member will see the defined bookmarks on the SonicWALL SSL VPN appliance Virtual Office home page.

This section contains the following subsections:

- "Configuring an Offloaded Application" section on page 15
- "Creating an HTTP or HTTPS User Bookmark" section on page 19
- "Configuring Single Sign-On" section on page 21
- "Creating User/Group/Global Policies for URL Objects" section on page 23

Configuring an Offloaded Application

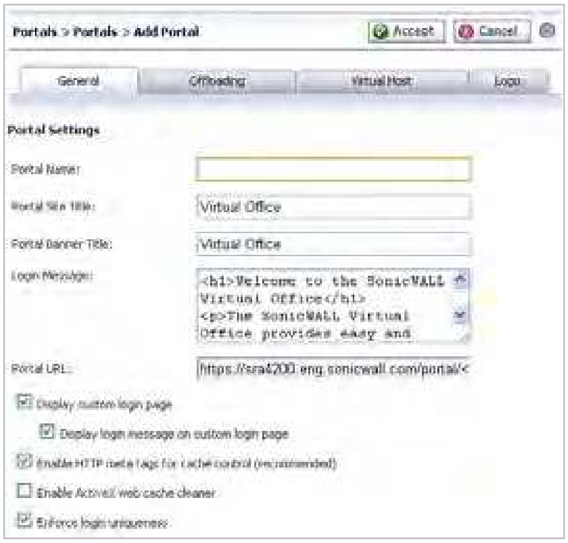
To configure an offloaded application, you must be logged in as an administrator.

Note The Application Offloading feature will not work well if the application refers to resources within the same host using absolute URLs. In this case, you may need to convert an absolute URL reference to its relative form.

On SonicWALL SSL-VPN models 2000 and higher, to configure an offloaded Web application, perform the following steps:

Step 1 Navigate to **Portals > Portals** and click the **Offload Web Application** button. The Add Portal screen opens.

Step 2 Configure the fields on the **General** tab. See the "Configuring General Portal Settings" section on page 17 for information about the settings on the **General** tab.



Portal Settings

Portal Name:

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the SonicWALL
Virtual Office</h1>
<p>The SonicWALL Virtual
Office provides easy and
```

Portal URL: https://sra4200.eng.sonicwall.com/portal/<

☑ Display custom login page

☑ Display login message on custom login page

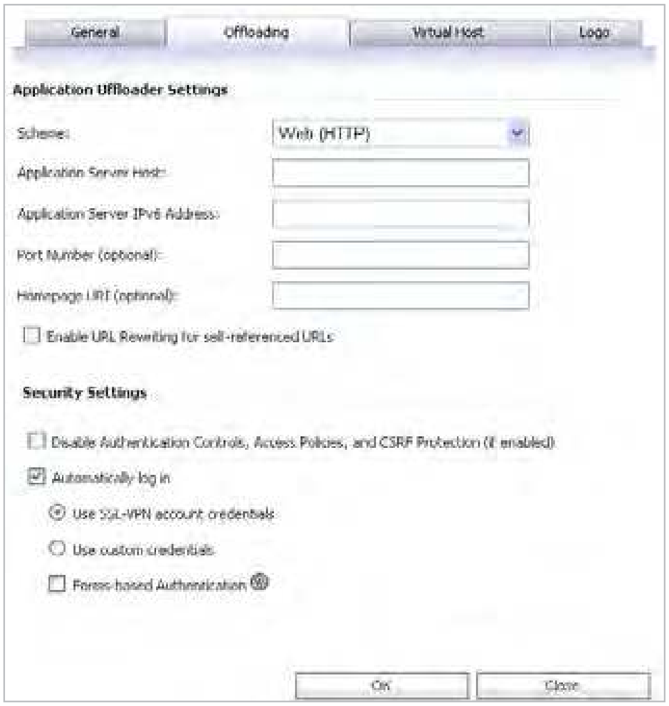
☑ Enable HTTP meta tags for cache control (recommended)

□ Enable ActiveX web cache cleaner

☑ Enforce login uniqueness

Step 3 On the **Offloading** tab, select one of the following from the **Scheme** drop-down list:

- **Web (HTTP)** – access the Web application using HTTP
- **Secure Web (HTTPS)** – access the Web application using HTTPS



Application Offloader Settings

Scheme: Web (HTTP)

Application Server Host:

Application Server IPv6 Address:

Port Number (optional):

Homepage URI (optional):

□ Enable URL Rewriting for self-referenced URLs

Security Settings

□ Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)

☑ Automatically log in

● Use SSL-VPN account credentials

○ Use custom credentials

□ Forms-based Authentication

Step 4 Enter the host name or private IP address of the backend host into the **Application Server Host** field.

