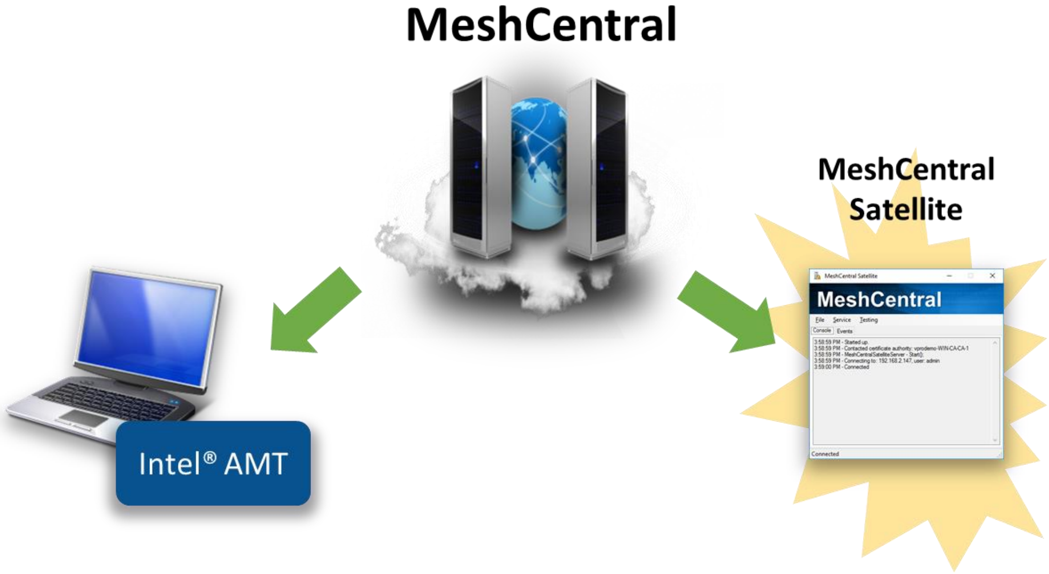
MeshCentral

Satellite



```
3:58:59 PM - Started up.
3:58:59 PM - Contacted certificate authority: vprodemo-WIN-CA-CA-1
3:58:59 PM - MeshCentralSatelliteServer - Start();
3:58:59 PM - Connecting to: 192.168.2.147, user: admin
3:59:00 PM - Connected
```

Version 0.0.1

Monday, April 11, 2022
Ylian Saint-Hilaire

Table of Contents

Document Changes

April 11, 2022 – 0.0.1

Initial version.

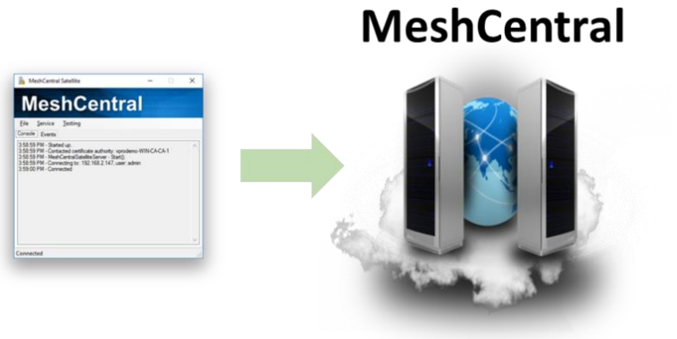
1. Abstract

MeshCentral Satellite is a Windows application that acts as a relay between a Windows Active Directory Domain and a MeshCentral Server. Once setup, the MeshCentral server can request that MeshCentral Satellite create an 802.1x computer profile for Intel AMT in the domain, or ask a certificate authority to issue or revoke a certificate.

2. Introduction

A MeshCentral server can run in the cloud on a Linux server, but it may occasionally need to interact with a domain controller to perform some operations. MeshCentral Satellite is built to perform this function. MeshCentral Satellite is a Windows application built in C# and must run on a computer that is part of a domain and must run with sufficient rights to perform LDAP object addition and removal. If a certificate authority (CA) needs to be used, MeshCentral Satellite needs to have sufficient rights to ask the CA issue or revoke certificates.

