CA Unified Infrastructure Management On-Demand Trial
The Unified Infrastructure Management (UIM) on-demand trial is an alternative means for customers to validate the CA UIM solution in the context of their specific goals and objectives, without having to provide an environment or infrastructure to host and demonstrate the CA solution. Instead, the environment is hosted by CA and remote access is granted to the customer. This allows for customers to move at their own pace, work with the CA UIM solution and gain an understanding of the solutions basic capabilities.

The environment contains a variety of systems and technologies available for monitoring with the UIM solution. These include:

- Windows and Linux systems
- MS SQL and mysql databases
- Cisco routers and switches
- Vwware
- Microsoft Active Directory and Exchange
- Tixchange Application (Tomcat/Mysql)

In addition, this is not a limited version of the product. You are free to demonstrate all the capabilities of the solution. From alarming, dashboards and reports, the data that is collected can be managed and visualized in any way that you desire.

This document outlines how the solution can be used to monitor and report on the infrastructure. It includes getting started material and information about how to use the CA UIM solution to meet various monitoring requirements. Keep in mind, this is a trial. The environment has a clean installation of the CA UIM solution, just as a normal on premise trial would. This is intended for folks who intend to use and administer the solution.
<table>
<thead>
<tr>
<th>TOPIC</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Infrastructure Management</td>
<td>6</td>
</tr>
<tr>
<td>UIM Overview</td>
<td>7</td>
</tr>
<tr>
<td>Architecture and Terminology</td>
<td>8</td>
</tr>
<tr>
<td>Overview of the Environment</td>
<td>9</td>
</tr>
<tr>
<td>Getting Started with UIM</td>
<td>13</td>
</tr>
<tr>
<td>UI’s</td>
<td>15</td>
</tr>
<tr>
<td>Navigation</td>
<td>16</td>
</tr>
<tr>
<td>Discovery and Robot Deployment</td>
<td>20</td>
</tr>
<tr>
<td>Autodiscovery of the Environment</td>
<td>21</td>
</tr>
<tr>
<td>Robot Deployment</td>
<td>25</td>
</tr>
<tr>
<td>Monitoring Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Admin Console</td>
<td>28</td>
</tr>
<tr>
<td>TOPIC</td>
<td>PAGE</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Deploying Probes</td>
<td>32</td>
</tr>
<tr>
<td>Configuring Probes</td>
<td>33</td>
</tr>
<tr>
<td>Monitoring Configuration Examples</td>
<td>35</td>
</tr>
<tr>
<td>Server Monitoring – Probe Config – CPU, Disk, Memory (CDM)</td>
<td>36</td>
</tr>
<tr>
<td>Server Monitoring – Probe Config – Process Monitoring</td>
<td>38</td>
</tr>
<tr>
<td>Network Monitoring – Probe Config - SNMPCollector</td>
<td>39</td>
</tr>
<tr>
<td>Database Monitoring – Probe Config – MS SQL</td>
<td>40</td>
</tr>
<tr>
<td>Response Monitoring – Probe Config – Response Monitoring</td>
<td>42</td>
</tr>
<tr>
<td>Monitor the Infrastructure</td>
<td>45</td>
</tr>
<tr>
<td>Creating Groups</td>
<td>46</td>
</tr>
<tr>
<td>TOPIC</td>
<td>PAGE</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Viewing Device Details and Performance</td>
<td>47</td>
</tr>
<tr>
<td>Alarm Management</td>
<td>53</td>
</tr>
<tr>
<td>Working with Alarms</td>
<td>54</td>
</tr>
<tr>
<td>Advanced Event Correlation, Enrichment and Notification</td>
<td>59</td>
</tr>
<tr>
<td>Dashboards</td>
<td>65</td>
</tr>
<tr>
<td>Out-of-Box Dashboards</td>
<td>66</td>
</tr>
<tr>
<td>Creating your Own Dashboards</td>
<td>67</td>
</tr>
<tr>
<td>Creating a New Page</td>
<td>75</td>
</tr>
<tr>
<td>Reporting</td>
<td>78</td>
</tr>
<tr>
<td>SLAs</td>
<td>82</td>
</tr>
<tr>
<td>Reference Material</td>
<td>85</td>
</tr>
</tbody>
</table>
In this section you’ll find a high level overview of UIM, as well as a basic architecture and terms to know as you get started.
UIM Overview
CA Unified Infrastructure Management delivers the essential capabilities you need to proactively monitor and manage alarms, performance and SLAs across the most dynamic and complex environments. Instead of having to deploy multiple point solutions, you can leverage CA Unified Infrastructure Management and get a single platform to manage your IT infrastructure and services—whether they’re on premise or in the cloud. CA Unified Infrastructure Management is an efficient, scalable platform that you can use to monitor and manage all the elements of your infrastructure.

Extensive Technology Support:
- Broad systems coverage
- Multi-Vendor network monitoring
- Databases, such as Oracle, Sybase, Microsoft SQL Server, mysql and IBM DB2.
- Applications like Microsoft Exchange, Active Directory, Citrix, Cisco UCS, and much more.
- Virtualization platforms, such as VMware, Microsoft Hyper-V, Solaris Zones, IBM PowerVM, Citrix XenServer and Red Hat Enterprise Virtualization
- Synthetic application transaction recording, generation and monitoring
- Public and private cloud environments, such as Amazon Web Services, Rackspace, Google Apps, Salesforce.com, Vblock and FlexPod.