Step 5 Optionally enter the IPv6 address of the backend host into the **Application Server IPv6 Address** field.

Step 6 In the **Port Number (optional)** field, optionally enter a custom port number to use for accessing the application.

Step 7 In the **Homepage URI (optional)** field, optionally enter a URI to a specific resource on the Web server to which the user will be forwarded after logging in. This is a string in the form of: **/exch/test.cgi?key1=value1&key2=value2**

Step 8 Select the **Enable URL Rewriting for self-referenced URLs** checkbox if you want absolute URLs that refer to this application server in HTML, Javascript, or CSS content to be rewritten.

Step 9 Under Security Settings, select the **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** checkbox if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.

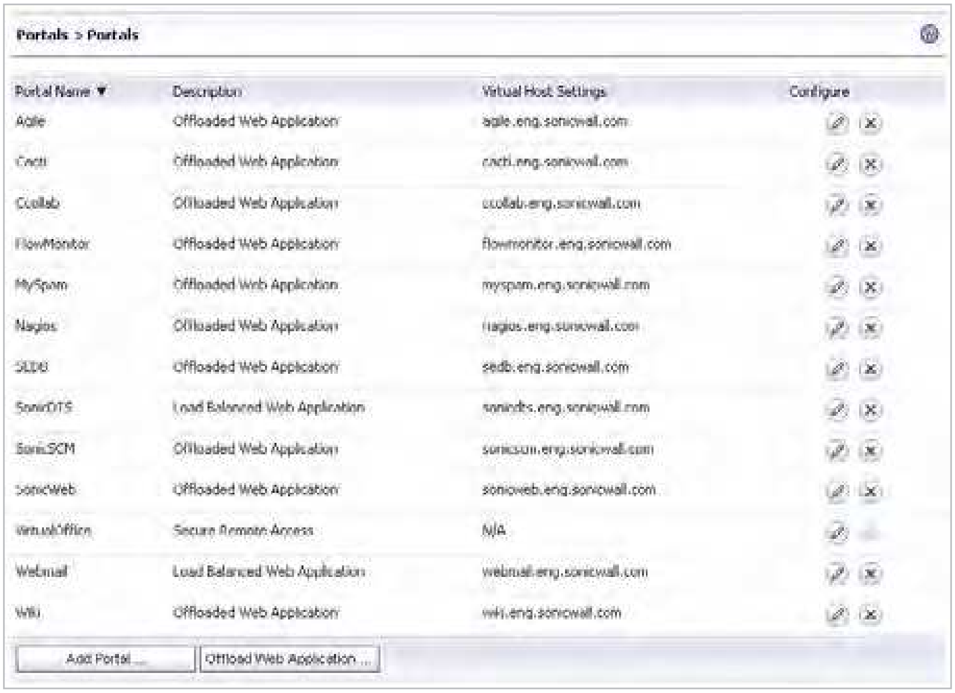
If you are setting up an offloaded application portal for your Exchange server and you want to allow ActiveSync for smart phones, you must select this checkbox. In this case, authentication is handled by the Exchange server rather than by the SonicWALL SSL-VPN.

If you want users to authenticate for portal access, do not select this checkbox. You will need to create a domain for this portal (Step 13).

Step 10 Select the **Automatically Login** checkbox to use Single Sign-On. See the "Configuring Single Sign-On" section on page 21 for information about configuring SSO options for an offloaded application.

