Sentinel Action Plugin:

# Start Rogue Admin Workflow

## **Getting Started**

SENTINEL ACTION PLUGIN QUICK START

This Novell Sentinel Action Plugin extends Sentinel to perform additional tasks for rapid remediation of detected issues. Sentinel must be installed and operational before attempting to use this Action Plugin. For further information, refer to the Sentinel product documentation or the full Start Rogue Admin Workflow documentation (see URLs below).

Action Plugins are used by Actions that can be attached to a Correlation Rule or a right-click Menu Tool. When an Action is configured, an instance of the Action Plugin along with associated configuration parameters is created. This pre-defined Action can then be associated so that it can be automatically triggered when a Correlation Rule fires, or triggered when a set of events is selected and a right-click Menu Tool is selected.

| Action Manager:                          |  |  | Add Action:   |
|--|--|--|---|
| Use the Action Manager to                | Action Manager   |  | This button opens the   |
| manage all actions including             | Add Manage Plugins   | Configure Action ×   | Configure Action dialog.  |
| Action Plugins. Access via the           | Send Email   | Action Name  |   |
| Sentinel Control Center, Tools           | S Disable Rogue Admin View/Edit Delete   | Disable Identity   |   |
| Menu > Action Manager.                   |  | Action   | - Select Action Plugins:  |
| inena inenagen /                         | Ready all Refreshed At: 7/28/08 9:25:04 PM   | Manage Views   | This dropdown shows the   |
| Action Plugin Manager: <                 |  | Action Plugin To Execute   | available Action Plugins  |
| Use this tool to import and              |  | Integrator Identity Vault  | as well as other types of   |
| manage Action Plugins that               | Action Plugin Manager x  | Help Add Integrator Add Action Plugin Save                               | Actions   |
| can be instantiated as Actions           |  |  | / lettoris:   |
| can be instantiated as retions.          | 1 😌 🗸 🥺 🔍 🔍  |  | Action Baramotors:  |
| Add Action Blugin:                       | Name   | Deploy Rule ×  | Sot the parameters that   |
| This button triggers the Import          | Disable Identity 6.1r1   | Select engine to deploy Rule to:   | Set the parameters that   |
| Diversion Million inggers the import     | Send Email   | sent1.devlab.net:127.0.0.2   | Division will an arrate   |
| Plugin Wizard. The first part of         | Set LDAP Attribute   | Select Actions to be performed when rules fires:                         | Plugin will operate.  |
| the wizard allows you to select          |  | V Disable Identity   |   |
| a ZIP file or directory that             |  | Send Email   | -Associate a Rule with  |
| contains the source of the               |  |  | an Action:  |
| Plugin to import.                        |  | Add Action   | Set the parameters that   |
|  |  |  | configure how the Action  |
|  | ■ Import Plugin Wizard ×   | Ok Cancel  | Plugin will operate.  |
|  | Plugin Details   |  |   |
|  | plugin.  |  |   |
|  |  | Event Menu Configuration ×   |   |
| Plugin Details:                          | Description Name Disable Identity 6.1r1  | Name: Disable Rogue Administrator  |   |
| Displays details about the               | Type JAVASCRIPT_ACTION   | Description:   |   |
| Plugin you are about to install.         | Author Novell Engineering  | Action: S Disable Identity   |   |
| The <b>Id</b> is a unique identifier for | Version 6.1n<br>Release Date 7/24/08 10:13 PM  | Options  | Associate a Menu Tool   |
| this Plugin: if you attempt to           |  | Use browser:   | with an Action:   |
| re import a plugin with the              | Supported US Platforms   |  |   |
| re-import a bludin with the              | Id 1DB52CEC-597D-1029-8F81-0014223D9DEC  | File type:   | Set the parameters that   |
| same Id it will replace the old          | Id 1DB52CEC-697D-1029-8F81-0014223D9DEC Description This Novell Sentinel Action allows you to: Disable Identity. Sentinel must be installed and operational  | File type:<br>Command / URL:   | Set the parameters that   |
| same Id it will replace the old          | Supported US Flatforms<br>Id 1DE52CEC-697D-1029-6781-0014223D9DEC<br>Description This Nevel Somtnel Action allows you to: Disable<br>Identity, Sentinel must be instatled and operational<br>before attempting to use this Action. For further<br>information, refer to the heplife included in the Action.      | File type:<br>Command / URL:<br>Parameter:                               | Set the parameters that<br>configure how the Action<br>Plugin will operate  |
| same ld it will replace the old version. | Supported US Francins<br>Id 1DE52CEC-697D-1029-8781-0014223D9DEC<br>Description This Nevell Sentimel Action allows you to: Disable<br>Identity, Sentinel must be installed and operational<br>before attempting to use this Action. For further<br>information, refer to the helpfile included in the Action.    | File type: Command / URL: Parameters:                                    | Set the parameters that<br>configure how the Action<br>Plugin will operate. |
| same ld it will replace the old version. | Supported US Flatforms Id 1DE52CEC-697D-1029-6781-0014223D9DEC Description This Novell Sentinel Action allowy you to: Disable Identity Sentinel must be installed and operational before attempting to use this Action. For further information, refer to the helpfile included in the Action.                   | File type:<br>Command / URL:<br>Parameters:<br>Help Add Action Ok Cancel | Set the parameters that<br>configure how the Action<br>Plugin will operate. |
| same ld it will replace the old version. | Supported US Flatforms Id 1DE52CEC-697D-1029-6781-0014223D9DEC Description Identify Sentinel Arction allows you to: Disable Identify Sentinel must be installed and operational before altempting to use this Action. For further information, refer to the helpfile included in the Action.  Back Finish Cancel | File type:<br>Command / URL:<br>Parameters:<br>Help Add Action Ok Cancel | Set the parameters that<br>configure how the Action<br>Plugin will operate. |

