

Exchange Configuration

1. Sign-in as administrator.
2. Go to **Users → Roles → Select the Role → General → Overview**.

Mails can be accessed from **Exchange** server using **Outlook 2000, Outlook XP or Outlook 2003**. We can configure **JSAM (Java Secure Application Manager)** or **WSAM (Windows Secure Application Manager)** for **Outlook 2000, Outlook XP**. **Outlook 2003** will only work with **WSAM**.

JSAM Configuration:

3. Scroll down and check **Secure Application Manager** and select **JSAM** and save the changes.
4. Go to **Users → Roles → Select the Role → SAM → Applications**.
5. Click on **New Application**.
6. The **Name** field is arbitrary.
7. Select **Standard Application** and from the list select **Microsoft Outlook/Exchange** and save the changes.
8. Go to **SAM → Options**.
9. Under **Secure Application Manager Options** check the box **Auto-launch Secure Application Manager**. Then further down, under **Java SAM Options** check the box **Automatic host-mapping** and **Save the changes**.
10. Go to **Resource Policies → SAM** and click on **New Policy**.
11. The **Name** field is arbitrary.
12. In **Resources** field enter the resource FQDN or Hostname or IP address or Network Address/Subnet Mask and for port you can enter wild card (*) which means you allow all the ports for the resource(s) or you can just specify the ports as shown in the example beside **Resources** field. Since exchange uses dynamic ports you have to use wild card (*). We suggest creating resource policy with IP address.
13. Under **Roles** select the appropriate option. If you want to apply the policy to all the roles, select **Policy applies to ALL roles** or select appropriate option from other two and select the roles from **Available roles** list.
14. Under Action select Allow socket access.
15. Save Changes.

WSAM Configuration

16. Scroll down and check **Secure Application Manager** and select **WSAM** and save the changes.
17. Go to **SAM → Options**.
18. Under **Secure Application Manager Options** check the box **Auto-launch Secure Application Manager** and **Auto-allow application Servers**. If you want to uninstall WSAM every time user signs-out then check the box **Auto-uninstall Secure Application Manager**.
19. Under **Windows SAM Options** check the box **Auto-upgrade Secure Application Manager**.
20. Go to **SAM → Applications**.

WSAM can be configured in two modes

- a. Application Mode
- b. Host Mode

You can use one or both simultaneously.

Application Mode Configuration

21. Click on **Add Application**.
22. We have defined few **Standard Applications**. If you are configuring any one of them, then select/enable **Standard Applications** and select any application from the list and click on **Save Changes**. In this case select **Microsoft Outlook/Exchange** and Save Changes.
23. Save the changes.
24. Go to **Resource Policies → SAM**.
25. Click on New Policy.
26. The **Name** field is arbitrary.
27. In **Resources** field enter a wild card (*) which means you allow access to all the backend resource(s). If you want to control the access to backend resource(s), then create a resource policy based on FQDN or Hostname or IP address or Network Address/Subnet Mask of the resource(s) and for port you can enter wild card (*) which means you all the ports for the resource(s) or you can just specify the ports as shown in the example beside **Resources** field. Since exchange uses dynamic port use a wild card (*).

28. Under Roles select the appropriate option. If you want to apply policy to all the roles, select **Policy applies to ALL roles** or select the appropriate option from other two and select the roles from **Available roles** list.

29. Under **Action** select **Allow socket access**.

30. Save Changes.

Host Mode Configuration

31. Click on **Add Server**.

32. The **Name** field is arbitrary.

33. In the **Server** field enter the Network Address/Subnet Mask (e.g. 192.168.0.0/255.255.0.0) and in the **Port** field you can put a wild card (*) or enter the ports on which users can connect (e.g. Ports 23; 80; 443 etc) users can connect to the server(s) or machine(s) in the subnet on the defined ports only. If you want to restrict access to particular server or machine, in the **Server** field you can enter the FQDN (Fully Qualified Domain Name) or Hostname or IP address and in **Port** field you can put a wild card (*) or enter the ports on which users can connect (e.g. Ports 23; 80; 443 etc).

34. Click on Save Changes.

35. Go to **Resource Policies** → **SAM**.

36. Click on **New Policy**.

37. The **Name** field is arbitrary.

38. In **Resources** field enter a wild card (*) which means you allow access to all the backend resource(s). If you want to control the access to backend resource(s), then create a resource policy based on FQDN or Hostname or IP address or Network Address/Subnet Mask of the resource(s), and for the port you can enter a wild card (*) which means you allow access to all the ports for the resource(s) or you can specify the ports as shown in the example beside **Resources** field. Since exchange uses dynamic port we have to use a wild card (*). If you have selected the option **Auto-allow application servers** in step 18 then a resource policy is automatically created for the resource(s) defined in step 38.

39. Under Roles select the appropriate option. If you want to apply policy to all the roles, select **Policy applies to ALL roles** or select appropriate option from other two options and select the roles from **Available roles** list.

40. Under Action select **Allow socket access**.

41. Save Changes.