Key Capabilities:
- Custom and out-of-box dashboards and reports
- Alarm management and intelligent performance alerts
- Monitoring services levels with SLA/SLOs
- Extendable platform with open APIs
Architecture and Terminology

The UIM architecture is extremely flexible; built for scale, high availability and multi-tenancy. Below is a small scale example of the architecture, and common terms to familiarize you with the UIM landscape. NOTE: All components shown below are on the single UIM system in this environment, but can and often are separated.

Terms to Know

Robot – Robots are the onboard intelligence that are deployed servers. Once deployed, the Server can now be used as a platform for running probes (monitoring or utility) – Think Agent.

Probe – Software package which either collects metrics based on technology types and/or helps run the solution.

Hub – The hub exists as a probe which, when deployed to a robot, causes that robot to now handle the communications required to receive messages from subordinate or children robots as well as forward those and other Hub’s messages to the primary Hub.

QoS – Quality of Service – Performance trend data for analyzing historical behavior. Simply put, Metrics.

NAS – Nimsoft Alarm Server, responsible for processing and responding to any and all alarms through the AutoOperator mechanism

Go Here for additional UIM Architecture Reference.
Here you will find out about the environment that you have at your disposal to monitor. It includes a number of systems, network and application components.
As mentioned in the introduction, there are a number of systems and technologies that can be monitored with UIM within the trial environment. Shown below is the architecture for the Tixchange application which is also hosted within the environment and can be leveraged for monitoring.
**Overview of the Environment**

Listed in the table below are all of the devices in the environment.

<table>
<thead>
<tr>
<th>Name/IP</th>
<th>login</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UIM 192.168.200.11</td>
<td>administrator/CAdemo123</td>
<td>System where all UIM components are installed (this includes the UPM, Database and Primary HUB).</td>
</tr>
<tr>
<td>SAG-APP 192.168.40.11</td>
<td>admin/CAdemo123</td>
<td>This is the jump station (where you login to). This is the system where the Uis are run from and can be used for robot/probe deployment.</td>
</tr>
<tr>
<td>SAG-SOI 192.168.32.11</td>
<td>admin/CAdemo123</td>
<td>This is a system running a MS SQL DB. <strong>DB access credentials:</strong> sa/CAdemo123</td>
</tr>
<tr>
<td>SAG-NFA 192.168.49.11</td>
<td>admin/CAdemo123</td>
<td>Windows OS</td>
</tr>
<tr>
<td>SAG-VC 192.168.71.11</td>
<td>admin/CAdemo123</td>
<td>Virtual Center Sysetm (2 ESX Hosts) <strong>VC Credentials:</strong> admin/CAdemo123</td>
</tr>
<tr>
<td>SAG-ESX1 192.168.69.11</td>
<td>Root/CAdemo123</td>
<td>Esx host</td>
</tr>
<tr>
<td>SAG-ESX2 192.168.70.11</td>
<td>Root/CAdemo123</td>
<td>Esx host</td>
</tr>
<tr>
<td>AZ-SITE 10.10.1.6</td>
<td>public (SNMP Comm string)</td>
<td>Cisco Router</td>
</tr>
<tr>
<td>FL-SITE 10.10.1.5</td>
<td>public (SNMP Comm string)</td>
<td>Cisco Router</td>
</tr>
<tr>
<td>MI-SITE 10.10.1.1</td>
<td>public (SNMP Comm string)</td>
<td>Cisco Router</td>
</tr>
<tr>
<td>NY-WAN 10.10.1.3</td>
<td>public (SNMP Comm string)</td>
<td>Cisco Router</td>
</tr>
</tbody>
</table>
### Overview of the Environment

Listed in the table below are all of the devices in the environment (cont)

<table>
<thead>
<tr>
<th>Name/IP</th>
<th>login</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAG-TIX-WEB-1</td>
<td>root/CAdemo123</td>
<td>Tomcat webserver (linux)</td>
</tr>
<tr>
<td>192.168.100.101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAG-TIX-APP-1</td>
<td>root/CAdemo123</td>
<td>Tixchange app server (linux)</td>
</tr>
<tr>
<td>192.168.100.102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAG-TIX-DB</td>
<td>root/CAdemo123</td>
<td>Mysql db (linux)</td>
</tr>
<tr>
<td>192.168.100.103</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAG-CLIENT-AZ-1</td>
<td>root/CAdemo123</td>
<td>Linux tixchange client</td>
</tr>
<tr>
<td>10.10.10.45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAG-CLIENT-FL-1</td>
<td>root/CAdemo123</td>
<td>Linux tixchange client</td>
</tr>
<tr>
<td>10.10.20.45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAG-CLIENT-MI-1</td>
<td>root/CAdemo123</td>
<td>Linux tixchange client</td>
</tr>
<tr>
<td>10.10.30.45</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CA UIM ON DEMAND TRIAL
GETTING STARTED WITH UIM

In this section you understand how to access UIM, and some of the basics on the UI.
Getting Started with UIM

By now, you’ve received your access to the UIM trial environment and have logged in. The Citrix login takes you to the SAG-APP system within the environment. From here, you can RDP/SSH to any of the other systems in the environment if desired, but you should be able to run your entire trial from this system. Upon logging in to the system, you’ll be greeted by the CA On Demand POC Landing page:

Here, you are provided direct links to the Tal Runbook (this document), a link to the UIM Unified Management Portal and links to the official UIM Documentation.

As you may have guessed, the UIM software is already installed and you ready to begin your trial!
UI’s

There are two user interfaces for the UIM solution. The Infrastructure Manager and the Unified Management Portal (UMP). The infrastructure manager is a legacy thick client that can still be used for monitoring configuration. The majority of all administration, configuration and usage of the UIM solution will be in the UMP. We are currently transitioning all capabilities to that UI, but there are still some pieces needed for the Infrastructure Manager.

