Cyber Security Initiative
UAB Campus SCCM Agent Installation
Prerequisite & Deployment Guide

June 2015
Summary

This document provides UAB departments and schools with the steps necessary to fully participate in the Campus SCCM environment. Prior to requesting agent installation, each department will need to complete a readiness survey to provide UAB IT with information needed to configure SCCM to support reporting for their systems. They will also need to review readiness participation criteria and make any adjustments to their computing environment that are necessary for participation. Once the environment meets appropriate readiness criteria, each department will deploy SCCM agents to their computing assets following the guidance provided in this document. For clarification on any aspect of these guidelines, please email ITIS-WTA@mail.ad.uab.edu.

SCCM Agent Deployment Checklist
*see below for additional details

- Complete Readiness Survey (see criteria below)
- Address Readiness Gaps
- Open AskIT Ticket (SCCM Service Configuration Request)
- Determine SCCM Agent Deployment Methods
- Test SCCM Agent Deployments
- Deploy SCCM Agents
- Complete Feedback Survey

SCCM Participation Readiness Criteria
*additional information provided in Appendix below

- IP Addresses used are either public or NAT IP addresses.
- Windows desktops / laptops are Windows 7 or higher.
- Windows servers are Windows 2003 or higher (with latest SP).
- Supported versions of Mac, Linux, or Unix-based systems are deployed (see appendices).
- SCCM is not running in your environment.
- Systems must have 500 MB free. 5GB free is preferred.
- Systems must be able to initiate communication with the campus SCCM servers.
### Steps to Deploy SCCM Agents

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1:</strong> Complete Readiness Survey</td>
<td>Please visit <a href="https://uab.co1.qualtrics.com/SE/?SID=SV_eFqUr0hshacoYXb">https://uab.co1.qualtrics.com/SE/?SID=SV_eFqUr0hshacoYXb</a> and provide the requested information. Be prepared to provide estimates on the number of servers, desktops, and laptops that run Windows, Mac, or Linux / Unix operating systems as well as AD domain (where appropriate) information. Information on IP address ranges in use by computing assets will also be required.</td>
</tr>
<tr>
<td><strong>Step 2:</strong> Address Readiness Gaps</td>
<td>If any of the readiness criteria listed above are not met, then those systems for which this is the case cannot participate in the Campus SCCM. Changes necessary to make them comply with these criteria such as OS upgrades or firewall configuration adjustments will be needed or these systems will need to be declared exempt from SCCM management. UABIT recommends as much as possible that your systems be Domain joined and not workgroup computers. While SCCM will work with workgroup computers deployment is faster and much easier with computers that are members of the UAB domain.</td>
</tr>
<tr>
<td><strong>Step 3:</strong> Open AskIT Ticket</td>
<td>Email <a href="mailto:askit@uab.edu">askit@uab.edu</a> with this subject line: <code>&lt;Department&gt;</code> - SCCM Service Configuration Request Replace “&lt;Department&gt;” with the name (or acronym) of your department or school. In the body of the email, indicate that you have completed the Readiness Survey (Step 1) and let us know of any specific questions or concerns. After this ticket has been submitted, someone on the SCCM support team will contact the department. If the person who should be contacted is not the person submitting the ticket, please provide name, phone, and email contact information for the appropriate party.</td>
</tr>
<tr>
<td><strong>Step 4:</strong> Determine SCCM Agent Deployment Methods</td>
<td>Divide the systems on which agents are to be deployed into groups based on their OS and domain membership. Review the relevant agent deployment instructions in the appendix for each group of systems.</td>
</tr>
<tr>
<td><strong>Step 5:</strong> Test SCCM Agent Deployments</td>
<td>It is recommended that agent deployment be piloted on a small number of computing assets to ensure the process is well-understood before moving forward with a larger deployment. <strong>Please note that when installing the agent any OS update settings may be overwritten one time by the agent installation. The settings will need to be added back via GPO or any another desired method.</strong></td>
</tr>
<tr>
<td><strong>Step 6:</strong> Deploy SCCM Agents</td>
<td>Follow the recommended steps for agent deployments. Be sure to consider any prerequisites listed when installing agents and see the appendix for step-by-step instructions for agent installation and SCCM Console Installation. <strong>Please Note:</strong> Some agent installations may fail even though vendor-provided instructions are correctly followed. In these cases, the agents can usually be deployed by simply attempting the process a second time. If this is not the case, the SCCM support team is available to assist in troubleshooting the problem.</td>
</tr>
<tr>
<td><strong>Step 7:</strong> Complete Feedback Survey</td>
<td>Once agents have been deployed, please complete the feedback survey at <a href="https://uab.co1.qualtrics.com/SE/?SID=SV_efcvkU35IzeSbTf">https://uab.co1.qualtrics.com/SE/?SID=SV_efcvkU35IzeSbTf</a></td>
</tr>
</tbody>
</table>
## Appendix 1 – Windows Agents

