UP L03 – Implementing the Zero Day Patch Template

Description

Most corporations today have some form of patch process in place. In this session, you will learn how to meet industry standards when working with currently released workflows within Patch Management Solution and when applying best practices.

At the end of this lab, you should be able to

- Understand the value of automating backend Altiris actions with Workflow
- Create Filters that will be used to create a Target
- Create a predefined Target from a set of Filters
- Create Reports to find GUIDs for the Target & Company Names
- Unpackage a Workflow Project
- Import and Edit an Application Profile into the Process Manager
- Add an Application Profile to a Workflow project
- Set a auto run schedule for a Workflow project
- Run a Workflow project in Debug
- Create a Report in Process Manager

Notes

- A brief presentation will introduce this lab session and discuss key concepts.
- The lab will be directed and provide you with step-by-step walkthroughs of key features.
- Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace.
- Be sure to ask your instructor any questions you may have.
- Thank you for coming to our lab session.

Introduction

The following lab will walk though the steps required to implement the Zero Day Patch Workflow template. The lab is also intended to serve as an example of how you can utilize Workflow to automate backend Altiris processes.

The Zero Day Patch template will run on a schedule to automatically download and stage applicable bulletins based on configurable criteria, create a policy for each bulletin and apply the policy to a pre-defined set of targets. The template also creates an audit trail of all activities and sends a summary email of all policies, bulletins, and targets.

Exercise 1: Meeting the Zero Day Patch Process Prerequisites

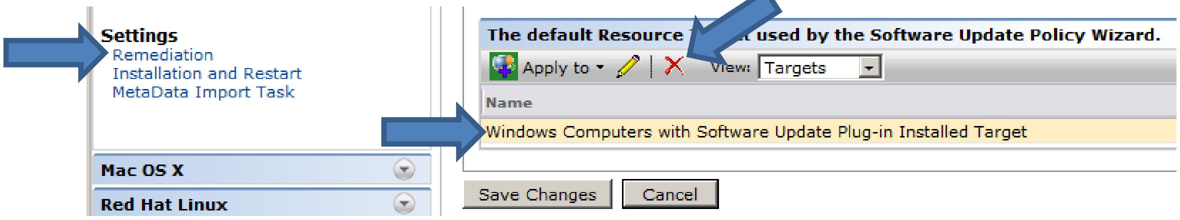
The Zero Day Patch workflow depends on a Target to be defined in its configuration. Administrators routinely utilize filters to group resources for use in management tasks. Filters are easily managed within the console and provide flexible options for defining complex inclusions and exclusions of resources within them.

For these reasons, we will create a Filter to allow the administrator to define and maintain the group of "Zero Day Safe" computers, then apply that filter to a specific Target for use in the configuration with the workflow process. The following are the [prerequisites to ensuring that the Zero Day Patch process operates as designed:

- Patch Management 8.0 and either Workflow 8.0 or ServiceDesk 7.5.
- The Default Software Update Policy Target must be cleared
- A Filter must be created to contain computers that will apply the Zero Day Patch Process
- A Target must be created that contains the created Filter for the Zero Day Patch Process

Clearing the Default Software Update Policy Target

1. Make sure that the **DC, NS75** and **SD7** Virtual Machines are powered on
2. Switch to the **NS75** Virtual Machine
3. Open the Console by clicking on the **Symantec Management Console 7.5** icon on the desktop
4. Navigate to **Home > Patch Management** in the main menu bar
5. On the Left pane, under **Settings**, select the **Remediation** link
6. On the Right Pane, under "**The default Resource Target used by the Software Update Policy Wizard**", Select the "**Windows Computers with Software Update Plug-in Installed Target**", and press the **Red X** in the menu above it. This should delete the Target.


Settings
Remediation
Installation and Restart
MetaData Import Task
Mac OS X
Red Hat Linux
The default Resource used by the Software Update Policy Wizard.
Apply to
View:
Targets
Name
Windows Computers with Software Update Plug-in Installed Target
Save Changes
Cancel

7. Press the **Save Changes** button

Creating the Filters used by the Zero Day Patch Computers

In this example, the administrator is tasked with the creation of a filter that will:

- **Include** specific Computers in the environment (with the Software Update Plug-in Installed)
- **Exclude** a list of Computers they should NEVER be included in a Patch Management Process

1. Switch to the **NS75** Virtual Machine
2. Navigate to **Manage > Filters** in the menu bar
3. In the Left Pane, Right Click on the **Filters** folder and select New Folder
4. Name it **Zero Day Patch Process**
5. Right Click on the **Zero Day Patch Process** folder and select **New > Filter**
6. Change the filter name to **Patch Management Excluded Computers**
7. Expand the **Filter Definition** section by pressing the downward facing arrow at the right. This is where you would define the computers that are exempt from the Patch Management Process.
8. Under the Inclusions section, press the link next to the "**Resources Included in this Filter**" label. The Selected Resources window will appear.
9. In the left pane, type **DC** in the search box
10. Select **DC** and press the right arrow (>) to add it to the right pane
11. Press **OK**
12. Press the **Save Changes** button
13. Press the **Update Membership** button in the **Filter Membership** area on the right pane. You should see 1 computer in the list named "DC".
14. In the left pane, right click on the **Zero Day Patch Process** folder and select **New > Filter**
15. Change the filter name to **Zero Day Patch – Applicable Computers**
16. Expand the **Filter Definition** section by pressing the downward facing arrow at the right

    This is where you would define the applicable computers as well as the exclusions. We also need to consider that the Patch Management Process requires the Software Update Plug-in to be installed so these criteria must be included.
17. Under the **Inclusions** section, press the link next to the "**Resources Included in this Filter**" label. The Selected Resources window will appear.
18. In the left pane, type **DC** in the search box
19. Select **DC** and press the right arrow (>) to add it to the right pane
20. In the left pane, type **NS75** in the search box
21. Select **NS75** and press the right arrow (>) to add it to the right pane
22. In the left pane, type **SD7** in the search box
23. Select **SD7** and press the right arrow (>) to add it to the right pane
24. Press **OK**

25. Under the **Exclusions** section, press the link next to the “**Filters excluded in this Filter**” label. The Select Filters window will appear.

26. In the left pane, type **Software Update** in the search box

27. Select **“Windows Computers without Software Update Plug-in Installed”** and press the right arrow (>) to add it to the right pane. Adding this filter ensures that computers that are not ready to receive software updates are not included in the list.

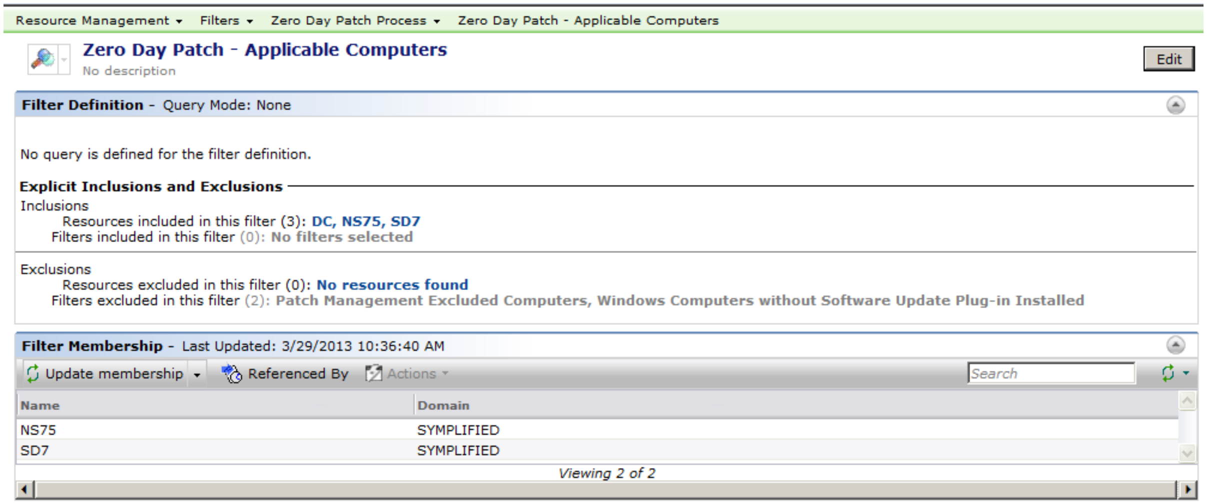
28. In the left pane, type **Excluded Computers** in the search box

29. Select **Patch Management Excluded Computers** and press the right arrow (>) to add it to the right pane. Adding this Filter to the exclusions ensures that computers in this filter will never receive patch management updates.

30. Press **OK**

31. Press the **Save Changes** button

32. Press the **Update Membership** button in the **Filter Membership** section. You should see 2 Resources in this Filter; the DC computer does not appear in the list as it is excluded when the filter calculates the Inclusions and Exclusions. Your Filter should look like this:



Zero Day Patch - Applicable Computers
No description

Filter Definition - Query Mode: None

No query is defined for the filter definition.

Explicit Inclusions and Exclusions

Inclusions
Resources included in this filter (3): DC, NS75, SD7
Filters included in this filter (0): No filters selected

Exclusions
Resources excluded in this filter (0): No resources found
Filters excluded in this filter (2): Patch Management Excluded Computers, Windows Computers without Software Update Plug-in Installed

Filter Membership - Last Updated: 3/29/2013 10:36:40 AM

Name	Domain
NS75	SYMPLIFIED
SD7	SYMPLIFIED

Viewing 2 of 2

Note: *You may use any combination of filters and specific resources to be included and excluded in your Filter. This filter can contain multiple filters like Windows Servers, Windows Workstation, with custom filters to create a Filter that will fit your requirements.*

Creating the Target for use in the Zero Day Patch Workflow

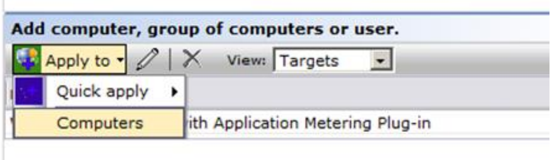
The process for creating a Target based on a Filter (or set of Filters) and locating the Guid for that Target requires a few unconventional steps. Filters can only be created inside an existing policy; they do not have their own standalone UI.

