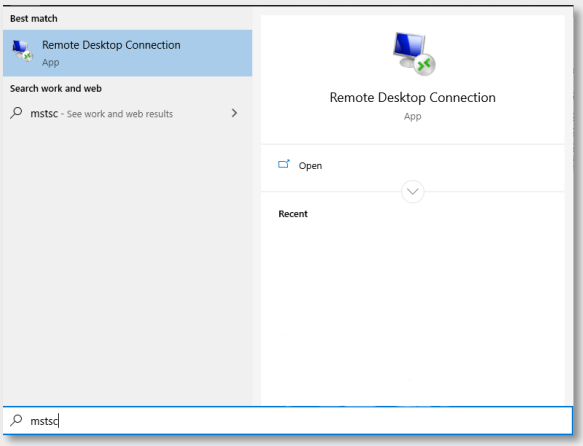
Lab i - Connect to the Ipswitch Training Environment (ITE)

i-1 Open Remote Desktop

Windows

- On the desktop, click the Windows button

- Immediately start typing **MSTSC** on your keyboard
  - The Windows search will find Remote Desktop Connection
    - Click on it



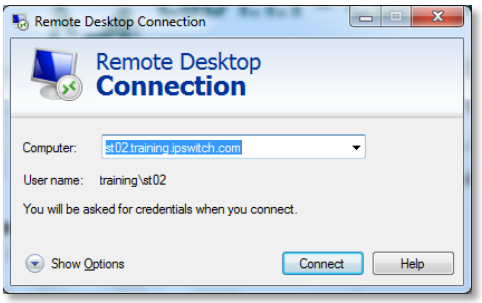
MAC

- You must have Microsoft Remote desktop installed
- Launch Microsoft Remote Desktop

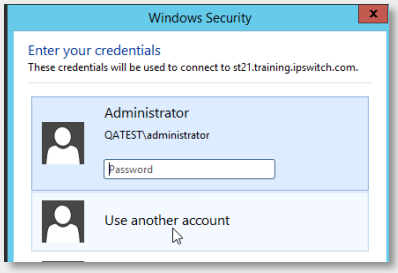
i-2 Connect to your Apps Server in the ITE

In the Remote Desktop Connection Dialog:

- Enter your server name:
  - The server name is
    <The studentID you were given>.training.ipswitch.com
    - As Examples.
      - If you were given *st01* as your studentID, then the server address would be: *st01*.training.ipswitch.com
      - If you were given *st16* as your studentID, then the server address would be: *st16*.training.ipswitch.com
      - And so on …

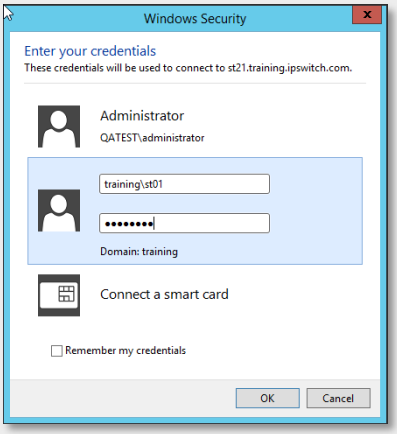


i-3	Enter Username and password	When the RDP Session opens, click on Use another account



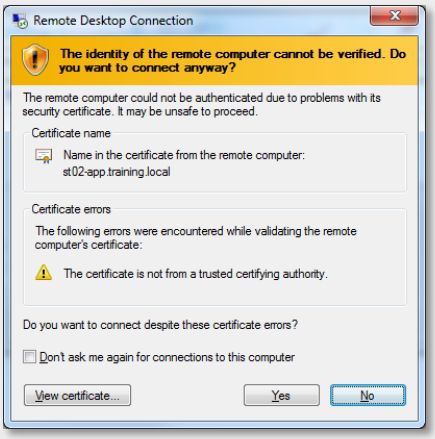
Then type in your username and password (sent to you with your server name) into the appropriate fields.

- User training\< *Your StudentID*>
  - As an Example, you were given studentID *st01*, you would then type training\st01

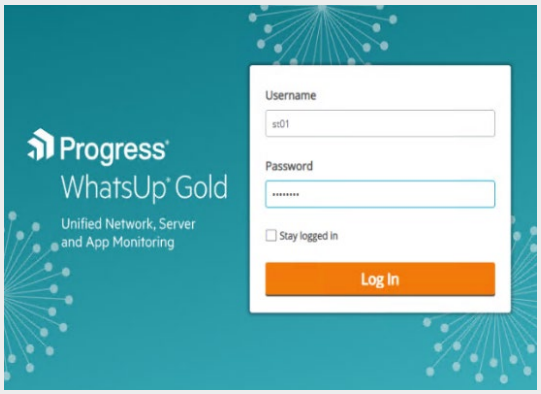
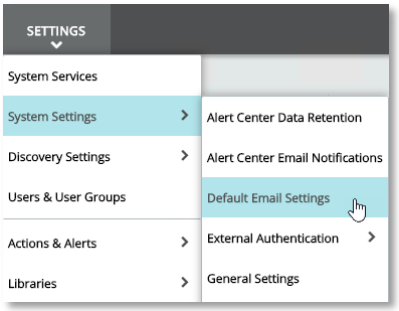


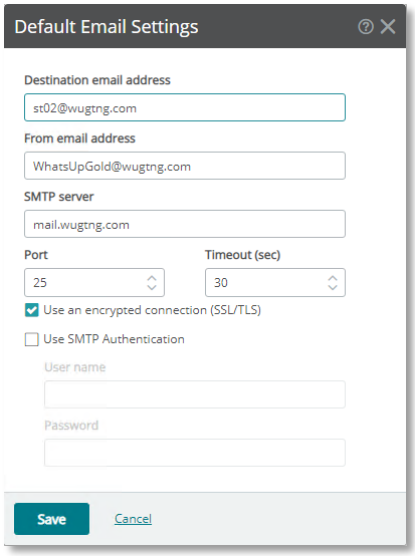
- Password: <the password you were given>

- Click Yes on when asked if you want to connect



i-4	Verify Connection	Once you are connected to the Desktop of your Apps server, look in the upper right-hand corner. • Make sure you see Hostname: <YourStudentID>-app where <YourStudentID> is the student number you just logged in with 
You are now connected to the ITE.		

Lab 1 - Default Email Settings		
1-1	Log in as your studentID	At the login Screen • Username: Your <studentID> ○ Use the student ID you were given, example: st01 • Password: <Your Student Password>  Don't forget to close the Welcome screen.
1-2	**Configure Email settings**	• Click the SETTINGS menu • Select System Settings • Select Email Settings  In the Email Settings Dialog • Destination email address: **Enter *YOUR* studentID followed by @wugtng.com** ○ For Example, ***if your*** studentID is st02, you would enter st02@wugtng.com • From: WhatsUpGold@wugtng.com • SMTP: **mail.wugtng.com** • Port: **25** • Use an encrypted connection (SSL/TLS): checked • Click Save

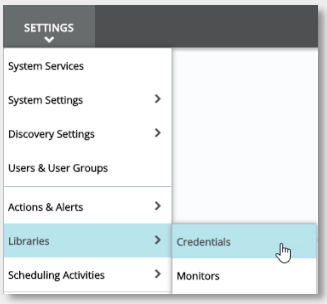
		

You have now completed Lab 1 – External Authentication and Email Settings.

Lab 2 - Adding Credentials

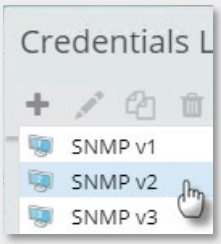
2-1 Add SNMP v2 Credential

- Click Settings Menu: Libraries: Credentials



In the Credentials Library

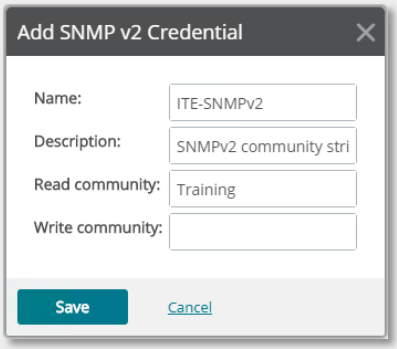
- Click add ✚



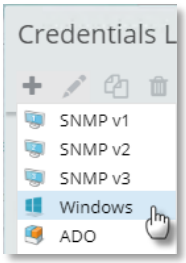
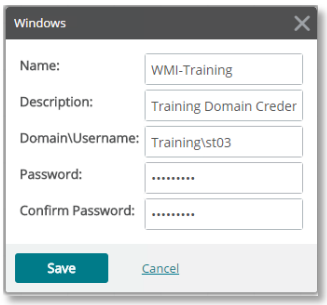
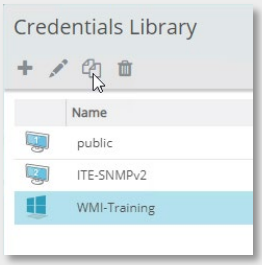
- Select SNMPv2

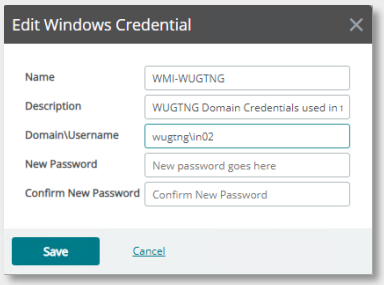
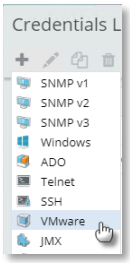
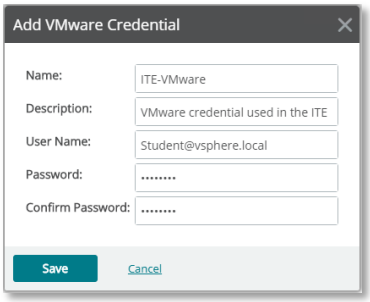
In the SNMPv2 dialog

- Name: **ITE-SNMPv2**
- Description: **SNMPv2 community string used in the ITE**
- Read community: **Training**



- Write community: (leave blank)
- Click Save

2-2	Add WMI credentials for the Training Domain	In the credential library • Click add ✚  • Select Windows In the Windows dialog • Name: **WMI-Training** • Description: **Training Domain Credentials used in the ITE** • Domain\Username: **Training\<studentID>** • Password: <password> ○ (*** password given to login into your server) • WMIConfirm Password: <password> ○ (*** password given to login into your server)  • Click Save •
2-3	Add WMI credentials for the wugtng domain	In the credential library • Select the Windows Credential you just created ○ And **click** copy 

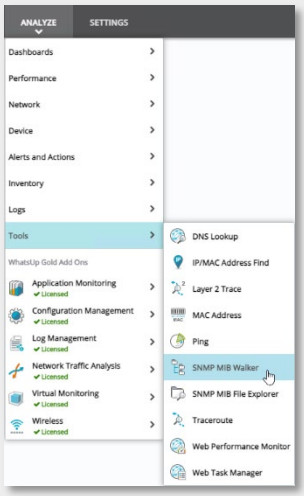
		In the Edit Windows dialog • Change the following fields ○ Name: **WMI-WUGTNG** ○ Description: **WUGTNG Domain Credentials used in the ITE** ○ Domain\Username: **wugtng\<studentID>**  • Click Save
2-4	Add VMware Credentials	In the credential library • Click add ✚  • Select VMware In the Windows dialog ***This is a unique username and password ***NOT your Student ID*** • Name: **ITE-VMware** • Description: **VMware credential used in the ITE** • Username: ***student@vsphere.local*** • Password: ***Training*** • Confirm Password: ***Training***  • Click Save
2-5	Close the credential library	• Click the X in the upper right-hand corner of the Credential Library to close it.
You have now completed Lab 2 - Adding Credentials.		