When to use what:
Infrastructure Manager – Alarm enrichment, correlation and notifications. Probe package configuration. HA and SSL tunnel setup and configuration. Small subset of probe configuration.
Unified Management Portal - Everything else! Included within the UMP is easy access to the UIM Admin Console. This is where probe deployment and configuration takes place.

The Infrastructure Manager can be launched from a shortcut located on the desktop. The UMP can be accessed via the web and is available from the launch page as well as desktop shortcut.

Use this icon for launching the Infrastructure Manager if needed
Upon launching the UMP, you see the login screen below. Login in with:

**User:** administrator  
**Password:** CAdemo123
The default landing page for the UMP is the Unified Service Model (USM). This is a standard portlet that can be added as desired (more on that later). Here is a basic breakdown of the USM view.

The USM view is used to view the objects that have been discovered in your environment. The default orientation is tree, but badge views can be selected as well (based on grouping).

You can view the details and status of groups and devices, as well as view alarms in context. Maintenance mode can also be set for groups and devices.

Once you discover the environment, groups (static and dynamic) can be created to organize your infrastructure. More on that to come....
Along the page header, there are links to other pages. Pages can be added and configured to include a variety of portlets (lists, dashboards, reports, web content etc...), there will be more on adding new pages later. The default pages are show below:

**Unified Dashboards** – This includes out of box pre-built dashboards that provide high level views and insight into specific technologies. The Unified Dashboards list can be modified to suit your needs (you can remove dashboards that are not relevant, or add new ones you may have created).

**Reports** – This page contains links to various aspects of reporting capabilities within UIM. You can create ad-hoc performance reports (Performance Reports) as well as run (and create) historical pre-defined reports (Unified Reports).

**Design** – The Design page provides access to a few design tools. Here you can design your own dashboards with the Dashboard Designer as well as create your own lists with the List Designer. Once saved, these are then available for you to make available in different Pages.

**Configuration** – Allows you to create User accounts and access policies.
Navigation

At the very top of the page, you’ll have options to modify the view(s) by adding new pages or portlets to existing pages. In addition, you can manage the sites, pages and appearance of the portal by changing the appearance with logos, style sheets and more. You can customize the UMP to make it unique and specific to your organization or different customers you service. There will be specific use cases for these techniques in the run book.

Add – Add new pages and/or portlets to existing pages.

Manage – Add child pages, update existing pages, export and more.

Go to – Go to the Control Panel (for managing sites and pages), and quickly switch between sites (which contain different pages).
In this section, you’ll see how quick and easy the discovery process is, then how to deploy robots to selected systems.
Autodiscovery of the Environment

First thing you want to do is discovery the devices in the environment.

1. You’ll notice that when you first login to the UMP, the Discovery Wizard launches automatically. You can choose to start there, or if it’s not currently open from the Home tab in the UMP, select Actions->Discovery Wizard.

2. The Discovery Wizard will now open. Here you will enter scope, credentials and scheduling information for the discovery.

GOOD TO KNOW: The UIM API’s can also be leverage for discovery purposes.
3. Go through the credentials portion (WMI, Linux/Unix, SNMP) and add the following credentials:

**WMI**
- User: admin
  - Password: CAdemo123
- User: administrator
  - Password: CAdemo123

**Unix/Linux**
- User: root
  - Password: CAdemo123

**SNMP:**
- public
- private

4. In the Scope section, select “New Range Scope”
Autodiscovery of the Environment

5. Enter a scope name.
6. Select the “Import” button.
7. Copy the IP’s from the “POC_Discovery_List.txt” file on the desktop, to the import window.
8. Hit OK. Select Next, which brings you to the Schedule section. Hit Finish (the Run Discovery Now is checked).
Autodiscovery of the Environment

9. Once the discovery completes, you’ll see the results in the Inventory view of the USM.
Robot Deployment

Now that the environment has been discovered, Robots can be deployed to different systems.
1. From the USM Inventory View, select the UM_Hub
2. Select the Actions Button
3. Select Deploy Robots
Discovery and Robot Deployment

Robot Deployment

Now that the environment has been discovered, Robots can be deployed to different systems.

1. Select the systems (via the check box) with an OS Name of Windows or Linux
2. In the Hub field, select the SAG-UIM hub from the drop down
3. Select the Deploy button
4. You’ll then get a job status window giving you the deployment status
Here we will cover how to configure monitoring. In this trial we only cover configuring individual probes, but it should be noted that UIM does support bulk configuration.
Admin Console (AC)

Now that Robots have been deployed, you’ll want to deploy probes to monitor system, network, database, application and response components. The Admin Console is where you will do the majority of your UIM probe deployment and configuration. The Admin Console can be accessed through the Actions menu within the USM.

NOTE: UIM provides the ability to deploy robots and probes (with configuration) with the use of Packages and Super Packages (currently done through the Infrastructure Manager). For more information on packages and bulk deployment reference: The Wiki here.
Admin Console (AC)
The Admin Console allows you to deploy and configure probes (in addition to things like stop/start/restart robots and probes, update license info and more). Shown below are the navigation basics on the Admin Console Infrastructure View (default):

1. The HUB in the environment (you could have many, here we have 1).
2. Robots reporting to that Hub
3. Toggle between the Infrastructure view and Archive view (more on that next).
Admin Console (AC)

By selecting a Robot, you can then see the probes deployed to it and basic information about them.

