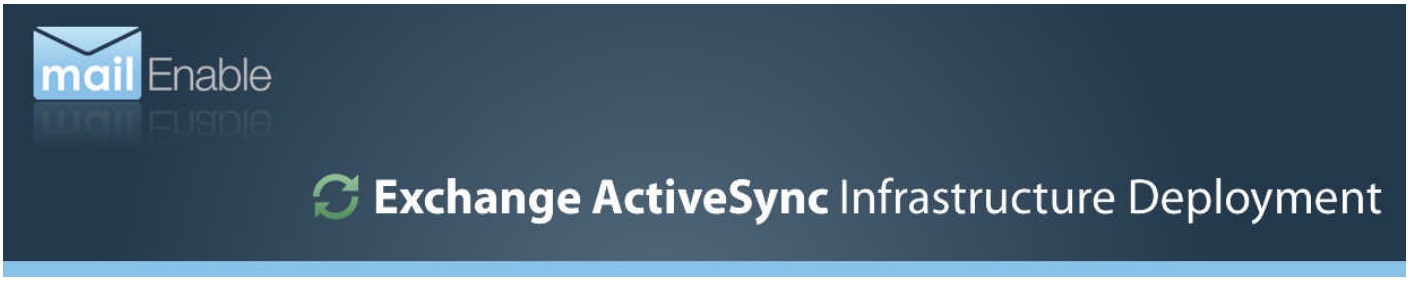


This whitepaper outlines how to configure the operating environment for MailEnable's implementation of Exchange ActiveSync.

Table of Contents

Overview

Exchange ActiveSync (or EAS as it is commonly abbreviated) allows mobile devices to synchronize Appointments, Contacts, Tasks and E-Mail over the Internet. EAS is the premium solution for rich messaging and collaboration on mobile devices.

MailEnable's implementation of the Exchange ActiveSync protocol is implemented through Microsoft IIS and MailEnable's Synchronization/HTTPMail Service. By default, MailEnable provides ActiveSync connectivity on port 8080 and also installs a special Web Site under IIS called "MailEnable Protocols" . The MailEnable Protocols site provides Autodiscovery and ActiveSync through host headers to any IP addresses that are bound to IIS.

MailEnable also provides on online utility that allows you to verify that ActiveSync is correctly configured. Once you have installed MailEnable, you can verify that ActiveSync is working correctly using the testing tool provided at: www.mailenable.com/tools/activesync

Evaluating Exchange ActiveSync for MailEnable

Exchange ActiveSync for MailEnable is installed with Professional, Enterprise and Premium Editions and can be evaluated for a period of 30 days once it is activated. Activation is done by the "ActiveSync Configuration Manager" which can be found under the "Mail Enable" program group.

Before activating the evaluation, you should first ensure that you have the ActiveSync environment configured and that the online test tool indicates that ActiveSync is contactable and functioning.

You should then follow the instructions to configure *Basic ActiveSync Support*. Having done so, you can then commence the evaluation, which will allow you to connect a mobile device to MailEnable via ActiveSync without SSL.

You can then review the extended scenarios with implement SSL, autodiscovery and multi-tenancy according to your requirements.

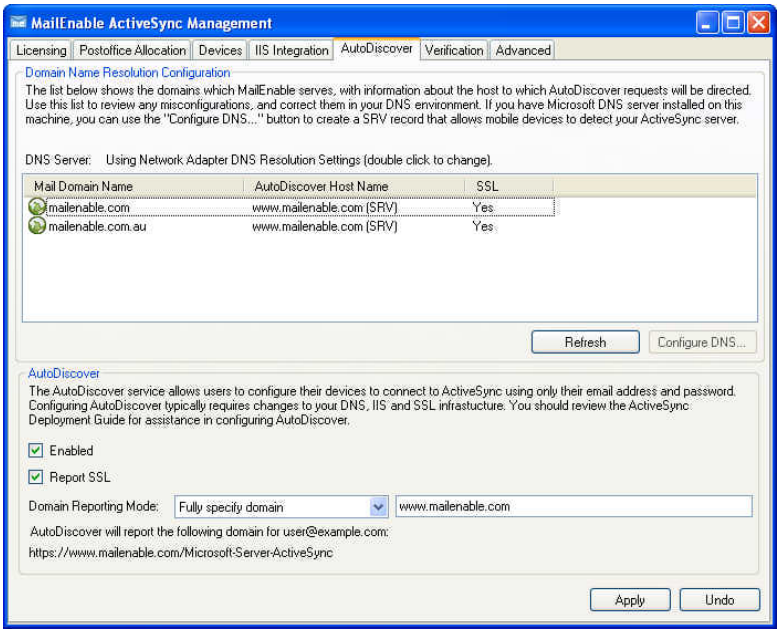
Configuring ActiveSync and AutoDiscovery using the Configuration Manager

The ActiveSync Configuration Manager provides a simple interface for configuring AutoDiscovery and ActiveSync. The utility now diagnoses your system and provides a simple point and click interface for deploying ActiveSync.