Lab 3 – Add Active Monitors

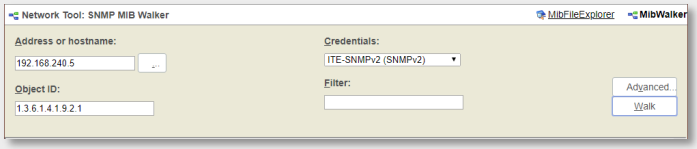
3-1 Open MIB Walker

On the Menu Bar

- Click ANALYZE
- Mouse over Tools
- Click on MIB Walker

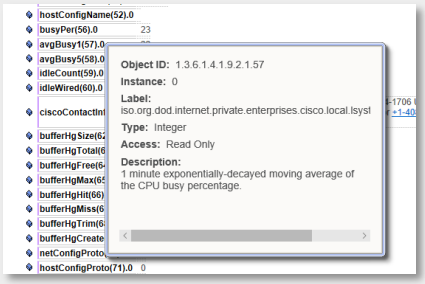
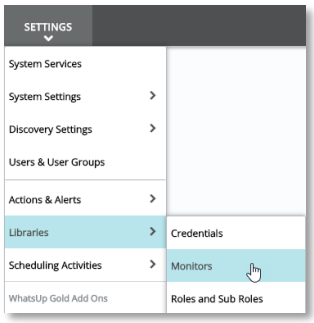
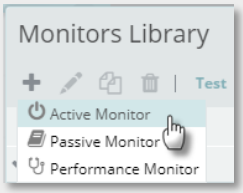


- In the Network Tool: SNMP MIB Walker dialog: Under "Address or hostname:" type: **192.168.240.5**
- Credentials: **Training (SNMPv2)**
- Object ID: **1.3.6.1.4.1.9.2.1**
- Click the Walk button to retrieve all the objects and their OIDs for this Cisco Catalyst switch.



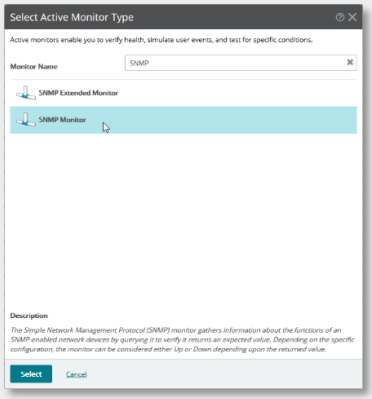
- Once the Stop button is greyed out
  - Scroll these 69 results to locate the entry for avgBusy1(57).0 this is near the bottom of the list.
  - Hover your cursor until a popup window appears.

    Note: this *may or may* not pop up in your browser. If it doesn't, continue on to next step.

		○ This contains information about that object, including Object ID (OID), Instance, Label, Type, Access and Description. Read the Description for the object, then copy the Object ID (with your mouse – right-click - Copy). 
3-2	Open Monitor Library	On the Menu bar • Click on Settings • Mouse over libraries • Click Monitors 
3-3	Create new SNMP Monitor	In the Monitor library dialog • Click the plus ✚ • Select Active Monitor 

In the Select Active Monitor Type dialog

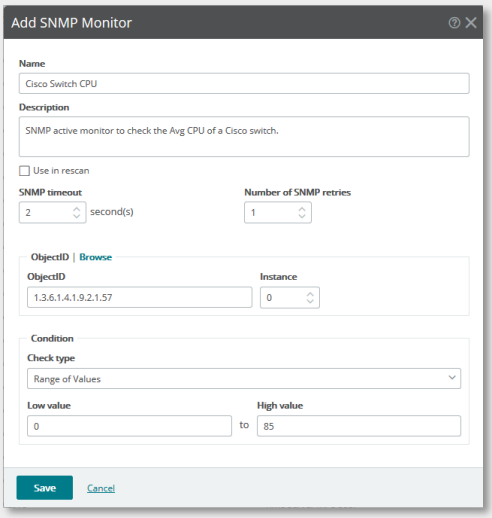
- Type **SNMP** in the search text box then **select SNMP Monitor** from the list

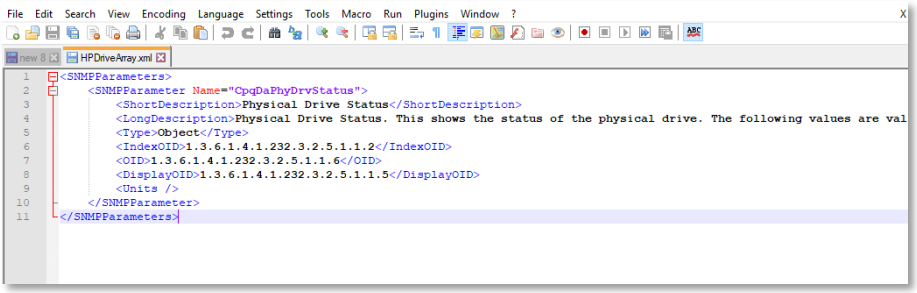


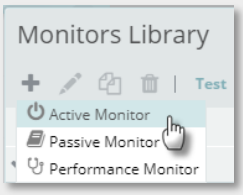
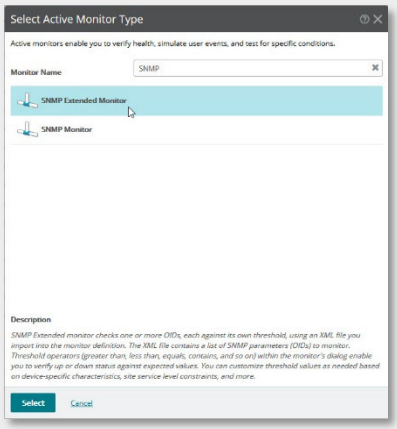
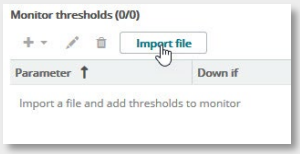
- Click Select

In the Add SNMP Monitor Dialog

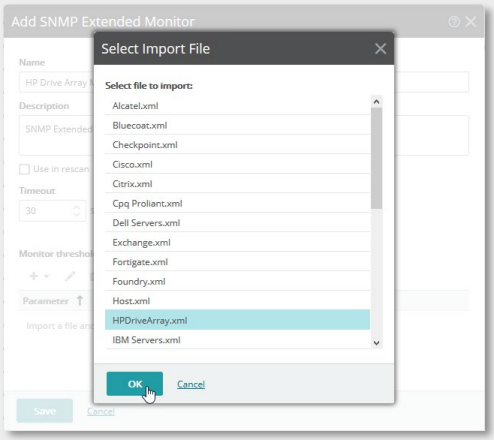
- Name: **Cisco Switch CPU**
- Description: **SNMP active monitor to check the Avg CPU of a Cisco switch.**
- Object ID: (paste the OID you copied) Or Type: **1.3.6.1.4.1.9.2.1.57**
- Instance: **0**
- Check Type: Range of Values
  - Low value: **0**
  - High value: **85**
- Click Save to save Service monitor to the library



3-4	Create New SNMP Extended Monitor HTML file	Open Notepad ++ or Notepad.exe • Copy the below text and then paste into the blank document <SNMPParameters> <SNMPParameter Name="CpqDaPhyDrvStatus"> <ShortDescription>Physical Drive Status</ShortDescription> <LongDescription>Physical Drive Status. This shows the status of the physical drive. The following values are valid for the physical drive status: Other (1) Indicates that the instrument agent does not recognize the drive. You may need to upgrade your instrument agent and/or driver software. Ok (2) Indicates the drive is functioning properly. Failed (3) Indicates that the drive is no longer operating and should be replaced. predictiveFailure(4) Indicates that the drive has a predictive failure error and should be replaced. If you suspect a problem, run Compaq Diagnostics.</LongDescription> <Type>Object</Type> <IndexOID>1.3.6.1.4.1.232.3.2.5.1.1.2</IndexOID> <OID>1.3.6.1.4.1.232.3.2.5.1.1.6</OID> <DisplayOID>1.3.6.1.4.1.232.3.2.5.1.1.5</DisplayOID> <Units /> </SNMPParameter> </SNMPParameters>  • Save the file as HPDriveArray.xml to desktop • To connect to the WUG server ○ Double click on the WUG RDP shortcut on your desktop  ○ When it opens ▪ Use your StudentID and password • Paste HPDriveArray.xml to WUG Server desktop • Open Windows file explorer and navigate to: ○ C:\Program Files (x86)\Ipswitch\WhatsUp\Data\ SNMPExtended • Drag and drop the HPDriveArray.xml file into the SNMPExtended directory ○ Click continue on the UAC denied access dialog • Return to your App Server.

3-5	Create New SNMP Extended Monitor	In the Monitor library dialog • Click the plus ✚ • Select Active Monitor  In the Select Active Monitor Type dialog • Type **SNMP** in the search text box then **select SNMP Extended Monitor** from the list  • Click **Select** In the Add SNMP Extended Monitor Dialog • Name: **HP Drive Array Monitor** • Description: **SNMP Extended Monitor for an HP Drive Array** • **Uncheck** Use in rescan • Click Import File 

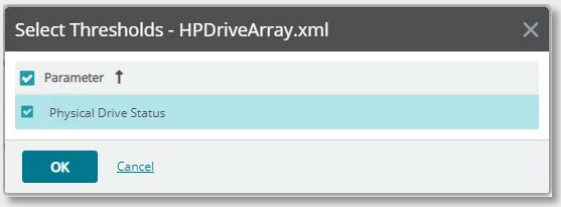
- In the Select Import File dialog
  - Select **HPDriveArray.xml** in the drop down



  - Click OK

In the Select Thresholds – HPDriveArray.xml Dialog

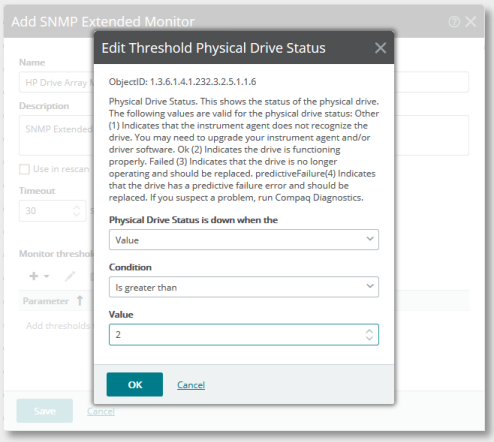
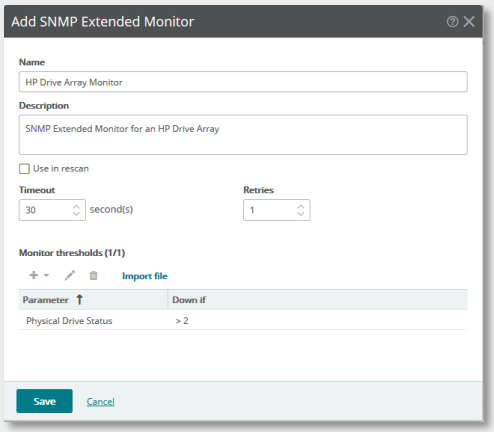
- Select Physical Drive Status



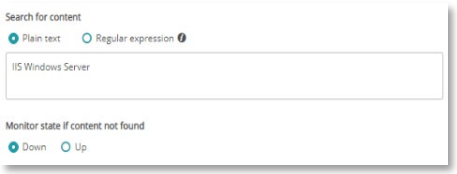
- Click OK

Under the Monitor thresholds (1/1) section

- Select Physical Drive Status
- Click Edit

		• In the Edit Threshold Physical Drive Status dialog
		  ○ Physical Drive Status is down when the: **value**
		  ○ Condition: **is greater than**
		  ○ Value: **2**
		 
		
		  ○ Click OK
		 
		
		• Click Save to save monitor to library

3-6	Create New Http Content Monitor	In the Monitor library dialog • Click the plus ✚ • Select **Active Monitor** In the Select Active Monitor Type dialog • Type HTTP in the search text box then **select HTTP Content Monitor** • **Click** Select In the Add HTTP Content Monitor Dialog • Name: **App Web Site Content Monitor** • Description: **HTTP Content Monitor to check the contents of app server web site** • **Uncheck** Use in rescan

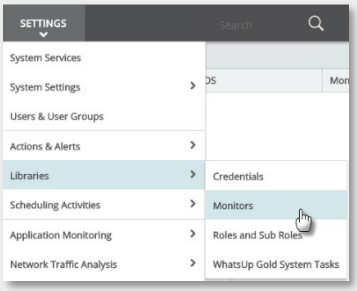
		• In the HTTP Server section ○ Change URL to http://app  • Scroll down to the Search for content section ○ Select Plain text ○ Enter the text **IIS Windows Server** ○ Monitor state if content not found ▪ Ensure **Down** is selected  ○ Click OK to save
You have completed Lab 3 – Active Monitors		

Lab 4 - Performance Monitors

4-1 Open the Monitor Library

The Monitor library should still be open, if not:

- Click on Settings
- Mouse over libraries
- Click Monitors



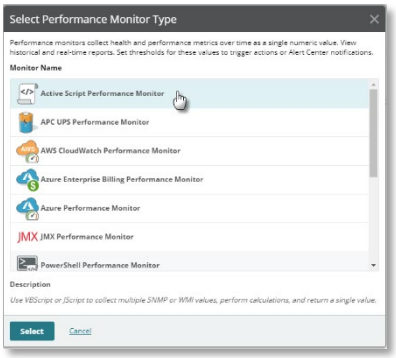
4-2 Create Active Script Performance monitor using two reference variables

