How to Secure a Groove Manager Web Site

Like other Web applications, the Groove Manager's administrative IIS Web interface must be secured against unauthorized access and interference. Controlling network access, instituting a reliable authentication system, configuring SSL, and defining administrative roles for the administrative Web pages are important steps you should take toward securing your administrative environment.

The following sections describe the following essential minimal measures for securing your Groove Manager's administrative Web pages:

- Controlling Network Access to the Groove Manager Web Site
- Implementing SSL
- Implementing an Authentication System
- Implementing Role-based Access
- Securing the SQL Server Backend
- Configuring and Securing SMTP for Groove Manager

Controlling Network Access to Groove Manager Web Site

Once you have installed Groove Manager, take an essential step towards securing it by controlling access to the Groove Manager Web site on IIS. The following procedure provides guidelines for configuring network settings.

To configure network settings to help secure a Groove Manager Web site:

1. From the IIS machine, right-click on **My Network Places**, then select **Properties** to open the **Network Connections** window.
2. Right-click on the external connection (network interface card) that you want to edit, then select **Properties**.
3. Remove or disable the **Client for Microsoft Networks** component.
4. Remove or disable the **File and Printer Sharing for Microsoft Networks** component.
5. If the Internet Protocol (TCP/IP) component is not already present and enabled, add and enable it.
6. Select **Properties**/**Advanced**, then the **Options** tab to configure TCP/IP Filtering of Ports to **Permit only** the following:
   - 80 (TCP port for the Groove Manager Web site)
   - 443 (SSL port for GMS and Auto-Configuration directories)
   - 3389 (optional for Remote Desktop administration)
7. Configure UDP Ports to **Permit All**.
8. Configure IP Protocols to **Permit only** the following:
   - 6 (TCP)
   - 17 (UDP)

Now, set up SSL for the administrative site, as described next.

Implementing SSL

Further secure the administrative side of the Groove Manager Web site with the Secure Socket Layer (SSL) encryption protocol, as described here.

To enable SSL for the Administrative Web pages:

1. Select IIS Manager from the Windows Administrative Tools and navigate to the GMS Website.
2. From the Groove Manager root directory in IIS, right-click and select Properties, select the **Directory Security** tab, and setup an SSL (x.509) certificate for the Groove Manager Web site using either the Web Server Certificate Wizard and Microsoft Certificate Services, or an outside certification authority (CA). Refer to Microsoft online IIS documentation for Configuring SSL on Servers.
3. From the Groove Manager root directory in IIS, right-click and select **Properties**, select the Directory Security tab, and setup an SSL (x.509) certificate for the Groove Manager Web site using either the Web Server Certificate Wizard and Microsoft Certificate Services, or an outside certification authority (CA). Refer to Microsoft online IIS documentation for Configuring SSL on Servers.
4. If the new Groove 2007 auto-configuration feature is to be used, from the AutoActivate directory, right-click and select **Properties**, then specify settings to enable SSL and require 28-bit encryption.

If the pre-Groove 2007 auto-activation feature is to be used, leave SSL disabled for the AutoActivate directory.

Now, specify an authentication scheme for Groove Manager administrators, as described next.

Implementing an Authentication System

Windows Internet Information Services (IIS) supports several authentication schemes for securing IIS Web sites via passwords, smart cards, or SecureID tokens. Authentication options include: Integrated Windows Authentication, Basic Authentication, and Digest Authentication. Of these, Integrated Windows is the strongest and recommended authentication system for the Groove Manager administrative (GMS) Web site. If you prefer, you can implement your own custom login authentication mechanism. Designed to be independent of any specific authentication system, the Groove Manager allows you to choose the one that will properly secure your Groove Manager administrative Web pages.

The following is a sample procedure to guide you in setting up Groove Manager authentication:

1. From the IIS machine, select IIS Manager from Windows Administrative Tools and navigate to the GMS Website.
2. Ensure that authentication for the Groove Manager Web site root is set to **Anonymous** access, as follows:
   a. Right-click the Groove Manager Web site root and select **Properties**.
   b. On the **Directory Security** tab, set authentication to **Anonymous** access, and disable all other authentication schemes.
3. Set authentication for the administrative **GMS** directory of the Groove Manager Web site, as follows:
   a. Right-click the **GMS** directory and select Properties.
   b. On the **Directory Security** tab, set authentication to **Integrated Windows** authentication, and disable **Anonymous** access, for strong authentication across your enterprise.

      Note Basic Authentication, which sends unencrypted passwords over the network, and Digest Authentication, which hashed passwords over the network, provide weaker protection than Integrated Windows authentication, which utilizes a challenge/response protocol to authenticate users instead of sending credentials over the network.
4. To support Automatic Account Configuration/Restore, set authentication for the GMS Website **AutoActivate** directory to **Integrated Windows** authentication and disable all authentication schemes, including **Anonymous** access.
5. Configure IIS logon accounts (local or domain logons as needed) for Groove Manager administrators.

