Bradford Wired Rollout Process

This contains the process for rolling out Bradford to the wired networks, with some step by step instruction. The goal is to have a smooth transition for technicians, with as little disruption as possible to end users. This documentation is specifically for the wired networks, however much of the information is relevant for the wireless networks.

The sections of this document generally match the phases of the implementation.

Sections
Pre-registering Hosts......................................................................................................................... 2
  Registering many hosts.................................................................................................................... 2
  Registering a single “Rogue” host.................................................................................................. 3
  Registering a single host that has never connected to the wired network................................. 5
  Registering a host through a web browser on the end station....................................................... 6
Notification to End Users.................................................................................................................. 7
Deploying the Persistent Agent .......................................................................................................... 8
Finding remaining Rogue Hosts ........................................................................................................ 8
Checking/Adding hosts Groups.......................................................................................................... 8
Requiring Registration and the Persistent Agent............................................................................... 9
Antivirus and OS Policy .................................................................................................................... 9
**Pre-registering Hosts**

When a host is connected to the network, it will show up as a “rogue” until it is registered. Hosts can be registered through the Network Sentry Control Server at any time, and basically adds a database entry with the host information associated with an end user. This is separate from persistent agent installation, but usually performed at the same time. Logging in to the persistent agent will also register the host.

Preferably, registration is done before installing the agent, but can be done after to correct data or register a rogue host that hasn’t logged in. If a host is not registered, it will eventually be put into remediation and the end user will likely need to register.

Correct registration of shared and lab computers is important because they will otherwise be registered to the first person who logs in to the Bradford agent.

**Registering many hosts**

Information needed to manually register multiple hosts should be put in a spreadsheet to be imported. Information fields include:

- AD account (for registration, can be generic)
- Wired MAC Address
- Device Type (Windows, Mac OS X, Linux, Printer, Server, etc.)
- If a lab computer, what lab (optional, for group membership)
- Host Name (optional)
- Notes (optional)

Please send a spreadsheet with this information to the networking team, and they can import it into the database. This is by far the fastest and easiest way to register a large number of hosts.

<table>
<thead>
<tr>
<th>Wired Adapter</th>
<th>Device Type</th>
<th>AD Account</th>
<th>Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:1E:C2:0E:8A:8B</td>
<td>Mac OS X</td>
<td>10506709</td>
<td></td>
</tr>
<tr>
<td>00:06:5B:B4:03:07</td>
<td>Windows</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>E0:69:95:69:2F:58</td>
<td>Windows</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>00:24:7E:0A:C3:3E</td>
<td>Windows</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>00:16:41:EE:EA:0E</td>
<td>Windows</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>00:1C:00:26:FA:F5</td>
<td>Windows</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>00:11:0A:BB:2C:77</td>
<td>Printer</td>
<td>CSHTECH</td>
<td>Chemistry Lab PS 007</td>
</tr>
<tr>
<td>2C:9E:FC:1B:EF:A8</td>
<td>Printer</td>
<td>10506709</td>
<td></td>
</tr>
<tr>
<td>00:9C:02:07:8E:43</td>
<td>Printer</td>
<td>CSHTECH</td>
<td></td>
</tr>
</tbody>
</table>

An example of data to be imported
Registering a single “Rogue” host
A host that has already connected to the network, but has not registered is considered “rogue”. These will display with a question mark on the icon in host view. To register one of these, do the following.

1. Log in to the Network Sentry Control Server (https://nsc-wired.ad.uvu.edu:8443)
2. Select Hosts > Host View
3. In the Search box, enter the hostname, MAC address, or IP (IP may not be accurate if disconnected)
4. Right click on the rogue host and select Modify Host
5. In the Modify Host window, select Register Host to User
6. Enter the User ID (UVID or AD account)
7. Select the appropriate Device Type (Registered Host is OK for PCs and Macs)
8. Click OK, the icon will no longer have a question mark on it
Figure 2 - Modifying a host from Host View

Figure 3 - A host that has been registered and is online
Registering a single host that has never connected to the wired network

Hosts can also be registered one at a time, even if they have never connected to the network. These won’t show up in the host view, even as rogue, so the details must be entered.