Step 11 Configure the fields on the **Virtual Host** tab. See the "Configuring Virtual Host Settings" section on page 18 for information about the settings on the **Virtual Host** tab.

Step 12 Click **OK**. You are returned to the Portals > Portals page where you will see the Web application listed as an **Offloaded Web Application** under **Description**.



Portals > Portals

Portal Name ▼	Description	Virtual Host Settings	Configure
Agile	Offloaded Web Application	agile.eng.sonicwall.com	✎ ✕
Cacti	Offloaded Web Application	cacti.eng.sonicwall.com	✎ ✕
Ccollab	Offloaded Web Application	ccollab.eng.sonicwall.com	✎ ✕
FlowMonitor	Offloaded Web Application	flowmonitor.eng.sonicwall.com	✎ ✕
MySpam	Offloaded Web Application	myspam.eng.sonicwall.com	✎ ✕
Nagios	Offloaded Web Application	nagios.eng.sonicwall.com	✎ ✕
SEDB	Offloaded Web Application	sedb.eng.sonicwall.com	✎ ✕
SonicDTS	Load Balanced Web Application	sonicdts.eng.sonicwall.com	✎ ✕
SonicSCM	Offloaded Web Application	sonicscm.eng.sonicwall.com	✎ ✕
SonicWeb	Offloaded Web Application	sonicweb.eng.sonicwall.com	✎ ✕
VirtualOffice	Secure Remote Access	N/A	✎
Webmail	Load Balanced Web Application	webmail.eng.sonicwall.com	✎ ✕
Wiki	Offloaded Web Application	wiki.eng.sonicwall.com	✎ ✕

Step 13 If you want users to authenticate when accessing the offloaded application (you have not disabled authentication in Step 9 above), navigate to the **Portals > Domains** page and create a domain for this portal. See the *SonicWALL SSL VPN Administrator's Guide* for information about creating a domain.

Step 14 Update your DNS server for the virtual host domain name and alias (if any).

Configuring General Portal Settings

To configure the settings on the General tab for an offloaded application portal, perform the following steps:

Step 1 On the General tab, enter a descriptive name for the portal in the **Portal Name** field. This name will be part of the path in the portal URL. For example, if your SonicWALL SSL-VPN portal is hosted at **https://vpn.company.com**, and you created a portal named "sales", then users will be able to access the sub-site at **https://vpn.company.com/portal/sales**.

Note Only alphanumeric characters, hyphen (-), and underscore (_) are accepted in the **Portal Name** field. If other types of characters or spaces are entered, the portal name will be truncated before the first non-alphanumeric character.

Step 2 Enter the title for the Web browser window in the **Portal Site Title** field.

Step 3 To display a banner message to users before they login to the portal, enter the banner title text in the **Portal Banner Title** field.

Step 4 Enter an HTML compliant message, or edit the default message in the **Login Message** field. This message is shown to users on the custom login page.

Step 5 The **Portal URL** field is automatically populated based on your SSL-VPN network address and Portal Name.

Step 6 To enable visibility of your custom logo, message, and title information on the login page, select the **Display custom login page** checkbox.

Note Custom logos can only be added to existing portals. To add a custom logo to a new portal, first complete general portal configuration, then add a logo.

Step 7 Select the **Enable HTTP meta tags for cache control** checkbox to apply HTTP meta tag cache control directives to the portal. Cache control directives include:

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

These directives help prevent client browsers from caching SonicWALL SSL VPN portal pages and other Web content.

Note Enabling HTTP meta tags is strongly recommended for security reasons and to prevent out-of-date Web pages and data being stored in a user Web browser cache.

Step 8 Select the **Enable ActiveX Web cache cleaner** checkbox to load an ActiveX cache control when users log in to the SonicWALL SSL-VPN appliance. The Web cache cleaner will prompt the user to delete all session temporary Internet files, cookies and browser history when the user logs out or closes the Web browser window. The ActiveX Web cache control is ignored by Web browsers that don't support ActiveX.