1. Switch to the **NS75** Virtual Machine

2. Navigate to **Manage>Policies** in the menu bar

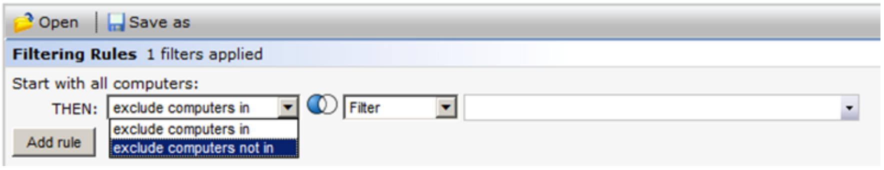
3. You can select any existing policy to create a Target, for this example we will select **Software > Application Metering > Blacklisted Applications** from the left side of the console

4. Once the sample policy opens in the main window, click the **Apply to** button and select **Computers** to open the form to create a new target utilizing existing Filters.


Add computer, group of computers or user.
Apply to
View: Targets
Quick apply
Computers
ith Application Metering Plug-in

5. In the popup window click on the **Add Rule** button

6. In the first dropdown box select **exclude computers *not* in**. This will include all computers in the subsequent filter as part of this Target

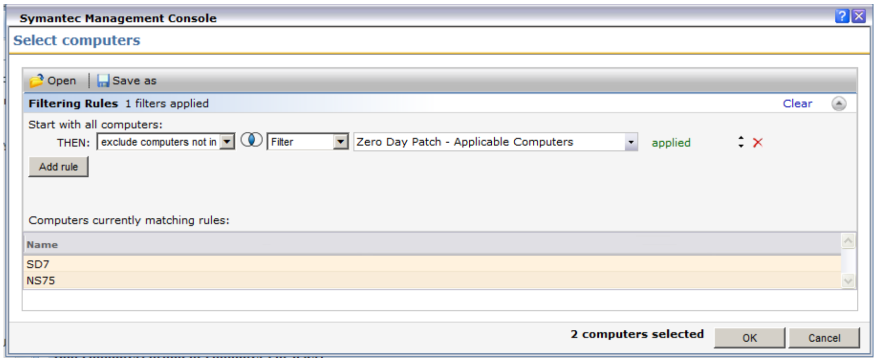

Open
Save as
Filtering Rules 1 filters applied
Start with all computers:
THEN: exclude computers in
Filter
Add rule
exclude computers in
exclude computers not in

7. In the middle dropdown leave **Filter** selected

8. In the last box select **Zero Day Patch – Applicable Computers (**you can start typing and the dropdown list will be automatically filtered)

Note: If you plan to implement Zero Day Patch in your environment, we recommend that you create a custom filter excluding any high risk computers or servers which should not be a candidate for zero day patches

9. Click the **Update results** button to test your target. You should see these results:


Symantec Management Console
Select computers
Open
Save as
Filtering Rules 1 filters applied
Clear
Add rule
OK
Cancel

Start with all computers:
THEN: exclude computers not in | Filter | Zero Day Patch - Applicable Computers | applied

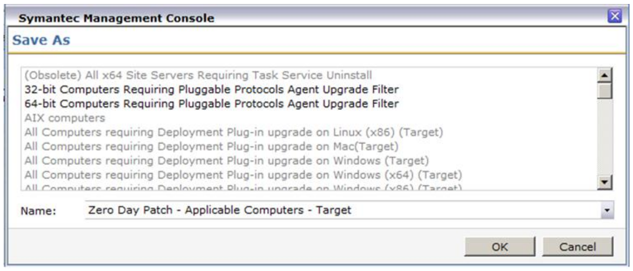
Computers currently matching rules:

Name
SD7
NS75

2 computers selected

10. Click on the **Save As** button on the upper left to save the Target for use in the process

11. On the pop up save window type "**Zero Day Patch - Applicable Computers - Target**" in the **Name** field then click the **OK** button to save the Target.



(Obsolete) All x64 Site Servers Requiring Task Service Uninstall
32-bit Computers Requiring Pluggable Protocols Agent Upgrade Filter
64-bit Computers Requiring Pluggable Protocols Agent Upgrade Filter
AIX computers
All Computers requiring Deployment Plug-in upgrade on Linux (x86) (Target)
All Computers requiring Deployment Plug-in upgrade on Mac(Target)
All Computers requiring Deployment Plug-in upgrade on Windows (Target)
All Computers requiring Deployment Plug-in upgrade on Windows (x64) (Target)
All Computers requiring Deployment Plug-in upgrade on Windows (x86) (Target)

Name: Zero Day Patch - Applicable Computers - Target

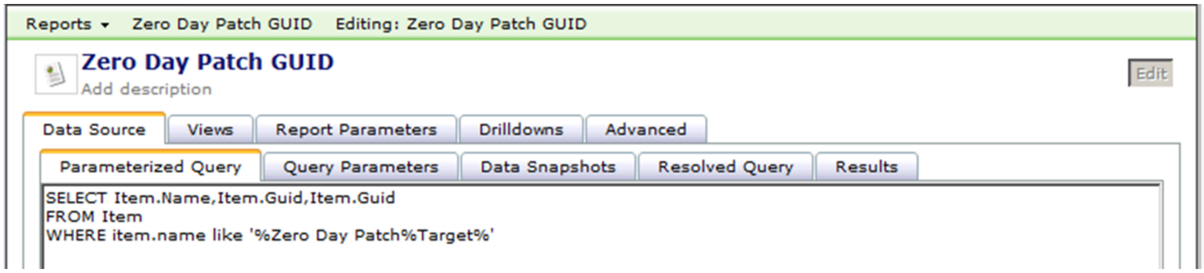
12. Once the new Target has been saved, click the <u>**Cancel**</u> button to close the pop up window. **Note:** clicking the Cancel button will not affect the exiting policy.

Locating the Guid Required for the Zero Day Patch Target

Target properties are not available in the Console UI; therefore locating the Guid for an existing Target requires a SQL Query to be run on the CMDB. The easiest way to accomplish this is to create a simple report that will display the recently created Target and its associated Guid.

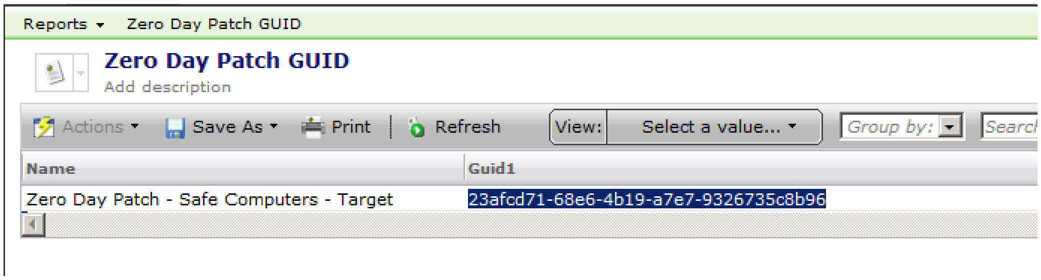
1. In the main menu, select **Reports > All Reports**
2. Right Click on the Reports folder and select **New > Folder**
3. Rename the folder to **Zero Day Patch Reports**
4. Right click on the **Zero Day Patch Reports** folder and select **New > Report > SQL Report**
5. Change the report name to **Zero Day Patch GUID**
6. In the **Parameterized Query** tab, delete the current query and type the following text:

```
SELECT Item.Name,Item.Guid,Item.Guid

FROM Item

WHERE Item.Name like ‘%Zero Day Patch%Target%’
```



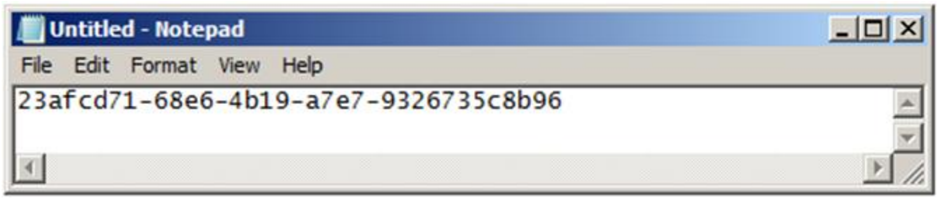
```
SELECT Item.Name,Item.Guid,Item.Guid
FROM Item
WHERE item.name like '%Zero Day Patch%Target%'
```

7. Press the **Save Changes** button. The results of the report should appear



Name	Guid1
Zero Day Patch - Safe Computers - Target	23afcd71-68e6-4b19-a7e7-9326735c8b96

8. Highlight the **GUID** in the report, and copy the text by pressing **CTRL-C**. This can be tricky, but you can highlight it by left mouse clicking an empty area below it and moving the mouse up to the GUID entry.
9. Open Notepad in Windows (Start > Accessories> Notepad) and paste it. Do not close Notepad, as we will be adding more to this file.