NOTE: The blue highlight around the SAG-UIM-WIN robot indicates that the HUB has been deployed to that system.
Admin Console (AC)
The UIM Archive is where probes are stored for deployment. There is a Local Archive (stored locally on the system) and a Web Archive where you can access probes that get updated by CA Technologies. This allows you easily get updated probes and deploy them to systems, without having to upgrade or install patches (NOTE: The Web Archive requires a CA Support ID, so it will not be available for the On-Demand Trial, however you should have all you need).
Deploying Probes
Let’s walk through deploying a probe or probes:
1. In the Admin Console, select the Archive Tab
2. Select Local Archive
3. In the probe list, select the check box next to the CDM (CPU, Memory, Disk) Probe
4. Select one or more robots (via the check box)
5. Select the “Deploy” button

GOOD TO KNOW: Robots and probes (and their configuration) can be packaged as files and included or deployed with 3rd party software delivery programs.
Configuring Probes

Once probes are deployed, they can be configured right from the Admin Console. Configuring probes allows you to specify what metrics to monitor, and how to monitor them. To configure a probe:

1. Select a probe from the right hand navigation window of the Infrastructure tab (i.e. UIM)
2. In the probe list to the right find the **cdm** probe
3. Click the downward facing arrow next to **cdm** to bring up the probe configuration context menu
4. Select **Configure** from the context menu (note you have other options such as restart, delete, view log...etc)
5. This brings up the probe configuration window (a new window)

**REMEMBER:** While this On-Demand trial focuses on simply configuring individual probes, bulk probe configuration can be pushed out to multiple systems.
Configuring Probes

In the probe configuration window, you can make general probe configuration changes as well as metric collection, baselines and thresholds.

1. The probe configuration window defaults to the high level probe configuration (i.e. log level). You will see the probe name highlighted in the navigation pane on the left.
2. You can select other objects in the tree to configure specific items on the probe for monitoring (store metrics, compute baseline, configure static and dynamic thresholds...etc).

GOOD TO KNOW: You can also set a “base” configuration (or multiple) for different probes, then store that updated probe (with the config) to your local archive. That probe can then be deployed to multiple robots with that base configuration.
Included in this section are a few examples of configuring specific probes for different monitoring domains/technologies. The intent is to simply get you familiar with probe configuration, and give you some data for your trial.

We hope you go BEYOND the examples and configure more.

REMEMBER – For this trial, we are configuring probes individually, UIM certainly supports the ability to distribute probe configurations to multiple systems.
In this example, we’ll setup some basic monitoring for the CDM probe (CPU, Disk, Memory). Let’s start with static alarms, and enabling performance data collection.

1. Ensure the CDM probe is deployed to the SAG-APP robot, and open the CDM probe config for the SAG-APP system.
2. Next, select the “Disk Usage” folder under the C:\ drive on the left side navigation tree.
3. In the “Alarm Thresholds” section, check the “Enable High Threshold” box and set the threshold to 50 (this will ensure you get an alarm).
4. Scroll down, under “Monitors” ensure the “Disk Usage (% )” is selected, check the “Publish Data” checkbox.
5. Enable others as desired.
6. **HIT THE SAVE BUTTON**

**Enable High/Low Threshold**: As you might expect, by checking these, you enable static thresholds and can set the value.

**Publish Data**: This instructs the probe to collect and store the specific metric. When checked you can view the data historically.
Server Monitoring – Probe Config – CPU, Disk, Memory (CDM)

Now let's look at dynamic thresholds. In this example we'll set up an alarm for if Total CPU is over 95% for 20 out of 30 minutes.

1. Select “Total CPU” under the “Processor” folder.
2. Select “Total CPU Usage” from the monitors table (notice out of box static thresholds are enabled).
3. Select “Compute Baseline”.
4. Select “Dynamic Alarm” and choose Percent from the algorithm menu.
5. Set a critical level of “> 20”.
6. Enter a custom alarm message.
7. This will generate an alarm if CPU is 20% is normal “baseline” value.

As you can see, there are many dynamic alarm capabilities. These include Deviation from normal (in algorithm section - % and std dev), as well as “Time to Threshold” and “Time TO Threshold.

For more information on setting thresholds, you can go here.
In this example, we will demonstrate how to setup process monitoring.

1. Deploy the “processes” probe to the SAG-APP system
2. Open the probe configuration for the processes probe. Explore some of the options, on the high level processes view you can see how you can monitor things like “total number of processes”.
3. Select the SAG-APP system (under processes). Here you can see the currently running processes etc.. Select the icon next to the SAG-APP system and select “Add Process”
4. In the process monitoring profile, enter a Profile Name and the process name of “cmd.exe”
5. Now select the Process State folder (under cmd.exe) and select “Publish Alarms” and “Process Down Alarm”
6. SAVE CHANGES

GOOD TO KNOW: This is easy to test, just stop/start a command window on the SAG-APP box
Network Monitoring – Probe Config - SNMPCollector

For monitoring network devices and interfaces, the SNMPCollector probe is used.

1. From the AC, select the UIM system, the Configure on the snmpcollector probe.
2. In the snmpcollector probe configuration, you’ll see various information including a link to supported vendors, devices and metrics.
3. To the right of the Discovery Filters folder, select the ⋮ button, and select “Query Discovery Server”.
4. This will pull back the SNMP devices from the initial Discovery under the Profiles folder.

5. Once this is complete, the SNMPCollector will start collecting SNMP device and interface metrics based on the default profile templates.
6. Shortly after this the metrics will be available in the USM (more on this later).
7. The “Template Editor” allows you to change what metrics are collected and how UIM monitors them.
Let’s monitor a MS SQL DB, there is one installed on the SAG-SOI system.