Step 9 Select the **Enforce login uniqueness** checkbox to restrict each account to a single session at a time. When login uniqueness is not enforced, each account can have multiple, simultaneous sessions.

Configuring Virtual Host Settings

Creating a virtual host allows users to access the application using a different host name than your default URL. For example, sales members can access https://sales.company.com instead of the default domain, https://vpn.company.com that you use for administration. The portal URL (for example, https://vpn.company.com/portal/sales) will still exist even if you define a virtual host name. Virtual host names enable administrators to give separate and distinct login URLs to different groups of users.

To configure the settings on the Virtual Host tab for an offloaded application portal, perform the following steps:

Step 1 Enter a host name in the **Virtual Host Domain Name** field, for example, sales.company.com.

Only alphanumeric characters, hyphen (-) and underscore (_) are accepted in the **Virtual Host Domain Name** field.

Step 2 Optionally enter a descriptive alias in the **Virtual Host Alias** field.

Step 3 If you are using IP based virtual hosting, select a specific **Virtual Host Interface** for this portal. If using name based virtual hosts — where more than one hostname resides behind a single IP address — choose **All Interfaces**.

When selecting **All Interfaces**, you can import a wildcard certificate for all virtual hosts on the SSL-VPN. See Step 6.

Step 4 If you selected a specific interface for this portal in the previous step, enter the desired **Virtual Host IP Address** in the field provided. This is the IP address users will access in order to access the portal.

Note For external access, be sure to add an entry in your external DNS server to resolve the virtual hostname and domain name to the external IP address of your SonicWALL SSL-VPN appliance.

Step 5 If you selected a specific interface for this portal, you can specify an IPv6 address in the **Virtual Host IPv6 Address** field. You can use this address to access the virtual host. Enter the IPv6 address using decimal or hexadecimal numbers in the form:

```
2001::A987:2:3:4321
```

Step 6 If you plan to use a unique security certificate for this sub-domain, select the corresponding port interface address from the **Virtual Host Certificate** list.

If you need to associate a certificate to this host, first import the relevant SSL certificate into the SSL-VPN appliance:

- For name-based virtual hosting, you can import a wildcard certificate to use for all virtual hosts on the SSL-VPN.
- For IP-based virtual hosting, import a regular SSL certificate. This type of certificate includes the hostname of the server.

Note Unless you have a certificate for each virtual host domain name, or if you have purchased a ***.domain** SSL certificate, your users may see a **Certificate host name mismatch** warning when they log into the portal. The certificate hostname mismatch only affects the login page; SonicWALL SSL VPN client applications will not be affected by a hostname mismatch.

Note Some ActiveSync clients do not work well with servers that have invalid SSL certificates.

Creating an HTTP or HTTPS User Bookmark

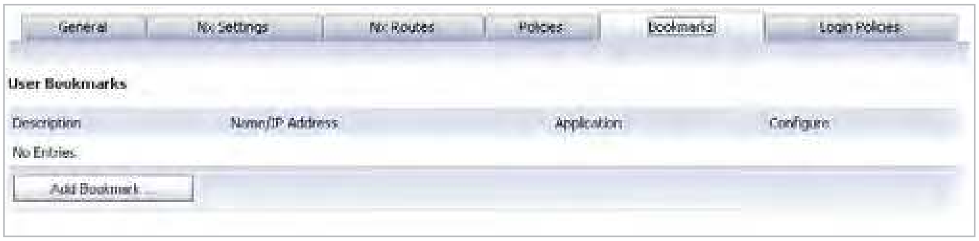
To create HTTP or HTTPS user bookmarks, perform the following steps:

Step 1 Log into your SonicWALL SSL VPN.

Step 2 From the **Users** tab, select either **Local Users** or **Local Groups**.

Step 3 Click the **Configure** icon next to the user or group for which you want to create the bookmark.