In the Monitor library

- Click the plus
- Select Performance Monitor

In the Select Performance Monitor Type dialog

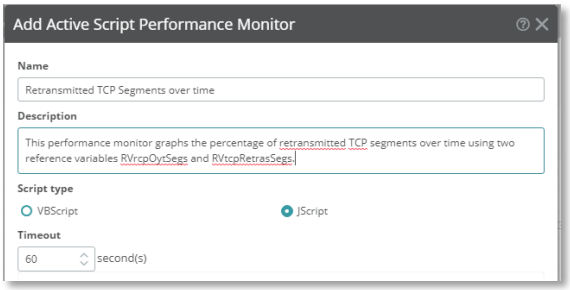
- In the drop down select **Active Script Performance Monitor**



- Click Select

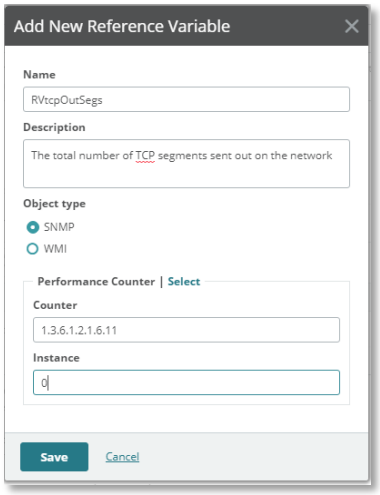
In the Add Active Script Performance Monitor Dialog

- Name: **Retransmitted TCP segments over time**
- Description: **This performance monitor graphs the percentage of retransmitted TCP segments over time using two reference variables: RVtcpOytSegs and RVtcpRetransSegs.**
- Script Type: **JScript**



In the Reference Variables Section

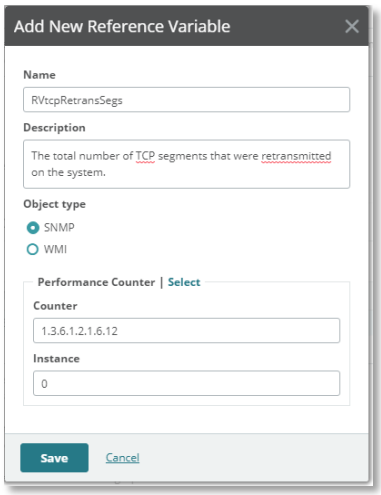
- Click the Add button ✚
- In the Add New Reference Variable dialog
  - Name: **RVtcpOutSegs**
  - Description: **The total number of TCP segments sent out on the network**
  - Object Type: **SNMP**
  - Counter: **1.3.6.1.2.1.6.11**
  - Instance: **0**



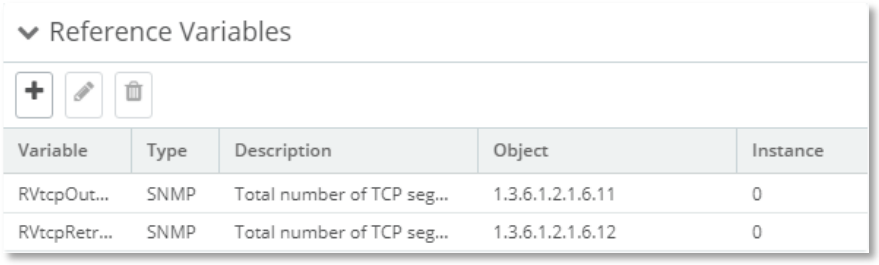
- Click Save

In the Reference Variables Section

- Click the Add button ✚
- In the Add New Reference Variable dialog
  - Name: **RVtcpRetransSegs**
  - Description: **The total number of TCP segments that were retransmitted on the system**
  - Object Type: **SNMP**
  - Counter: **1.3.6.1.2.1.6.12**
  - Instance: **0**



- Click Save



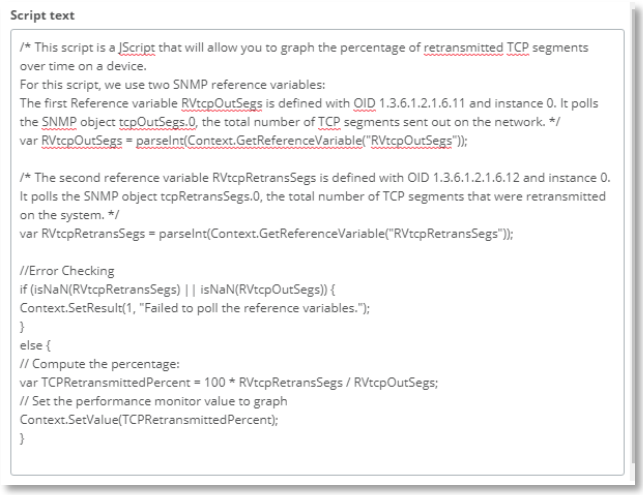
In the Script Text area

- Enter the following Script:

```
/* This script is a JScript that will allow you to graph the percentage of retransmitted TCP segments over time on a device. For this script, we use two SNMP reference variables: The first Reference variable RVtcpOutSegs is defined with OID 1.3.6.1.2.1.6.11 and instance 0. It polls the SNMP object tcpOutSegs.0, the total number of TCP segments sent out on the network. */
var RVtcpOutSegs = parseInt(Context.GetReferenceVariable("RVtcpOutSegs"));

/* The second reference variable RVtcpRetransSegs is defined with OID 1.3.6.1.2.1.6.12 and instance 0. It polls the SNMP object tcpRetransSegs.0, the total number of TCP segments that were retransmitted on the system. */
var RVtcpRetransSegs = parseInt(Context.GetReferenceVariable("RVtcpRetransSegs"));

//Error Checking
if (isNaN(RVtcpRetransSegs) || isNaN(RVtcpOutSegs)) {
Context.SetResult(1, "Failed to poll the reference variables.");
}
else {
// Compute the percentage:
var TCPRetransmittedPercent = 100 * RVtcpRetransSegs / RVtcpOutSegs;
// Set the performance monitor value to graph
Context.SetValue(TCPRetransmittedPercent);
}
```



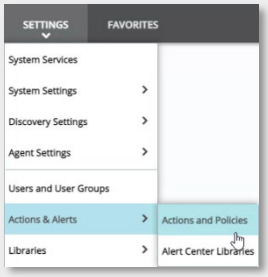
- Click Save

You have now completed Lab 4 – Performance Monitors.

Lab 5 - Actions

5-1 Open Actions and Policies Library

- Click the Setting menu
- Mouse over Actions & Alerts
- Select Actions and Polices



5-2 Create new Scripting Action

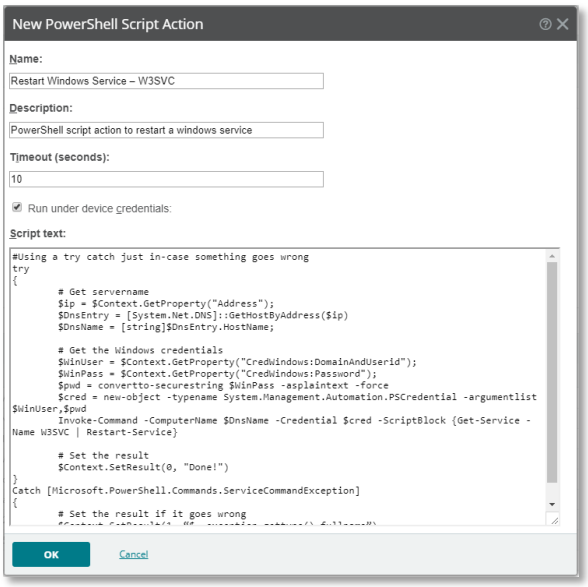
In the Action Library (bottom half have the dialog)

- Click the plus ✚
- Select **PowerShell**
- In the New PowerShell Script Action dialog
  - Name: **Restart Windows Service – W3SVC**
  - Description: **PowerShell script action to restart a windows service**
  - Timeout (seconds): **10**
  - Run under device credentials: **Checked**
  - Script text:

```
#Using a try catch just in-case something goes wrong
try
{
    # Get servername
    $ip = $Context.GetProperty("Address");
    $DnsEntry = [System.Net.DNS]::GetHostByAddress($ip)
    $DnsName = [string]$DnsEntry.HostName;

    # Get the Windows credentials
    $WinUser = $Context.GetProperty("CredWindows:DomainAndUserid");
    $WinPass = $Context.GetProperty("CredWindows:Password");
    $pwd = convertto-securestring $WinPass -asplaintext -force
    $cred = new-object -typename System.Management.Automation.PSCredential -
argumentlist $WinUser,$pwd
    Invoke-Command -ComputerName $DnsName -Credential $cred -ScriptBlock
{Get-Service -Name W3SVC | Restart-Service}

    # Set the result
    $Context.SetResult(0, "Done!")
}
Catch [Microsoft.PowerShell.Commands.ServiceCommandException]
{
    # Set the result if it goes wrong
    $Context.SetResult(1, "$_.exception.gettype().fullname")
}
```



- Click OK to save

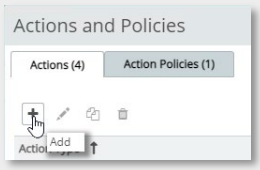
You have finished Lab 5 - Actions

Lab 6 - Add More Actions and Action Policies

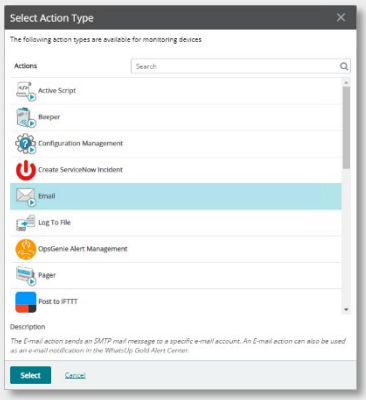
6-1 Create new State Change Email Action

In the Action Library, Actions Tab

- Click the plus ✚

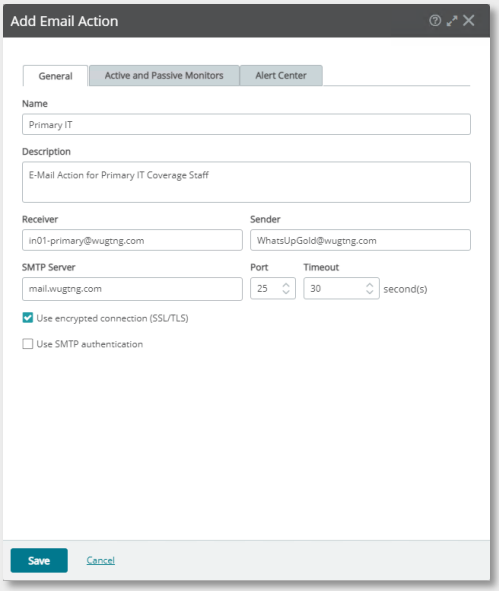


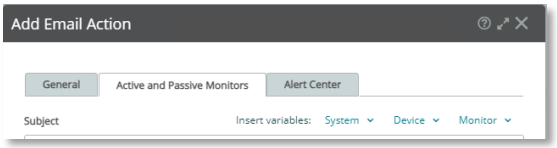
- Select **Email Action**

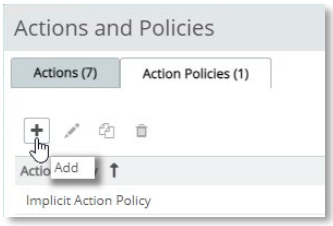
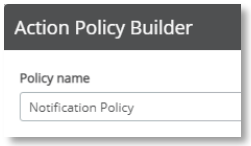


- In the New Email Action dialog General Tab:
  - Name: **Primary IT**
  - Description: **E-Mail Action for Primary IT Coverage Staff**
  - Mail to: <yourStudentID>-primary@wugtng.com
    - Example: st03-primary@wugtng.com

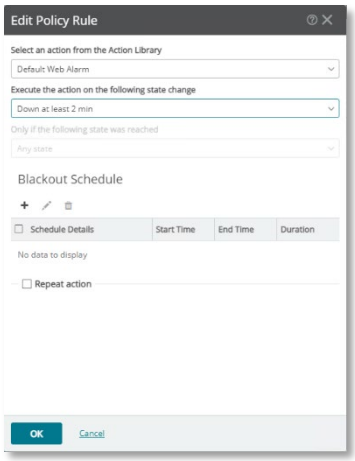
Note: The IMail server we use will automatically create a sub mailbox named whatever is following the – before the @ sign in your email address