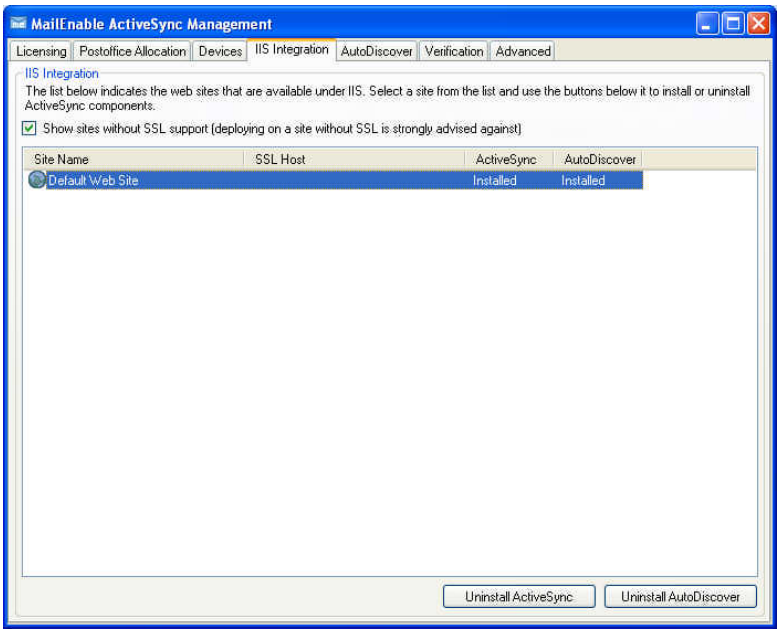
Whilst ActiveSync can be deployed without SSL, most devices are much simpler to configure if you have SSL available. You only need a single SSL certificate configured on your server to deploy ActiveSync.

The steps for configuring ActiveSync and AutoDiscovery using the ActiveSync Configuration Manager follow:

1. Firstly, access the **IIS Integration** tab from within the ActiveSync Configuration Manager and select the site that has the **SSL Host** (certificate) associated with it. You will see that the host name for the certificate will be listed against the site. Click the button to **Install ActiveSync** and **Install AutoDiscovery** for this IIS Site.



2. Next select the **AutoDiscovery** tab and select the mail domain for which you wish to provide ActiveSync Services. If that site does not report an **AutoDiscover Host Name**, then you should click the **Configure DNS …** button to create one. When prompted for the host name, you should enter an **SSL Host** from Step 1.



3. Access the AutoDiscover section under the AutoDiscovery tab, click the **Enabled** and **Report SSL** checkboxes. From the **Domain Reporting Mode** dropdown, select **Fully specify domain** and enter an **SSL Host** name from Step 1.

Notes: *The **Configure DNS…** button will only be available if you have a local Microsoft DNS Server installed, otherwise you will need to create the autodiscovery record SRV manually).*

Manually Configure ActiveSync Support (in 3 Simple Steps)

This section explains how to implement ActiveSync in its most basic form (without requiring SSL, autodiscovery, or multi-tenancy). Please follow these steps to configure basic public ActiveSync Support for your mobile devices.

1. **ActiveSync DNS Host Record** - Firstly, you will need to add a new Host (A Record) to your public DNS. It is recommended that the name be **eas** and it point to public IP address that is bound to IIS (which will most likely be the same address as the **www** host that you use for your web site).
2. **IIS Host Binding** - Next you will need to create a host header under the 'MailEnable Protocols' Web Site. This can be done as follows:
   - Open the Internet Information Services (IIS) manager under Start|Control Panel|Administrative Tools
   - Locate the "MailEnable Protocols" Web Site and Edit its bindings adding a host called eas.yourdomainname, binding to all IP addresses for port 80.
3. **Verify Connectivity** - You can verify connectivity using the online test tool at www.mailenable.com/tools/activesync and connecting to your *eas.yourdomain* on port 80 (using the credentials of any mailbox on the server).