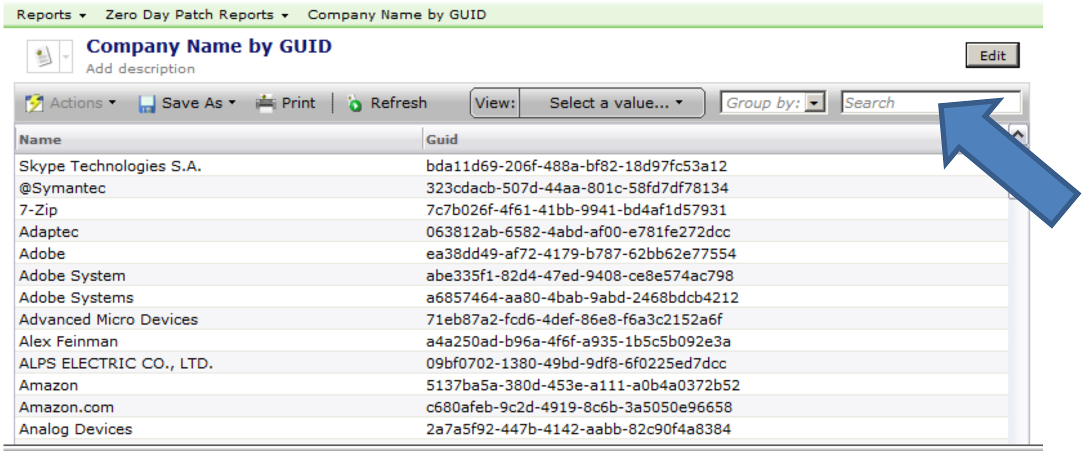


```
23afcd71-68e6-4b19-a7e7-9326735c8b96
```

10. Right click on the **Zero Day Patch Reports** folder and select **New > Report > SQL Report**
11. Change the report name to **Company Name by GUID**
12. In the **Parameterized Query** tab, delete the current query and type the following text:

    ```
    Select Name,_ResourceGuid,_ResourceGuid AS GUID
    FROM vCompany
    ORDER BY Name
    ```

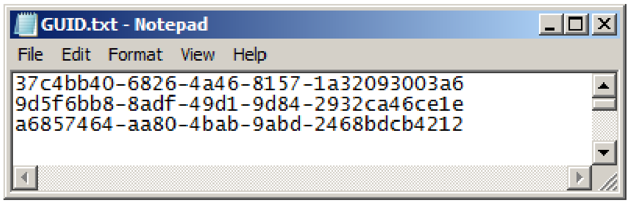
13. Press the **Save Changes** button. The results of the report should appear as the Company Name and its associated GUID



Name	Guid
Skype Technologies S.A.	bda11d69-206f-488a-bf82-18d97fc53a12
@Symantec	323cdacb-507d-44aa-801c-58fd7df78134
7-Zip	7c7b026f-4f61-41bb-9941-bd4af1d57931
Adaptec	063812ab-6582-4abd-af00-e781fe272dcc
Adobe	ea38dd49-af72-4179-b787-62bb62e77554
Adobe System	abe335f1-82d4-47ed-9408-ce8e574ac798
Adobe Systems	a6857464-aa80-4bab-9abd-2468bdcb4212
Advanced Micro Devices	71eb87a2-fcd6-4def-86e8-f6a3c2152a6f
Alex Feinman	a4a250ad-b96a-4f6f-a935-1b5c5b092e3a
ALPS ELECTRIC CO., LTD.	09bf0702-1380-49bd-9df8-6f0225ed7dcc
Amazon	5137ba5a-380d-453e-a111-a0b4a0372b52
Amazon.com	c680afeb-9c2d-4919-8c6b-3a5050e96658
Analog Devices	2a7a5f92-447b-4142-aabb-82c90f4a8384

Since the Administrator is only including Microsoft and Adobe Systems updates in the Zero Day Patch process, we need to find them in this report and copy them to the Notepad file

14. To find the GUID for Microsoft, type **Microsoft** in the search field at the top right corner of the report.
15. Highlight the **GUID** in the report (like you did in step 8), and copy it by pressing **CTRL-C**.
16. In the opened Notepad document, Paste this GUID under the first GUID you pasted.
17. To find the GUID for Adobe Systems**,** type **Adobe Systems** in the search field at the top right corner of the report.
18. Highlight the **GUID** in the report (like you did in step 8), and copy it by pressing **CTRL-C**.
19. In the opened Notepad document, Paste this GUID under the Second GUID you pasted. You should now have 3 GUIDs pasted in the notepad document. ***Remove any extra spaces.***



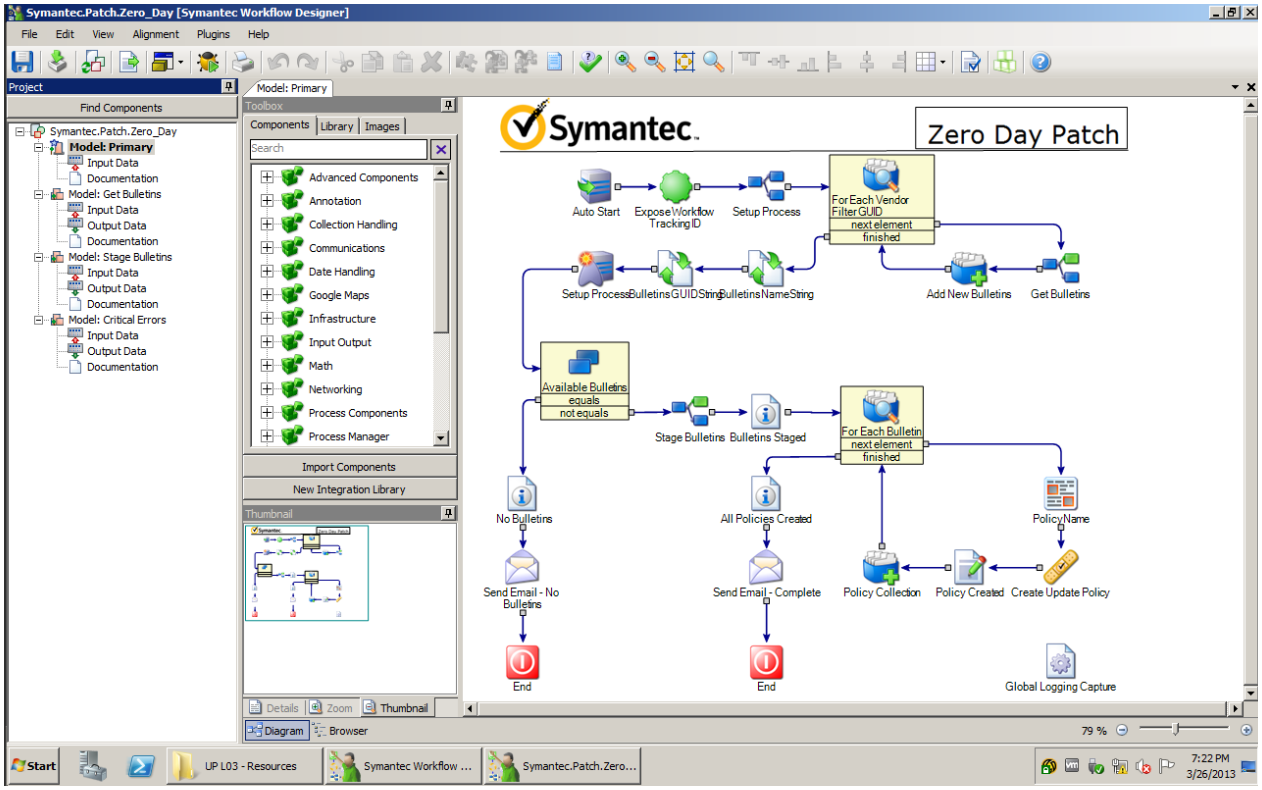
```
37c4bb40-6826-4a46-8157-1a32093003a6
9d5f6bb8-8adf-49d1-9d84-2932ca46ce1e
a6857464-aa80-4bab-9abd-2468bdcb4212
```

Note: The GUIDs in this picture will be different.

20. Save the Notepad file as \\SD7\c$\Administrator.SYMPLIFIED\Desktop\GUID.TXT so you can open it from the SD7 Virtual Machine desktop.

Exercise 2: Unpacking the Zero Day Patch template

1. Switch to the **SD7** Virtual Machine
2. Open the **Computer** icon on the desktop and navigate to **C:\Lab Resources\Zero Day Patch** and select **Symanect.Patch.Zero_Day.package** and double click it.
3. Click the **OK** button to unpackage the project, this will also open Workflow in the background and may take a couple of minutes.
4. The opened package should look like this:



Exercise 3: Importing and Configuring the Application Profile

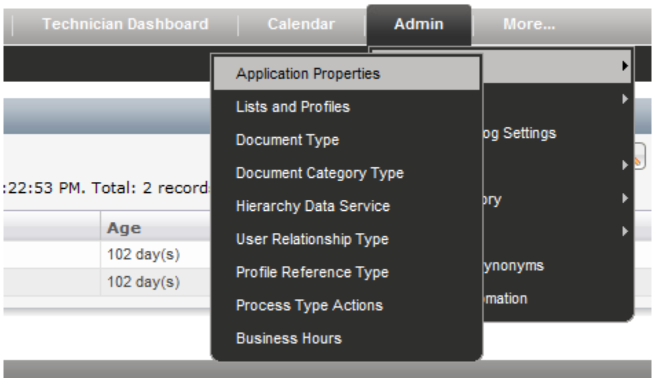
The Zero Day Patch template includes an Application Profile to store all environmental and template configuration variables. This will allow administrators to configure and edit many of the template options without needing to open and republish the Workflow project.

1. Open the **Process Manager** by clicking on the **Process Manager** icon on the desktop
2. It should automatically login as administrator@symplified.org in a few seconds. If it does not, you can log in with these credentials:

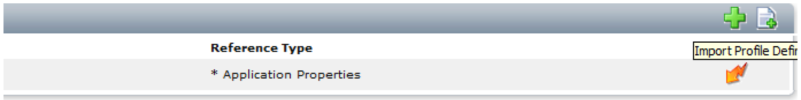
User Name: administrator@symplified.org

Password: symc4now!

3. Navigate to **Admin > Data > Application Properties**



4. Click on the **Import Profile Definition** Icon on the right side (Document with a green +)

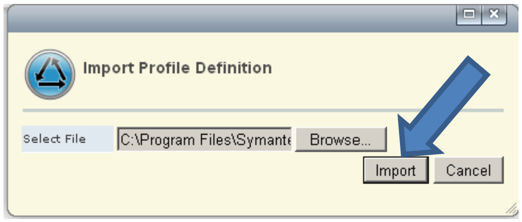


Reference Type
* Application Properties

5. In the pop up box click the **Browse** button

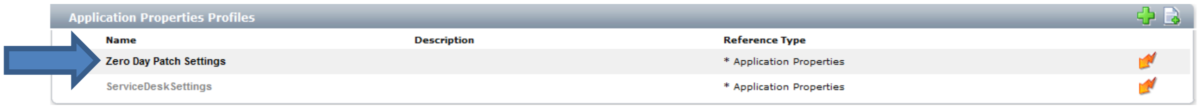
6. Navigate to **c:\Program Files\Symantec\Workflow\WorkflowProjects\Symantec.Patch.Zero_Day\resource** and choose **Zero_Day_Patch_Settings.pfl.** Then click the **Open** button.