1. From the AC, deploy the “sqlserver” probe to the SAG-SOI system (note, this probe does not have to be deployed to the actual DB system).
2. Once deployed, open the probe configuration for the sqlserver probe.
3. Select ..., next to sqlserver and “Create new connection”
4. Enter a Name of “TEST DB”, User ID of “sa”, Password of “CAdemo123” and Server Name of “SAG-SOI”.

Probe Information

Name *
Description
Authentication
Encryption
Detect domain automatically
User ID *
Password
Server name *
Retry attempts
Retry delay
Retry delay unit
Timeout
Timeout unit
5. Once created, select “Create new profile” next to the new “TEST DB” connection.
6. Enter a **Name** of “POC DB Profile”, and select “TEST DB” from the **Connection** dropdown.
7. Under your newly created profile, you’ll have a number of default checkpoints that you can inspect and change if desired.
8. Additionally there are a number of other checkpoints/metrics that can be monitored. Those can be added by selecting “Add Profile Checkpoints” next to your POC DB Profile.
9. There, you will see additional checkpoints that can be added and modified.

**GOOD TO KNOW:** Another great way to monitor DBs is with the **sql_response** probe – use it to run sql queries to db’s for availability and response time...try it out!
CA UIM provides the ability to execute a number of different application/protocol response tests (DNS, DHCP, HTTP, ICMP, Citrix, Jitter, email, SQL…and more). In this example, we’ll configure an http test with the url_response probe.

1. From the AC, deploy the “url_response” probe to the UIM system.
2. Once deployed, open the probe configuration.
3. Select next to url_response and select “new profile”.
4. In the New Profile window, enter a **Profile Name** of CA Wiki, and a **URL** of http://wiki.ca.com
5. Once created, you can select the Metric folder under the new profile and enable data collection (Publish Data) and Thresholds.

6. Once the configuration is saved, you will be able to see the data (graphically) in the Metrics tab for the UIM system in the USM (we’ll learn more on that in the next section).
Let’s now use the net_connect probe to create ping tests for network devices (it could certainly be servers as well). Net_connect not only can test icmp response times and packet loss (and jitter), but it can also run port scans on systems to determine which services/applications are running.

1. From the AC, select the UIM system, then Configure on the net_connect probe.
2. Select “Add New Host” to the right of net_connect.
3. Enter **Hostname** “ny-wan” and **IP** 10.10.1.3 (* ensure you enter the IP correctly)
4. Now, under ny-wan, select the ICMP folder. Here you can enable metric collection and thresholds
5. Ensure Publish Data is check under Response time (and enable any other). You can do the same for the Packet Loss folder.
Now that you have things setup, let's take a look at how you can monitor the infrastructure using CA UIM.
Creating Groups

A key to effectively monitoring and visualizing the infrastructure is grouping objects that may be relevant to different users or organizations. UIM groups can be created to represent technologies, device types, locations, applications...etc. Groups can be static or dynamic (based on search criteria). Groups are pretty simple, here is an sample dynamic group.

1. In the group tree, select the + button next to the Groups.
2. In this example, lets do a dynamic group type.
3. For the criteria, select “hostname contains tix” and select “Apply Filters”
Viewing Device Details and Performance

The USM (your Home page) is where operations and engineers can inspect groups, devices and interfaces. It provides quick and easy access to details, alarm information and performance details. In the next few pages we’ll highlight a few different devices and review the available data and workflow.

1. In the USM view, select the SAG-APP system. You can quickly find this in the group tree (Operating Systems -> Windows), or leverage the search in the upper right.
2. In the details tab, you’ll quickly see device information as well has key performance indicators to the right.
3. If you select the “pop out” in one of the charts, it will allow you view a full performance report for that metric.
4. As you might expect, the Alarms tab shows context alarm information (more on That to come).
5. The metrics tab is where you can see ALL the metrics that you are collecting for that system (across multiple probes, so if you are monitoring a database, or processes, those will also show).
6. The Groups tab will show you all groups that the selected device is a member of.
Viewing Device Details and Performance

1. Let’s take a look at a network device. Select ny-wan.
2. The Response Time metric is directly from net_connect probe we configured earlier.
3. The metrics tab here will have all the default SNMP metrics also.
4. Next, select the Interfaces tab.
5. Here, you’ll get a list of interfaces on the device, and high level metrics.
6. Double-click the gig3 interface, and you’ll have the interface view with details and metrics.
We will review the reporting capabilities of later in greater detail, however it’s easy to leverage pre-configured reports available for Groups and individual devices. Let’s briefly review those.

1. To access the reports, from either a device OR group within the USM, select the “Reports” tab. From Sag-App, select Reports-&gt; At a Glance Report.
2. The configuration section can be left as is, select Run.
3. The at a glance report shows high level information about the system in question. The USM Dynamic report will show more metrics, and the Trend report will allow you to choose metrics.
1. As was mentioned, you can also select a Group and the Reports tab now has group context reports.

2. In this example, select the Windows group, then select Reports -> TopN Report

3. In the Configuration window, select “CPU Usage (%) – System.CPU”

4. Select Run

A key report for **proactive** monitoring is the “Situations to Watch” report. This provides you with a report that highlights systems and metrics that are approaching threshold values so you can understand where you have to focus BEFORE problems happen.

**NOTE:** For Situations to Watch to work, the objects in the group you are running it against must have metrics with “Baseline” and “Time TO Threshold” values configured.
Alarm Management is a key feature of any monitoring tool. CA UIM provides actionable and flexible alarming, with the ability to perform advanced correlation.
Working With Alarms

Often times the first priority is alarm management. CA UIM not only alerts on faults and performance violations, but also allows you to be proactive with things like Time TO Threshold alarms. Letting you know BEFORE the threshold is breached. CA UIM supports advanced event correlation, enrichment as well as multiple methods of notification. One of the core components of the UMP is the alarm console (you’ve likely already seen it if you’ve made it this far).