6-2	Modify State Change Mail Content	At the top of New Email Action • Click the Active and Passive Monitors Tab  In the Subject: • Change it to %Device.DisplayName (%Device.Address) is %Device.WorstState - %Device.Status In the Message Body: • Replace the entire body with: %Device.HostName (%Device.Address) is %Device.State. Details: Monitors that are down include: %Device.ActiveMonitorDownNames Monitors that are up include: %Device.ActiveMonitorUpNames Contact: %Device.Attribute.Contact Location: %Device.Attribute.Location Notes on this device (from device property page): %Device.Notes --- This mail was sent on %System.Date at %System.Time By Ipswitch WhatsUp Gold • Click Save to save Primary IT Email Action
6-3	Create new Passive Email Action	In the Action Library, Actions Tab • Click the plus ✚ • Select Email Action • In the New Email Action dialog General Tab: ○ Name: **Passive** ○ Description: **E-Mail Action for Passive Monitors** ○ Mail to: <yourStudentID>-passive@wugtng.com ▪ Example: st04-passive@wugtng.com
6-4	Modify Passive Monitor Mail Content	At the top of New Email Action • Click the Active and Passive Monitors Tab In the Subject: • Change "%Device.Type is %Device.State (%Device.HostName)." to "%PassiveMonitor.DisplayName rcvd from %Device.DisplayName (%Device.Address)"

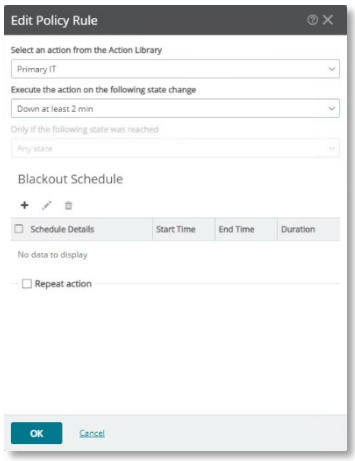
		In the Message Body: • Replace the entire contents with: %Device.HostName (%Device.Address) Details: %PassiveMonitor.Payload.* Notes on this device (from device property page): %Device.Notes ---------- This mail was sent on %System.Date at %System.Time Ipswitch WhatsUp Gold • Click Save to save Passive Monitor Email Action
6-5	Create new Secondary IT Email Action from the Primary IT action	In the Actions and Policies Library Dialog Actions Tab • Select the Primary IT Email Action • Click **Copy** • In the "Edit Email Action" dialog General Tab: ○ Name: **Secondary IT** ○ Description: **E-Mail Action for Secondary IT Coverage Staff** ○ Mail to: <YourStudentID>-secondary@wugtng.com ▪ Example: st10-secondary@wugtng.com • Click Save to save Secondary IT monitor Email Action
6-6	Add Email Notification Action Policy	• On the Action Policies Tab at the top ○ Click the ✚  • In the Action Policy Builder dialog ○ Policy Name: **Notification Policy** 

- Click Add…
- In the “Select an action from the Action Library:” drop down
  - Select **Default Web Alarm**
- In the Execute the action on the following state change: drop down
  - Select **Down at least 2 min**

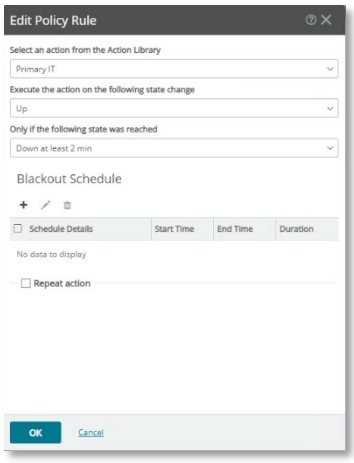
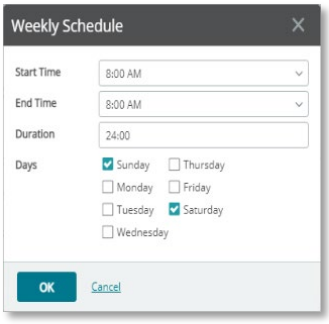


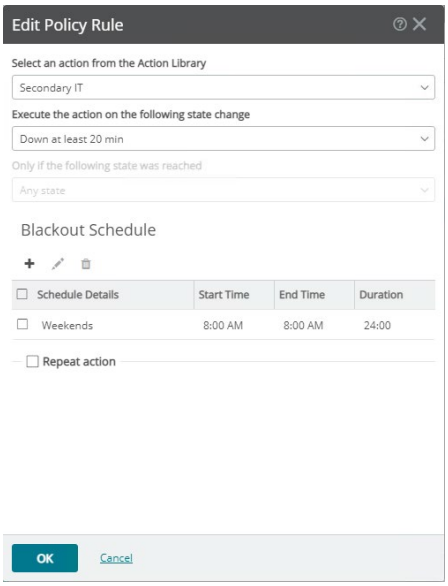
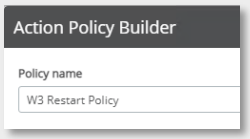
- Click OK

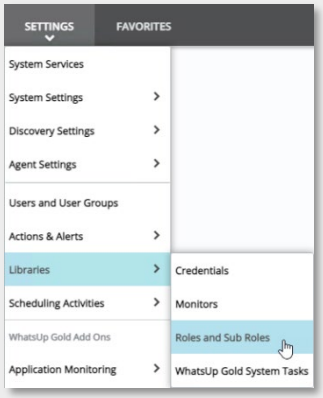
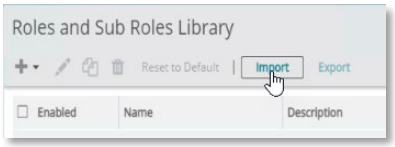
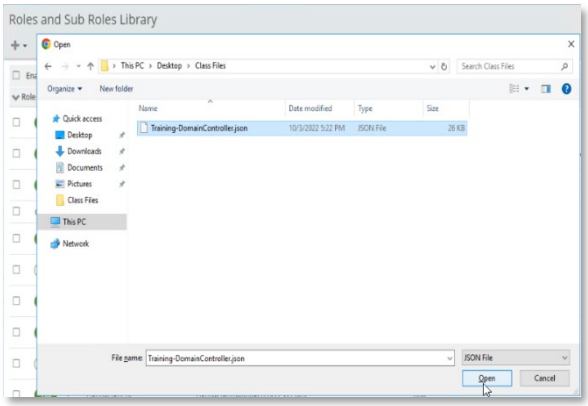
- Click Add…
- Select: Select an action from the Action Library
- In the “Select an action from the Action Library:” drop down
  - **Select Primary IT**
- In the Execute the action on the following state change: drop down
  - Select **Down at least 2 min**



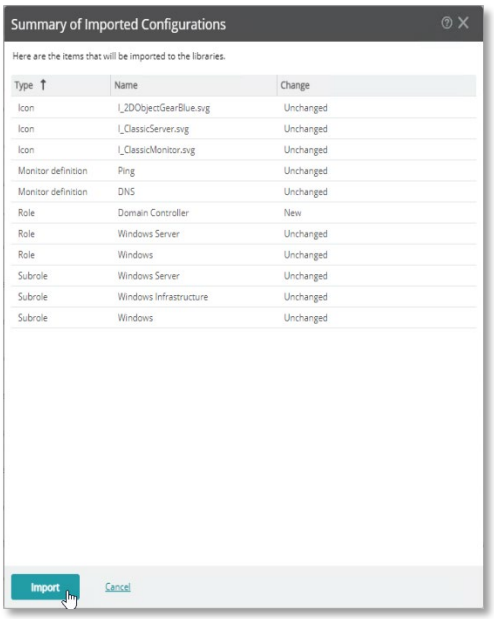
- Click OK

		○ Click Add… ○ In the “Select an action from the Action Library:” drop down ▪ Select **Primary IT** ○ In the Execute the action on the following state change: drop down ▪ Select **Up** ○ In the Only if the following state was reached: ▪ Select **2 minutes – (Down at least 2 min)**  ○ Click OK ○ Click Add… ○ In the “Select an action from the Action Library:” drop down ▪ Select **Secondary IT** ○ In the Execute the action on the following state change: drop down ▪ Select **Down at least 20 min** ○ Click Add in the Blackout Schedule Section ▪ In the Weekly Schedule dialog • Start time: **08:00 AM** • End time: **08:00 AM** • Check **Sunday and Saturday**  • Click OK

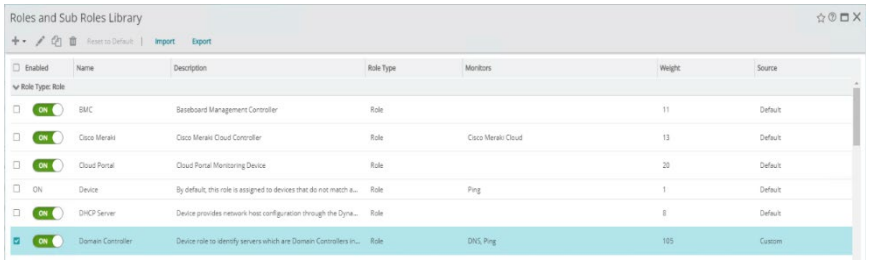
		 • Click OK Click Save to save to close the New Action Policy Window
6-7	Add W3 Service Restart Action Policy	On the Action Policies Tab at the top • Click the ✚ • In the Action Policy Builder Window ○ Policy Name: **W3 Service Restart Policy**  ○ Click Add… • In the Edit Policy Rule Dialog ○ In the “Select an action from the Action Library:” drop down ▪ Select **Restart Windows Service – W3SVC** ○ In the Execute the action on the following state change: drop down ▪ Select **Down at least 2 min** ○ Click OK • Click Save • Close the Actions and Policies Library window
You have now completed Lab 6 – More Actions and Action Policies		

Lab 7 - New Device Roles		
7-1	Open Role and Sub Role Library	On the Menu bar • Click on Settings • Mouse over libraries • Select Roles and Sub Roles 
7-2	Import Domain Controller role	In Roles and Sub Roles Library • Click Import  • In the file selector dialog ○ Navigate to **Desktop, Class files** ▪ **Select** Training-DomainController.json ▪ **Click Open** 

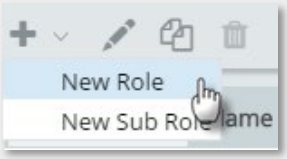
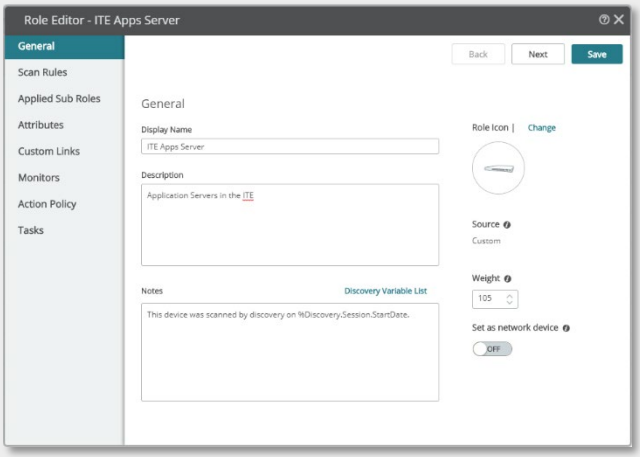
- Review the Summary of Imported Configurations dialog
  - Unchanged items already exist in WhatsUp Gold
  - New will be added to WhatsUp Gold
  - Modified are items that exist but will be changed.
- Click Import



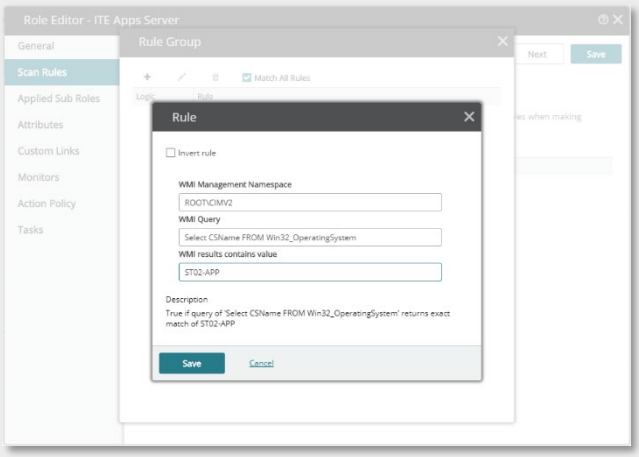
- Close the Roles and Sub Roles Library, then open it back up
  - Verify the Domain Controller now exists in the library



- Edit the Domain Controller Role to view the role's settings
- When you are satisfied, close the Role wizard

