Technical Brief

ActiveSync Configuration for WatchGuard® SSL 100

October 2009

Introduction

With ActiveSync, users get push functionality to keep email, calendar, tasks, and contacts up to date on a mobile device.

It is possible to securely run ActiveSync over SSL through the WatchGuard® SSL 100 appliance without having to install or start the Access Client on the mobile devices. To sync a mobile client it is necessary that an ActiveSync client is installed.

How Exchange ActiveSync Works

Exchange ActiveSync (EAS) is an HTTP/HTTPS-based communication between the client and the server. The client uses a virtual directory "/Microsoft-Server-ActiveSync" on the IIS server to access EAS.

There are no files in this directory; any request is handled by MASSYNC.DLL. MASSYNC needs access to the user's mailbox. MASSYNC uses only Outlook Web Access, not MAPI, CDO, or any other hidden connection.

Define a New Device Type for ActiveSync

The ActiveSync client on a mobile device does not support authentication through the HTML form. Therefore, the SSL 100 needs to be able to identify them as devices that only support Basic Authentication. That can be achieved by defining a new device type:

1. Select **Manage System** in the main menu and click **Device Definition** in the left-hand menu.
2. Click the **Add Device Definition** link.

3. Enter a display name.
4. In the definition text field add: uri = *Microsoft-Server-ActiveSync*
5. Click **Save**.
6. Select **Resource Access** in the main menu and click the **Global Resource Settings** link.
7. Click on the **Client Access** tab and then click on the **Add Device Setting** link.
8. Select the device you created for **ActiveSync** and check both **The device cannot authenticate using HTML or WML forms** and **The device does not support cookies**.
9. Click **Add**, then click **Save**.

Add an Additional Listener

Mobile devices based on Windows Mobile do not accept wildcard SSL certificates. Therefore, it is recommended you deploy a name-specific SSL certificate on the SSL 100. (Example: owa.company.com) However, in order to fully support DNS-based link translation (for standard web applications), the SSL 100 should have a wildcard certificate installed (*.company.com). The recommended configuration is to use a wildcard certificate on the SSL 100 main listener and create an additional listener with a name-specific certificate.

In the current release (3.0) it only possible to add an additional listener port to an external IP address; it is not possible to add a second IP address to the interface. You need to adjust your firewall policy so that the external IP will be translated from external port 443 to the internal port on the SSL 100.

Add an additional Listener on SSL 100:

1. Select **Manage System** in the main menu and click **Device Settings** in the left-hand menu.
2. Click the **Add Additional Listener** link.
3. Select a port, e.g. 444
4. Select the certificate you want to use for ActiveSync devices.
5. Click the **Add** link.
6. Click **Save**.

Upload a Name-specific SSL Server Certificate

1. Select **Manage System** in the main menu and click **Certificate** in the left-hand menu.
2. If the server certificate is provided by an external Certificate Authority, any Intermediate CA certificate must be uploaded to so that the SSL 100 can provide a trusted certification path to the connecting clients. To upload an intermediate CA certificate:
   a. Click **Add Certificate Authority**.
   b. Enter display name and click **Browse** to upload the certificate file.
   c. Check **No certificate revocation should be performed**.
   d. Click **Finish Wizard**.
3. To upload a new server certificate, click **Add Server Certificate**.
4. Enter display name and click **Browse** to upload the certificate file.

5. Click **Browse** to upload the private key file and enter the private key password if the key is encrypted.
6. Check the checkboxes for corresponding intermediate CA certificates, if any.

Define a new DNS name and map it to the additional Listener on the SSL 100

1. Register a new, fully qualified host name (this DNS name MUST be the same as the DNS name used in the name-specific SSL certificate) and map it to the additional listener.
2. Make sure that the external DNS server can resolve the DNS name.
3. Select **Resource Access** in the main menu and click **Global Resource Settings**.
4. Click **DNS Name Pool** tab and click on the **Add DNS** name for Access Point.
5. If not already configured, enter the main DNS name used to access to Application Portal on the SSL 100. This is NOT the DNS name for the ActiveSync Client.
6. Click **Add**.
7. Click **Add DNS** name to pool.
8. Enter the DNS name you want to use for the ActiveSync clients. This is the DNS Name you defined in step 1.
9. Click **Add** and then click **Save**.

Activate a Basic Authentication Method

The ActiveSync client is only capable of doing basic authentication with a static username and password. Any authentication methods can be used that is based on username and password, including WatchGuard SSL Password, Active Directory, LDAP and RADIUS-based authentication services. To get the best user experience we recommend using an authentication service that is connected to Active Directory, so that Single Sign-On can be used.

This document describes a configuration where the WatchGuard SSL Password authentication mechanism is used to enforce authentication for the ActiveSync users. To enable Single Sign-On, the WatchGuard SSL Password must be configured to integrate with Active Directory as the external directory service.

