Pre-Authentication for ActiveSync

https://campus.barracuda.com/doc/48660703/

Exchange ActiveSync

Exchange ActiveSync (EAS) is a synchronization protocol that enables users to synchronize their mobile phones/devices with their Exchange Mailbox, so they can access email messages, calendar information, contacts, and tasks associated with the Microsoft Exchange server. Users can also manage their deleted items folder, email signature and automatic reply settings. For more information, refer to the Exchange ActiveSync article in the Microsoft documentation.

Pre-Authentication

Pre-Authentication is a mechanism that allows a trusted third party to validate a user's identity before accessing the Exchange Mailbox. The Barracuda Web Application Firewall acts as a trusted third party that performs pre-authentication before processing the request to your Exchange Mailbox. In other words, when a user attempts to access a mail application, the Barracuda Web Application Firewall authenticates the user by validating the user credentials (username and password) with the Active Directory, and then processes the request to the mail application.

The steps below detail how the Barracuda Web Application Firewall can perform pre-authentication for your Exchange Mailbox.

Configuring the Barracuda Web Application Firewall for ActiveSync

Perform the steps below to configure the Barracuda Web Application Firewall for ActiveSync:

Step 1 (a) - Create an HTTPS Service

Create an HTTPS service by following the steps below:

1. Go to the **BASIC > Services** page.
2. In the **Add New Service** section, specify values for the following:
    - **Service Name** – Enter a name for the service.
    - **Type** – Select **HTTPS**.

    - **Version** – Select the Internet Protocol version (IPv4 or IPv6) for the service.
    - **Virtual IP Address** – Enter the virtual IP address that needs to be used for accessing this service.
    - **Port** – Enter the port number on which your web server responds.
    - **Version** – Select the Internet Protocol version (IPv4 or IPv6) for the server that hosts the service.
    - **Real Servers** – Enter the IP address of the server that hosts the service. This is the backend server that is protected by the Barracuda Web Application Firewall. Note: The IP address specified should be of an HTTPS server.
    - **Service Groups** – Select the group under which the service should be added.
    - **Certificate** – Select a certificate from the drop-down list. To upload a certificate, refer to the steps mentioned in the How to Add an SSL Certificate article.
3. Click **Add**.

Step 1 (b) - Associate the OWA (2010 or 2013) Policy with the Service

1. Go to the **BASIC > Services** page.
2. In the **Services** section, click **Edit** next to the service created in Step 1 (a) – Create an HTTPS Service.
3. In the **Service** window:
    1. Scroll down to the **Basic Security** section.
    2. Select *owa2010* or *owa2013* as the **Web Firewall Policy** for the service.
    3. Specify values for other parameters as required and click **Save**.

Step 1 (c) - Create an LDAP Authentication Service

An LDAP server should be configured as the authentication service on the **ACCESS CONTROL > Authentication Services** page, in the **LDAP** tab. The Barracuda Web Application Firewall uses this information to communicate with the LDAP server to authenticate a user. To configure an LDAP server, refer to the steps mentioned under **Configuring LDAP Database Server** in the How to Configure Authentication and Access Control (AAA) article.

Step 1 (d) - Associate the Authentication Service with the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the **Authentication Policies** section, click **Edit Authentication** next to the service created in Step 1 – Create an HTTPS Service. The **Edit Authentication Policies** page appears.
3. In the **Edit Authentication Policy** section:
    1. **Status** – Set to *On*.

    2. **Authentication Service** – Select the LDAP authentication service created in Step 1 (c) – Create an LDAP Authentication Service.
    3. Specify values for other parameters as required and click **Save**.

Step 1 (e) - Add Authorization Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. In the Authentication Policies section, click **Add Authorization** next to the service created in Step 1 – Create an HTTPS Service. The **Add Authorization Policy** page appears.
3. In the **Add Authorization Policy** section, do the following configuration:
    1. **Policy Name** – Enter a name for the policy.
    2. **Status** – Set to *On*.
    3. **URL Match** – Enter the URL that needs to be matched in the request. Any request matching the configured “URL” and “Host” is subjected to LDAP authentication. For example, if the web server URL is https://www.abc.com/sports/Tennis/group1, https://www.abc.com/sports/Football/group1, etc., then the URL Match can be one of the following: "/sports/Tennis/group1” OR “/sports/Tennis/*" OR “/sports/*” OR “/*”.
    4. **Host Match** – Enter the host name to be matched against the host in the request. For example, if the web server URL is "https://www.abc.com", then the **Host Match** should be "www.abc.com".
    5. **Login Method** – Select *HTTP ActiveSync*.
    6. Specify values for other parameters as required and click **Save**.