7-3	Create new role for Apps server	In Roles and Sub Roles Library • Click the Plus and select New Role  • In the Role Editor – New Role: General Tab ○ Name: **ITE Apps Server** ○ Description: **Application Servers in the ITE** ○ Weight: **105**  • Click Next or on the Scan Rules tab • On the Scan Rules tab ○ Click the Add button • On the Rule Group dialog ○ Click Add • On the Select a Rule Type ○ Scroll down and select **WMI query result(s) is** ○ Click Ok • On the Rule dialog ○ In the WMI Query text box ▪ Type**: Select CSName FROM Win32_OperatingSystem** ○ In the WMI results contains value ▪ Type: **<*your studentID*>-APP** Note: This needs to be in all caps

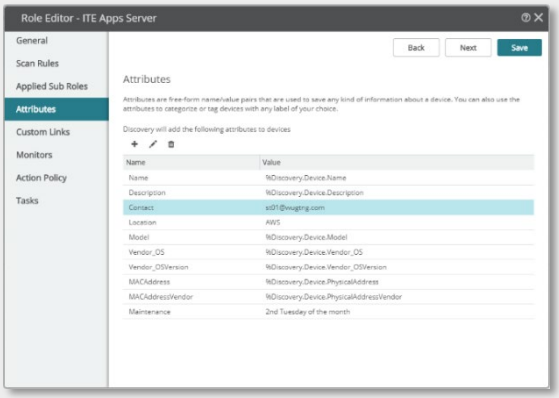
As an example, if *your* student ID is St02, you will enter ST02-APP



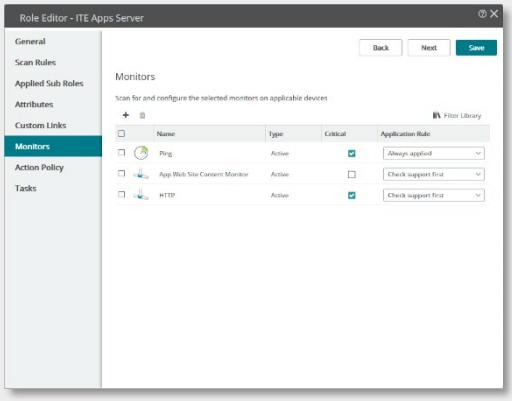
- Click Save
- Close the Rule Group Dialog by clicking the X in the upper right-hand corner of the dialog

- Click Next or on the Applied Sub Roles
- On the Applied Sub Roles tab click Add (✚) button
- In the Add Applied Sub Role dialog
  - Select (check the check boxes)
    - AWS Resource
    - Windows Infrastructure
    - Windows Server
  - Click OK
- Click Next or on the Attributes tab
- On the Attributes Tab
  - Click Add
- On the Add Attribute dialog
  - Enter
    - Name: **Maintenance**
    - Value: **2nd Tuesday of the month**
  - Click OK
- On the Attributes Tab
  - Click Add
- On the Add Attribute dialog
  - Enter
    - Name: **PzAlert-Drive-C:**
    - Value: **40**

- Click OK

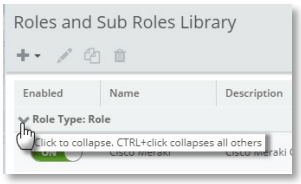
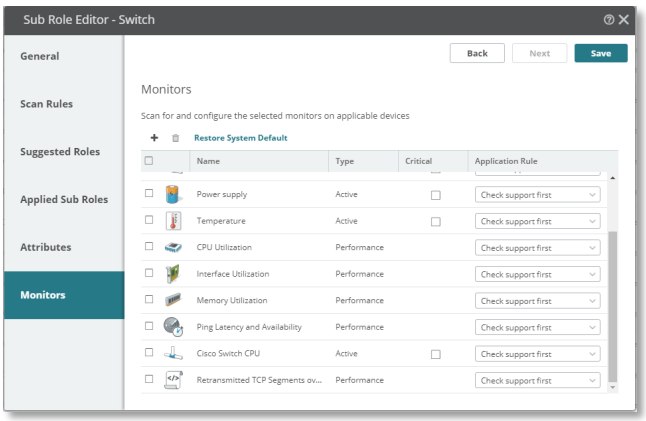


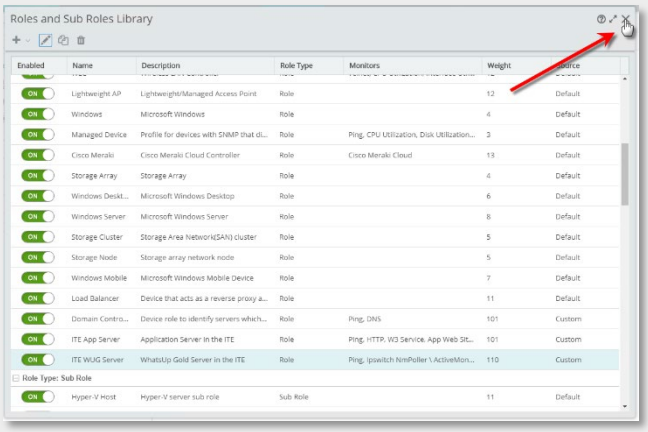
- Click Next or on the Monitors tab:
- On the Monitors tab
  - Click the Add (+) button
- In the Monitors dialog
  - Under the type: Active, select (check the check box)
    - HTTP (Hypertext Transfer Protocol (Web Server))
    - App Web Site Content Monitor
  - Click OK
- On the Monitors tab monitors list
  - Ping
    - Check Critical
    - Set to always applied
  - HTTP
    - Critical checked
    - Set to Check support first
  - App Web Site Content Monitor
    - Critical *NOT* checked
    - Set to Check support first



- Click Next or on the Action Policy Tab
- On the Action Policy Tab
  - In the Action Policy dropdown
    - Select Notification Policy

- Click Save

7-4	Edit default switch sub role	In Roles and Sub Roles Library • Click the ❯ to collapse the Role section  • In the Sub Role section ○ Scroll down and select the Switch sub role ○ Click on the Edit button • Click the Monitors tab • On the Monitors tab ○ Click the Add (+) button • In the Monitors dialog ○ Under the type: Active, select ▪ **Cisco Switch CPU** ○ Under the type: Performance, select ▪ **Retransmitted TCP Segments over time** ○ Click OK • On the Monitors tab monitors list ○ Cisco Switch CPU ▪ Critical ***NOT*** checked ▪ Set to check support first ○ Retransmitted TCP Segments over time ▪ Set to Check support first  • Click Save

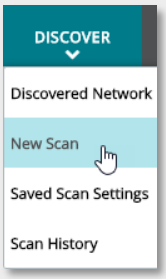
7-5	Close the Roles and Sub Roles Library	Click the X in the upper right-hand corner of the Roles and Sub Roles Library dialog box. 
You have now completed Lab 7 - New Device Roles.		

Lab 8 - Network Discovery

8-1 Schedule a Scan

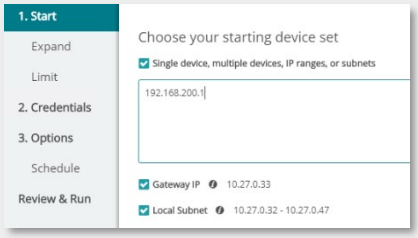
On the Main Menu Bar

- Click Discover
- Then Click New Scan

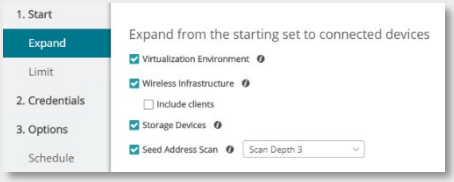


In the Discovery Scan Dialog

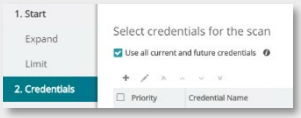
- On the Start Tab
  - Check Single device, multiple devices, IP ranges, or subnets
  - Type in the text box
    - **192.168.200.1**
  - Leave Gateway IP and Local Subnet checked



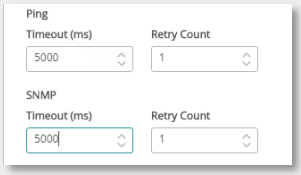
- Click Next or on the Expand tab
  - Ensure **All check boxes are checked EXCEPT Include Clients**



- Click Next or on the Credentials tab
  - **Verify** Use Current and future credentials is checked

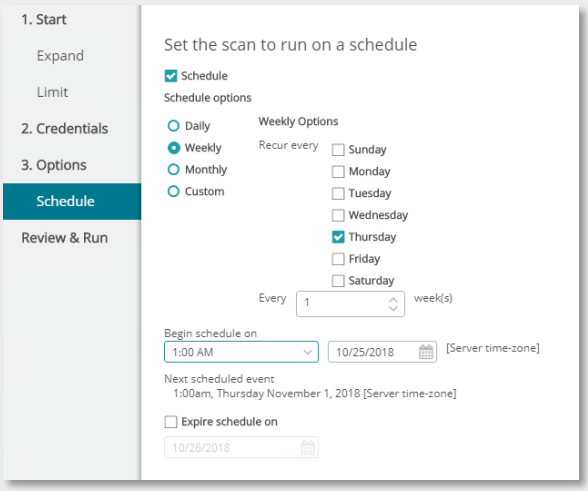


- Click Next or on the Options tab
  - **Increase** the Ping and SNMP Timeouts to **5000 ms**

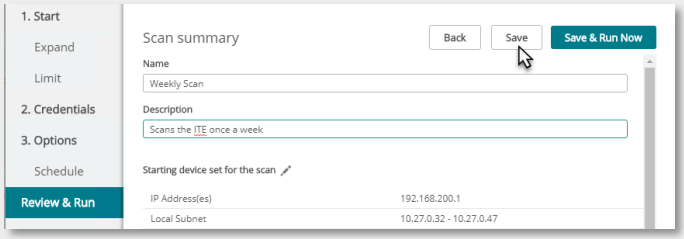


- Click Next or on the Schedule tab
  - Check Schedule
  - Under Schedule Options
    - Select Weekly
      - Schedule your scan based on the Table below (your instructor may change the times based on Non-US classes)

Student ID	Day	Time (GMT)
St01 / St16	Tomorrow (Thursday)	12:00 AM
St02 / St17	Tomorrow (Thursday)	12:30 AM
St03 / St18	Tomorrow (Thursday)	1:00 AM
St04 / St19	Tomorrow (Thursday)	1:30 AM
St05 / St20	Tomorrow (Thursday)	2:00 AM
St06 / St21	Tomorrow (Thursday)	2:30 AM
St07 / St22	Tomorrow (Thursday)	3:00 AM
St08 / St23	Tomorrow (Thursday)	3:30 AM
St09 / St24	Tomorrow (Thursday)	4:00 AM
St10 / St25	Tomorrow (Thursday)	4:30 AM
St11 / St26	Tomorrow (Thursday)	5:00 AM
St12 / St27	Tomorrow (Thursday)	5:30 AM
St13 / St28	Tomorrow (Thursday)	6:00 AM
St14 / St29	Tomorrow (Thursday)	6:30 AM
St15 / St30	Tomorrow (Thursday)	7:00 AM
*** Times are based on Server Time-Zone (GMT)		



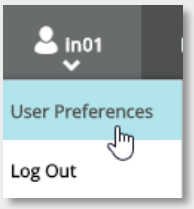
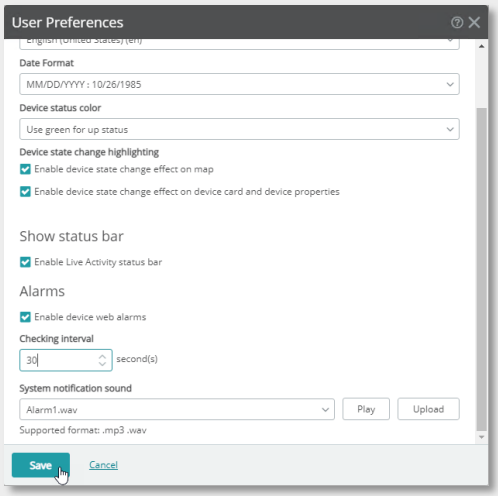
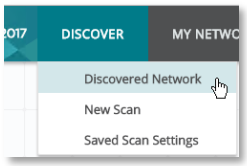
- Click Next or on the Review & Run tab
  - Name – **Weekly Scan**
  - Description – **Scans the ITE once a week**
  - Click Save



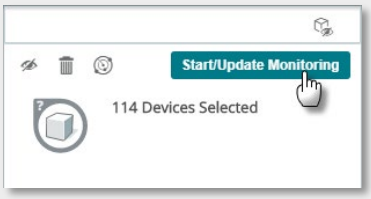
- Close the new scan dialog.