Sentinel product documentation:

http://www.novell.com/documentation/sentinel6/index.html

Full Start Rogue Admin Workflow Action Plugin documentation:

http://support.novell.com/products/sentinel/doc/actions/Start-Rogue-Admin-Workflow\_6.1r1.pdf

## **Integration Methods**

This Action Plugin uses functionality provided by the following Integrator Plugin(s):

SOAP

**NOTE:** This Integrator Plugin must be configured as an instance of an Integrator with name Identity Manager SOAP. Typically this is handled by the Solution Pack install process.

### Configuration

The following steps should suffice to configure this Action Plugin for use within the Sentinel environment. Additional configuration may be necessary for production environments or if your enterprise is configured in ways that vary from standard installations of integrated systems.

In general, it is recommended that this type of integration be performed first in a development environment where such restrictions can be relaxed so that basic communication can be established. If necessary, Novell Consulting or our qualified partners can advise you on ways in which the standard Integrator configuration can be customized for your enterprise.

#### Solution Packs and Action Plugins

In many cases, Action Plugins will be delivered as part of pre-defined controls within **Solution Packs**, where they will already be instantiated as Actions, attached to Rules or Menu Tools, and will already be configured to use the appropriate Integrator. In this scenario, the only configuration you will typically need to perform will be to modify the Integrator configuration (if applicable) to point to the correct integration targets. In some scenarios you may need to additionally change some Action parameters that control the Action Plugin.

In other cases, the Action Plugin is delivered as a standalone component that you will configure **manually**. In this case, you must download any applicable Integrator Plugin(s) for this Action Plugin and your version of Sentinel. You should create an instance of an Integrator for these Integrator Plugin(s) according to the configuration instructions included with the Integrator Plugin. Further, you will need to create an Action that uses this Action Plugin, plus configure any applicable parameters to control the Action Plugin operation. Finally, you will need to associate the Action with a Rule or Menu Tool.

This document covers both scenarios for installing this Action Plugin; follow the appropriate set of steps for the delivery method used.

#### Solution Pack Configuration

When Action Plugins are installed as part of a Solution Pack, they are typically associated with the Actions, Integrators, and any other components that they will need to function. Installing the Solution Pack control which uses the Action Plugin will be sufficient to install all necessary components in most cases.

In many circumstances, however, additional configuration may be required for this Action Plugin to function correctly. For example, the Action has a set of parameters that are used by the Action Plugin to control operation (see below), and the associated Integrator (if used) may need to be configured.

#### **Sentinel Execution Permissions**

Action Plugins run in a protected execution environment that is intended to help protect the system from accidental corruption of the data objects used by Sentinel. The Start Rogue Admin Workflow Plugin, however, needs to be able to look up information about the identity that it is planning to start a workflow for. To allow this, we need to modify the permissions for Action execution.

- 1. Log into the Sentinel Server machine as a user with privileges to edit files in the ESEC\_HOME directory.
- 2. Locate ESEC\_HOME/config/execution.properties and open it in a file editor.
- 3. Append the following line to the file:

esecurity.execution.script.context.restricted=false

- 4. Save and close the file.
- 5. Restart Sentinel:
  - 1. Windows: Stop and then Start the Sentinel service in the Services Control Panel applet.
  - 2. Linux: Execute the following commands as root:

/etc/rc.d/sentinel stop

/etc/rc.d/sentinel start

#### Integrator Configuration

**NOTE:** Novell Identity Manager's User Application must be configured with a service user allowed to connect to the SOAP service and start workflows. Configure the Integrator with this user's account information.

- 1. Log in to the Sentinel Control Center (SCC) as a user with rights to manage Integrators (*Permissions > Integrators > Manage Integrators*).
- 2. Select the menu Tools > Integrator Manager.
- 3. Select the Integrator that was installed as part of this control (this is set as a parameter on the Action if you don't know it) from the list at left.
- 4. In the *URL* field, enter the web services URL that you use to get the WSDL from IDM's SOAP provider. This is configured during the User Application install as part of the Tomcat configuration, and can be found in Tomcat's server.xml files. Shown is a commonly-used default.
- 5. Enter the SOAP Service and Port in the *ProvisioningService* and *ProvisioningPort* fields. Shown are the typical defaults.
- 6. Select whether the network port uses SSL or not.
- 7. Check *Use Authentication* and enter the account credentials of an account that can start workflows in Identity Manager's User Application.
- 8. Click Refresh Web Service API to regenerate the WSDL API.
- 9. Select *Test* and ensure that the Integrator test completes correctly.
- 10. Select Save to save your changes.