7. Click the **Import** button to import the Zero Day Patch Application Profile.



Select File C:\Program Files\Symante

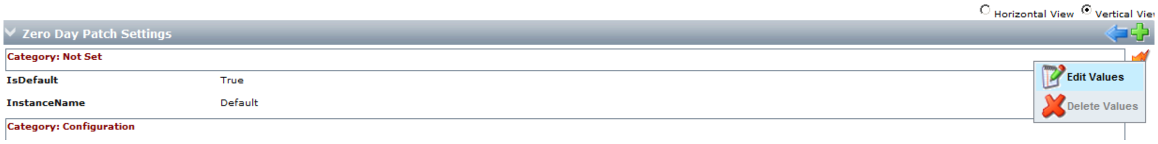
8. Click on the **Zero Day Patch Settings** link to access the Application Profile.



Application Properties Profiles

Name	Description	Reference Type
Zero Day Patch Settings		* Application Properties
ServiceDeskSettings		* Application Properties

9. Click on the **Lighting Bolt** to the right, then select **Edit Values** to make changes to the Zero Day Patch Settings



Zero Day Patch Settings

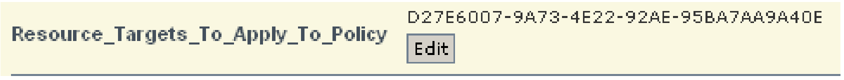
Category: Not Set

IsDefault	True
InstanceName	Default

Category: Configuration

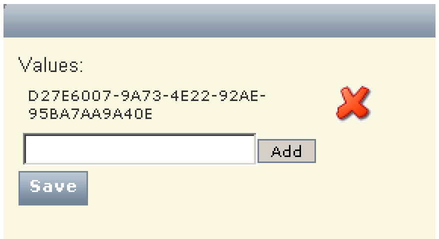
10. Check the box for **Enable_Policy_After_Creation**

11. Click the **Edit** button next to **Resource_Targets_To_Apply_To_Policy** to modify the target list



Resource_Targets_To_Apply_To_Policy D27E6007-9A73-4E22-92AE-95BA7AA9A40E

12. Click on the red **X** button to remove the existing target Guid



Values:

D27E6007-9A73-4E22-92AE-95BA7AA9A40E

13. Open the GUID.TXT you saved to the desktop, and copy the ***First*** GUID in the list.

14. Paste in the Guid you copied, make sure there are no leading/trailing spaces, then click the **Add** button

15. Press the **Save** button to close the pop up window. In your own environment you can apply several targets if you wish.

16. Scroll down to **Age_Date** and change it from 15 to **48**. In production you might set the Age Filter for less than 15 Days as the assumption might be that all computers in the applicable filter are patched since the last run. In the case of this lab, we need to set it to 48 Days due to the fact that this lab was developed a few weeks ago and is only pre-staged to a certain level.

17. You will notice that a GUID of 000000-0000-0000-0000-000000000 is set for **Vendor_Filter**. This GUID is a representation of "All Vendors" and if left as is will run the process for all vendor updates. In this example, the administrator has been instructed to only include the updates from Microsoft and Adobe Systems.

18. To set the Vendor Names that are to be included, Press the **Edit** button next to Vendor_Filter.

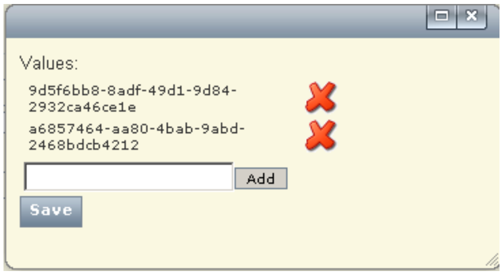
19. Click on the red **X** button to remove the existing target Guid

20. Return to the GUID.TXT notepad document and copy the ***Second*** GUID from it.

21. Paste in the Guid you copied, make sure there are no leading/trailing spaces, then click the **Add** button

22. Return to the GUID.TXT notepad document and copy the ***Third*** GUID from it.

23. Paste in the Guid you copied, make sure there are no leading/trailing spaces, then click the **Add** button



Values:

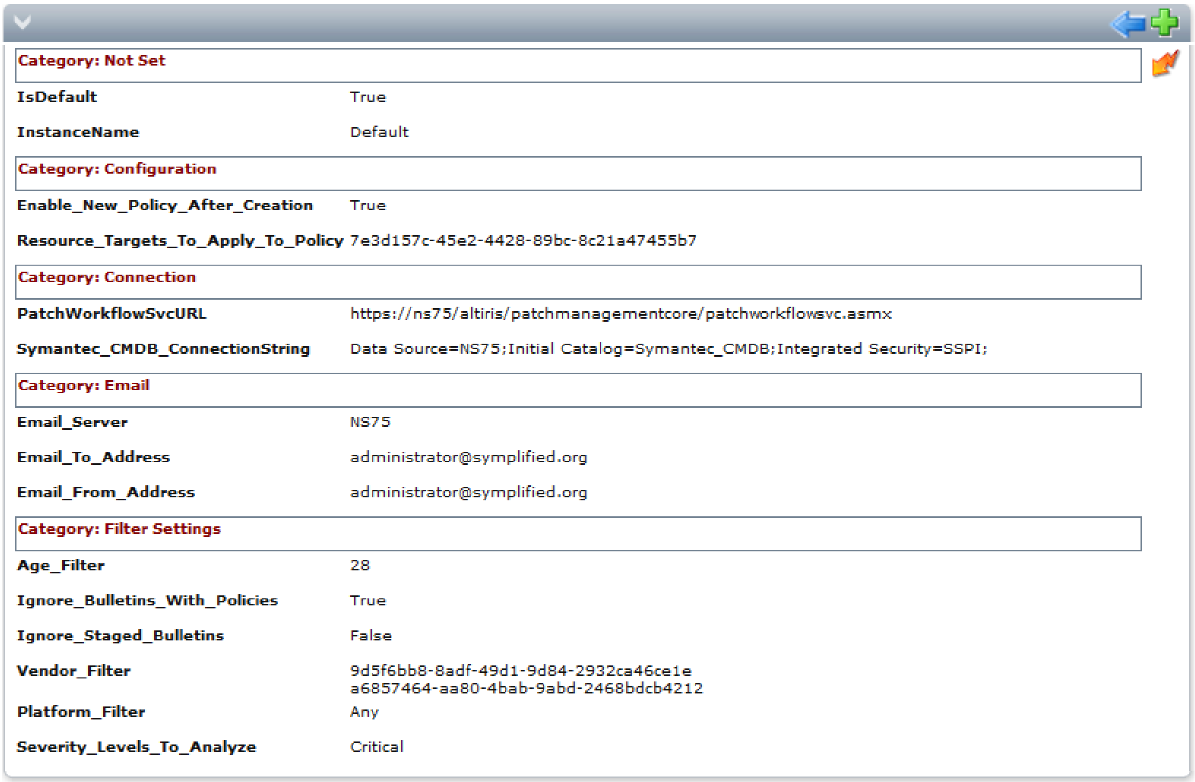
9d5f6bb8-8adf-49d1-9d84-2932ca46ce1e

a6857464-aa80-4bab-9abd-2468bdcb4212

24. Press the **Save** button

25. Click the **Save** button to save your changes and to close the Application Profile Editor

26. The settings should look like this: (With possibly different GUIDs)



Category: Not Set	
IsDefault	True
InstanceName	Default
Category: Configuration	
Enable_New_Policy_After_Creation	True
Resource_Targets_To_Apply_To_Policy	7e3d157c-45e2-4428-89bc-8c21a47455b7
Category: Connection	
PatchWorkflowSvcURL	https://ns75/altiris/patchmanagementcore/patchworkflowsvc.asmx
Symantec_CMDB_ConnectionString	Data Source=NS75;Initial Catalog=Symantec_CMDB;Integrated Security=SSPI;
Category: Email	
Email_Server	NS75
Email_To_Address	administrator@symplified.org
Email_From_Address	administrator@symplified.org
Category: Filter Settings	
Age_Filter	28
Ignore_Bulletins_With_Policies	True
Ignore_Staged_Bulletins	False
Vendor_Filter	9d5f6bb8-8adf-49d1-9d84-2932ca46ce1e a6857464-aa80-4bab-9abd-2468bdcb4212
Platform_Filter	Any
Severity_Levels_To_Analyze	Critical

Definition of the Zero Day Patch Process Values

Variables for all Application Profiles:

Instance Name: In Application Properties you can have multiple instances of values for the same profile. You can use multiple instances for several scenarios, for example an instance for your Dev, QA and Production environment. For the Zero Day Patch process you might also create separate instances for different vendors with different filter or target values.

Is Default: One instance must be marked as the default instance

Zero Day Patch Setting Specific Variables:

Enable_New_Policy_After_Creation: This is a check mark to enable or not enable the policy on creation. By default this is set to false (unchecked). For this lab please **check this box**

Resource_Targets_To_Apply_To_Policy: This is an array of Guids that represent the pre-defined targets for the policies.

Symantec_CMDB_ConnectionString: This variable is the connection string to your Altiris Database, for this lab, this variable was preset, in your environment you will need to change the connection string to your database.

PatchWorkfklowSvcURL: This variable is the URL of the Patch API. For this lab you do not need to make any changes, in your environment you will need to change the server name (NS75) in the string to your SMP Server Name

Email Server: Your SMTP email server

Email_To_Address: The address all summary and error messages will be sent to

Email_From_Address: The email address that will be used as the from address for all summary and error message emails

Platform_Filter: A variable to limit the platforms that are a part of this process. Any = All Platforms, other choices are Windows, Novell, Red Hat

Ignore_Staged_Bulletins: When checked, this variable causes the process to filter out any pre-staged bulletin. For this lab, this field needs to remain uncheck as we have pre-staged applicable patches for bandwidth and time.

Ignore_Bulletins_With_Policies: When checked, this variable will cause the process to filter out any bulletins that already have an associated policy so that you do not end up with duplicate policies.

