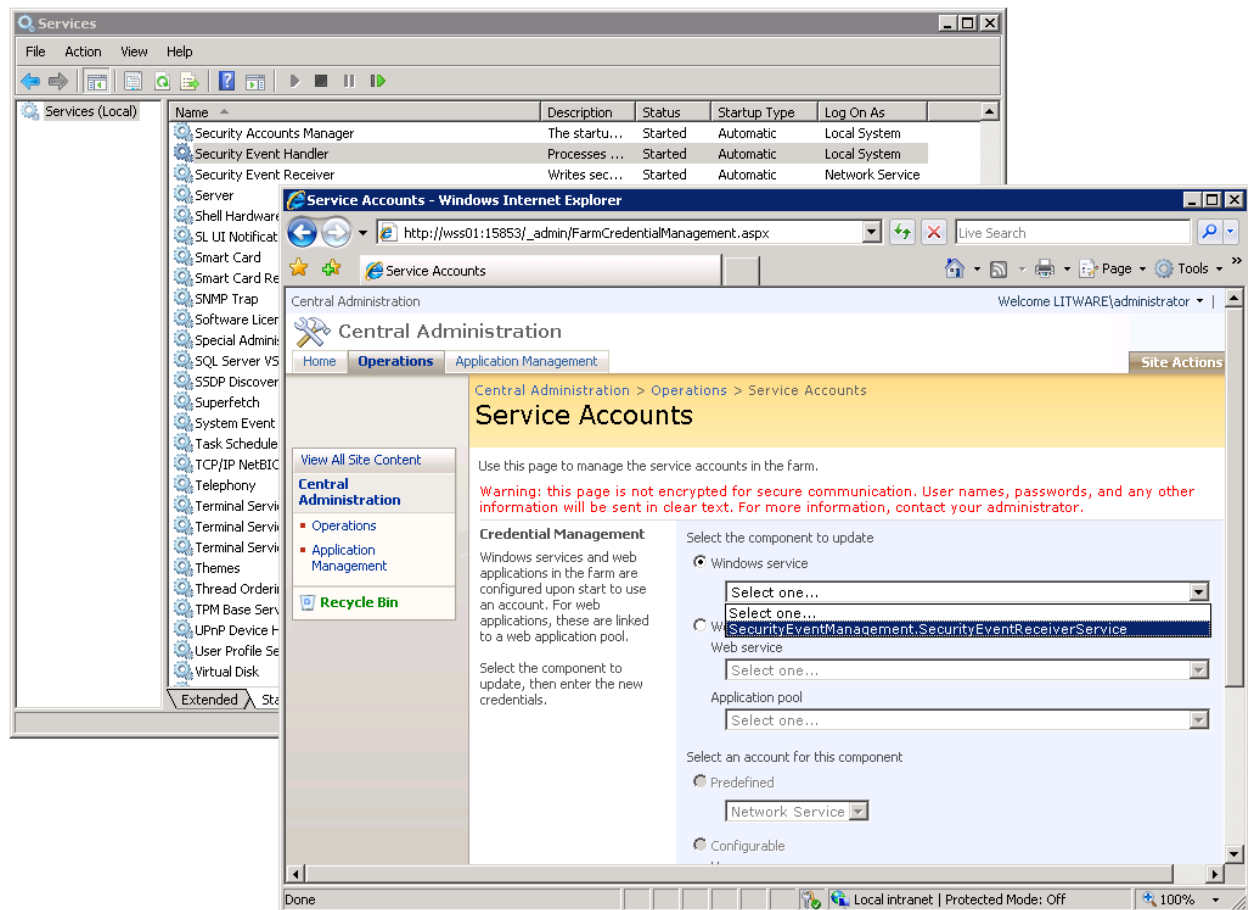


Deploying the Security Audit Solution with Correct Security Accounts

The following procedures describe step by step how to deploy the integrated version of the Security Audit solution with support for security accounts added to the service classes. By default, SharePoint configures services to run in the context of the Local Service account, which doesn't meet the requirements of the Security Audit solution.



Prerequisites:

- You have completed the step-by-step instructions to deploy and test the non-integrated version of the Security Audit, as outlined in the worksheet "02 Deploying the Minimally Integrated Security Audit Solution" that you can find in the companion material.

To delete the SharePoint Solution Package deployed in the Previous Worksheet:

1. Log on to WSS01 as Litware\Administrator, click **Start** and then click **Command Prompt**.
2. Type `cd /D "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Bin"` and press Enter to change into the SharePoint Bin directory.

3. Type **Stsadm.exe -o deactivatefeature -filename SecurityAuditList\feature.xml -url http://wss01** and press Enter to deactivate the custom list feature in the http://wss01 Web application.
4. Type **Stsadm.exe -o retractsolution -name SPSecAudit.wsp -local** and press Enter to retract the custom solution from the SharePoint farm.
5. Type **Stsadm.exe -o deletesolution -name SPSecAudit.wsp -override** and press Enter to delete the custom solution from the SharePoint farm.

To deploy the extended SharePoint solution package:

1. Logged on to WSS01 as Litware\Administrator, copy the **Step3** folder from the companion material to the server's C:\ drive.
2. At the **Command Prompt**, type **Stsadm.exe -o addsolution -filename C:\Step3\SPSecAudit.wsp** and press Enter to add the custom solution to SharePoint.
3. Type **Stsadm.exe -o deploysolution -local -allowgacdeployment -name SPSecAudit.wsp -force** and press Enter to deploy the custom solution in the SharePoint farm.
4. Type **Stsadm.exe -o activatefeature -filename SecurityAuditList\feature.xml -url http://wss01** and press Enter to activate the custom list feature in the http://wss01 Web application.
5. Type **Stsadm.exe -o securityevents -uninstall** and press Enter to provision service and service instance objects for the Windows services in the SharePoint configuration.
6. Type **Stsadm.exe -o securityevents -install -username "NT AUTHORITY\NETWORK SERVICE" -provision** and press Enter to provision service and service instance objects for the Windows services in the SharePoint configuration.
7. Close the **Command Prompt**.

To verify the Configuration of the Windows Services in SharePoint 3.0 Central Administration:

1. Logged on to WSS01 as Litware\Administrator, click **Start**, point to **Administrative Tools**, and then click **SharePoint 3.0 Central Administration**.
2. On the home page, under **Farm Topology**, click on **WSS01**.
3. Verify that the list of services includes references for **SecurityEventManagement.SecurityEventHandlerService** and **SecurityEventManagement.SecurityEventReceiverService** with a **Status** of **Stopped**.
4. Next to the **SecurityEventManagement.SecurityEventReceiverService** click **Start**.
5. Next to the **SecurityEventManagement.SecurityEventHandlerService** click **Start**.
6. Note that both services start successfully.
7. Click on the **Operations** tab, and then under **Security Configuration**, click **Service accounts**.
8. Open the Windows Service listbox and note that you can only change the security account for the **SecurityEventManagement.SecurityEventReceiverService** and that it defaults to the Network Service account as specified in the provisioning command (-username "NT AUTHORITY\NETWORK SERVICE").
9. Close Internet Explorer and log off on WSS01.