1. The Alarm Views are context driven. There is a global Alarm View, which is accessible via the Alarm View icon in USM. This show all alarms.

2. Also, there are “Alarms” tabs for groups and devices. These show only alarms in the context of the contents of a group, or device.

3. When looking at an alarm view, you get a graphical representation of alarm counts (configurable). This view can be minimized by clicking the small arrow in the upper right.

4. You also get the context driven alarm list. This can be filtered, sorted and formatted in list and table formats.
Working With Alarms

You can take many different actions on alarms such as acknowledgement, assignment and annotations. These are useful collaboration tools to help you be more effective and proficient when troubleshooting problems. The alarm details provides important information about the alarm (and can be customized if needed).

1. In the filter window, enter “disk”. It should find the disk threshold set in the examples section.
2. Select the “More” tab. You can also see icons for acknowledgement, assignment, custom URL actions, and annotations.
3. In the details section, you get a bit more info on “where” the alarm came from.
4. Select the “Metric” tab. For performance based alarms, you’ll then get to see a brief history of the trend and what has led up to the threshold breach.
Working With Alarms

5. You can also select the “Annotation” button.
6. You can now add a note that others who may be working on this issue can easily see.
7. Once you click OK, you’ll notice the annotation button has change to indicate that a use has entered a note.
8. If you select it again, you’ll see that it indicates who and when the note was made.
9. You can also multi-select alarms (with the checkboxes to the left) and use the “Actions” button to perform these tasks in bulk.

GOOD TO KNOW:
Annotations can be automatically updated using alarm enrichment. Many customers use this to programmatically add more information to the alarm (i.e. top consuming processes).
Another important feature of UIM’s alarm management capabilities is Maintenance Mode. Maintenance mode allows you to put devices or groups of devices in a state where alarms will not be processed. Maintenance Mode can be initiated ad-hoc or on a scheduled basis. This is a great way to prevent false or known alarms during maintenance windows. When a device is in maintenance mode, data is still collected, but alarms will not be generated.

1. You can set an individual device to Maintenance Mode by selecting the “wrench” icon in the details view of USM.
2. You’ll then set your schedule.
3. Once you do this, you’ll then see your schedule(s) in the Details view.
Working With Alarms

1. You can also set maintenance mode for groups as well. Select the Maintenance tab (with a group selected).
2. Create a new schedule (all existing schedule will be shown here as well).
3. Once you have your schedule, you can drag a group over to the existing schedule by selecting the three vertical bars icon next to the group ( ), You will then be able to drag your group to the schedule you choose.
Advanced Event Correlation, Enrichment and Notification

CA UIM has very powerful event correlation, enrichment and notification capabilities. These can be configured with the Nimsoft Alarm Server (nas) probe. Nas is one of the few probes that requires the Infrastructure Manager client for configuration (at least for now). In this section we’ll walk through some of the basic concepts of the nas. We will only touch on a few of the most important concepts, so please reference the nas documentation for more information.

1. To launch the Infrastructure Manager, from the desktop double click the Infrastructure Manager icon (select the Advanced button, in the HUP IP at the bottom, enter UIM, then enter the password of CAdemo123).
2. In the Infrastructure Manager, select the “UIM” robot under UIM_Hub. In the probe list, double click on “nas”
3. In the nas configuration UI, select the “Auto Operator” tab.

GOOD TO KNOW: The Infrastructure Manager can also be used to configure other probes as well.
As was mentioned before, the nas is very powerful, here we will focus on a few elements of the Auto Operator tab (again please reference the documentation for more detail). Auto Operators allow you to perform actions based on different event criteria and filters. Those actions include creating new alarms, running commands or scripts, suppression, or email notifications. Here is a quick summary of what some of the items provide:

1. **Scheduler**: You can schedule your auto operators. Perhaps you only want certain notifications at certain times.
2. **Pre-processing Rules**: Here you can choose to filter out (exclude) certain events/alarms from even being handled by the nas. Maybe there are certain events that are completely meaningless and you do not want UIM to process them.
3. **Scripts**: Here you can upload scripts that can then be run by an auto operator based on different criteria.
4. **Triggers**: Think of triggers as alarm filters. You can setup multiple triggers that will catch different alarms based on the criteria you specify.
5. **Profiles**: Here is where you set Auto Operator profiles. These will take action based on specific criteria that is set (for example you can reference one or multiple triggers mentioned above).
Now let's walk through a quick example in which we see 2 specific types of alarms on a system, and correlate those to a new alarm.

1. In the triggers tab, we'll need to create 2 new triggers. One for a CPU alarm, and one for a memory alarm. In the triggers window, right-click in the triggers area and select “New”.

2. We do a very simple trigger here. For the trigger: select minor, major and critical in the severity buttons. Enter UIM in the hostname field, enter *cpu* in the Message String field (this will catch any message with “cpu” in the string). Click OK, and give a name. Create a second trigger (you can select Copy, on the one you just created) and replace *cpu* with *memory*.

3. You should have two new triggers. Select the “Apply” button.

4. The color of the “flag” next to your trigger indicates if there are alarms currently present that meet your criteria (blue = yes).
5. You can also right click on your trigger and select “Show Events” to see the events that meet your criteria.

6. Now let’s create the auto operator profile. In the “Profiles” tab, right-click in the window and select “New”.

7. Select “new_alarm” as the Action Type (you can see a variety of others as well). For the message, enter something to indicate that both CPU and Memory are high. Select a severity of Critical.