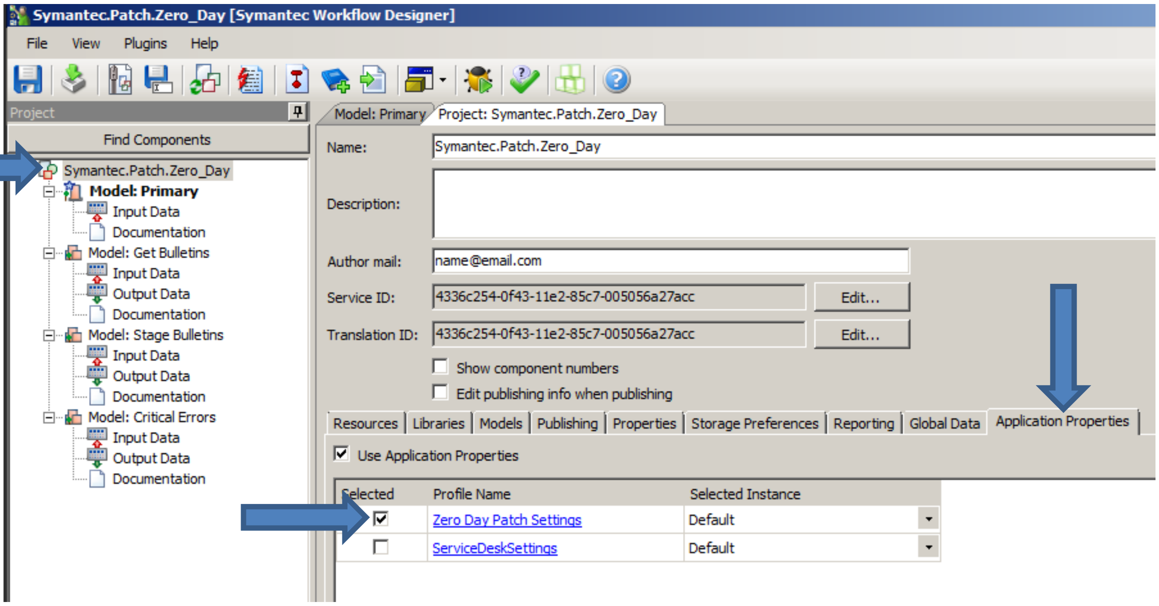
Severity_Levels_To_Analyze: This is an array of severity levels you would like to include as part of the process. You may add as many values (e.g. Critical, Important, etc.) as you feel are applicable to your organization. For the lab, please contain this to only **critical** patches as we have pre-staged them.

Vendor_Filter: This is an array of vendor's guids to include in the Zero Day process. Adding a Guid of only 0's will include all vendors, otherwise you will need to find and enter the Guid for the desired vendors. The easiest way to find a Guid for a patch vendor is **Right Click** on a bulletin for that vendor and choose **Resource Manager,** then inside the resource manager click the vendor's name link which will open the Resource Manager for that vendor, where you will find the Guid in the header section.

Exercise 4: Editing the Zero Day Patch Workflow Template

The Zero Day Patch template is just a template, you are welcome to edit and change the template to fit the needs of your organization. The template was designed to work “out of the box” utilizing the configuration properties in the Application Profile. There are two changes that must be made to the process to work out of the box, first to associate this project with the Application Profile we just imported to the Process Manager, and second to set the schedule

1. Switch to the **Workflow Designer**, this should already be open if you have not closed it.
2. In the left pane, select **Symantec_Patch_Zero-Day** from the top level
3. Click on the **Application Properties** Tab
4. Wait a few seconds for the tab to update with the latest Application Profile data and when it appears **check the box** next to **Zero Day Patch Settings** to associate the newly imported Application Profile to this process.



Name: Symantec.Patch.Zero_Day

Description:

Author mail: name@email.com

Service ID: 4336c254-0f43-11e2-85c7-005056a27acc

Translation ID: 4336c254-0f43-11e2-85c7-005056a27acc

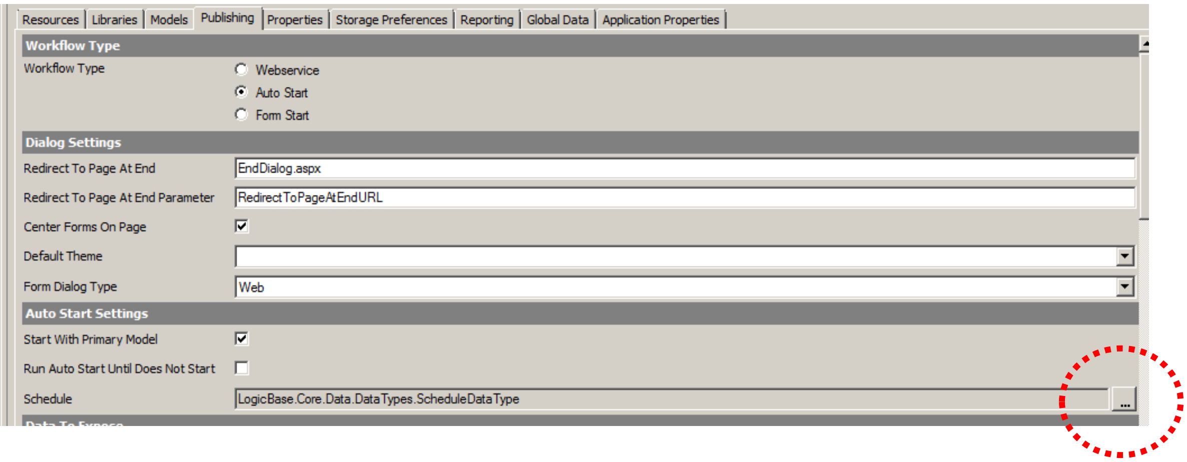
☐ Show component numbers

☐ Edit publishing info when publishing

☑ Use Application Properties

Selected	Profile Name	Selected Instance
☑	Zero Day Patch Settings	Default
☐	ServiceDeskSettings	Default

5. Select the **Publishing** Tab to modify the run schedule
6. Find and click on the **ellipsis** next to **Schedule** to open the schedule editor



Workflow Type

Workflow Type: ○ Webservice ● Auto Start ○ Form Start

Dialog Settings

Redirect To Page At End: EndDialog.aspx

Redirect To Page At End Parameter: RedirectToPageAtEndURL

Center Forms On Page: ☑

Default Theme:

Form Dialog Type: Web

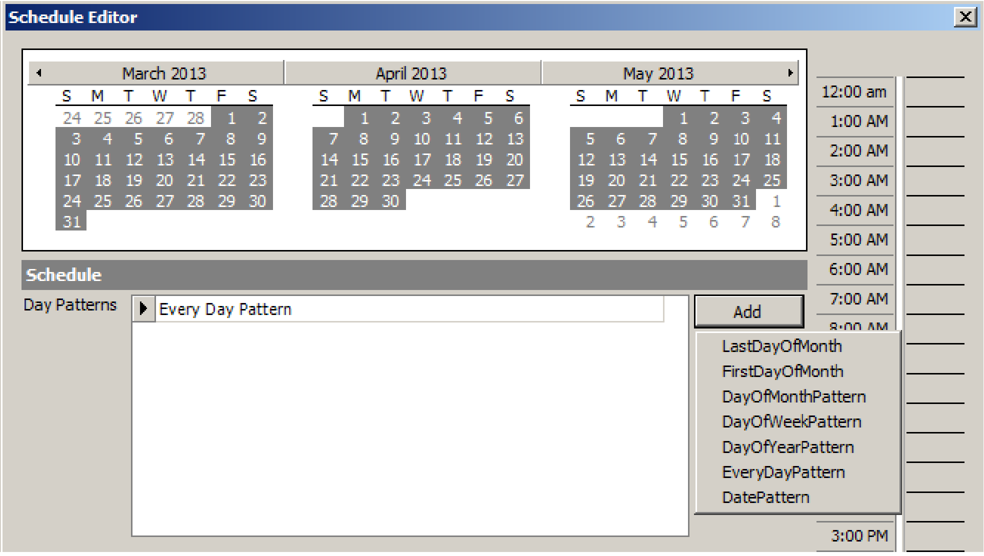
Auto Start Settings

Start With Primary Model: ☑

Run Auto Start Until Does Not Start: ☐

Schedule: LogicBase.Core.Data.DataTypes.ScheduleDataType

7. The default schedule is set to run once a day at 5:00 AM. You can modify this schedule to run at the interval that meets the needs of your organization. A schedule is separated into two pieces, one to configure the day and another to configure the time or times in that day for the process to execute. By clicking the Add button you can see the list of options for daily schedule.



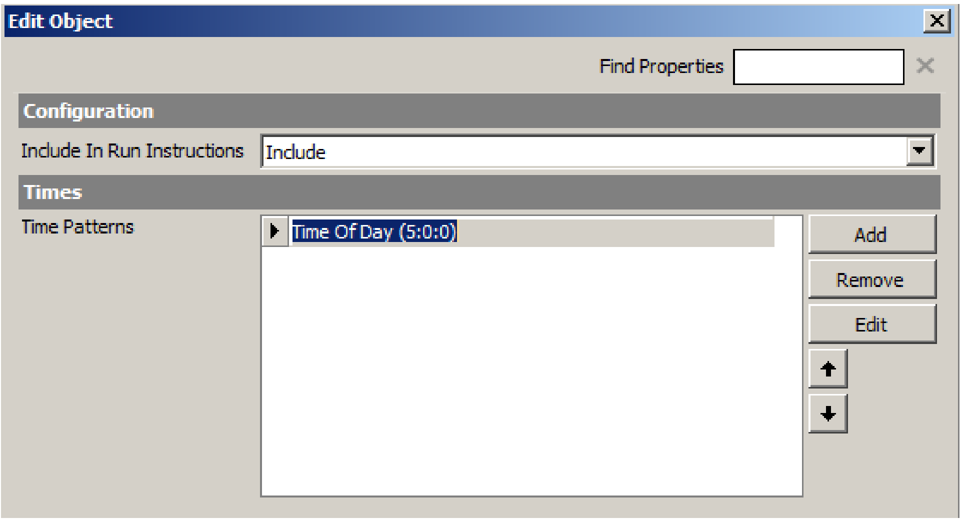
Schedule Editor

Schedule

Day Patterns: Every Day Pattern

8. Instead of adding a new day pattern, highlight the existing **Every Day Pattern** and click the **Edit** button to access the time of day pattern options