Create a new Single Sign-On Domain

1. Select **Resource Access** in the main menu and click **SSO Domains** in the left-hand menu.
2. Click on the **Add SSO Domain** link.
3. Enter a display name and click **Next**.
4. Click **Add Domain Attribute** to add the following domain attributes:

Attribute Name	Attribute Restriction	Reference by	Value
User Name			
Password			
Domain	Locked	Static	<your domain>

5. Enter a display name and click **Next**.

6. Protect the SSO Domain with **Any Authentication** and click **Next**.
7. Click on **Finish Wizard**.

Edit WatchGuard SSL Password Authentication Method

1. Select **Manage System** in the main menu and click **Authentication Methods** in the left-hand menu.
2. Click on the **WatchGuard SSL Password** link.
3. Select the **Extended Property** tab and click on the **Add Extended Property** link.
4. Add the **Save credentials for SSO domain** extended property from the list.
5. Enter your SSO domain´s display name in the **Value** field then click **Add**.
6. Click **Save**.

Make sure that all ActiveSync users have the WatchGuard SSL Password method enabled, and that Use password from External Directory is enabled.

Add the Outlook Web Access Resource

If Outlook Web Access (OWA) is already a published resource, the web resource can be used for ActiveSync clients as well. To enable on an existing OWA resource it is sufficient to configure a new resource path to the existing web resource host, skip to Configure the ActiveSync Resource Path. If no OWA resource has been previously configured, the OWA resource path must first be configured before the ActiveSync Resource Path can be enabled.

Configure the OWA Web Resource

1. Select the **Resource Access** in the main menu and select for OWA resource.
2. Click on the **Add Web Resource link**.
3. Enter a display name, the IP address or hostname to the resource and HTTPS port 443. No HTTP port is required.
4. Click **Enable Single Sign-On**, specify **Text-based Single Sign-On** and select your SSO domain from the list.
5. Disable **Make resource available in Application Portal**.
6. Click **Next**.
7. Remove **Any Authentication** from Selected Access Rules.
8. Click **Next** and **Finish Wizard.**

Configure the ActiveSync Resource Path

1. Select the **Resource Access** in the main menu and select for OWA resource.
2. Click on the **Add Resource Path** link.
3. Enter Path *Microsoft-Server-ActiveSync*
4. Disable **Use Parent Authentication**.

5. Disable **Make resource available in Application Portal.**
6. Click on the **Add Access Rule** link, select **Authentication Method**, then click **Next**.
7. Add WatchGuard SSL Password then click **Next** until you can click **Finish Wizard**.

8. Again, select the OWA resource and click **Edit Resource Host**.
9. Click **Enable Single Sign-On**, specify **Text based Single Sign-On** and select your SSO domain from the list.
10. Click on the **Advanced Settings** tab.
11. Set **Link Translation Type** to **Reserved DNS Mapping**.
12. Set **Mapped DNS name for HTTPS** to the DNS name you defined for ActiveSync access.
13. Click **Save.**
14. Click **Publish** to publish the configuration.

Activate Device Lock (optional)

Device Lock is design to address the issue of lost or stolen mobile devices. When an ActiveSync client connects through the SSL 100, a unique device identifier is passed as part of the SSL encrypted data. This ID is automatically associated to the particular user account the first time the user connects. If another user attempts to synchronize with this device, the connection will be blocked. Furthermore, if a device with cached user credentials gets lost or stolen, this device can easily be disabled for the particular user account, effectively preventing the device from getting any further access.

To enable Device Lock, do the following:

1. Select **Manage System** in the main menu and click **Authentication Methods** in the left-hand menu.
2. Click on the **WatchGuard SSL Password** link.
3. Select the **Extended Property** tab and click on the **Add Extended Property** link.
4. Set the **ActiveSync DeviceID Locking** to **True**.
5. Click **Add** and **Save**.

With ActiveSync DeviceID enabled, each user that connects with an ActiveSync client and authenticates with WatchGuard SSL Password will get a new custom user attribute containing the device unique identifier.

Appendix A: Configure the ActiveSync Client on a Apple iPhone

1. Click on the **Settings** Icon.
2. Click on **Mail, Contact, Calendars**.
3. Click on **Add Account…**
4. Select **Microsoft Exchange**.
5. Enter your Account Settings.
6. In the **Server Address** field, enter the DNS name you defined for the SSL 100 ActiveSync listener.
7. Click **Next** to verify the settings.
8. Select info to synchronize.
9. Click **Done**.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD
Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. The WatchGuard SSL 100 delivers secure remote connectivity for anywhere, anytime access. Our newest solution – the WatchGuard XTM 1050 – provides high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66651_112009