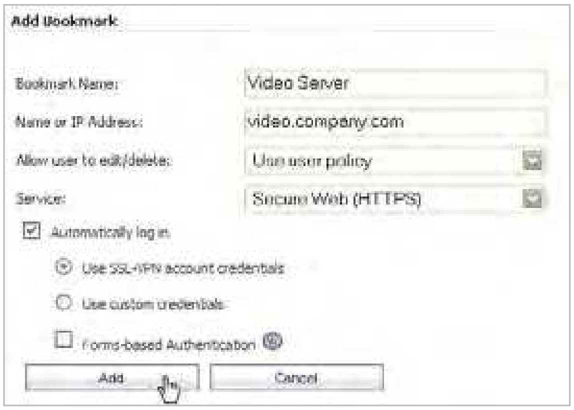
Step 4 Select the **Bookmarks** tab.



User Bookmarks

Description	Name/IP Address	Application	Configure
No Entries			

Step 5 Click **Add Bookmark**. The **Add Bookmark** dialog box displays.



Add Bookmark

Bookmark Name: Video Server

Name or IP Address: video.company.com

Allow user to edit/delete: Use user policy

Service: Secure Web (HTTPS)

☑ Automatically log in

● Use SSL-VPN account credentials

○ Use custom credentials

□ Forms-based Authentication

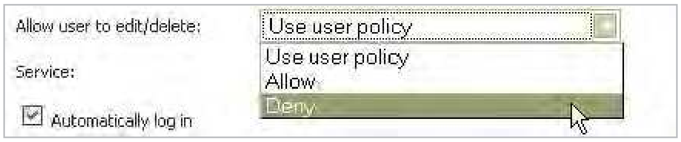
Step 6 Type the name of the bookmark in the **Bookmark Name** field.

Step 7 Enter the HTTP or HTTP(S) address of your Web mail server in the **Name or IP Address** field. For example, *webmail.company.com* or *company.notes.net/example/mail*.

Note For HTTP and HTTPS bookmarks you can specify custom ports and paths, for example *www.mycompany.com:8080*.

Step 8 If you are creating the bookmark for a **Local User**, you have the option to allow or deny users the ability to edit or delete this bookmark.

- Select **Allow** from the **Allow user to edit/delete** drop-down menu to allow them to edit or delete the bookmark.
- To prevent users from editing or deleting the bookmark, select **Deny**.
- To allow or deny based on the individual user policy, select **Use user policy**.



Allow user to edit/delete: Use user policy

Service:

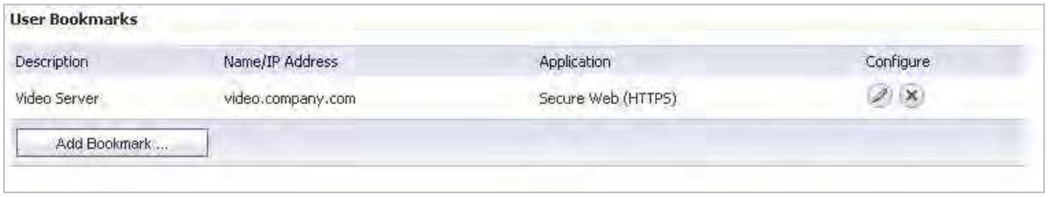
☑ Automatically log in

Note Only **Local Users** bookmarks have the option of allowing users edit/delete privileges. Bookmarks created in the **Local Groups** tab are permanently displayed on portals for all users in the group and can only be removed or edited by the administrator.

Step 9 Select **Web (HTTP)** or **Secure Web (HTTPS)** the service type in the **Service** pull-down menu.

Step 10 Select the **Automatically Login** checkbox to use Single Sign-On. See the "Configuring Single Sign-On" section on page 21 for information about configuring SSO options for a bookmark.

Step 11 Click **Add** to add the bookmark. Once the configuration has been updated, the new user bookmark will be displayed in the **Edit User Settings** window as shown below:



User Bookmarks

Description	Name/IP Address	Application	Configure
Video Server	video.company.com	Secure Web (HTTPS)	

Configuring Single Sign-On

The administrator can configure Single Sign-On (SSO) for each user, each group, or globally for offloaded applications and HTTP or HTTPS bookmarks. Either straight textual parameters or variables may be used for login credentials.