Once an administrator logs into the administrative Web interface as required by the chosen authentication system, access within the site can be controlled by defining administrator roles, described next.

Implementing Role-Based Access

To control access to the Groove Manager administrative Web site, you must enable the Roles Based Access Control (RBAC) on the Groove Manager. Enabling RBAC requires that you establish yourself as the Groove Manager server administrator. RBAC lets you specify who can access the Groove Manager administrative interface and which tasks they can perform. Omitting this step leaves the entire Groove Manager administrative interface open for viewing and modification by anyone who learns the login credentials.

To define an initial administrator role and enable role-based access control:

1. Make sure that you set up an authentication system for the Groove Manager directory in IIS. Otherwise, RBAC cannot effectively safeguard the Groove Manager's administrative interface.
2. Start the Groove Manager from Internet Explorer.
3. Select the Groove Manager from the left navigation pane. The Groove Manager page appears.
4. Click the **Roles** tab.
5. From the Groove Manager Roles tab, select **Add Administrator** in the toolbar. The Add Administrator page appears. For reference, this page displays the name that you used to log in to the Groove Manager administrative Web site.
6. In the **Name** field, enter the exact login name (in this initial case, your login name) that the administrator will use to log in to the Groove Manager Web site, as defined by your authentication system.

   Note Make sure that the administrator name that you specify exactly matches the login name used by your Web site authentication scheme, or you will not have any privileges on the Groove Manager after RBAC is enabled.
7. From the **Scope** drop-down menu of the Groove Manager, listing server and domain names defined on this machine, select Groove Server Manager.
8. Click the **Add** button. The selected Groove Server Manager name appears in the **Assigned Scopes** scrolling list, and the role of Server Administrator appears under **Assigned Roles Within Select Scope**. Select this role by selecting the check box.

   Later, if you enter a domain as the scope for an administrator name, selecting that domain in the Assigned Scopes displays a list of Assigned Roles options that you can select. Note that at least one administrator must be assigned the Scope of <Groove Server Manager> and the Role of Server Administrator.
9. Click **OK** to accept the server name and Server Administrator role.

   This enters your name as the first administrator in the name list on the front page of the Roles tab and gives you, as Server Administrator, management access to all Groove Manager fields. You cannot remove this role. However, if

you assign another administrator to the Server Administrator role, that administrator can edit your role.

Note You must be logged into the Groove Manager Administrative Web site using the account that you created as Server Administrator before you can select the option to enable role-based access control.

10. From the Groove Manager Roles page, select the option, '**Enable role-based access control**'. This allows only those administrators listed in the Name list to access the Groove Manager.

    Note If you do not turn on **Enable role-based access control**, anyone who accesses the Groove Manager's administrative site will have full access to all administrative fields and pages on the site.

11. Click **OK**.

    Note You can add only one administrator at a time in the Add Administrator dialog box. To add another, select Add Administrator in the toolbar again.

When you have completed the above measures to help secure your Groove administrative Web site, configure and secure SMTP, described next.

Securing the SQL Server Backend

The Groove Manager stores data in a SQL Server database, which is installed on a separate machine from the IIS front end. To maximize security protections, the SQL Server should be isolated behind a port-restricted and IP address-restricted firewall. It should always have the latest Critical Update Package and Security Rollup installed.

Configuring and Securing SMTP for Groove Manager

In order to enable the Groove Manager to support sending account configuration and password reset e-mail to Groove clients, you must configure the IIS Simple Message Transfer Protocol (SMTP) virtual server. While the Groove Manager does not require many special e-mail settings, you still need to configure security settings, as indicated in the procedure below.

To configure the IIS SMTP virtual server to deliver e-mail via your enterprise's SmartHost:

1. Open Internet Information Services on the Groove Manager machine.
2. Right-click on **Default SMTP Virtual Server** and select **Properties**. The Default SMTP Virtual Server Properties page appears.
3. Clickthe **Delivery** tab.
4. Click the **Advanced** button.
5. In the **Host name** field, enter the fully qualified domain name in the form <GrooveManagerhostname>.domain.com.
6. In the **SmartHost** field, enter the name of the SMTP server that will be used for mail routing in the form, <smarthostname>domain.com, then click **OK**.
7. Secure the SMTP environment as follows:
   - Configure the SMTP virtual server not to accept external connections

(allowing only connections from itself, LocalHost).

- Set Access\Relay restrictions on the virtual SMTP server as follows:
  > Set to Only the list below: Granted 127.0.0.1 (localhost).
  > Clear the 'Allow all computers...' check box.
- Set Access\Connection control on the virtual SMTP server as follows:
  > Set to Only the list below: Granted 127.0.0.1 (localhost).
  > Enable logging and define a Logfiles drive.

Upon successful completion of the installation procedures, the Groove Manager should be ready for domain administration, described in the Groove Manager Domain Administration portion of the Help. The Domain Administration portion of the Help provides instructions for defining groups in a management domain, setting domain policies, defining domain relay servers, and adding users and devices to a domain.