MeshCentral Satellite should run on a computer that is always on. Once running, it will attempt to connect to the MeshCentral server and keep the connection open awaiting requests.



```
3:58:59 PM - Started up.
3:58:59 PM - Contacted certificate authority: vprodemo-WIN-CA-CA-1
3:58:59 PM - MeshCentralSatelliteServer - Start().
3:58:59 PM - Connecting to: 192.168.2.147, user: admin
3:59:00 PM - Connected
```

Currently, MeshCentral Satellite can perform four operations on behalf of the MeshCentral server:

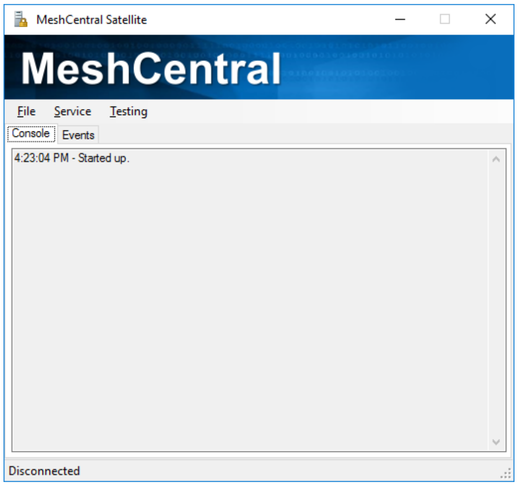
- Create an Intel AMT domain computer.
- Remove an Intel AMT domain computer.
- Issue a certificate for Intel AMT.
- Revoke an Intel AMT certificate.

MeshCentral Satellite can run both as a standalone application which is practical to get started and it can be setup as a background Windows Service for long term operations. To get started, we will run it as a standalone application and start working on getting it setup.

3. Installation and Configuration

Start by creating an empty folder on a computer that is part of the domain you need to interact with. For example, create a “c:\MeshCentralSatellite” then copy “MeshCentralSatellite.exe” into that folder. You can find that executable in the “node_modules/meshcentral/agents” folder of your server. If it’s not present, update your server to the latest version and look again.

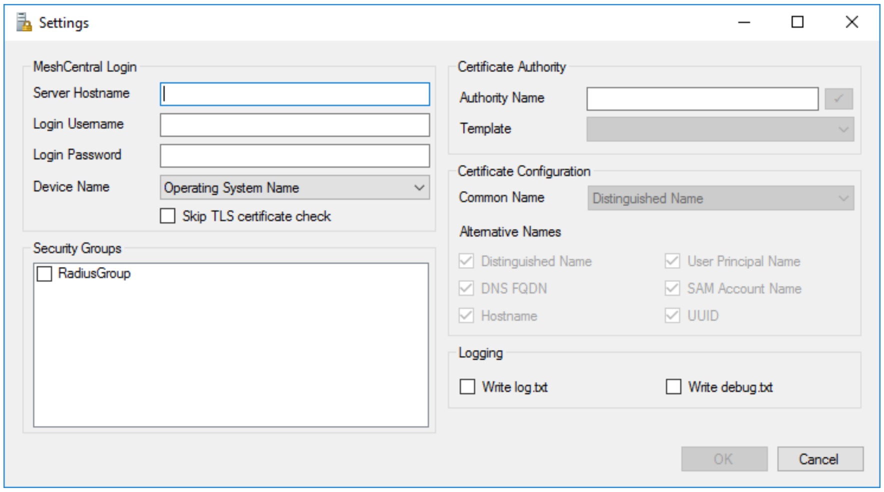
Once started you should see something this:



4:23:04 PM - Started up.

Disconnected

Go in the file menu and select “Settings…”, this is where all of the MeshCentral Satellite setting are. It includes sections to connect to your MeshCentral server. Security groups you want device to join and Certificate settings.