Note: The online test tool can be invoked without needing to activate the evaluation. You only need to activate the evaluation when you wish to use EAS with mobile devices to actual e-mail accounts.

Environment and Configuration

MailEnable's ActiveSync can be used without needing to configure autodiscovery and SSL, however a complete ActiveSync implementation requires the configuration of *secure transmission* (SSL) and *autodiscovery*, and you may need to make adjustments to your network to support these.

Ideally, the network environment needs to provide the following:

- ***ActiveSync Port and IP Bindings*** **-** the ability to access the ActiveSync protocol over ports 80 and 443 on a designated IP address
- ***SSL Infrastructure*** - the ability to provide an SSL certificate for a designated host (ideally the domain portion of your e-mail address). Wildcard SSL certificates (eg: *.example.com) provide the most flexibility since they allow you to create new host names that can be secured via SSL. Eg: eas.example.com. Whilst they are desirable, you can configure ActiveSync with a single host certificate.
- ***Autodiscovery Service*** - the configuration of a host site (and associated DNS and SSL infrastructure) that allows devices to resolve e-mail addresses to user accounts on a host computer.

This whitepaper outlines implementation scenarios and explains their associated network configurations.

Implementation Example

This section provides an example implementation for configuring ActiveSync and Autodiscovery (in this case for the fictitious domain example.com).

Assuming the domain name example.com, the following SSL infrastructure would provide Autodiscovery and ActiveSync support over SSL. We will assume that an SSL certificate exists for www.example.com in which case we will need to configure:

1. **Autodiscover Host Record:** Create a DNS HOST (A record) under example.com and point it to an IP address assigned to your MailEnable Server (this is for the Autodiscovery Host). The host name used should be serviceable via SSL.

   The Autodiscover host will set up as one of the following:
   - defined as a host under the *MailEnable Protocols* Web site under IIS,
   - created as a virtual application under an existing web site,
   - resolved to an IP address that is serviced by the *MailEnable Synchronization Service*.

2. **ActiveSync Host Record:** Create a DNS A record for eas.example.com and point it to an IP address assigned to your MailEnable Server (this is for the Exchange ActiveSync Host). As with the autodiscovery host, you will need to configure this under IIS or the *MailEnable Synchronization Service*.

3. **Autodiscover SRV DNS Record:** Create the _autodiscover SRV record for the domain example.com. It should point to a host that responds provides Autodiscovery Service (in this case autodiscover.example.com which could be configured under IIS or provided by the MailEnable Synchronization Service)

4. **Test the Configuration:** Finally, you can verify that the ActiveSync and Autodiscover Services are responding to requests and are contactable over the internet.

   The following wizards can be used to check that ActiveSync and Autodiscovery are working correctly:

Test Type	URL
ActiveSync	http://www.mailenable.com/Tools/ActiveSync
Autodiscover	http://www.testexchangeconnectivity.com
General Tests	http://www.testexchangeconnectivity.com

   You should verify that both services are working for both secure (SSL) and insecure requests. If you have problems accessing the services, the wizard should explain any problems and direct you to review the configuration of IIS or the Synchronization Service.

Multiple Domain/Multi-Tenancy Implementations

MailEnable is typically installed to service as a Multi-Tenant/Multiple Domain messaging solution. In these environments, it is necessary to provide ActiveSync and Autodiscovery for all the domains that MailEnable services.

This section describes how you can implement ActiveSync and Autodiscovery for the email domains serviced by MailEnable.

The simplest multi-domain configuration involves configuring a single ActiveSync SSL host. This can be done as follows:

1. **Autodiscover Host:** Firstly, you will need to configure an Autodiscovery host so that each of your domains/sites can easily be configured to locate your ActiveSync host (which you will set up later). You should configure Austodisovery for a host name that you are able to provide SSL support for. For example, if you only have a single host SSL certificate for www.example.com then you will need to configure Austodisovery for that host (which in this case will be serviced by IIS by adding an autodiscover virtual directory/application to the IIS Site). Importantly, even though you are intending to service multiple postoffices/domains, they can all share the same autodiscovery host. Details for implementing Autodiscover are provided later in the document.