### I. Windows Agent Prerequisites

<table>
<thead>
<tr>
<th>Dependencies external to Configuration Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Installer version 3.1.4000.2435</strong></td>
</tr>
<tr>
<td><strong>Microsoft Background Intelligent Transfer Service (BITS) version 2.5</strong></td>
</tr>
<tr>
<td><strong>Microsoft Task Scheduler service</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dependencies automatically supplied during installation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Update Agent version 7.0.6000.363</strong></td>
</tr>
<tr>
<td><strong>Microsoft Core XML Services (MSXML) version 6.20.5002 or later</strong></td>
</tr>
<tr>
<td><strong>Microsoft Remote Differential Compression (RDC)</strong></td>
</tr>
<tr>
<td><strong>Microsoft Visual C++ 2010 Redistributable version 10.0.40219.1</strong></td>
</tr>
<tr>
<td><strong>Microsoft Visual C++ 2005 Redistributable version 8.0.50727.42</strong></td>
</tr>
<tr>
<td><strong>Windows Imaging APIs 6.0.6001.18000</strong></td>
</tr>
<tr>
<td><strong>Microsoft Policy Platform 1.2.3514.0</strong></td>
</tr>
<tr>
<td><strong>Microsoft Silverlight 4.0.50524.0</strong></td>
</tr>
</tbody>
</table>
*Please be advised that some prerequisites may require a restart upon installation.*

---

### II. Manual Windows Agent Installation

All the installation files needed for installing the agent on a Windows client can be found at \uabfile.ad.uab.edu\SCCM. If needed, please copy all contents of this location except for the tools folder to C:\SCCMINSTALL. This will only be required if you run into issues installing the agent on a non-domain desktop or laptop.

**Installing the SCCM Agent on:**

| Non-domain Desktop | 1. Copy the ccmsetup.exe file to the target computer.  
2. Logon the target computer with an administrator acct.  
3. Open an administrator command prompt.  
4. Change the directory to the ccmsetup.exe location and run the following command (Use Caps where noted): ccmsetup.exe SMSSITECODE=IT1 DNSSUFFIX=ad.uab.edu SMSMP=itis-sccmmp1.ad.uab.edu |
|-------------------|--------------------------------------------------------------------------------------------------|
| An ad.uab.edu domain Desktop | 1. Copy the ccmsetup.exe file to the target computer.  
2. Logon the target computer with an administrator acct.  
3. Open an administrator command prompt.  
4. Change the directory to the ccmsetup.exe location and run the following command (Use Caps where noted): ccmsetup.exe SMSSITECODE=IT1 |
| A non-AD.UAB.EDU domain/Workgroup Windows laptop | 1. Make sure that a Certificate has been issued from the Template OFF DOMAIN CLIENT for the laptop. ([see Appendix 4 – PKI Certificates](#))  
2. Open a web browser and go to https://clavisweb1.ad.uab.edu and log in with uab\blazerid and password.  
3. Select “Download a CA certificate, certificate chain, or CRL” |
4. Select “Download CA Certificate Chain”. It will ask you to save it and the default name of certnew.p7b can be used.

5. Open the file, under the certificates list you should see UABCERT1-SUBCA and UABROOT-CA. Open both of them individually and under the general tab select install.

6. Install both under the Local Machine account not the current user. The UABROOT-CA file needs to go into the Trusted Root Authorities folder and the UABCERT1-SUBCA file needs to go into the Intermediate Certificate Authorities folder.

7. Copy the contents of `\uabfile.ad.uab.edu\sccm\tools\CARegKeys` to the computer you are installing SCCM on and merge the registry keys into the computer’s registry.