MeshCentral Login

Server Hostname
Login Username
Login Password
Device Name: Operating System Name
☐ Skip TLS certificate check

Security Groups

☐ RadiusGroup

Certificate Authority

Authority Name
Template

Certificate Configuration

Common Name: Distinguished Name

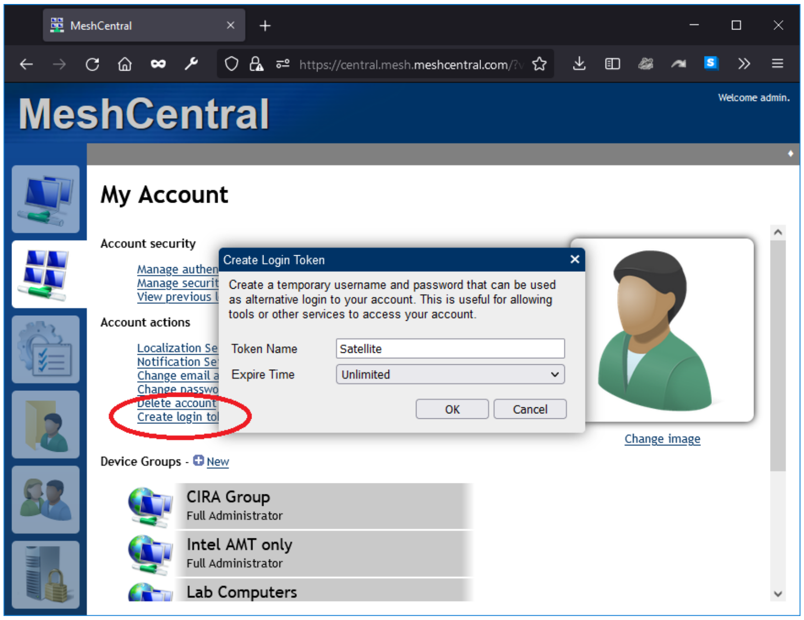
Alternative Names

☑ Distinguished Name ☑ User Principal Name
☑ DNS FQDN ☑ SAM Account Name
☑ Hostname ☑ UUID

Logging

☐ Write log.txt ☐ Write debug.txt

First, enter your MeshCentral server hostname and username and password. MeshCentral Satellite can’t use two-factor authentication (2FA) so you need to create a user account in MeshCentral for Satellite or you can create a login token in the “My Account” section of MeshCentral with an unlimited expire time and cut & paste the username and password given into MeshCentral Satellite.



Create Login Token

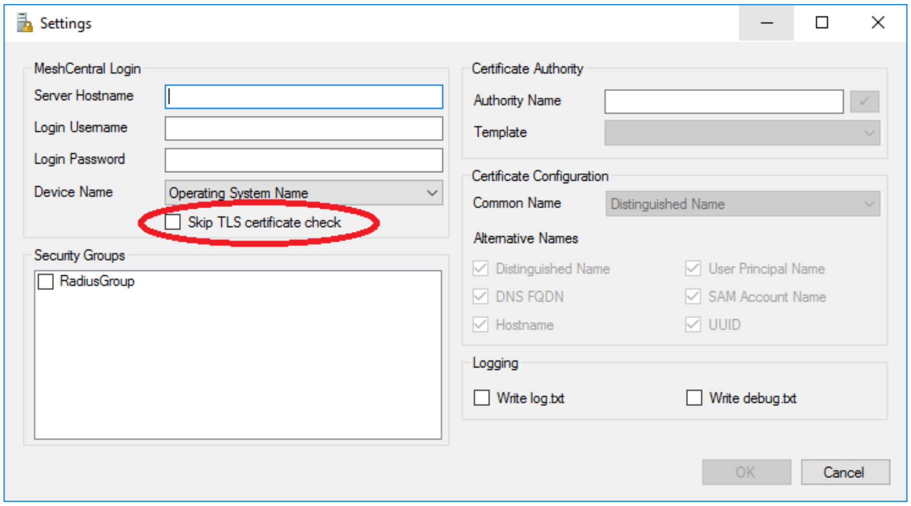
Create a temporary username and password that can be used as alternative login to your account. This is useful for allowing tools or other services to access your account.

Token Name: Satellite

Expire Time: Unlimited

OK Cancel

If your MeshCentral server is a test server that does not have a real TLS certificate, you can opt to ignore the TLS certificate on connection but this is not secure and so, not recommended.