8. Under Action Mode, select “On Trigger”. In the Triggers tab, select the two you just created and move them over to Selected Triggers.

9. Select OK.

10. Back in the main UI, select the Apply button.

11. Next we’ll show a quick way to test your profile.
Advanced Event Correlation, Enrichment and Notification

1. To test your new profile, select the “Status” tab.
2. Select the “Send Test Alarm” button.
3. In the Alarm Properties window, enter a Message text of something that includes “memory”. Set the Source of Sender as “UIM”.
4. Click Send
5. Send another test alarm that has a string that include “cpu” and has a Source Sender of UIM.
1. You should now see your new alarm.

This was a very simplistic (and manufactured) scenario. Hopefully however you can see how you can use the nas to provide more detailed correlation, enrichment and notifications for alarms based on a wide range of criteria.
CA UIM ON DEMAND TRIAL

DASHBOARDS

CA UIM provides both out-of-box and customizable dashboards. This section will walk you through some examples. Including creating your own dashboard.
Out Of Box Dashboards

There are many dashboards available to you out of box. These are found in the Unified Dashboards page in the UMP. The majority of these dashboards are technology focused and a great place to get started.

1. In the Unified Dashboards drop down, select the “Servers” dashboard.
2. Each dashboard provide context drill downs to each of the objects within them (select the system name).
3. Select the Network Device Health dashboard.

GOOD TO KNOW: You can add or remove dashboards from the Unified Dashboards list. Many of them will not have data for this on demand POC but you can still select them and see what metrics are present.
Creating Your Own Dashboards

Hopefully you are starting to see the tremendous capability of CA UIM to collect fault and performance data from a wide range of technologies. We’ve quickly walked through the USM to view data on individual devices/interfaces and demonstrated some of the out of box dashboards. The Dashboard Designer provides you with a simple way of creating very basic to extremely detailed dashboards in any way that you choose. The only limit to the way you can visualize the data is your imagination. The dashboard designer allows you to create dashboards using icons, lists, gauges, charts and graphs leveraging the vast data that UIM is collecting (and even external data). Dashboards can be tailored to specific style sets and include images and logos as you choose. In this section, we will walk through a brief example to get you started. For more information on creating dashboards the documentation can be referenced here.

1. To access the Dashboard Designer, select the “Design” page, then “Dashboard Designer”.
2. You’ll now see the “Open Dashboard” window. Select “New”.

![Dashboard Designer screenshot]
3. You will now see the canvas to design your new dashboard.
4. In the canvas area, you can drag different widgets and set data sources and properties for those widgets to build out your dashboard. Before we give an example, let's start with some basics.
5. To the right of the screen are the tools for designing dashboards. Select the “Canvas Properties” button. Here you can change the size of the dashboard, color, grid and add background images.
6. To the left, you have the Dashboard menu. This is where you will save your dashboard. You can also use the “Live view” selection to bring your dashboard to life for testing purposes.
7. To add contents to a dashboard, you simply need to drag widgets to the canvas. Select the “Widgets” button. Here you will see a few categories for different types of widgets.

8. Drag a Circle, Gauge and Line (chart) into the canvas area.

9. You can now select the “Widget Properties” button (with a widget in the canvas selected) and change the name, color, URL (for context drill down), and other properties of the widget.
Creating Your Own Dashboards

1. Data Sources determine what data is feeding your widget. Data sources can be alarms, performance metrics, SLAs, or even a custom SQL query.
2. With the Circle widget selected, in the widget properties section, scroll down to the “Data Sources” selection.
3. In the “Type” field, select Alarm. You can create data sources in bulk using the “Data Source” button, however you can also do them for individual widgets on the fly. Select the + button to create a new data source.
4. The create alarm filter window will come up. Enter a “Name” and select the + button next to Alarm Filters.
5. Enter “Hostname is sag-app” for the filter. As you can see you can create all kinds of filters to find one or more alarms that would then impact your widget (you can test the results with the Test button).
6. Click “Create”. Now the circle widget will change status based on any alarms present of the sag-app system.
Creating Your Own Dashboards

1. For the next widget, the gauge, we’ll use the Data Sources button to demonstrate defining data sources there (as opposed to within the widget properties like we did with the circle).
2. Select the “Data Sources” button, then expand the Metric section. Here you can quickly find systems by navigating the “Groups” structure. You can also select the search button to quickly find systems that are being monitored.
3. Find the “sag-app” system and navigate to the CPU Usage metric.
4. Now drag the CPU Usage metric (highlighted in blue) over onto the gauge widget in the canvas.
Creating Your Own Dashboards

1. Let's now add a data source for the Line chart. Select it in the canvas and then the Widget Properties button.
2. Scroll down to the Series section and select QoS under the Series Data Source Type. Select the + button to add a new data source.
3. In the Create QoS Data Source, select QOS_NET_CONNECT with a Source of UIM. Then select the ny-wan:ping in the Target window (this is the ping response test we set up earlier).
4. You can also modify additional chart properties like the axis names and scales.
Creating Your Own Dashboards

1. Let's now add a data source for the Line chart. Select it in the canvas and then the Widget Properties button.
2. Scroll down to the Series section and select QoS under the Series Data Source Type. Select the + button to add a new data source.
3. In the Create QoS Data Source, select QOS_NET_CONNECT with a Source of UIM. Then select the ny-wan:ping in the Target window (this is the ping response test we set up earlier).
4. You can also modify additional chart properties like the axis names and scales.
Creating Your Own Dashboards

You’ve now created a simple dashboard leveraging a few different widget types. Hopefully you’ll take some time to build out additional components to your dashboard(s). The last step for our example is to save, test and publish the dashboard. In the next section, we’ll show how to add your dashboard to the UMP as a different page.