You have now completed Lab 8 - Network Discovery.

Lab 9 - Start Monitoring

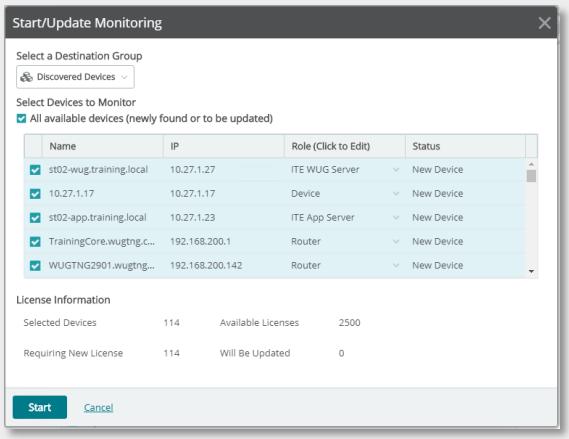
9-1	Change Web Alarm Checking Interval	On the WhatsUp Gold Menu bar • Click on the UserID menu ○ Select User Preferences  In the User Preferences dialog • Change the Alarms Checking Interval to **30** second(s) • Click Save 
9-2	Open Discover Network	Click The discover Menu • Select Discovered Network 
9-3	Start monitoring devices	In Discovered Devices list • Check the top box of the list to select all your devices 

- In the information Card
  - Click Start/Update Monitoring

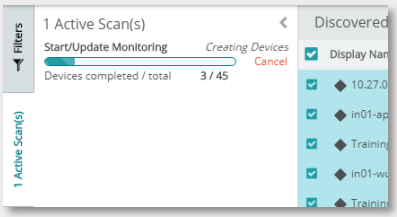


In the Start/Update Group dialog

- Click Start



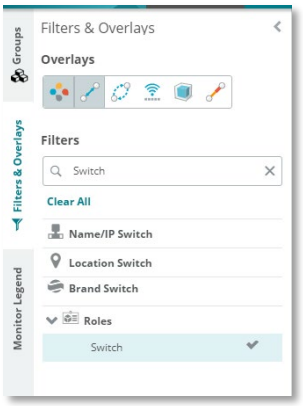
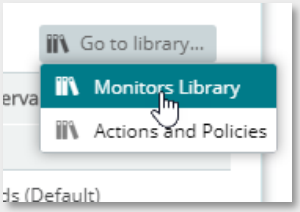
- You will notice the Start/Update Monitoring scan will show up in the Active Scan(s) tab

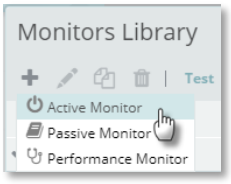
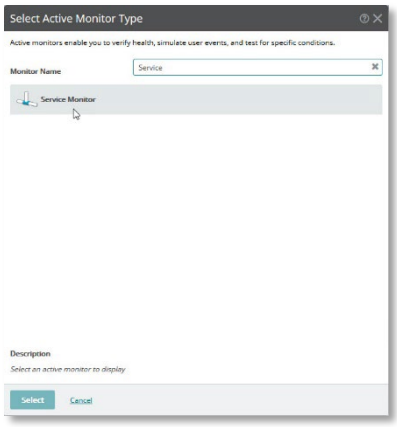
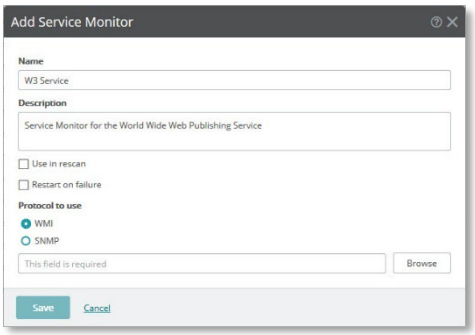


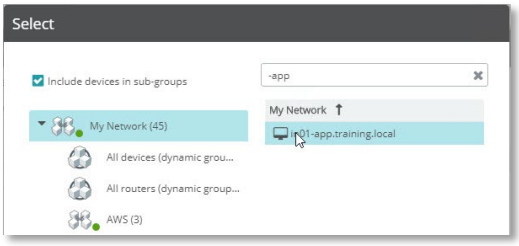
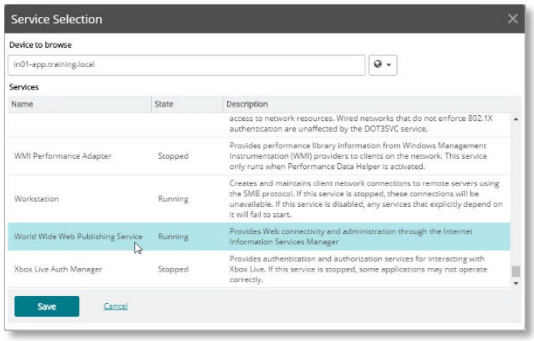
- Click My Network Button in the menu bar

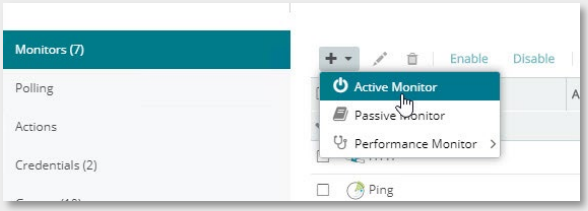
Notice device will start populating in the My Network Map/List

Once all your devices are being monitored, you can proceed to the next step

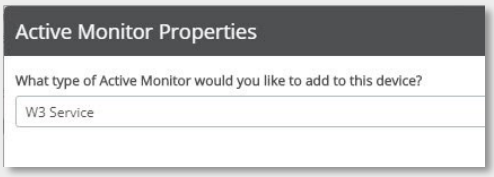
9-4	Verify Role and Sub Role Applications	In the My Network • Click on the Filters & Overlays tab • Apply Switch Role filter ○ In the filter text box type: **Switch** ▪ In the Roles • **Select Switch** to apply the filter  ○ Open a Switch's device properties ▪ Verify that the custom Active Script monitors were added to the Cisco Switches • Clear Filters • Apply Domain Controller Role Filter ○ In the filter text box type: Domain Controller ▪ In the Roles • Select Domain Controller to apply filter ○ Open a Device's device properties ▪ Verify everything which was supposed to be applied was applied • Clear Filters • Apply ITE App Server Role Filter ○ On the Filters and Overlays tab ▪ Start typing ITE Apps Server in the filter text box ▪ Under Roles • Select ITE Apps Server ○ Open you App Server's device properties ▪ Verify everything which was supposed to be applied was applied • Don't close the device properties
9-5	Open Monitor Library	On the Monitors tab on the far-right side • Click on Go to library… menu button ○ Click Monitors Library 

9-6	Create new Service Monitor	In the Monitors Library • Click on the Plus ✚ and select Active Monitor  In the Select Active Monitor Type dialog • Type **Service** in the search text box then **select Service Monitor** from the list  • Click **Select** In the Add Service Monitor Dialog • Name: **W3 Service** • Description: **Service Monitor for the World Wide Web Publishing Service** • **Uncheck** Use in rescan • Protocol to use: Select **WMI**  • Click the Browse button

		• In the Service Selection dialog
		  ○ Click Browse in the browse for device dropdown
		 
		• In the Select Dialog Search text box
		  ○ Enter **-app**
		  ○ Select your App server in the device list
		 
		  ○ **Click** Apply
		• Back in the Service Selection dialog
		  ○ Scroll down and select World Wide Web Publishing Service
		 
		  ○ **Click** Save
		• **Click** Save
		• Close the Monitors Library

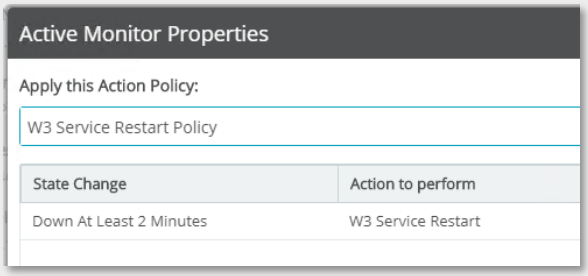
9-7	Add additional Monitor to App Server	Still in the Device Properties dialog on the Monitors tab • Click the Add Button and select Active Monitor  • In the Active Monitor Properties Dialog ○ In the What type of Active Monitor would you like to add to this device? Dropdown

- Select **W3 Service**



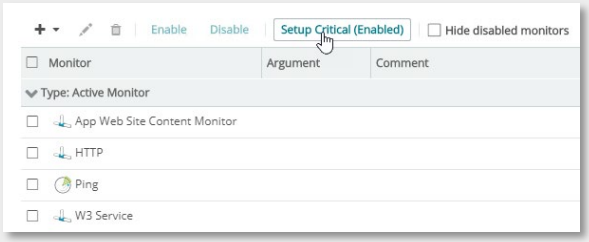
- **Click** Next
- **Review** the monitor settings then **click** Next

- In the Apply this Action Policy drop down
  - Select W3 Service Restart Policy

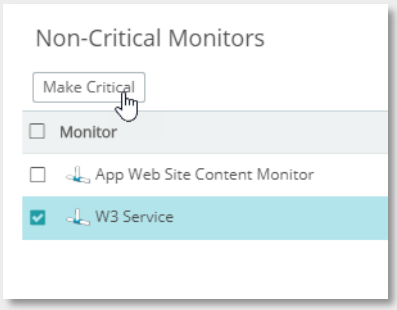


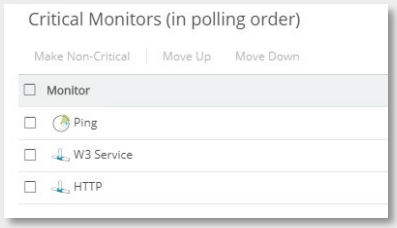
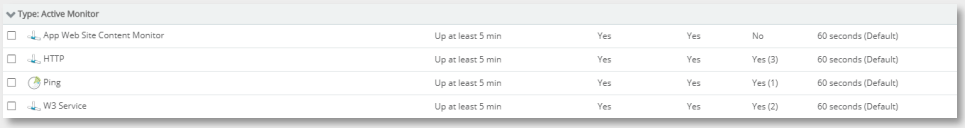
  - Click Finish
- Close the device properties

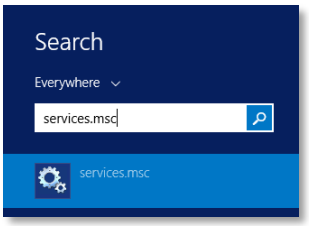
- Click **Setup Critical (Enabled)** to open the Critical Active Monitor Setup dialog

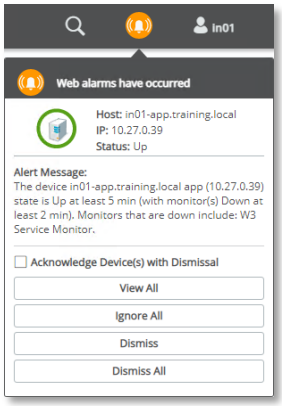


- In the Critical Active Monitor Setup dialog
  - Select W3 Service and click Make Critical button



		• Under the Critical Monitors section
		  ○ Using the Move Up or Move down buttons, arrange the monitors
		  ▪ Ping
		  ▪ W3 Service
		  ▪ HTTP
		 
		
		• Click Ok
		• Critical Monitors are now set with the proper order
		 

9-8	Verify Actions and Action Policies	On your ***App Server,*** the one you are RDP'd to
		• Open the Windows Service manager by
		  ○ clicking the Start Button
		  ○ Then type Services.msc
		  ○ Click on the Services Icon that appears below the search box
		 
		
		• In the Services manager
		  ○ Scroll to the bottom of the services list
		  ○ Select the World Wide Publishing Service
		  ○ Click Stop Service
		 
		
		• Return to WhatsUp Gold Web Interface
		  ○ Clear all filters from the My Network Map

		• After two minutes (plus the web interface interval), you should see a large popup window on your screen, as the web alarm action triggers
		 
		
		• Click the Dismiss button on the Web Alarm
		• Go into the web mail
		  ○ Open another web browser tab
		  ▪ Enter url: mail.wugtng.com
		  ○ Enter your email address and student password
		  ○ Verify Down Notification was sent
		• In Windows Services Manager
		  ○ *Verify* World Wide Web Publishing Service Restarted
		• Back in Web Mail
		  ○ Verify Up Notification was sent
		• Return to WhatsUp Gold Web Interface

You now completed Lab 9 - Start Monitoring.		