Settings

MeshCentral Login

Server Hostname:

Login Username:

Login Password:

Device Name: Operating System Name

□ Skip TLS certificate check

Security Groups

□ RadiusGroup

Certificate Authority

Authority Name:

Template:

Certificate Configuration

Common Name: Distinguished Name

Alternative Names

☑ Distinguished Name ☑ User Principal Name

☑ DNS FQDN ☑ SAM Account Name

☑ Hostname ☑ UUID

Logging

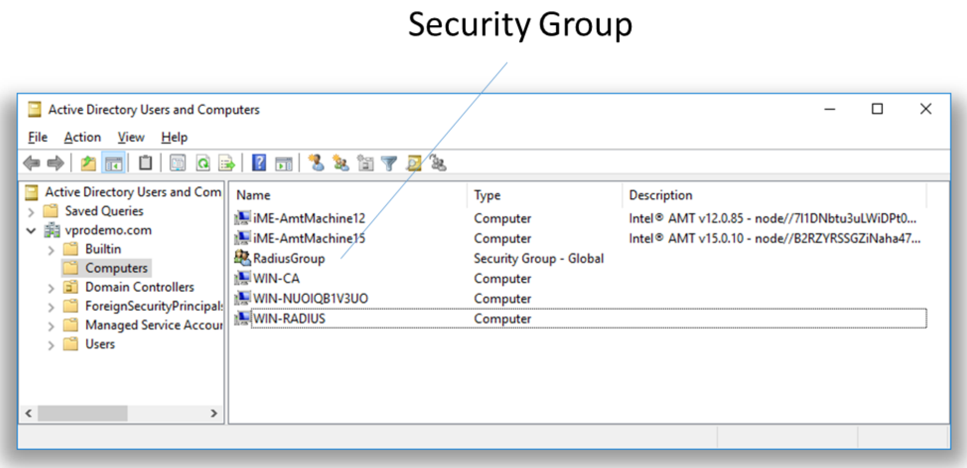
□ Write log.txt □ Write debug.txt

OK Cancel

The “Device Name” has two options, “Operating System Name” or “Node Identifier”. If you opt for “Operating System Name”, Intel AMT devices will show as, for example, “iME-ComputerName” in the list of domain computers. If “node identifier” is used, Intel AMT devices will look like “iME-xxxxxxxxxxx” where xxx is the start of the MeshCentral node identifier for this device.

Using the node identifier is more secure as it can’t easily be replicate by any other device. The operating system name would be impersonated by another device causing various security issues.

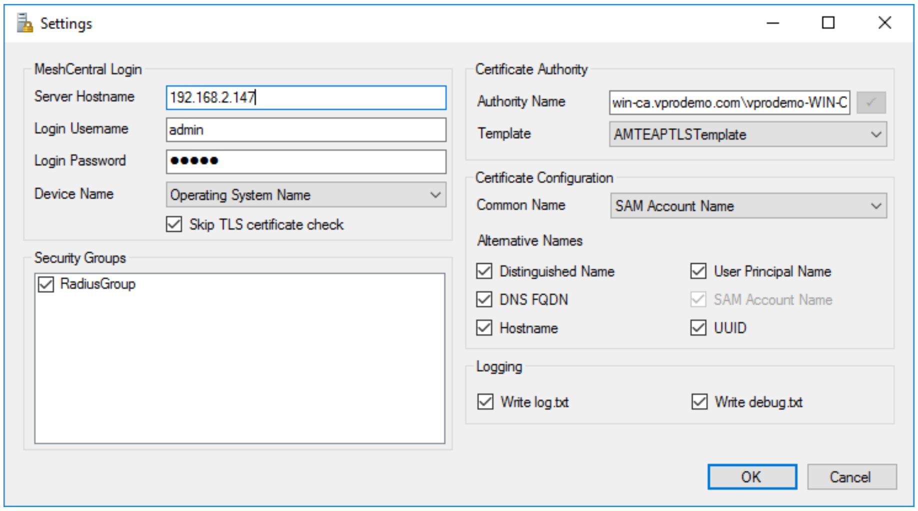
The security groups section will list any security groups created until the “Computers” section of the domain controller. Checking one or more of these security groups will automatically going new Intel AMT devices to these groups.