2. **ActiveSync Host:** Next you will need to configure a host for ActiveSync. Again you need to do this for a DNS hostname that is able to provide SSL. As with Autodiscover Host, if you have only an SSL certificate for a single host, you need to configure the autodiscovery service for that host. If you only have an SSL host certificate and IIS is already using it, then you will need to adopt the IIS integration option and create the Microsoft-Server-ActiveSync virtual application as described later in this document (since IIS will already be servicing the SSL host www.example.com on port 443). As with the autodiscovery host, you only need to configure a single activesync host that can be used by all your domains/postoffices.

3. **Verify ActiveSync Connectivity:** Next you should test that you are able to connect to your ActiveSync host via SSL. This can be verified using the test utility at http://www.mailenable.com/Tools/ActiveSync.

4. **Configure AutoDiscovery Service**: You will need to use the "ActiveSync Configuration Manager" under the MailEnable program group to conifigure the AutoDiscovery response. In this case you should configure the service to respond with the host name you configured in the previous step.

5. **Configure AutoDiscovery for Tenants/Domans**: Finally, you will need to create the autodiscovery DNS SRV records for each e-mail domain you are servicing. This will allow clients to determine which auto discovery host to use (in this case www.example.com), which will then direct them to use the correct/shared ActiveSync host. Instructions for doing this using Microsoft DNS are outlined under the Autodiscovery Section of this document.

The balance of the document elaborates on the underlying constructs associated with the implementation.

Additional Information

ActiveSync Port and IP Bindings

ActiveSync requires that the server listens and responds to client requests on Port 80 (and ideally 443 for SSL). Because Microsoft's IIS typically binds to port 80 of the server, the server must be configured to either:

- allow ActiveSync requests to be either handled by IIS under the Microsoft-Server-Activesync Virtual Directory/Application,
- be bound to an isolated IP address using the Synchronization Service or
- Proxied /translated to an internal address/port via an edge router or network appliance.

These approaches/options are outlined as follows:

IIS Integration

IIS can be configured to service ActiveSync and Autodiscovery requests either via the pre-installed *MailEnable Protocols* web site or by enabling existing sites by creating Virtual Directories. Your IIS SSL configuration determines whether you should configure virtual directories for existing SSL sites, or simply add a new host name to the MailEnable Protocols web site.

Specifically, if you are only able to configure SSL for a single IIS site/host (and do not have a wildcard certificate), then you will need to create autodiscover and Microsoft-Server-Activesync under your existing site.

Using the MailEnable Protocols Web Site

This option is best if you have a wildcard certificate or are able to allocate an additional IPAddress and SSL certificate to IIS for ActiveSync and Autodiscovery. You can register the host with IIS by defining host headers

under the MailEnable Protocols Web Site via the Internet Service Manager. This will allow IIS to handle any requests for these hosts and pass them through to MailEnable's ActiveSync Module for processing.

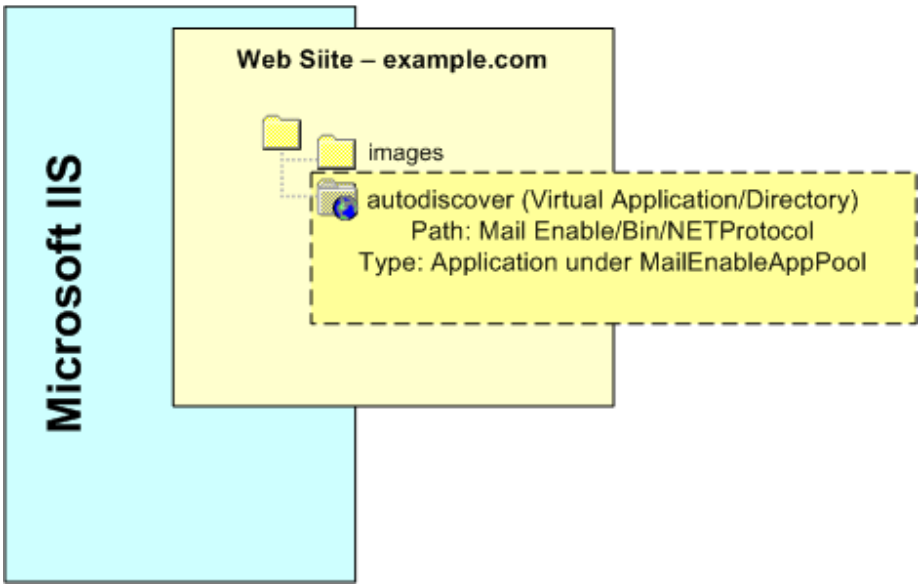
Enabling existing SSL IIS Web Sites to service ActiveSync and Autodiscovery

To enable an existing web site for Autodiscovery and Activesync, you can also create virtual applications for **autodiscover** and **Microsoft-Server-ActiveSync** and map these to the NETProtocol directory.