Lab 10 - Place Device into and out of Maintenance using Swagger

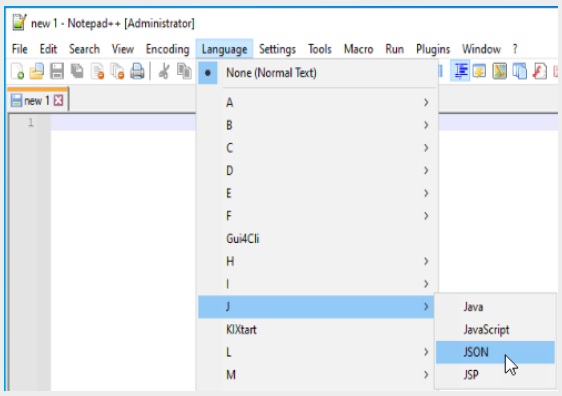
10-1 Create JSON data to use

Open Notepad ++

If Notepad ++ is not on a blank page, click File: New

On the New page in Notepad ++

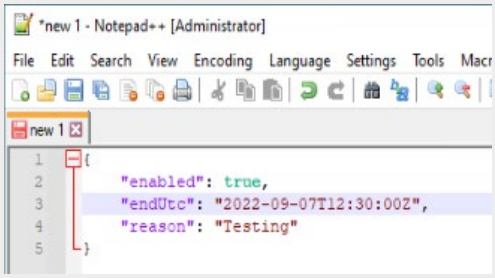
- Change the page language to JSON by clicking Language on the menu bar
  - Then mouse over the letter J
  - Click JSON

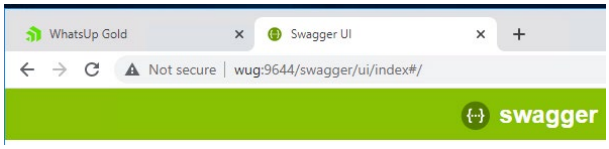
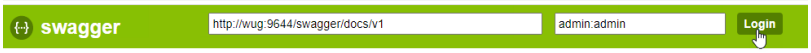
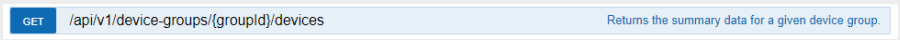
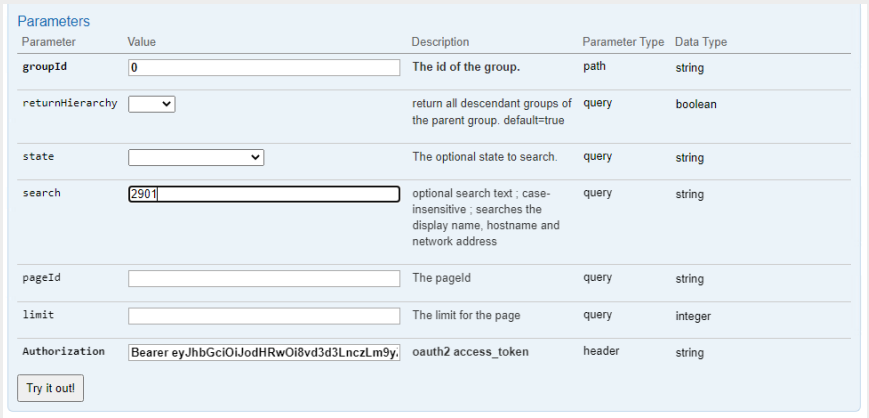


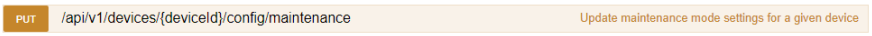
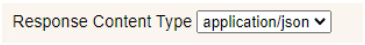
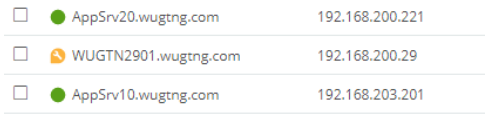
- Type the following in the window
  {
  “enabled”: true,
  “endUtc”: “

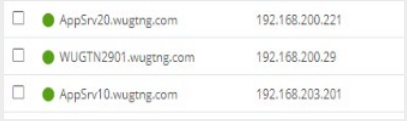
- After the “endUtc”: “
  - Enter tomorrow’s date in the format of “yyyy-mm-dd
    - Followed by a T
    - Then the time in the format of “hh:mm:ss
    - Followed by a Z
  - So, it would look like
    - 2022-09-15T12:30:00Z”,
- Finish up the file with
  "reason": "Testing"
  }

- When competed it should look like

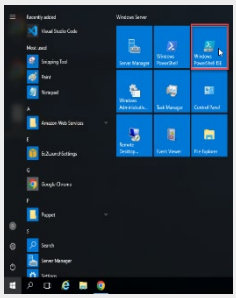
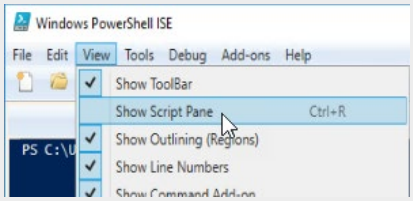
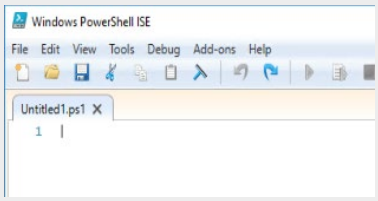


10-2	Login to API using Swagger UI	In the Web Browser, • open and other tab and type: http://wug:9644/swagger/ui/index#/  • Click the Login button at top right  • You should receive the following message ○ login was successful, you have a token now!
10-3	Get DeviceID for specific device	• Click on DeviceGroup to expand the device group section  • In the groupID value textbox, **type** zero (0) • In the search value textbox, **type** 2901  • **Click** Try it out! • Scroll down and view the Response Body ○ Take note of the “id”: value  Note: the device id returned may ***NOT*** be the same as the one pictured

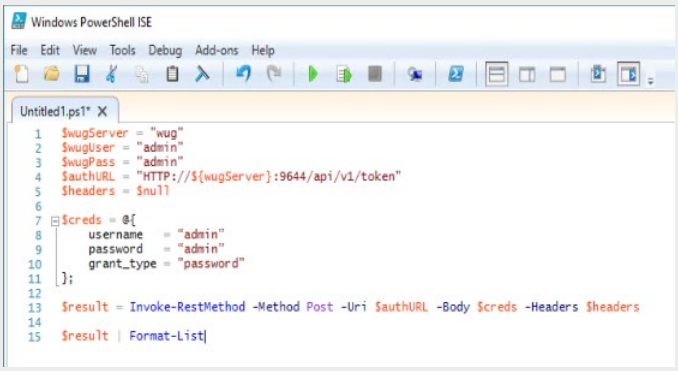
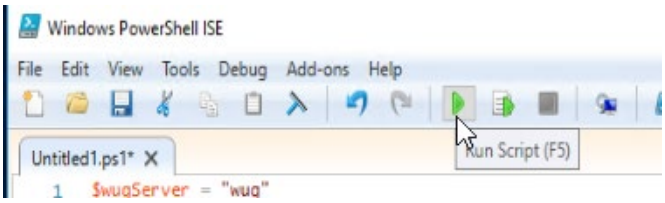
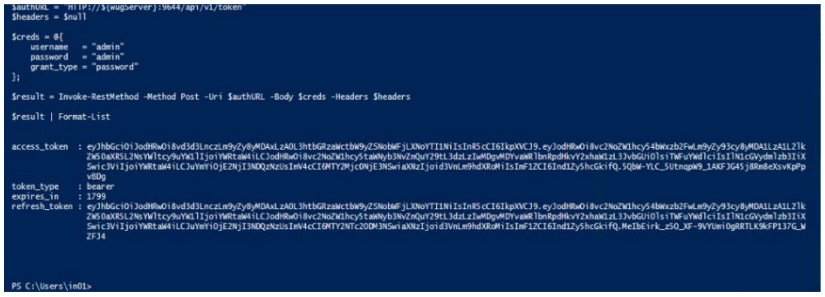
10-4	Put Device into Maintenance mode	• Click on Device to expand the device section
		  ○ Scroll down and click on
		 
		• Ensure the Response Content Type is set to application/json
		 
		• In the deviceID field, type in the device ID you recorded in the last step
		• In the cfg field, paste in the JSON you created in step 10-1
		  ○ Making sure you have all of the curly brackets and commas needed
		 
		• And ensure the Parameter content type is also set to application/json
		• Click the Try it out! Button
		• Check the Response Body
		  ○ You should see
		 
		• Go into the WhatsUp Gold Web Admin and verify wugtn2901 is in maintenance mode
		 

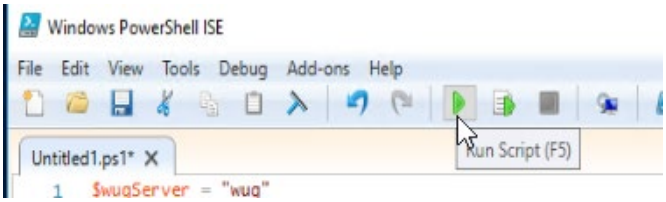
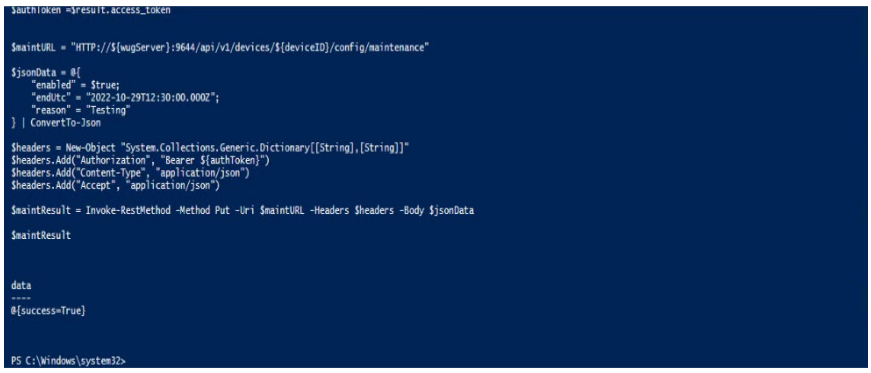
10-5	Remove device from maintenance mode	• Back in the swagger UI, edit the JSON data in the cfg field to only include
		{
		“enabled”: false
		}
		• Then click the Try it out! Button
		• Go into the WhatsUp Gold Web Admin and verify wugtn2901 is out of maintenance mode
		 

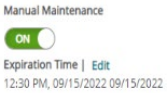
You have completed Lab 10 – Place Device into and out of Maintenance using Swagger		

Lab 11 - Place Device into and out of Maintenance using PowerShell		
11-1	Open Windows PowerShell ISE	• On you App server (the one you are logged into), • Click the start button then Windows PowerShell ISE  • On the Menu bar of the ISE ○ Click on View and then Show Script Pane to show the script pane  

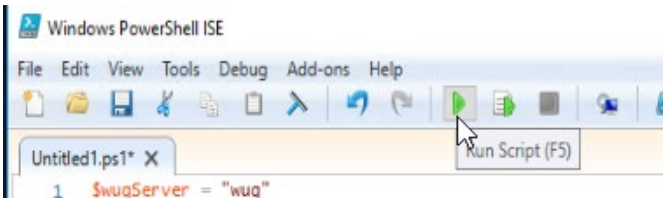
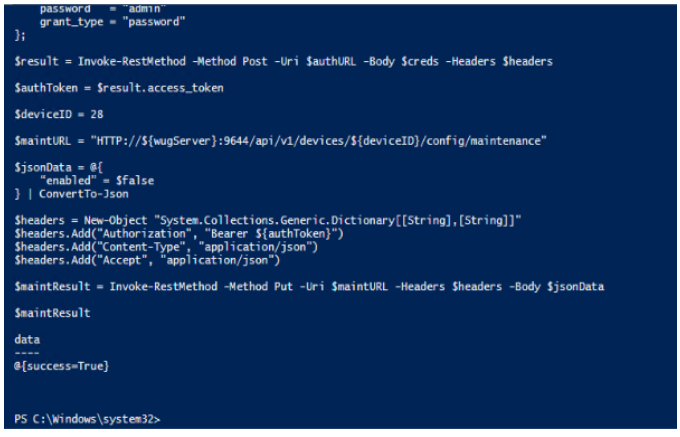
11-2	Enter configuration variables in your script	• In the script pane of the ISE,
		
		Note: you will notice when you type in the ISE, it will offer suggestions for what you are typing, and you can either hit the tab key or click it with your mouse to select your choice.
		