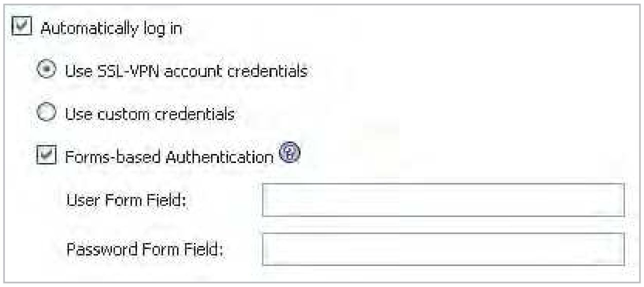
You can configure SSO with the **Use SSL-VPN account credentials** option to use account information from the local SSL-VPN appliance, or with the **Use custom credentials** option to enter the credentials here while configuring the offloaded application or bookmark. You can also select **Forms-based Authentication** to configure the appliance to display an HTML-based Web form to prompt the user for login credentials.

Note When using forms-based authentication, application support may be limited based on the complexity of the login page.

To configure Single Sign-On options, perform the following steps:

Step 1 Create or edit an offloaded application or a bookmark as described in the "Configuring an Offloaded Application" section on page 15 or the "Creating an HTTP or HTTPS User Bookmark" section on page 19.

Step 2 Select the **Automatically Login** checkbox to configure Single Sign-On settings. The SSO settings appear on the **Offloading** tab when configuring an offloaded application or on the **Add Bookmark** page when configuring an HTTP(S) bookmark.



☑ Automatically log in

● Use SSL-VPN account credentials

○ Use custom credentials

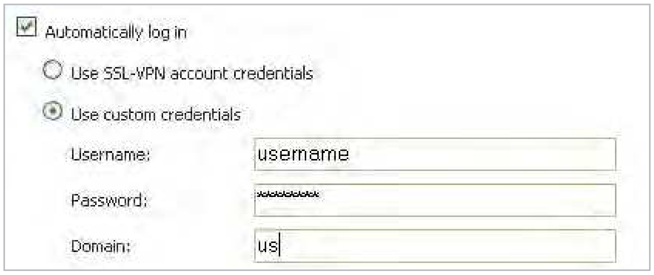
☑ Forms-based Authentication

User Form Field:

Password Form Field:

Step 3 Select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow login to the offloaded application or bookmark using the local user credentials configured on the SSL-VPN appliance
- **Use custom credentials** – allow login to the offloaded application or bookmark using the credentials you enter here; when selected, this option displays **Username**, **Password**, and **Domain** fields:



☑ Automatically log in

○ Use SSL-VPN account credentials

● Use custom credentials

Username: username

Password: ********

Domain: us

You can enter the custom credentials as text or use dynamic variables such as those shown below:

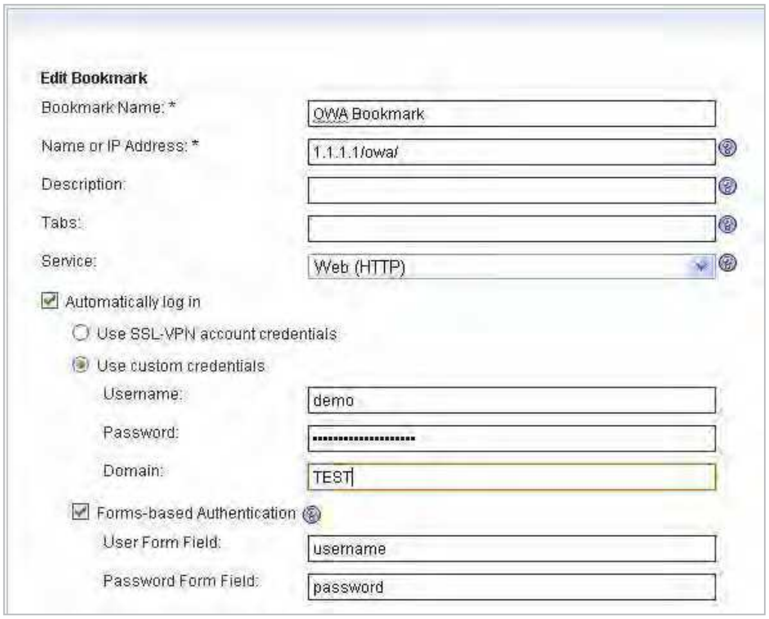
Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%
Password	%PASSWORD%	%PASSWORD% or leave the field blank

Step 4 To configure forms-based authentication for Single Sign-On, select the **Forms-based Authentication** checkbox.

