

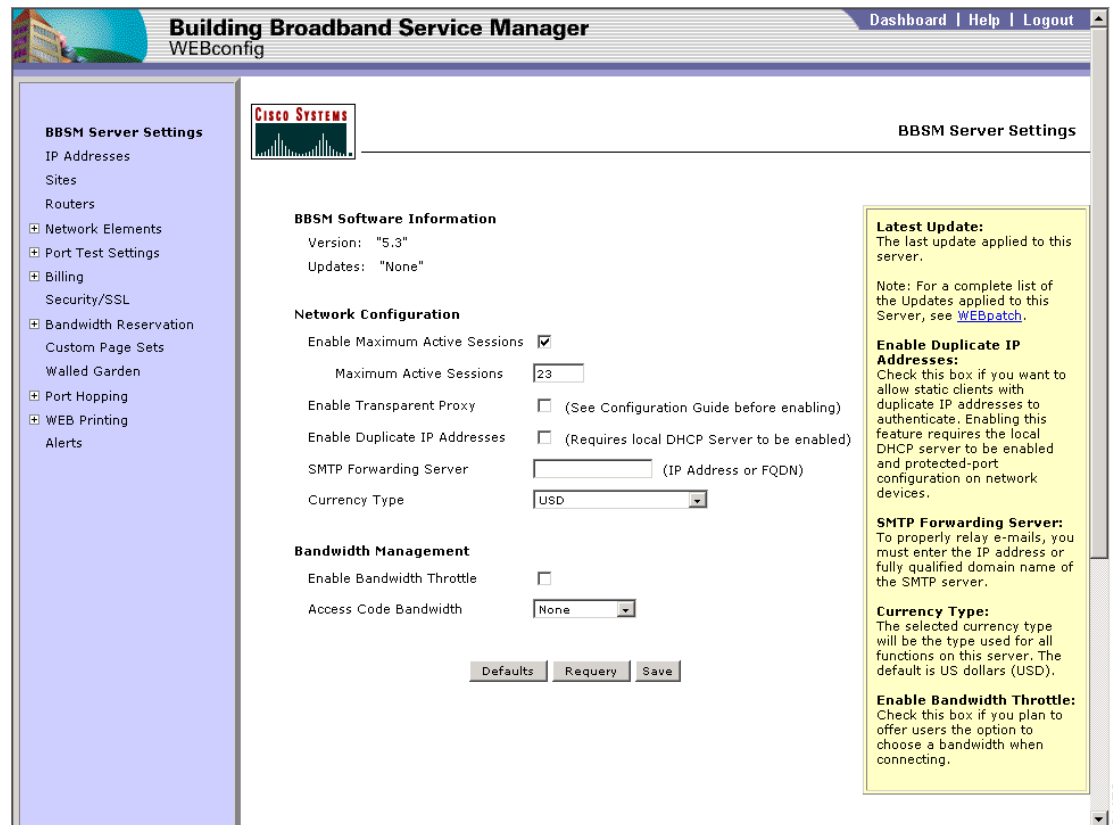


# Configuring the Network and Bandwidth Management Settings

Follow this procedure to configure the basic network and bandwidth management settings. You must complete the procedures in [Chapter 3, “Getting Started”](#) before beginning the initial system configuration.

**Step 1** From the Dashboard, click **WEBconfig**. The BBSM Server Settings web page appears. (See [Figure 8-1](#).)

**Figure 8-1** BBSM Server Settings Web Page



- Step 2** Configure the network configuration and bandwidth management options using the information shown in [Table 8-1](#). and click **Save**.