Security Group

Name	Type	Description
iME-AmtMachine12	Computer	Intel® AMT v12.0.85 - node//7I1DNbtu3uLWiDPt0...
iME-AmtMachine15	Computer	Intel® AMT v15.0.10 - node//B2RZYRSSGZiNaha47...
RadiusGroup	Security Group - Global	
WIN-CA	Computer	
WIN-NUOIQB1V3UO	Computer	
WIN-RADIUS	Computer	

Lastly, we have the certificate authority and certificate settings. If a certificate authority needs to used, enter the name of the CA which is in the format "<computername>\<caname>" you can then hit the check box next to the name and select the certificate template to use.



MeshCentral Login

Server Hostname: 192.168.2.147
Login Username: admin
Login Password: ●●●●●
Device Name: Operating System Name
☑ Skip TLS certificate check

Security Groups

☑ RadiusGroup

Certificate Authority

Authority Name: win-ca.vprodemo.com\vprodemo-WIN-C
Template: AMTEAPTLSTemplate

Certificate Configuration

Common Name: SAM Account Name

Alternative Names

☑ Distinguished Name ☑ User Principal Name
☑ DNS FQDN ☑ SAM Account Name
☑ Hostname ☑ UUID

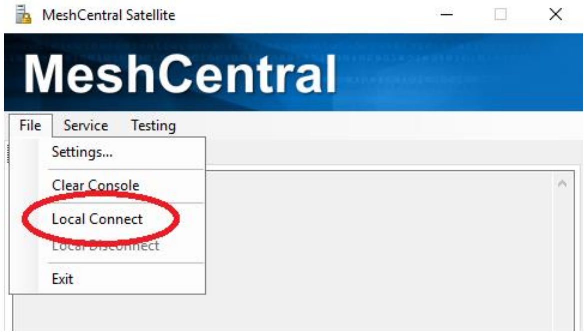
Logging

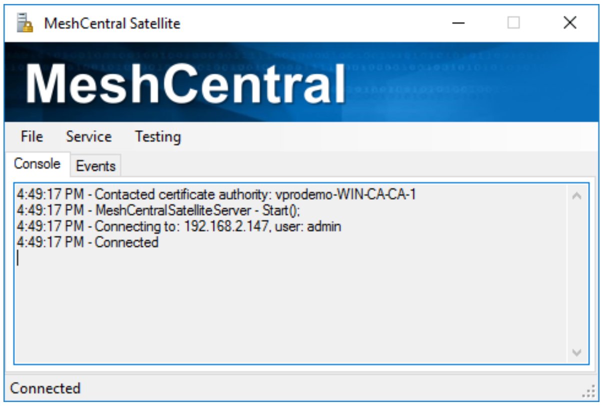
☑ Write log.txt ☑ Write debug.txt

For certificate configuration, you can leave it as-is with "SAM Account Name" and the common name and all alternative names selected.

Once done, you can hit ok. The settings will be saved in a file called "config.txt" in plain text in the same folder as "MeshCentralSatellite.exe". Make sure not to grant access to this file to anyone not authorized to do so as it will have the MeshCentral login username and password.

Once done, select "Local Connect" the "Files" menu to connect to the MeshCentral server.





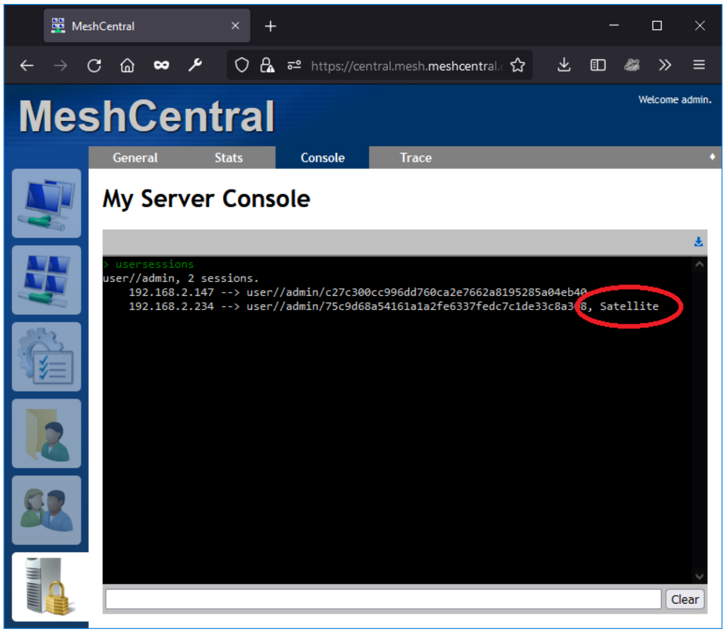
```
4:49:17 PM - Contacted certificate authority: vprodemo-WIN-CA-CA-1
4:49:17 PM - MeshCentralSatelliteServer - Start();
4:49:17 PM - Connecting to: 192.168.2.147, user: admin
4:49:17 PM - Connected
```

Connected

MeshCentral Satellite should be connected and ready to receive commands from the server.