- Configure the **User Form Field** to be the same as the 'name' and 'id' attribute of the HTML element representing User Name in the Login form, for example: **<input type=text name='userid'>**
- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example: **<input type=password name='PASSWORD' id='PASSWORD' maxlength=128>**

Note If SSO is configured for an HTTP URL, the credentials entered for that user/group will also be used for HTTPS transactions within the specified site. However, the converse is not true. HTTPS credentials specified in SSO will not automatically be used for HTTP authentication.

SonicWALL SSL VPN supports SSO with forms-based authentication for both Outlook Web Access bookmarks and OWA offloaded application portals. Set the **User Form Field** to **username** (literally) and set the **Password Form Field** to **password**.



Edit Bookmark

Bookmark Name: * OWA Bookmark

Name or IP Address: * 1.1.1.1/owa/

Description:

Tabs:

Service: Web (HTTP)

☑ Automatically log in

○ Use SSL-VPN account credentials

● Use custom credentials

Username: demo

Password: ••••••••••••••••••••

Domain: TEST

☑ Forms-based Authentication

User Form Field: username

Password Form Field: password

Creating User/Group/Global Policies for URL Objects

You can create user policies to control access to Web resources available at a specific location defined in a URL object. Policies apply to HTTP/HTTPS bookmarks and to offloaded application portals.

When an External Website Bookmark is configured for an offloaded application portal, access to the bookmark is not controlled by policies. However, once the portal is reached through the bookmark, policies control further access. If the policy denies access, the user will be denied access after attempting to log in.

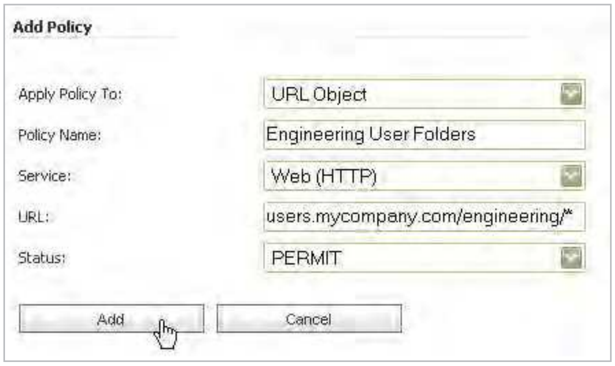
To create object-based HTTP or HTTPS user policies, perform the following steps:

Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy** to display the Add Policy window.



Add Policy

Apply Policy To: URL Object

Policy Name: Engineering User Folders

Service: Web (HTTP)

URL: users.mycompany.com/engineering/*

Status: PERMIT

Step 5 In the **Apply Policy To** drop-down menu, select the **URL Object** option.

Step 6 Type in a descriptive name for the policy in the **Policy Name** field.

Step 7 In the **Service** drop-down menu, choose either **Web (HTTP)** or **Web (HTTPS)**, or select the backend Web server for the offloaded application portal.

Step 8 In the **URL** field, add the URL string to be enforced in this policy.

Note In addition to standard URL elements, the administrator may enter port, path and wildcard elements to the URL field.

If a path is specified, the URL policy is recursive and applies to all subdirectories. If, for example “www.mycompany.com/users/*” is specified, the user is permitted access to any folder or file under the “www.mycompany.com/users/” folder.

For more information on using these additional elements, refer to the “Policy URL Object Field Elements” section on page 24.