1. In the dashboard menu (top left), select Save As (provide a name).
2. Next, select “Live View”. This allows you to see your dashboard with the data sources feeding it (to return to edit mode, select the pull down in the center of the view, then the edit button).
3. Select “Publish” from the dashboard menu. Choose “Public” in the Visibility drop down, then the Publish button.
Creating a New Page

You’ve now successfully created a new dashboard, the next step is to make it viewable from a UMP Page. In this section, we will create a new page, show how you can add different portlets, and add the dashboard you just created.

1. From the “Add” menu of the UMP, select “Page”.
2. Enter a Name for your new Page.
3. Now select your new Page (it will be blank).
4. Again, select the “Add” menu, and this time choose “Portlet”.
5. You’ll get a list of portlets to choose from. Click the Add button next to Monitoring -> “Dashboard” and Tools -> “WebContent”.
Creating a New Page

1. You now have 2 portlets in your Page. Select the Options button (small wrench) in the upper right of the Dashboard portlet you added and select the “Preferences” option.
2. In the preferences screen, adjust the height to 200 and choose your newly created dashboard in the Default Dashboard section.
3. You can also change the name of the dashboard portlet and other cosmetic items in the “Look and Feel” menu under Options.
4. Last, for the WebContent portlet, select Options -> Configuration. This will allow you to enter the URL (try http://wiki.ca.com).
Creating a New Page

There are a variety of other options when working with Pages and Sites. For example, you can go to Manage-> Page Layout option to change the layout of your page. You can reference the documentation for more info on sites and pages.

Your new page should look something like this.
In this section, we’ll review some of the vast reporting capabilities of CA UIM.
CA UIM offers a few different ways to report on your infrastructure. We will cover a few examples here to get you started. Let’s start with “Performance Reports”. Performance Reports allow you to visualize one or more data points (QoS Metrics) in a chart format. These reports can be accessed via the Performance Reports designer in the UMP and allow you to create, save or modify existing reports. These can be displayed as a part of a dashboard or even called from other dashboards as drill downs.

1. In the UMP, select the Reports page pull-down, then “Performance Reports”.
2. In the Host window, filter for “sag-app”, then in QoS, select “QOS_CPU_USAGE”. In the target window, drag the CPU_Usage object into the chart window. Do the same for the “QOS_MEMORY_PERC_USAGE”.
3. You’ll now see the 2 metrics in the report (note you can add multiple systems/objects as well).
The performance charts are very flexible and data can be modified, viewed in different ways, exported or saved (for reference in a dashboard).

1. Configure the report to display baselines, percentiles...etc.
2. View the raw data, generate a URL link to the report....
3. Add more charts to your report...
4. Save and export your data.
Another reporting capability is Unified Reporter. The Unified Reporter is an engine that lets you produce pre-configured reports for a variety of needs, as well as create your own custom reports.

1. Select “Unified Reports” under the Reports page pull down.
2. You can find the pre-created reports by navigating the Folder Hierarchy to the Nimsoft Monitor reports in the Public folder, or choose the Library from the menu.
3. Select the Servers folder, then the Servers By CPU Usage report.
4. The reports can also be exported in a variety of formats.
Here you will find out about creating SLA’s in UIM. SLAs are powerful ways in which you can understand service levels and report on service delivery.
SLA’s are an extremely powerful way to monitor your infrastructure in business terms. With SLAs, you can create service level objectives (SLOs) that are comprised of different performance and availability metrics. The SLA status is then driven by the metrics defined within associated SLOs. You can represent the delivery of applications and services as SLAs, providing high level visibility on how well those services are performing. For more detail on SLAs, you can reference the documentation here.

1. To create an SLA(s), you must first add the SLM portlet to a new or existing page. Select Add->Page to add a new page. In the new page, select Add->Portlet and choose “SLM”.
2. In the SLM view, select NEW->Service Level Agreement
3. In the SLA creation window, give it a name and select New in the “Objectives” tab.

4. As you can see, there is a great deal of options and flexibility. In the quality of service tab, select the New button.

5. As an example select QOS_NET_CONNECT, source of UIM and target of “ny-wan:ping” (that was configured previously).

6. You can set a threshold as well.

7. You now have a simple SLA, looking at response time for the ny-wan device. You can now choose your compliance period (day, week, month)

You can now leverage the sla data in dashboards and reports, as well as receive alerts on breaches of compliance. This gives you the ability to understand at a high level how services, groups or locations are performing.
In this section, we’ll review some of the vast reporting capabilities of CA UIM.
Thank you for your interest in CA UIM. We hope the On-Demand Trial experience was a positive one. Please remember, we took you through a very small subset of use-cases just to give you a basic understanding of UIM. We can certainly assist you with other use-cases or capabilities that you require. Listed below is additional reference material you might find helpful.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA UIM Product Documentation</td>
<td>Links to all of the product documentation.</td>
</tr>
<tr>
<td>CA UIM Probe List</td>
<td>Listing of all probes, with links to associated documentation.</td>
</tr>
<tr>
<td>CA UIM Architecture White Paper</td>
<td>Much more detail on the CA UIM architecture.</td>
</tr>
<tr>
<td>CA UIM Reporting and UI Reference White Paper</td>
<td>More detail on the various ways to view data and report on your infrastructure.</td>
</tr>
<tr>
<td>CA UIM API’s Whitepaper</td>
<td>UIM has a powerful set of APIs you can leverage to integrate with other data sources – learn more!</td>
</tr>
</tbody>
</table>