4. Checking the connection

In order to make sure the server correctly recognizes the MeshCentral Satellite connection, you can go to the server console and type “usersession”. The Satellite session should be marked.



```
> usersessions
user//admin, 2 sessions.
    192.168.2.147 --> user//admin/c27c300cc996dd760ca2e7662a8195285a04eb40
    192.168.2.234 --> user//admin/75c9d68a54161a1a2fe6337fedc7c1de33c8a308, Satellite
```

Currently, you should only have a single satellite session per user. In the future, multiple sessions could be supported for redundancy.

5. Configuring Intel® AMT 802.1x

To start using MeshCentral Satellite, you can configure Intel AMT with an 802.1x profile, this is done in the domain section of the config.json. Here is an example of an 802.1x EAP-TLS profile that will require that Intel AMT be issued a certificate:

```
"AmtManager": {
  "802.1x": {
    "AuthenticationProtocol": "EAP-TLS",
    "SatelliteCredentials": "admin"
  },
  "WifiProfiles": [
    {
      "ssid": "Network-8021x",
      "authentication": "wpa2-802.1x",
      "encryption": "ccmp-aes"
    }
  ]
}
```

In this following example, MSCHAPv2 is used and so, MeshCentral Satellite will need to generate a random password, save it in the active directory and send the password back to MeshCentral for Intel AMT configuration:

```
"AmtManager": {
  "802.1x": {
    "AuthenticationProtocol": "PEAPv0/EAP-MSCHAPv2",
    "SatelliteCredentials": "admin"
  },
  "WifiProfiles": [
    {
      "ssid": "Network-8021x",
      "authentication": "wpa2-802.1x",
      "encryption": "ccmp-aes"
    }
  ]
}
```

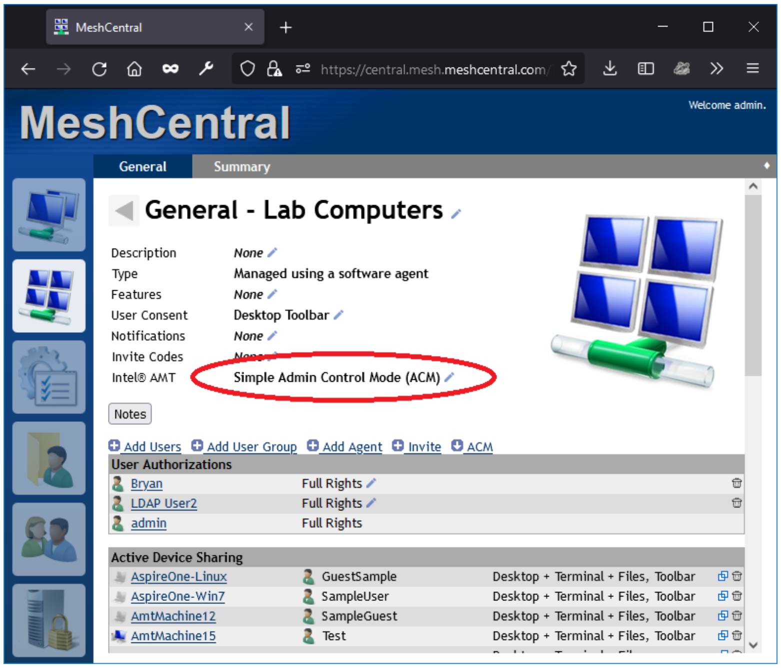
The second example does not require that a certificate authority be setup, the first example does. In both cases, the WIFI profile is set to “wpa2-802.1x” and so, the 802.1x profile will be setup for both the Intel AMT wired interface and the specified WIFI profile for wireless.

