ZENworks Mobile Management 3.1.x

Blocking Mobile Devices from Accessing ActiveSync Servers Directly

Novell

Best practices recommend that you configure ActiveSync so that users who are not enrolled through ZENworks Mobile Management are blocked from accessing the ActiveSync server. This forces all mobile device users to enroll against the ZENworks Mobile Management server, allowing you to manage all devices through ZENworks Mobile Management.

Procedures for implementing best practices are outlined below for Exchange, GroupWise, and FirstClass servers. For those servers not listed below, administrators can create a firewall policy that blocks users from the ActiveSync server. This also blocks users from web access. If you choose not to block access, you should closely monitor the traffic coming through the ActiveSync server.

You should implement this configuration after you have installed the ZENworks Mobile Management system and given users ample time to enroll through the ZENworks Mobile Management server. Users who have not enrolled through ZENworks Mobile Management by the set deadline will be blocked from the ActiveSync server.

1 Exchange ActiveSync Servers

1. Launch the IIS Manager on your Microsoft Exchange Server:
   - **Windows Server 2003 (IIS 6.0):** Click Start and navigate to Settings > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
   - **Windows Server 2008 or 2012 (IIS 7.0/8.0):** Navigate to Administrative Tools and select Internet Information Services (IIS) Manager.
2. Expand your website:
   - **Windows Server 2003 (IIS 6.0):** Click the + symbol next to *Default Website*.
   - **Windows Server 2008 or 2012 (IIS 7.0/8.0):** Click the + symbol next to *Default Website*.
3. Select the IIS Application for Microsoft Exchange ActiveSync:
   - **Windows Server 2003 (IIS 6.0):** While navigating through the Default Website, select *Microsoft-Server-ActiveSync*.
   - **Windows Server 2008 or 2012 (IIS 7.0/8.0):** While navigating through the Default Website, select *Microsoft-Server-ActiveSync*.
4. Open up the *Security Properties* for the IIS Application and navigate to the *IP Address and Domain Restrictions*:
   - **Windows Server 2003 (IIS 6.0):** Right-click the application and select *Properties*. Select the *Directory Security* tab and click the *Edit* button under *IP Address and Domain Restrictions*.
   - **Windows Server 2008 or 2012 (IIS 7.0/8.0):** With the Microsoft-Server-ActiveSync application selected, double-click *IP Address and Domain Restrictions*.

5 Set a default rule to deny all traffic over the ActiveSync Protocol. Then add the exceptions or computers (including all ZENworks Mobile Management servers) that you will allow to communicate with the Microsoft-Server-ActiveSync application.

- **Windows Server 2003 (IIS 6.0):** Select the dot next to *Denied Access* to configure the application so that *By Default, all computers will be denied access. Except the following…*". Then, click the *Add* button and enter the IP address of the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered here.
- **Windows Server 2008 or 2012 (IIS 7.0/8.0):** Click Edit Feature Settings to be prompted to configure the access for unspecified clients. Configure this setting to Deny the traffic and click OK. Click Add Allow Entry. At the prompt, enter the IP address for the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered here.

2 GroupWise Mobility Servers

Systems Using SSL

Create a firewall policy that blocks incoming traffic to your GroupWise Mobility Server over TCP Port 443. Include an exception to allow traffic from the ZENworks Mobile Management Server by entering the IP address of the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered for the exception.

Systems Not Using SSL

Create a firewall policy that blocks incoming traffic to your GroupWise Mobility Server over TCP Port 80. Include an exception to allow traffic from the ZENworks Mobile Management Server by entering the IP address of the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered for the exception.

3 FirstClass Servers

Systems Using SSL

ActiveSync devices communicate with the server using port 443 for HTTPS Web Services. You need to create a firewall policy to block all devices except those enrolled through ZENworks Mobile Management.

However, so that you do not block PC Webmail users, you must first change the number of the TCP port that FirstClass uses for Webmail access over SSL. Assign it a unique, non-standard number so that PC Webmail users are not blocked when you create the firewall policy that blocks port 443.

1 Log into the FirstClass Administration Panel.

2 Double-click the Internet Services icon to enter the Web Services configuration for this server.

3 Double-click the Advanced Web & File icon to modify the port configuration for the FirstClass Web Services.

4 By default, FirstClass uses TCP port 443 for Webmail access over SSL. Change this port to a unique, non-standard number such as 8443.

Now, create a firewall policy that blocks incoming traffic to your FirstClass Server over TCP Port 443. Include an exception to allow traffic from the ZENworks Mobile Management Server by entering the IP address of the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered for the exception.

Systems Not Using SSL

ActiveSync devices communicate with the server using port 80 for HTTP Web Services. By default, FirstClass uses TCP port 8080 for Webmail access over HTTP. Because PC Webmail users use a different port number than devices, creating a firewall policy to block non-ZENworks Mobile Management devices does not affect PC Webmail users.

For systems not using SSL, create a firewall policy that blocks incoming traffic to your FirstClass Server over TCP port 80. Include an exception to allow traffic from the ZENworks Mobile Management Server by entering the IP address of the ZENworks Mobile Management Server. ZENworks Mobile Management users should contact Novell Technical Support for the range of IP addresses that should be entered for the exception.