		• type in:
		
		$wugServer = "wug"
		$wugUser = "admin"
		$wugPass = "admin"
		$authURL = "HTTP://${wugServer}:9644/api/v1/token"
		$headers = $null
		
		$creds = @{
		username = “admin”
		password = “admin”
		grant_type = "password"
		};

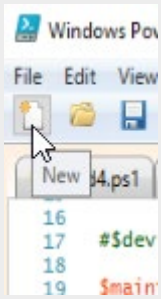
11-3	Enter Invoke-RestMethod into script	• In the script pane of the ISE and line or so below your current text, enter: $result = Invoke-RestMethod -Method Post -Uri $authURL -Body $creds -Headers $headers $result | Format-List 
11-4	Test your script so far	• On the ISE's menu bar, click on the Run Script button  Or you can press the F5 button. • In the bottom output pane if your script ran correctly, you should see the ○ Access_Token ○ Token_type ○ Expires_In ○ And the refresh_token 

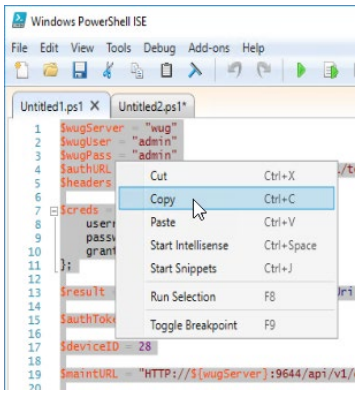
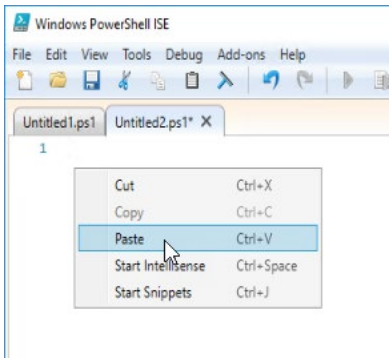
11-5	Edit script to place device into maintenance	• Back in the script pane, edit the script as follows: • **Replace** $result | Format-List with $authToken = $result.access_token • Then add the following: $deviceID = 28 $maintURL = "HTTP://${wugServer}:9644/api/v1/devices/${deviceID}/config/maintenance" $jsonData = @{ “enabled” = $true; “endUtc” = “2022-10-25T12:30:00.000Z”; "reason" = "Testing" } | ConvertTo-Json NOTE: for the JSON data, enter the values you used for the swagger $headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]" $headers.Add("Authorization", "Bearer ${authToken}") $headers.Add("Content-Type", "application/json") $headers.Add("Accept", "application/json") $maintResult = Invoke-RestMethod -Method Put -Uri $maintURL -Headers $headers -Body $jsonData $maintResult
11-6	Put device into maintenance via PowerShell	• Click the Run Script button in the ISE  • View the output in the bottom Output pane of the ISE 

		• In the WhatsUp Gold web admin
		  ○ Check that the device did go into maintenance mode
		• Go to the device properties page on the polling tab
		  ○ View that Maintenance mode is turned on
		  ○ And that the Expiration Time matches what you set
		 

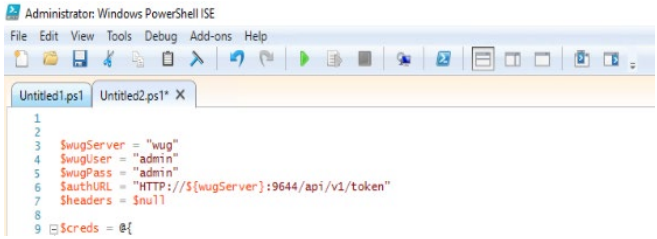
11-7	Edit script to take device out of maintenance	• Back in the script pane of the ISE, edit the script as follows:
		  ○ Edit your script as follows
		Change: $jsonData = @{
		“enabled” = $true;
		“endUtc” = “2022-10-25T12:30:00.000Z”;
		"reason" = "Testing"
		} | ConvertTo-Json
		To: $jsonData = @{
		“enabled” = $false
		} | ConvertTo-Json)

11-8	Take device out of maintenance via PowerShell	• Click the Run Script button in the ISE  • View the output in the bottom Output pane of the ISE  • In the WhatsUp Gold web admin ○ Check that the device is out of maintenance mode
You have completed Lab 11 - Place Device into and out of Maintenance using PowerShell		

Lab 12 - Place Multiple Devices into and out of Maintenance using PowerShell		
12-1	Open new script pane in Windows PowerShell ISE	• On the Menu bar of the ISE ○ Click on New to open a new blank script pane 

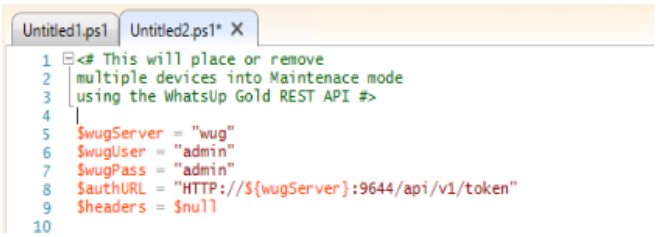
12-2	Copy and edit your script	• In the script pane of the ISE,
		• Back on what might be called Untiled1.ps1
		  ○ Select all of your script
		  ○ Copy it
		 
		  ○ And paste into the new script pane you just opened in the prev0ious step
		 

- Place your cursor in front of the first line of the code you just pasted in and hit the enter key two times to add two new lines at the start of the code

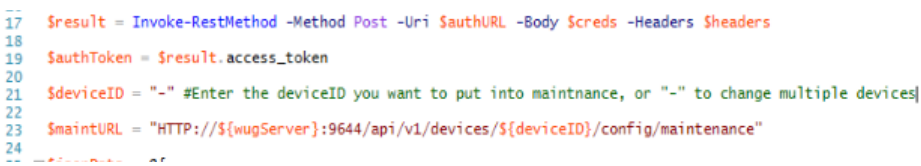


- On line one (the first line of your code)
  - Enter the following block comment

    <# This will place or remove
    multiple devices into Maintenace mode
    using the WhatsUp Gold REST API #>

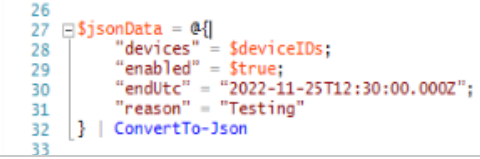


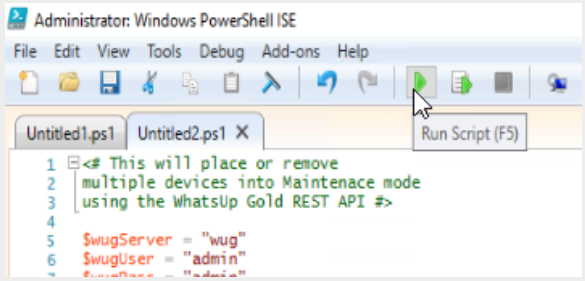
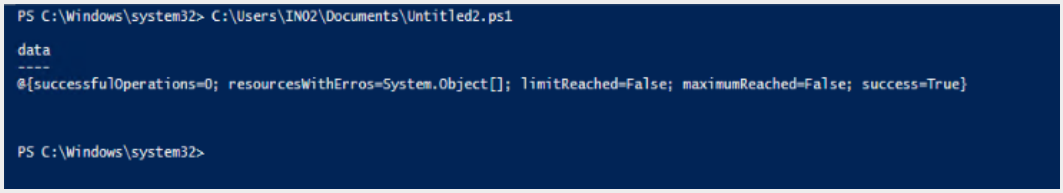
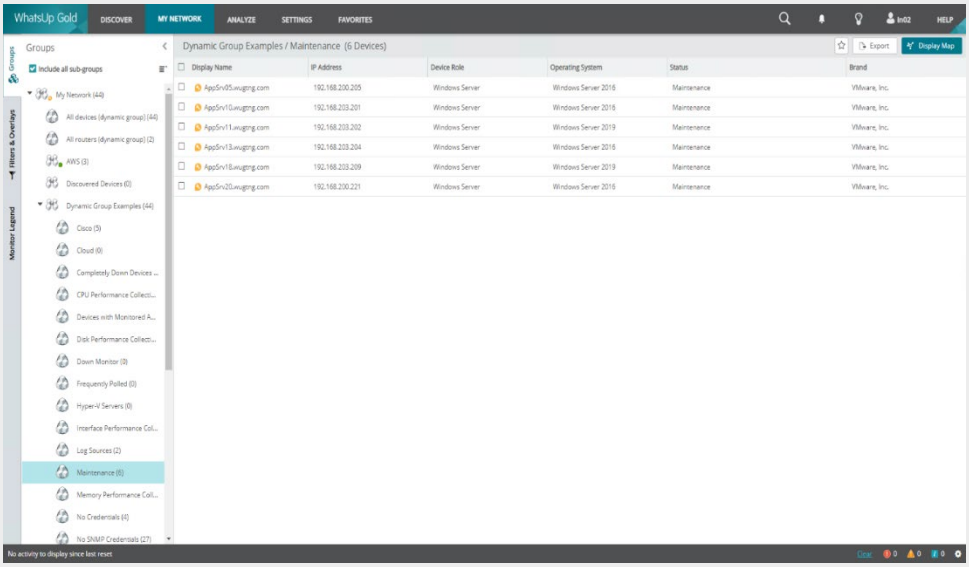
- On line 28 (or there abouts) where it has $deviceID = 28 (or whichever deviceID you used)
  - Change $deviceID = … to $deviceID = "-"
  - Then add the comment
    - #Enter the deviceID you want to put into maintnance, or "-" to change multiple devices



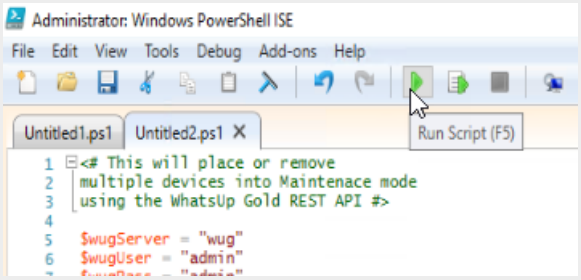
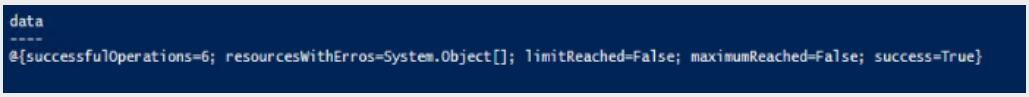
- Place your cursor at the end of the line starting with $maintURL … and hit enter twice
- **Enter:** $deviceIDs = @(1,3,5,7,9,11) #Enter the list of multiple deviceIDs separated with a comma you want to put into/out of maintenance mode

- Find the line "enabled" = … after the $jsonData = @{
  - Place your cursor before "enabled" and hit enter
  - On the new line enter:
    - "devices" = $deviceIDs;



		• Go down to the line with $maintResult = Invoke-RestMethod ○ Change -Method Put to -Method Patch 38 39 $maintResult = Invoke-RestMethod -Method Patch -Uri $maintURL -Headers $headers -Body $jsonData 40 41 $maintResult
12-3	Put devices into maintenance via PowerShell	• Click the Run Script button in the ISE  • View the output in the bottom Output pane of the ISE  • In the WhatsUp Gold web admin ○ Check that the devices did go into maintenance mode  NOTE: Your devices might be different than those pictured

12-4	Edit script to take device out of maintenance	• Back in the script pane of the ISE, edit the script as follows:
		○ Edit your script as follows
		Change: $jsonData = @{
		"devices" = $deviceIDs;
		“enabled” = $true;
		“endUtc” = “2022-10-25T12:30:00.000Z”;
		"reason" = "Testing"
		} | ConvertTo-Json
		To: $jsonData = @{
		"devices" = $deviceIDs;
		“enabled” = $false
		} | ConvertTo-Json)

11-8	Take device out of maintenance via PowerShell	• Click the Run Script button in the ISE  • View the output in the bottom Output pane of the ISE  • In the WhatsUp Gold web admin ○ Check that the device is out of maintenance mode
You have completed Lab 12 – Place Multiple devices into and out of Maintenance using PowerShell		

About Progress

Progress gives you everything you need to create, deliver, manage and support consumer-grade end user experiences. Our singular focus is on application development and digital experience tools, platforms and cloud services that bring together your apps and content, while seamlessly and securely integrating with your enterprise data. The result is competitive differentiation and business success.

Rev 2020/04 | RITM0078077

Progress