9. Highlight the **Time of Day** time pattern and click the **Edit** button



Edit Object

Configuration

Include In Run Instructions: Include

Times

Time Patterns: Time Of Day (5:0:0)

10. Change the run time to **4:00 AM**.

11. When you are finished click the **OK** button to close

12. You can also see additional run options by clicking the **Add** button

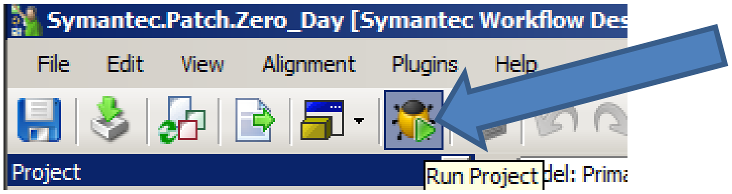
13. Click the **OK** button on this window and its parent form to close the schedule editor

Exercise 5: Testing the Zero Day Patch Process

Running the process in Debug Mode

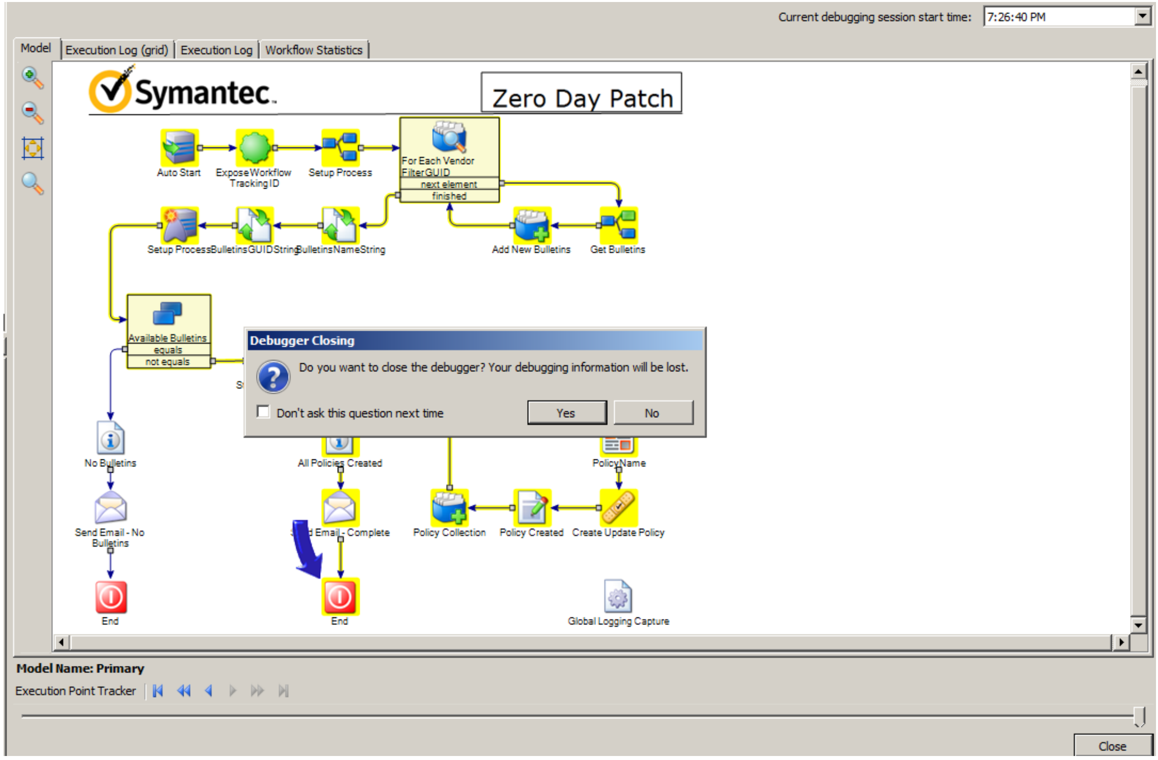
The project is now ready to test in the debug mode.

1. In the menu bar click on the **Run Project** icon to open the debugger.



2. The debugger will automatically execute this as an **Autostart Workflow**, you will only need to wait and watch the process execute. *Be Patient…*

3. Keep watching for the process to complete and the yellow line as made it to the end component. Close the debugger by clicking the **Close** button to prevent subsequent sessions form executing. Then click **Yes** in the pop up window.



Current debugging session start time: 7:26:40 PM

Debugger Closing

Do you want to close the debugger? Your debugging information will be lost.

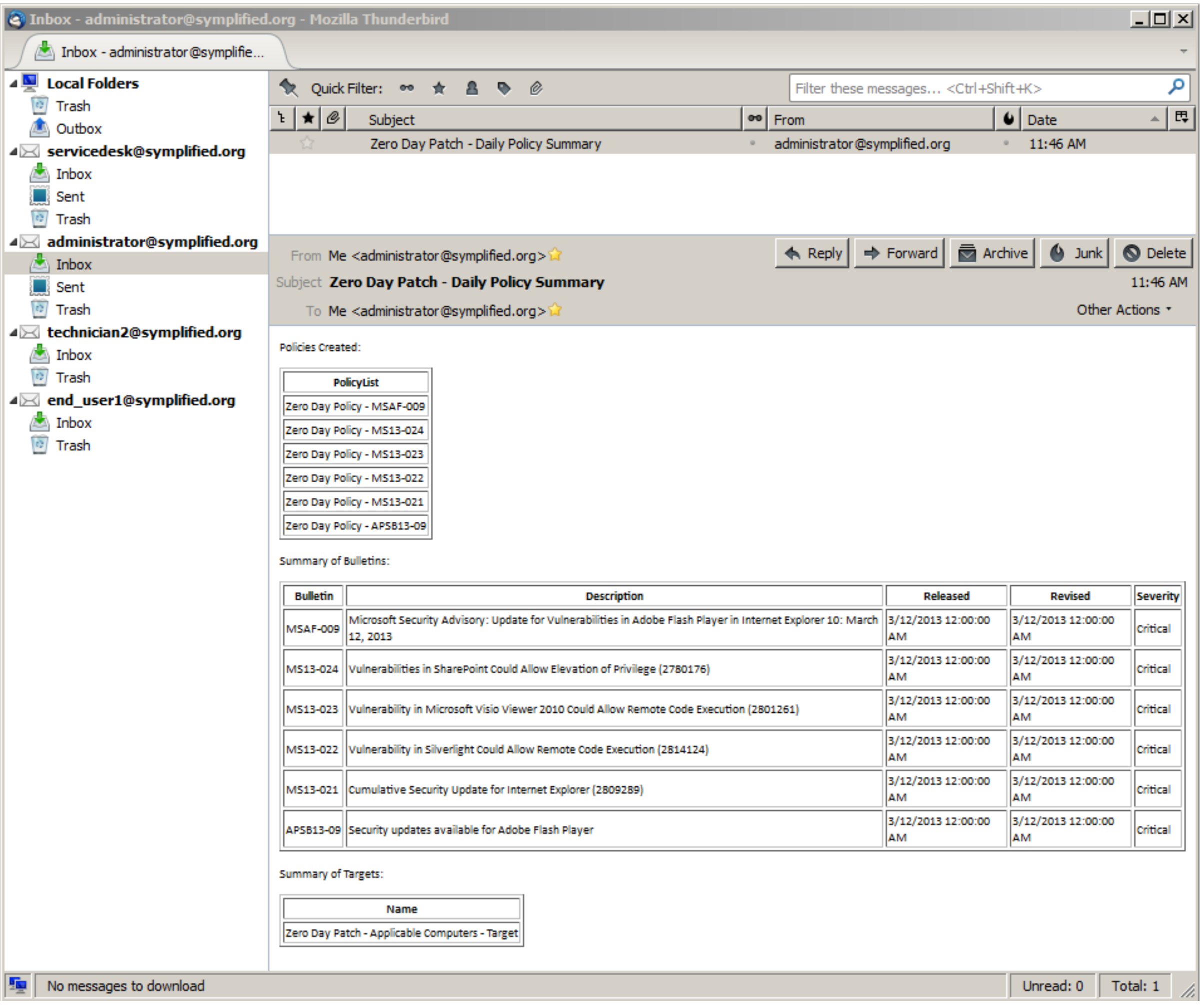
□ Don't ask this question next time

Model Name: Primary

Checking the Email Verification

1. Open the Mozilla email client to review the summary email by clicking **Start > Mozilla Thunderbird** or by double clicking the **Mozilla Thunderbird** icon on the Desktop

2. You may need to refresh the mail client by clicking the **Get Mail** button, then select and review the summary email in the administrator@symplified.org inbox. If you don't get an email in less than 3 minutes, then re-run the process in the last section.