**Table 8-1 BBSM Server Settings Web Page Options**

Field	Description
<b>BBSM Software Information</b>	
Version Updates	Displays the BBSM version number and any updates since the release.
<b>Network Configuration</b>	
Enable Maximum Active Sessions	Check this check box so the administrator can set the maximum number of active sessions.
Maximum Active Sessions	If the Enable Maximum Active Sessions check box is checked, this option sets the maximum number of allowable active sessions. The default of zero indicates that no maximum exists. This option controls the maximum number of simultaneous users.
Enable Transparent Proxy	<p>Check this check box to allow BBSM to force all clients to use a proxy even if they are not configured to do so. With web proxy enabled globally, you can use Microsoft ISA to monitor the Internet sites that the end users have visited. This information appears in the ISA log files.</p> <p>If your router is configured properly, transparent proxy does not need to be enabled for BBSM to operate correctly. Problems occur when the client is using a private IP address and the router is not configured with a static route to the BBSM internal network. In this case, the router cannot route packets to the client and the client cannot browse the Internet.</p> <p>For additional information on proxies, refer to the <a href="#">“Web Proxies” section on page 2-7</a>.</p> <p>To log the transparent proxy entries, refer to the procedure following this table.</p>
Enable Duplicate IP Address Support	<p>Check this box to allow static clients with duplicate IP addresses to authenticate. This feature allows a client with a duplicate IP address to be redirected to the appropriate Connect page and prompted to authenticate. If the feature is disabled, no client with a duplicate IP address can gain access to the BBSM network. (Before configuring this feature, be sure that no clients are connected to the internal network.)</p> <p><b>Note</b> For the Duplicate IP feature to work, the local DHCP server must be enabled and inter-client communication must be blocked on network devices. Inter-client communication on Cisco switches is blocked by enabling the protected port feature on client ports and enabling Publicly Secure Port Forwarding (PSPF) on Cisco access points. If you are using Cisco Aironet 1100 or 1200 Series access points with configured VLANs, you must use Cisco IOS Release 12.2(13)JA or later.</p> <p><b>Note</b> This feature is not supported with routed, combination bridged and routed, or CMTS networks. This field is disabled if these networks are configured.</p>
SMTP Forwarding Server	<p>Specifies the IP address or fully qualified domain name (FQDN) for SMTP forwarding of all emails. To enable the BBSM server to transmit emails, contact your ISP to register the internal BBSM IP network. Then enter an SMTP server relay IP address or FQDN in this field, which enables BBSM to forward emails to that SMTP server and then to the appropriate mail server.</p> <p>If this field is left blank, the server does not change the SMTP destination for emails being sent.</p>
Currency Type	From the drop-down menu, choose the local currency type for BBSM transactions. (When designated, this currency type is used in all BBSM options and reports.) The default type is <i>USD</i> .

Table 8-1 BBSM Server Settings Web Page Options (continued)

Field	Description
<b>Bandwidth Management</b>	
Enable Bandwidth Throttle	Check this box if you plan to offer end users the option to choose a bandwidth when they connect. Bandwidth throttling enables the administrator to control the maximum bandwidth allocated to end users per IP address. If you are using the AccessCode and MeetingRoom page sets, you can control bandwidth by using the Access Codes Bandwidth option below.
Access Code Bandwidth	From the drop-down menu, choose the desired bandwidth option. The option that you choose determines the bandwidth options that are available on the Access Code Management web page: <ul style="list-style-type: none"> <li>• None (default)—Disables bandwidth management for access codes.</li> <li>• Throttle—Enables bandwidth throttling for access codes.</li> <li>• Reservation—Enables bandwidth reservation for access codes.</li> </ul>
<b>Buttons</b>	
Defaults	Displays the default parameter settings.
Requery	Refreshes the web page (click before saving changes).
Save	Saves the changes made to the web page.

To log the transparent proxy entries, follow this procedure.

- 
- Step 1** Check **Enable Transparent Proxy**.
  - Step 2** Choose **Start > Programs > Microsoft ISA Server > ISA Management**.
  - Step 3** Open the **Servers and Arrays** folder and then open the **Monitoring Configuration** folder.
  - Step 4** Click **Logs**.
  - Step 5** Right-click **ISA Server Web Proxy Service**.
  - Step 6** Choose **Properties** and then the **Log** tab.
  - Step 7** Check **Enable logging for this service** and click **OK**.
-