Step 9 In the **Status** pull-down menu, click on an access action, either **PERMIT** or **DENY**.

Step 10 Click **Add**.

Policy URL Object Field Elements

When creating an HTTP/HTTPS policy, the administrator must enter a valid host URL in the **URL** field. In addition, the administrator may enter port, path and wildcard elements to this field. The following chart provides an overview of standard **URL** field elements:

Element	Usage
Host	Can be a hostname that should be resolved or an IP address. Host information has to be present.
Port	If port is not mentioned, then all ports for that host are matched. Specify a specific port or port range using digits [0-9], and/or wildcard elements. Zero “0” must not be used as the first digit in this field. The least possible number matching the wildcard expression should fall within the range of valid port numbers i.e. [1-65535].

Element	Usage
Path	This is the file path of the URL along with the query string. A URL Path is made of parts delimited by the file path separator '/'. Each part may contain wildcard characters. The scope of the wildcard characters is limited only to the specific part contained between file path separators.
Usernames	**%USERNAME%** is a variable that matches the username appearing in a URL requested by a user with a valid session. Especially useful if the policy is a group or a global policy.
Wildcard Characters	The following wildcard characters are used to match one or more characters within a port or path specification. ***** – Matches one or more characters in that position **^** – Matches exactly one character in the position. **[!<character set>]** – Matches any character in that position not listed in character set. E.g. [!acd], [!8a0] **[<range>]** – Matches any character falling within the specified ASCII range. Can be an alphanumeric character. E.g.) [a-d], [3-5], [H-X]

Note Entries in the **URL** field can not contain ("http://", "https://") elements. Entries can also not contain fragment delimiters such as "#".

Using Offloaded Applications

An offloaded application has its own portal page on the SSL-VPN appliance. The portal can be accessed directly by entering the URL in a Web browser. You can also create an External Website Bookmark on the SSL-VPN Virtual Office portal that takes you to the offloaded application portal. To use an offloaded application, perform the following steps:

Step 1 For direct access, point your Web browser to the URL of the offloaded application portal.

Step 2 For access via an External Website Bookmark, log into the SonicWALL Virtual Office and then click on the bookmark.

A new window is launched in your default browser that connects to the offloaded application portal specified in the bookmark.

Step 3 On the portal page, enter your login credentials to access the application if authentication is required.

Using HTTP and HTTPS Bookmarks

HTTP or HTTPS bookmarks are accessed directly from the Virtual Office. To use HTTP(S) bookmarks, perform the following steps:

Step 1 Log into the SonicWALL Virtual Office.

Step 2 Click on the **Web (HTTP)** or **Secure Web (HTTPS)** bookmark.

A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.

Note Microsoft OWA Premium and Lotus Domino Web Access are supported in SSL VPN 4.0. For information about non HTTP(s) bookmarks, refer to the *SonicWALL SSL VPN 4.0 Administrator’s Guide*.

Glossary

GAL: Global Address List maintained by MS Exchange server.

HTTP(S) Reverse Proxy: A reverse proxy that intercepts HTTP(S) requests and responses.

Reverse Proxy: A reverse proxy is a proxy server that is deployed between a remote user outside an intranet and a target Web server within the intranet. The reverse proxy intercepts and forwards packets that originate from outside the intranet.

Web beacon: A Web beacon is an often-transparent graphic image that is used to monitor the behavior of the user visiting the Web site or sending the email. It is used to send back information such as the IP address of the client, the browser type and any cookies that may have been set before.

Solution Document Version History

Version Number	Date	Notes
7	11/1/2010	Changed title and reorganized to include application offloading content (SW).
6	8/19/2009	Added forms-based authentication instructions (PL, SK).
5	2/11/2009	Updated for 3.5 release (PL, SK).
4	4/29/2008	Updated for 3.0 release (PL).
3	2/20/2008	Updated with OWA basic/premium login (PL, SK).
2	11/06/2007	Updated for 2.5, added Policy URL Field section (PL, SK).
1	10/11/2006	This document was created.

P/N 232-001684-00 Rev B