Inbox - administrator@symplified.org - Mozilla Thunderbird
Inbox - administrator@symplifie...
Local Folders
Trash
Outbox
servicedesk@symplified.org
Inbox
Sent
Trash
administrator@symplified.org
Inbox
Sent
Trash
technician2@symplified.org
Inbox
Trash
end_user1@symplified.org
Inbox
Trash
Quick Filter:
Filter these messages... <Ctrl+Shift+K>
Subject
From
Date
Reply
Forward
Archive
Junk
Delete
Other Actions
No messages to download
Unread: 0
Total: 1

Zero Day Patch - Daily Policy Summary | administrator@symplified.org | 11:46 AM

From Me <administrator@symplified.org>

Subject **Zero Day Patch - Daily Policy Summary** 11:46 AM

To Me <administrator@symplified.org>

Policies Created:

PolicyList
Zero Day Policy - MSAF-009
Zero Day Policy - MS13-024
Zero Day Policy - MS13-023
Zero Day Policy - MS13-022
Zero Day Policy - MS13-021
Zero Day Policy - APSB13-09

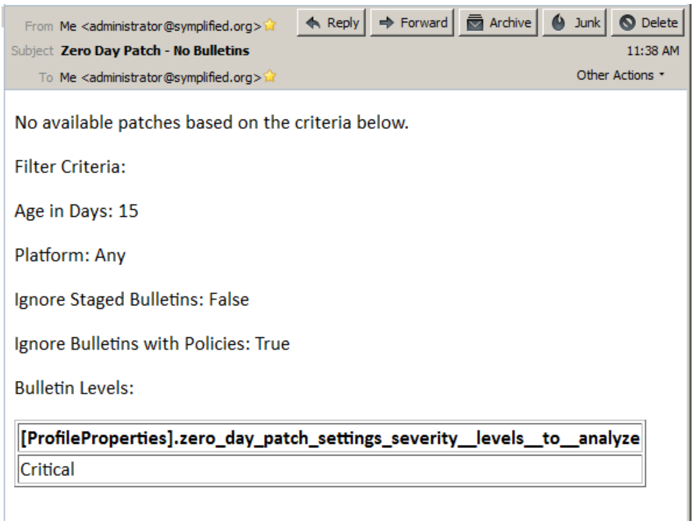
Summary of Bulletins:

Bulletin	Description	Released	Revised	Severity
MSAF-009	Microsoft Security Advisory: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10: March 12, 2013	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical
MS13-024	Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical
MS13-023	Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2801261)	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical
MS13-022	Vulnerability in Silverlight Could Allow Remote Code Execution (2814124)	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical
MS13-021	Cumulative Security Update for Internet Explorer (2809289)	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical
APSB13-09	Security updates available for Adobe Flash Player	3/12/2013 12:00:00 AM	3/12/2013 12:00:00 AM	Critical

Summary of Targets:

Name
Zero Day Patch - Applicable Computers - Target

3. ***For future reference***, this is what the email would look like if there were no bulletins to process.



From Me <administrator@symplified.org>

Subject **Zero Day Patch - No Bulletins** 11:38 AM

To Me <administrator@symplified.org>

No available patches based on the criteria below.

Filter Criteria:

Age in Days: 15

Platform: Any

Ignore Staged Bulletins: False

Ignore Bulletins with Policies: True

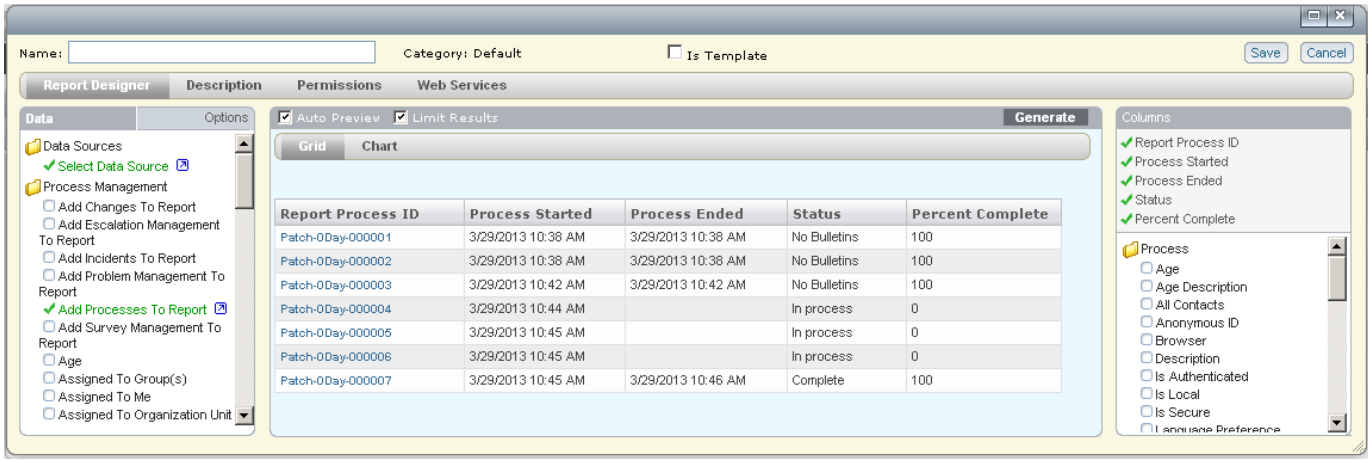
Bulletin Levels:

[ProfileProperties].zero_day_patch_settings_severity__levels__to__analyze
Critical

Creating a Zero Day Patch Report

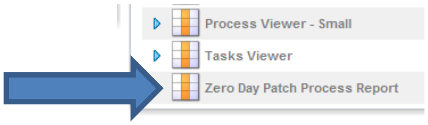
The Zero Day Patch process has created an audit trail in Workflow. You can take the time to create a report in the Process Manager that separates out this process.

1. Return to the **Process Manager** if it is open, or by double clicking the **Process Manager** icon on the desktop. Navigate the **Reports** Tab
2. Under the Reports area on the left pane, select the **Add Report** icon (Document with +), and select **Add Standard Report.** The Report Designer will appear
3. On the **Data** pane on the left, select "**Select Data Source**".
4. The Select Data Source window opens, then click **OK**
5. On the left pane, in the **Process Management** folder, select **Add Processes to Report**
6. Check the "**Only Processes I have permissions**" checkbox, then Click **OK**
7. On the left pane, under the **Process Management** folder, select **Include Process Actions**
8. On the left pane, under the **Process Management** folder, select **Report Process ID**
9. In the **ReportProcessID** field, type **Patch**, then click **OK**
10. On the right pane, under the **Process** folder:
    a. Select **Report Process ID**
    b. Select **Process Started**
    c. select **Process Ended**
    d. select **Status**
    e. **Percent Complete**
11. Adjust your report columns in the middle pane so they show all of the data in the report

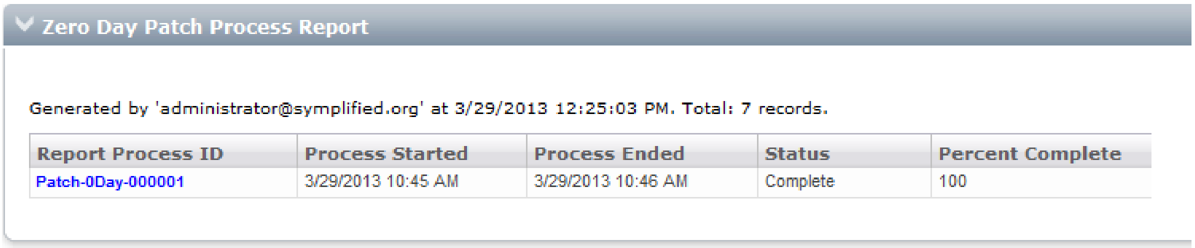


Report Process ID	Process Started	Process Ended	Status	Percent Complete
Patch-0Day-000001	3/29/2013 10:38 AM	3/29/2013 10:38 AM	No Bulletins	100
Patch-0Day-000002	3/29/2013 10:38 AM	3/29/2013 10:38 AM	No Bulletins	100
Patch-0Day-000003	3/29/2013 10:42 AM	3/29/2013 10:42 AM	No Bulletins	100
Patch-0Day-000004	3/29/2013 10:44 AM		In process	0
Patch-0Day-000005	3/29/2013 10:45 AM		In process	0
Patch-0Day-000006	3/29/2013 10:45 AM		In process	0
Patch-0Day-000007	3/29/2013 10:45 AM	3/29/2013 10:46 AM	Complete	100

12. Type **Zero Day Patch Process Report** in the Name: field at the top left corner
13. Press the **Save** button
14. Select the **Zero Day Patch Process Report** in the Reports Pane. The report will appear.



15. Depending on how many times the debugger ran the process, you may have more than one process in your report.

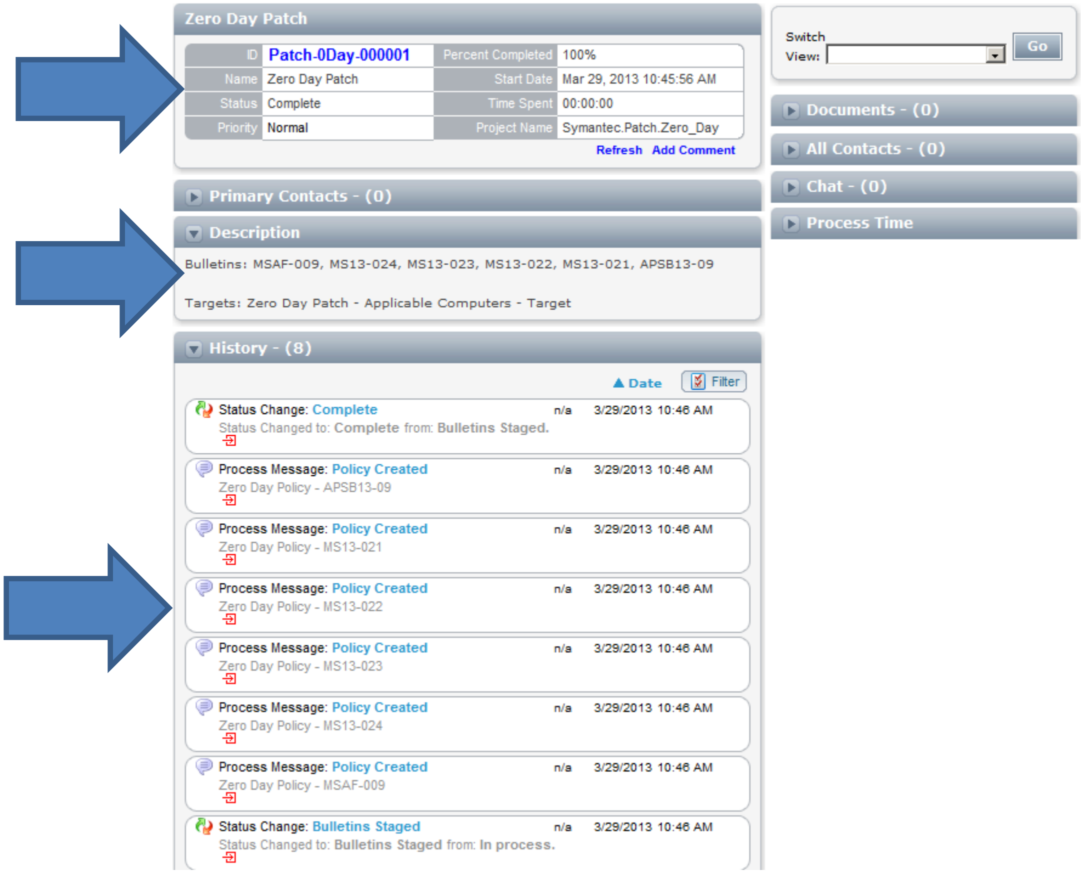


Zero Day Patch Process Report

Generated by 'administrator@symplified.org' at 3/29/2013 12:25:03 PM. Total: 7 records.