1. Log in to the Wired Network Sentry Control Server (https://nsc-wired.ad.uvu.edu:8443)
2. Select Hosts > Host View
3. Click the Add button at the bottom of the window
4. Enter the User ID (UVID or AD account)
5. Enter the Host Name
6. Select the appropriate Device Type (Registered Host is OK for PCs and Macs)
7. In the Adapters section, click the Add button
   a. Enter the Physical Address (MAC) of the host
   b. Select the appropriate Media Type
   c. Click OK, repeat for other adapters if necessary (not necessary to add all adapters, only those that will connect to the network)
8. When the host connects, it will already be registered on the network. (However, the agent may need to be installed, etc.)
Registering a single host through a web browser on the end station

End users can pre-register their own devices before it is required. This is done by going to the registration web page: https://nsa-wired.ad.uvu.edu/registration. This is the same web page they would get on the registration network, but can also be done on the production networks. Logging in to the web page will register the host, which will then automatically download the persistent agent. The agent should be installed at that point if possible.
Notification to End Users

End users should be notified of the changes that they will see, which will hopefully have minimal impact. This will be important for agent installation, as well as registration and policy enforcement. An example of an email to end users:

The Bradford Persistent Agent will be installed on computers connected to the wired network, starting on [Date]. You may see a popup window similar to the one below. This is safe and should be logged in with your UVID credentials in order to complete the registration.

If you have a Mac, or would like to install manually, the Bradford agent can be downloaded here: https://nsa-wired.ad.uvu.edu/registration. The software is also available from the UVU Network downloads page, as well as my.uvu.edu in this area:

My.uvu.edu
  Employees Tab
  Technology Services and Support
  Software Downloads area
  (Select Mac OS or Windows, then Bradford Agent)

Bradford is a software used to increase security and transparency on the network, and is already functioning on Wi-Fi connections. Eventually, the wired network will function in a similar way to the wireless, requiring a one-time registration before devices can access the network.

Please contact the IT Service Desk if you experience any problems.

We will also be sending out information through various media to inform the campus community.
Deploying the Persistent Agent
The persistent agent can be installed in the background through SCCM. When the software is installed, it will immediately start communicating with the Bradford servers, even if policy is not enabled on that part of the network. Because of this, the registration window may pop up.

If the host is already registered on the control server, the registration will not change. If the host is not registered, it will automatically register it to the logged in user, as long as it is an AD account.

The agent can also be manually installed. It can be downloaded from my.uvu.edu, or here: https://www.uvu.edu/network/wireless/downloads.html

End users can also install the agent from the registration page:
https://nsa-wired.ad.uvu.edu/registration

Managing Agent Notifications
Popup notifications can be managed through group policy. Currently there are two group policy objects. Note that these policies may prevent information showing why a host has a problem to the end user. Use with caution, the Bradford icon will show network status as normal even when it is not.

NET-BradfordPA-LABS
This group policy will disable balloon notifications, as well as the login dialogue. This policy is intended for use in labs, to prevent notifications to users that do not have access to resolve issues.

NET-BradfordPA
This group policy will disable the login dialogue, but not balloon notifications. This policy is intended for initial deployment of the agent, which should automatically register to the logged in user. It’s not recommended to leave this policy applied long term, in case the host needs to be re-registered.

Finding remaining Rogue Hosts
Before turning on any enforcement, all remaining rogue hosts should be found and registered. If these hosts are left as rogue, they will have limited or no access when registration is enforced, causing disruption to the end users. Hosts with no web browser cannot be registered by the end user at this time, but may be able to at a future date.

Checking/Adding hosts Groups
Hosts such as printers should be added to the printers group to ensure that they will not be scanned and put in remediation. If this was done correctly in pre-registration it is not an issue. These groups are typically for embedded devices and others that cannot install the agent. It’s also important to add lab
computers to a group so that these can have a separate policy. If the group already exists, hosts can be added from host view by right clicking and selecting Group Membership.

**Requiring Registration and the Persistent Agent**

When registration is required, hosts that are considered rogue will be put into a registration network until they are registered. Registration is enforced by policy, and can be implemented one switch at a time.

The persistent agent will also be required at this time, meaning that if the host was manually registered, but no agent installed, they will also be on the registration network, and get a captive portal until the agent is installed and communicating. It is important that devices that cannot have the persistent agent installed are members of the correct group to bypass the requirement for the agent.

**Antivirus and OS Policy**

Eventually the wired policy will match the wireless policy, which requires antivirus to be installed and updated, and operating systems to be current versions.