8. Open MMC and add the Certificates snapin for the Local machine account

9. Under Certificates right click personal and select Request new Certificate under All tasks.

10. Follow the prompt (logging in with BlazerID and password where asked) and select UAB Certificate Authority. Click next

11. You may be prompted again for a password but you should then see the OFF DOMAIN CLIENT Template. Click the check box beside it and then select the “More information is required” link underneath the template name.

12. Under Subject name Type select Common Name and then put in the computers Name (We suggest that all computers have a similar naming scheme). Click Add and then hit OK.

13. Click enroll and the certificate should place itself in the Local Computer’s personal store.

14. Copy the contents of the SCCM folder on UABFILE (leave out the tools folder) to a New Folder named SCCMINSTALL on the root of C:

15. Open an administrator command prompt.

16. Change the directory to the folder created previously and run the command: `ccmsetup.exe /usepkicert /source:"C:\SCCMINSTALL” DNSSUFFIX=AD.UAB.EDU SMSSITECODE=IT1 SMSMP=itis-sccmcdp3.ad.uab.edu CCMHOSTNAME=itis-sccmcdp3.ad.uab.edu CCMALWAYSINF=1`

* Please Note that for Certificate enrollment to work the machine must be on the UAB network and on a wired connection initially. It is also recommended that for the agent install the laptop be on the UAB network.
II. UAB IT AD Domain Windows Agent Installation

Windows-based systems within an AD domain can have agents automatically installed by using a GPO. This approach is recommended since it will ensure the agent gets deployed to new systems as they join the domain. However, to ensure the GPO is properly configured and applied, it is recommended that it be linked initially to a test OU where it can be deployed to a limited number of machines and validated.

Following a successful test of the template, link this GPO to the department’s or school’s OU so that the agent will be automatically deployed to remaining Windows-based systems.

The SCCM support team will provide departments with a preconfigured GPO.

III. Dept. / School AD Domain Windows Agent Installation

Windows-based systems within an AD domain can have agents automatically installed by using a GPO. This approach is recommended since it will ensure the agent gets deployed to new systems as they join the domain. However, to ensure the GPO is properly configured and applied, it is recommended that it be linked initially to a test OU where it can be deployed to a limited number of machines and validated.

Following a successful test of the template, link this GPO to the department’s or school’s Domain so that the agent will be automatically deployed to remaining Windows-based systems.

The SCCM support team will guide departments in creating their own GPO within their Domain.
Appendix 2 – Macintosh Agents

I. Macintosh Agent Prerequisites


II. Macintosh Agent Installation

2. Please note that in order for a Mac to be enrolled the machine must be on the UAB Campus Network initially. This can be done via VPN if necessary.
3. Download the Mac Install package on a Windows machine and follow Microsoft’s Instructions from the link above to create the .DMG installer.
4. Open a web browser on the Mac and go to https://clavisweb1.ad.uab.edu and log in with uab\BlazerID and password.
5. Select “Download a CA certificate, certificate chain, or CRL”
6. Select “Download CA Certificate Chain”. It will ask you to save it and the default name of certnew.p7b can be used.
7. Open Keychain on the Mac and select and unlock the system container. With system still selected double click the certnew file and let it import the certificate files. It will ask you to always trust the root. Make sure that the certificates get places in the system container. The certificate names are: UABROOT-CA and UABCERT1-SUBCA. Make sure that both certificates are always trusted. Once that is done please proceed to the next step. (The download process can be used once on any machine and then the certnew file can be moved and re-imported on any Mac that needs it.)
8. Copy the DMG to the Mac client and open it and run CMClient.pkg.
9. Once it is installed the machine will need to reboot.
10. After the reboot an enrollment window will come up. You will need to enter a username and password in the form of uab\BlazerID. The Enrollment Proxy Point address is itsissccmcdp3.ad.uab.edu. Please make sure that the user enrolling this machine has permissions to the ConfigMgr Mac Client Certificate Template (see Appendix 4 – PKI Certificates). You can also get to the enrollment window by going to system preferences and selecting the Configuration Manager Preference pain.
11. Once the machine is enrolled it should start reporting to SCCM at the pre-determined intervals.
Appendix 3 – Unix/Linux Agents

I. Unix / Linux Agent Prerequisites

Supported configurations and hardware requirements for UNIX/Linux: See the Client Requirements for Linux and UNIX Servers section in the Supported Configurations for Configuration Manager topic. http://technet.microsoft.com/en-us/library/gg682077.aspx