Report Process ID	Process Started	Process Ended	Status	Percent Complete
Patch-0Day-000001	3/29/2013 10:45 AM	3/29/2013 10:46 AM	Complete	100

16. Select the last Process ID in your report. The resulting pop up window should be the process view page for the instance we just ran in the debugger including an audit history of actions. If you do not see any history, select another Process ID from the Report.



Zero Day Patch

ID	Patch-0Day-000001	Percent Completed	100%
Name	Zero Day Patch	Start Date	Mar 29, 2013 10:45:56 AM
Status	Complete	Time Spent	00:00:00
Priority	Normal	Project Name	Symantec.Patch.Zero_Day

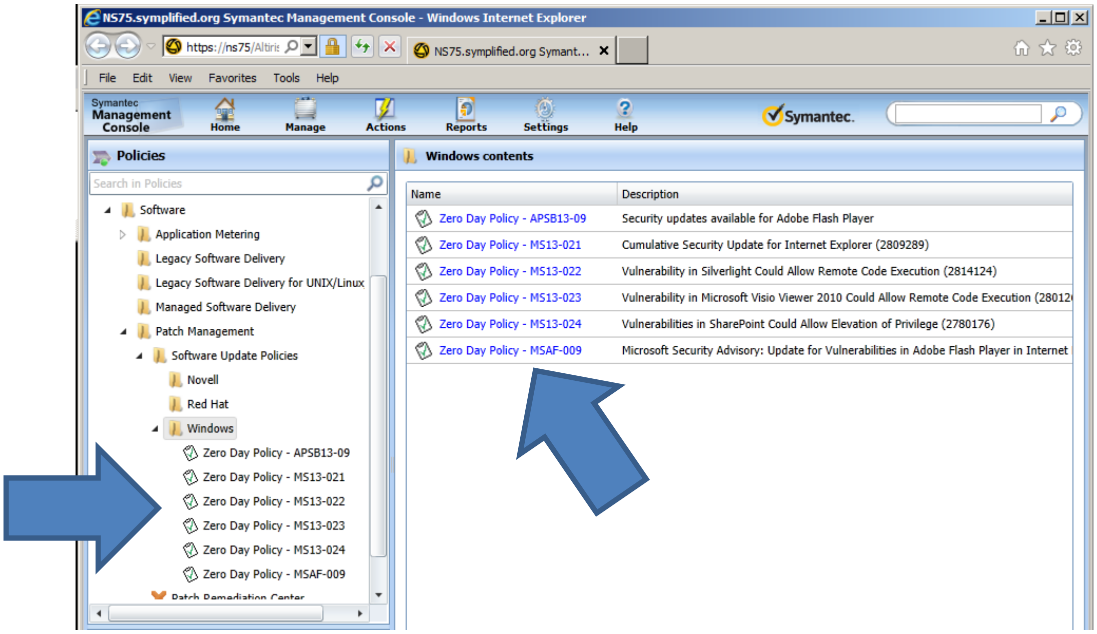
Bulletins: MSAF-009, MS13-024, MS13-023, MS13-022, MS13-021, APSB13-09

Targets: Zero Day Patch - Applicable Computers - Target

```
Status Change: Complete                                  n/a   3/29/2013 10:46 AM
Status Changed to: Complete from: Bulletins Staged.

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - APSB13-09

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - MS13-021

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - MS13-022

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - MS13-023

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - MS13-024

Process Message: Policy Created                          n/a   3/29/2013 10:46 AM
Zero Day Policy - MSAF-009

Status Change: Bulletins Staged                          n/a   3/29/2013 10:46 AM
Status Changed to: Bulletins Staged from: In process.
```

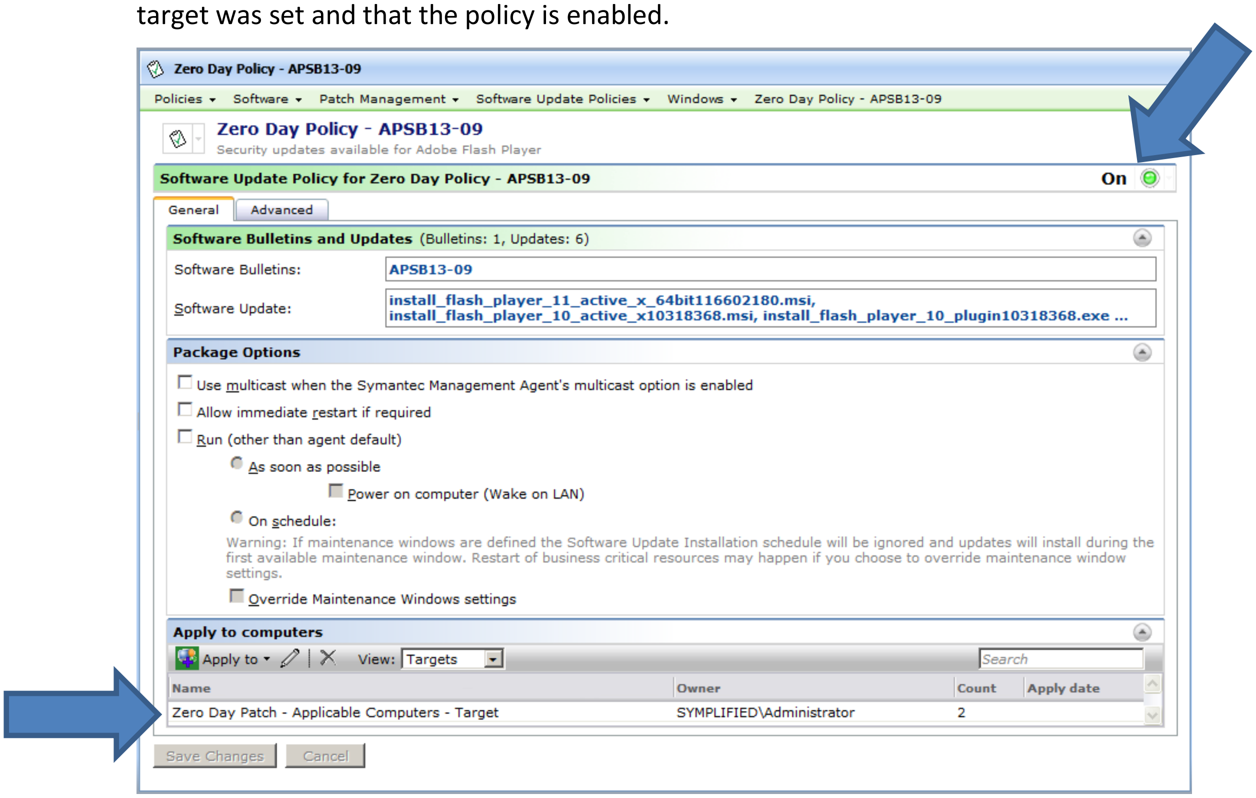
Verifying the Policy Creation on the SMP

1. Switch to the **NS75** Virtual Machine
2. Navigate to **Manage > Policies** from the main menu bar. Then in the folder structure on the left select **Software >Patch Management > Software Update Policies >Windows** to view the newly created Zero Day Patch policies


NS75.symplified.org Symantec Management Console - Windows Internet Explorer
https://ns75/Altiris
NS75.symplified.org Symant...
File Edit View Favorites Tools Help
Symantec Management Console
Home
Manage
Actions
Reports
Settings
Help
Symantec.
Policies
Search in Policies
Software
Application Metering
Legacy Software Delivery
Legacy Software Delivery for UNIX/Linux
Managed Software Delivery
Patch Management
Software Update Policies
Novell
Red Hat
Windows
Zero Day Policy - APSB13-09
Zero Day Policy - MS13-021
Zero Day Policy - MS13-022
Zero Day Policy - MS13-023
Zero Day Policy - MS13-024
Zero Day Policy - MSAF-009
Patch Remediation Center
Windows contents

Name	Description
Zero Day Policy - APSB13-09	Security updates available for Adobe Flash Player
Zero Day Policy - MS13-021	Cumulative Security Update for Internet Explorer (2809289)
Zero Day Policy - MS13-022	Vulnerability in Silverlight Could Allow Remote Code Execution (2814124)
Zero Day Policy - MS13-023	Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (28012
Zero Day Policy - MS13-024	Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)
Zero Day Policy - MSAF-009	Microsoft Security Advisory: Update for Vulnerabilities in Adobe Flash Player in Internet

3. Click on any software update policy link in the left pane and verify that the correct target was set and that the policy is enabled.


Zero Day Policy - APSB13-09
Policies ▾ Software ▾ Patch Management ▾ Software Update Policies ▾ Windows ▾ Zero Day Policy - APSB13-09
General
Advanced
Apply to ▾
View:
Search
Save Changes
Cancel

Zero Day Policy - APSB13-09
Security updates available for Adobe Flash Player

Software Update Policy for Zero Day Policy - APSB13-09 **On** ●

Software Bulletins and Updates (Bulletins: 1, Updates: 6)

Software Bulletins: APSB13-09

Software Update: install_flash_player_11_active_x_64bit116602180.msi, install_flash_player_10_active_x10318368.msi, install_flash_player_10_plugin10318368.exe ...

Package Options

□ Use multicast when the Symantec Management Agent's multicast option is enabled
□ Allow immediate restart if required
□ Run (other than agent default)
○ As soon as possible
□ Power on computer (Wake on LAN)
○ On schedule:
Warning: If maintenance windows are defined the Software Update Installation schedule will be ignored and updates will install during the first available maintenance window. Restart of business critical resources may happen if you choose to override maintenance window settings.
□ Override Maintenance Windows settings

Apply to computers

View: Targets

Name	Owner	Count	Apply date
Zero Day Patch - Applicable Computers - Target	SYMPLIFIED\Administrator	2	