#### Manual Configuration

Many Action Plugins require certain Integrator Plugins to be installed and configured in order to function (these Integrators are listed above). You can find any appropriate Integrator Plugins for this Action Plugin on our content website at:

#### http://support.novell.com/products/sentinel/index.html

Follow the instructions included with the Integrator Plugin to install the plugin and configure it as an instance of an Integrator. If necessary, refer to the Solution Pack instructions above which may provide more detail about specific types of target systems.

#### Action Configuration

To configure the Action Plugin to run as part of an Action, you need to perform the following steps. Before beginning this process, ensure that you have the Action Plugin downloaded and available on the machine on which you are running SCC.

**NOTE:** No changes should be necessary for this Action Plugin as it is included as part of a Solution Pack control. If, however, you have multiple User Applications, you may need to replicate the Integrator configuration and manually configure additional Actions.

| 8                 | mtegrat                        | or manager  | - 0                           |
|-------------------|--------------------------------|---|-------------------------------|
| Integrators:      | Identity Mar<br>For more in    | nager SOAP is healthy.<br>formation,see details.                                | Update<br>7/30/08 10:29:12 Al |
| Identity Vault    | Basic Informatio               | n SOAP Connection Settings I  | ntegrator Properties          |
| Senunei Maii      | URL:<br>Service Name:<br>Port: | http://130.57.171.11:3991/IDMProv/pr<br>ProvisioningService<br>ProvisioningPort | ovisioning/service?wsdl       |
|                   |                                | Vse Authentication  |                               |
|                   | Password:                      | cn=padmin,dc=admins,dc=system   |                               |
| 😹 🎯 🛛 Manage Plu. |                                | Refre   | esh Web Service API           |
|                   |                                | Help Test   | Save Revert                   |

- 1. Log in to the Sentinel Control Center (SCC) as a user with rights to manage Actions (*Permissions > Actions > Manage Actions*).
- 2. Select the menu *Tools > Action Manager*.
- 3. Select the Integrator that was installed as part of this control (this is set as a parameter on the Action if you don't know it) from the list at left.
- 4. Select the Add 🚽 button to create a new Action.
- 5. Give the Action a name in the entry box at top.
- 6. Select the Add Action Plugin button at the bottom of the dialog.
- Use the popup wizard to browse for and install this Action Plugin. Once complete, the name of the Action Plugin should appear in the drop-down list in the *Configure Action* dialog.
- 8. Select Start-Rogue-Admin-Workflow\_6.1r1 from the drop-down list. The list of configurable parameters for this Plugin should appear.

| N      | Action Manager              |        |       | ×     |
|--------|-----------------------------|--------|-------|-------|
| 🛟 Add  | Manage Plugins              |        |       |       |
| 😼 Send | Email                       |        |       |       |
| ₃ Disa | ale Rogue Admin .           | View/E | dit D | elete |
| Ready  | Refresh Refreshed At: 7/28/ | 08 9:2 | 5:04  | PM    |
|        |                             |        |       |       |

| Configure Action ×                   |                       |      |  |  |
|--------------------------------------|-----------------------|------|--|--|
| Action Name                          |                       |      |  |  |
| Start Rogue Admin Workflow           |                       |      |  |  |
| Action                               |                       |      |  |  |
| 😼 Start Rogue Admin Workflow 6.1r1 💌 |                       |      |  |  |
| Name                                 | Value                 |      |  |  |
| Action Plugin To Execute             |                       |      |  |  |
| Integrator                           | Identity Manager SOAP |      |  |  |
|                                      |                       |      |  |  |
| Help Add Integrator                  | Add Action Plugin     | Save |  |  |

- 9. Set the workflow DN for the Rogue Administration Activity workflow that is included as part of the Identity Manager Resource Kit (see the Resource Kit documentation for details). Browse the eDirectory tree and find the User Application container, then locate the workflow definition under that container.
- 10. Refer to the table below for the parameters that can be configured for this Action Plugin.

| Parameter<br>Name | Default Value  | Description   |
|-------------------|--|---|
| Integrator        | Identity Manager SOAP  | This parameter specifies which Integrator will<br>be used with this Action Plugin. The drop-down<br>list will display all the available, configured<br>Integrators. |
| Workflow<br>DN    | CN=Rogue_Administration_Activity,CN=Re<br>questDefs,CN=AppConfig,CN=UserApplicat<br>ion,CN=driverset1,DC=idm,DC=services,D<br>C=system | The LDAP Distinguished Name of the workflow definition – this will be passed to SOAP.   |

11. Configure the parameters with settings appropriate for your environment.

# **Revision History**

#### Release Notes

#### 6.1r1

• Initial version; connects to User Application and starts the Rogue Administration Activity workflow.

#### Known Issues

- Currently handles only a single User Application.