II. Unix / Linux Agent Installation

To install the client for Linux and UNIX, you run a script on each Linux or UNIX computer. The script is named install and supports command line properties that modify the installation behavior and reference the client installation package. The install script and client installation package must be located on the client. The client installation package contains the Configuration Manager client files for a specific Linux or UNIX operating system and platform. Each client installation package contains all the necessary files to complete the client installation and unlike Windows-based computers, does not download additional files from a management point or other source location. The SCCM install package For Unix/Linux can be downloaded at http://www.microsoft.com/en-us/download/details.aspx?id=39360

After you install the Configuration Manager client for Linux and UNIX, you do not need to reboot the computer. As soon as the software installation is complete, the client is operational. If you reboot the computer, the Configuration Manager client restarts automatically. The installed client runs with root credentials. Root credentials are required to collect hardware inventory and perform software deployments.

Following is the command format: ./install -mp <computer> -sitecode <sitecode> <property #1> <property #2> <client installation package>

Command line Actions Example: ./install -mp itis-sccmp1.ad.uab.edu -sitecode IT1 ccm-Universal-x64.<build>.tar

- install is the name of the script file that installs the client for Linux and UNIX. This file is provided with the client software.
- mp itis-sccmp1.ad.uab.edu specifies the initial management point that is used by the client.
- sitecode IT1 specifies the client is assigned to the site with the site code of IT1.
- ccm-Universal-x64.<build>.tar is the name of the client installation .tar package for this computer operating system, version, and CPU architecture.
Appendix 4 – PKI Certificates

I. Laptops, Unix, and Mac Computers

When configuring Windows laptops PKI certificates must be issued to the machines for Authentication purposes if they are going to be managed outside of the UAB network. Macs always require certificates regardless of their location. Three certificate templates have been made for these types of clients. In order for certificates to be issued you will need to create a number of AD groups within the AD.UAB.EDU Domain. Please see the below Bullet points for clarification on which groups you will need to create.

Please let the SCCM Admins know when you have completed this by updating your SCCM deployment ticket and we will add the groups created to the certificate templates and contact you for next steps.

• If you have Windows laptops that are on the AD.UAB.EDU domain please create a group called YOUR OU-cClient. Please populate this group with the computer accounts of your AD joined laptops.
• If you have Windows based Laptops that are not joined to the AD.UAB.EDU domain please create a group named YOUR OU-cOFFDOMAIN. Please populate this group with the user accounts of the person who will be using the laptop. Feel free to also add the user accounts of your admins as well.
• If you have Macs (whether they are laptops or desktops) please create a group named YOUR OU-cMacUser. Please populate this group with the user names of whoever will be enrolling these macs for SCCM. This can be your Admins or the users of the Macs.

In the case of deploying the Agent to All non-ad.uab.edu Domain computers (Mac, Linux, Windows) there may need to be changes made to the machine’s configuration. In the case of Windows, those computers that are not on a domain the Workgroup names of the computers will need to be changed to something that helps identify the department (ex. SOPH laptops not on any domain would have their workgroup names changed to SOPH). For Macs and Unix boxes it is recommended that the name be changed if at all possible to reflect the departments name (ex. Mac would be named SOPH-*). This change is necessary so that the auto-population of an SCCM collection can occur. Without this collections would have to be manually populated which takes longer. Please note that Macs that are on the domain will not need a name change.
Appendix 5 – SCCM Console Installation

To install the console please follow the steps below.

1. Copy the following folder to a local location \uabfile.ad.uab.edu\sccm\tools\ConsoleSetup.

2. Run ReportViewer.exe located in the ConsoleSetup folder and accept the default settings.

3. Run ConsoleSetup.exe located in the ConsoleSetup folder and accept the default settings. The site server is ITIS-SCCMPS1.ad.uab.edu.

4. Run CM12-R2CU3-KB2994331-X64-ENU.exe located in CU3 folder inside the ConsoleSetup folder and accept the default settings. The site server and site code is the same as step 2 if prompted.

The console should automatically connect to the proper server if installed on a computer in the AD.UAB.EDU domain. Please refer to the following link below when installing the console on a computer that is not a member of the AD.UAB.EDU domain.