Example details for the virtual directory follow:

Setting	Value
Name:	autodiscover
Path:	[Program Files]/Mail Enable/BIN/NETProtocol
Execute Permissions:	Scripts only
Application Pool:	MailEnableApp Pool
Authentication Pool:	Only enable anonymous authentication (No Windows or Forms Authentication)
Directory Security:	Enable Anonymous Authentication (All other authentication modes are turned off, eg: Integrated Windows Authentication, Digest, Basic, Forms, Passport)

Note: The Microsoft-Server-ActiveSync virtual directory has the same details, only with a different virtual directory name. (See Note for IIS 6 considerations).



Note: The same virtual directory mapping can be configured for the Microsoft-Server-ActiveSync URL to enable an IIS site to service ActiveSync requests.

Important (IIS 6 Configuration): IIS6 is not able to override the OPTIONS verb without the use of a wildcard script handler. If you are using IIS6, then you will need to configure a wildcard script map that points to the asp.net script processor ([WinDir] \Microsoft.NET\Framework[64]\[Version]\ aspnet_isapi.dll).

Example: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ aspnet_isapi.dll
The version and location of aspnet_isapi.dll should be copied from other script maps defined for the site.

It is only necessary to configure the wildcard script mapping for the Microsoft-Server-ActiveSync virtual directory, since autodiscover Virtual Directory does not use the OPTIONS verb.

Dedicated IP Address for ActiveSync/Autodiscovery

There is no additional setup required to configure the Synchronization service, except that you need to ensure that it is bound to ports 80 and 443. To do this may require that you reserve an IP address that IIS is not already bound to (since it is bound to those ports by default). The MailEnable Synchronization Service will respond to autodiscovery or ActiveSync requests. You can then have the service handle Autodiscovery and ActiveSync requests for any hosts you have defined (but you will need to ensure that you have a wildcard certificate for the domain or have the service respond to SSL requests for both the Autodiscovery and ActiveSync hosts). See "SSL Infrastructure"

Front End Firewall/Proxy Translation

If you have a routing proxy/firewall between mobile devices and the MailEnable server, you can map requests for a given host to a designated backend host and port. For more information on terminating SSL and re-mapping http requests you should contact the vendor of the appliance. The proxy should be configured to direct the request to the internal port used by MailEnable (which is typically port 8080).

SSL Infrastructure

It is preferable to run ActiveSync over SSL. Not only does this provide the most secure option, but it also allows you to configure autodiscovery (which requires SSL). Most devices will default to using a secure channel (443), and usually have an option to disable it.

If you deploy ActiveSync without SSL, you will need to provide your users with a guide as to how to manually configure the details for accessing the service.

ActiveSync SSL support operates on port 443, and this means that a separate IP address needs to be used for each certificate/activesync host. This means that you have two options:

1. **Single ActiveSync SSL Host:** You have all your MailEnable postoffices/users be serviced by the same activesync host and ensure that you have a valid certificate for that host. To do this would involve configuring DNS SRV records the host that is running ActiveSync and Autodiscovery.

2. **Per Domain ActiveSync SSL Hosts:** You need a separate IP address for each domain that is running activesync and you need to configure a separate activesync host for each domain.

The simplest implementation is to use the first option. This involves either using an existing hostname that is capable of SSL or creating a new SSL host for providing ActiveSync connectivity (eg: eas.domainname). You will also need to configure SSL for an autodiscovery host, and ideally need a certificate for your autodiscover.domainname (or preferably a wildcard certificate for *.domain.com).

AutoDiscovery

ActiveSync clients will use the Microsoft AutoDiscover mechanism to validate details. This allows users to simply enter their e-mail address and password, and the AutoDiscover library will resolve the domain portion of the address to establish which server they should use to establish mailbox details.

Step 1: Configure the AutoDiscover DNS Host (A) Record

Firstly, you should configure a DNS A record for autodiscover. *email domainname*, since ActiveSync devices will use the domain portion of your e-mail address to post the data to the autodiscover host for validation. For example, if your e-mail address was user@example.com, you would configure the autodiscover host to be autodiscover.example.com.

The DNS A (Host Record) should be configured to point to the IP address of the server that is running MailEnable ActiveSync.

AutoDiscovery occurs over SSL, and therefore you should have valid SSL certificate for the autodiscover host.