Step 1 (f) - (Optional) Configure Session Timeout for ActiveSync

You can configure the session timeout for ActiveSync by editing the authentication policy associated with the service. **Session Timeout for ActiveSync** is an advanced feature; therefore, set **Show Advanced Settings** to *Yes* under **Advanced Settings** on the **ADVANCED > System Configuration** page, and perform the following steps:

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
2. Click **Edit Authentication** next to the service created in Step 1 (a) - Create an HTTPS Service. The **Edit Authentication Policies** page appears.
3. In the **Edit Authentication Policy** section:
    1. Click **Show Advanced Settings**.
    2. Scroll down to the **Session Control** subsection.
        - **Session Timeout for ActiveSync** – Set the time (in minutes) that an ActiveSync session can remain valid, after which the Barracuda Web Application Firewall will communicate with the authentication server to validate the credentials again. By default, it is 480 minutes (8 hours).
        - Modify the values of other parameters (if required).

3. Click **Save**.

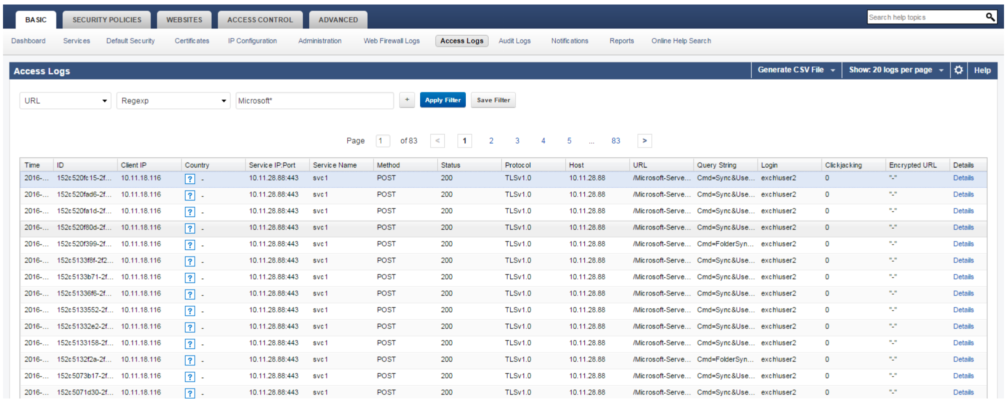
Step 2 - Configure the Mobile Phone for ActiveSync

Perform the following steps on your mobile phone:

1. Locate **Settings > Accounts** in your mobile phone.
2. Select **Add Account > Microsoft Exchange ActiveSync** and configure the following details:
3. Account Details:
   - **Email address**: Enter the email address. **Example**: user2@exch.adfs.com
   - **Domain\user name**: Enter the domain name of your organization followed by user name. Example: exch\user2
   - **Password**: Enter the password. Example: *******
4. Exchange Server Details:
   - **Server**: Enter the Virtual IP (VIP) address of the service configured in Step 1 (a) – Create an HTTPS Service.
   - **Port**: Enter the port number. Example: 443
5. Security Type:
   - SSL/TLS (Accept all certificates)
6. Select **Save**/**Done**.

Logs

All authentication and subsequent requests that pass through the Barracuda Web Application Firewall are logged in the **BASIC > Access Logs** page. The access logs generated for ActiveSync contain the user-id, device-id, device-type, etc.



URL | Regexp | Microsoft*

Time	ID	Client IP	Country	Service IP:Port	Service Name	Method	Status	Protocol	Host	URL	Query String	Login	Clickjacking	Encrypted URL	Details
2016-...	152c520fc15-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c520fad6-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c520fa1d-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c520f80d-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c520f399-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=FolderSyn...	exch\user2	0	"-"	Details
2016-...	152c5133f8f-2f2...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c5133b71-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c51336f6-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c5133552-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c51332e2-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c5133158-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c5132f2a-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=FolderSyn...	exch\user2	0	"-"	Details
2016-...	152c5073b17-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details
2016-...	152c5071d30-2f...	10.11.18.116	? -	10.11.28.88:443	svc1	POST	200	TLSv1.0	10.11.28.88	/Microsoft-Serve...	Cmd=Sync&Use...	exch\user2	0	"-"	Details

Figures