Action Plugin Version: 6.1r1

Release Date: Aug 2008

Sentinel Action Plugin:

Disable Identity

Getting Started

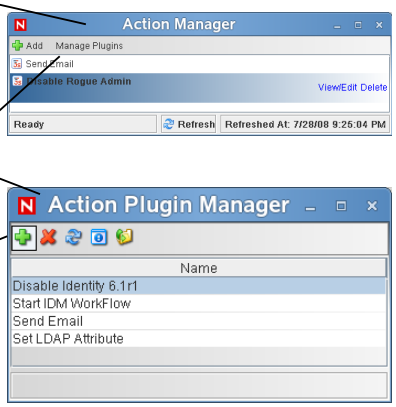
This Novell Sentinel Action Plugin extends Sentinel to perform additional tasks for rapid remediation of detected issues. Sentinel must be installed and operational before attempting to use this Action Plugin. For further information, refer to the Sentinel product documentation or the full Disable Identity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

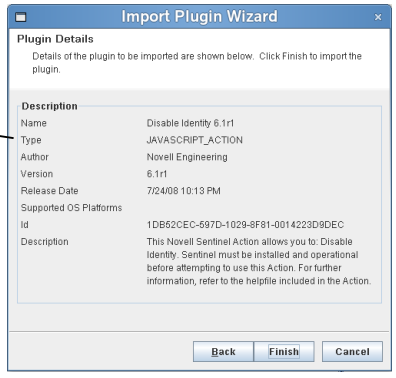
Action Plugins are used by Actions that can be attached to a Correlation Rule or a right-click Menu Tool. When an Action is configured, an instance of the Action Plugin along with associated configuration parameters is created. This pre-defined Action can then be associated so that it can be automatically 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:
Use the Action Manager to manage all actions including Action Plugins. Access via the Sentinel Control Center, Tools Menu > Action Manager.

Action Plugin Manager:
Use this tool to import and manage Action Plugins that can be instantiated as Actions.

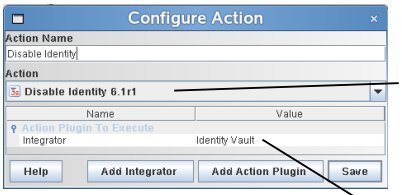
Add Action Plugin:
This button triggers the *Import Plugin Wizard*. The first part of the wizard allows you to select a ZIP file or directory that contains the source of the Plugin to import.





Plugin Details:
Displays details about the Plugin you are about to install. The **Id** is a unique identifier for this Plugin; if you attempt to re-import a plugin with the same Id it will replace the old version.

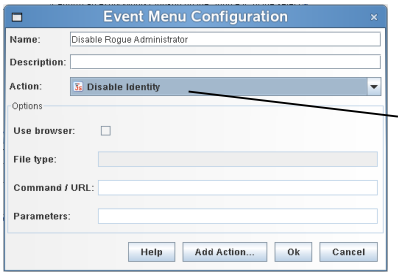
Add Action:
This button opens the *Configure Action* dialog.



Select Action Plugins:
This dropdown shows the available Action Plugins as well as other types of Actions.

Action Parameters:
Set the parameters that configure how the Action Plugin will operate.

Associate a Rule with an Action:
Set the parameters that configure how the Action Plugin will operate.



Associate a Menu Tool with an Action:
Set the parameters that configure how the Action Plugin will operate.

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

Full Disable Identity Action Plugin documentation:
http://support.novell.com/products/sentinel/doc/actions/Disable-Identity_6.1r1.pdf

Integration Methods

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

- **LDAP**

NOTE: This Integrator Plugin must be configured as an instance of an Integrator with name `Identity Vault`. 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 Disable Identity Plugin, however, needs to be able to look up information about the identity that it is planning to disable. 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:

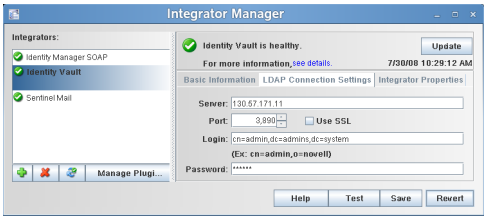
```
/etc/rc.d/sentinel stop
/etc/rc.d/sentinel start
```

Integrator Configuration

NOTE: Novell Identity Manager must be configured with a service user allowed to connect to the Identity Vault and change attributes on identities within the Vault. 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 Server field, specify the IP address of the system which hosts the Identity Vault.



5. If SSL will be used for the connection, check the *SSL* box.
6. Enter the port used for LDAP connections to the Identity Vault. The defaults are 389 for non-SSL and 636 for SSL connections.
7. In the *Login* field, enter the LDAP syntax of the user account with rights to modify Vault identities.
8. Enter the password for that user.
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.

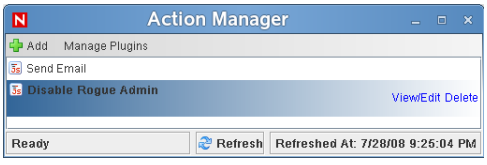
Action Configuration

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.

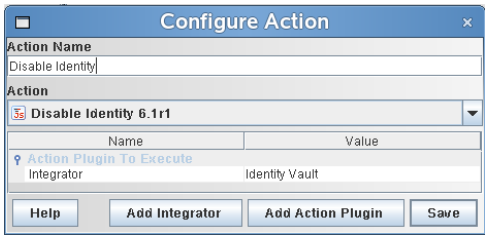
NOTE: No changes should be necessary for this Action Plugin as it is included as part of a Solution Pack control. If, however, you have multiple Identity Vaults, you may need to replicate the Integrator configuration and manually configure additional Actions.

---

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.
7. 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 Disable-Identity_6.1r1 from the drop-down list. The list of configurable parameters for this Plugin should appear.



9. Refer to the table below for the parameters that can be configured for this Action Plugin.

Parameter Name	Default Value	Description
Integrator	`Identity Vault`	This parameter specifies which Integrator will be used with this Action Plugin. The drop-down list will display all the available, configured Integrators.

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

Revision History

Release Notes

6.1r1

- Initial version; connects to Identity Vault and disables identity.

Known Issues

- Currently only handles a single Identity Vault.