Step 2: Configure a DNS Service (SRV) Record

Many client applications/devices use the domain portion of e-mail addresses to query DNS for SRV records to determine where they should direct the autodiscover request.

To implement this requires creating an SRV record for autodiscover under each domain.

The record above tells clients that any autodiscover requests for the domain example.com should be directed to host.example.com over SSL.

Exact steps for doing this with Microsoft's DNS Server follow:

1. Open the DNS Manager from under Administrative Tools.
2. Locate the domain under the Forward Lookup Zones branch
3. Right click on the domain and select Other New Records
4. Select Service Location (SRV) Record and click the Create Record Button
   Fill in the details for the record as follows:

```
Service: _autodiscover
Protocol: _tcp
Port Number: 443
Host: www.example.com
```

   Note: the host should be configured with the SSL certificate and provide autodiscovery

Step 3: Configure the AutoDiscovery Host to respond to the commands

As mentioned in our example, MailEnable has the capability to respond to AutoDiscovery requests for ActiveSync requests either through IIS or via its Synchronisation Service. There are 3 primary options for configuring access to the AutoDiscovery service.

1. **Dedicated IP Address for ActiveSync:** There is no additional setup required to configure the Synchronization service. The MailEnable Synchronization Service will respond to requests for hosts requests/headers that either start with *autodiscover* or request the /autodiscover directory under a host.
2. **IIS Integration:** to integrate the service with IIS requires the creation of a virtual directory/application under the root of the web site.

3. **Front End Firewall/Proxy Translation:** If you have a routing proxy/firewall between mobile devices and the MailEnable server, you can map requests for a given host to a designated backend host and port. For more information on terminating SSL and re-mapping http requests you should contact the vendor of the appliance.

Step 4: Configure the MailEnable AutoDiscovery settings

The ActiveSync Management application (which is located under the MailEnable Program group) allows you to specify how you would like to answer autodiscovery requests.

Testing

This section outlines how you can undertake some basic tests with the telnet utility to validate your configuration.

Online Testing Utilities

The following wizards can be used to check that ActiveSync and Autodiscovery are working correctly:

Test Type	URL
ActiveSync	http://www.mailenable.com/Tools/ActiveSync
Autodiscover	http://www.testexchangeconnectivity.com
General	http://www.testexchangeconnectivity.com

Testing Connectivity to the ActiveSync Host

You can simply test ActiveSync support as follows.

1. From the windows command prompt, type the following:

```
telnet hostipaddress 80
```

2. Paste the following into the telnet session, replacing the hostname with your activesync host (the hostname you configured for activesync in your public DNS server).

```
OPTIONS /Microsoft-Server-ActiveSync HTTP/1.1
Host: activesync.mailenable.com
```

3. Press enter 1 or 2 times afterwards

The service should respond with some text indicating that the request was serviced by MailEnable. Specifically, the return headers will contain the string: WWW-Authenticate: Basic Realm="MEHTTPMail" or will contain the word ActiveSync in the response.

Microsoft Remote Connectivity Analyzer

Microsoft provides a comprehensive test tool that diagnoses autodiscovery and ActiveSync connectivity. This utility is available here:

http://www.testexchangeconnectivity.com

The utility also provides further insight into how client devices use AutoDiscover and provides a chronology of the steps associated with connecting to an EAS service.

Frequently Asked Questions

Q. Do I need to configure Autodiscovery

A. No, but your clients will need to manually enter the host name and to turn off SSL support when they configure Exchange ActiveSync.

Q. I don't have any SSL certificates, can I still deploy ActiveSync

A. Yes, but it does mean that your clients will need to manually enter the host name and to turn off SSL support when they configure Exchange ActiveSync.

Q. Should I use the IIS Integration Module or should I use the Synchronization Service

A. The IIS Module is simpler to integrate with existing installations because it allows you to utilize any existing SSL, DNS and IP binding infrastructure used by IIS. The Synchronization Service should be used in large installations because it is more scalable and efficient. The Synchronization Service is, however, more difficult to implement because it requires exclusive access to a dedicated IP Address and will require a separate SSL certificate (unless you have a wildcard certificate for the domain).

Q. What happens when the evaluation expires?

A. When the evaluation expires, mobile devices will cease to exchange PIM data with the EAS server. The server will refuse the connection. Assuming you wish to continue using EAS, and you obtain a production license, then those devices configured to use EAS will reconnect and consume licenses as they do so.