Note that is both examples, “SatelliteCredentials” indicates the account name that MeshCentral Satellite will be connected on. In our case, we used the “admin” account that matches the account configuration we used in sections 3 and 4.

Make these changes to the config.json and restart the MeshCentral server. Once done, any device groups that are set to configure Intel AMT will generate operations for MeshCentral Satellite.

6. Computer and certificate operations

Once MeshCentral and MeshCentral Satellite are setup, make sure a device group has an active Intel AMT policy. In the example below, we have a device group with an Admin Control Mode (ACM) activation policy.



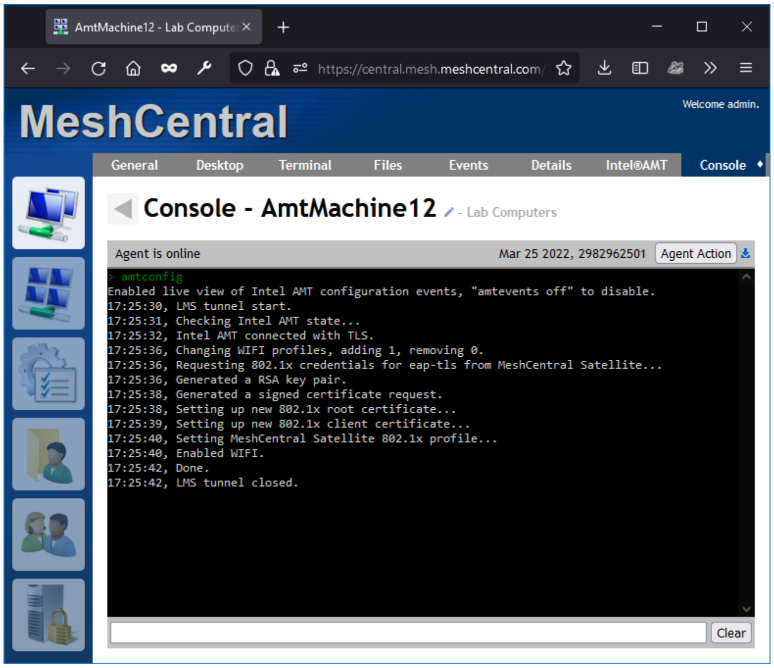
General - Lab Computers

Description None
Type Managed using a software agent
Features None
User Consent Desktop Toolbar
Notifications None
Invite Codes None
Intel® AMT Simple Admin Control Mode (ACM)

User Authorizations	
Bryan	Full Rights
LDAP User2	Full Rights
admin	Full Rights

Active Device Sharing		
AspireOne-Linux	GuestSample	Desktop + Terminal + Files, Toolbar
AspireOne-Win7	SampleUser	Desktop + Terminal + Files, Toolbar
AmtMachine12	SampleGuest	Desktop + Terminal + Files, Toolbar
AmtMachine15	Test	Desktop + Terminal + Files, Toolbar

Computers connecting to this device group will automatically be setup with the new 802.1x and WIFI profile, but you can go in an agent console and type “amtconfig” to force the check of the Intel AMT configuration. In our case, it looks like this:

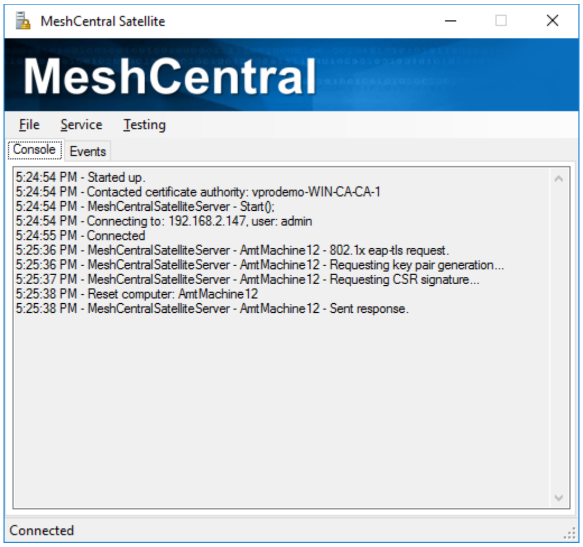


Console - AmtMachine12 - Lab Computers

Agent is online Mar 25 2022, 2982962501

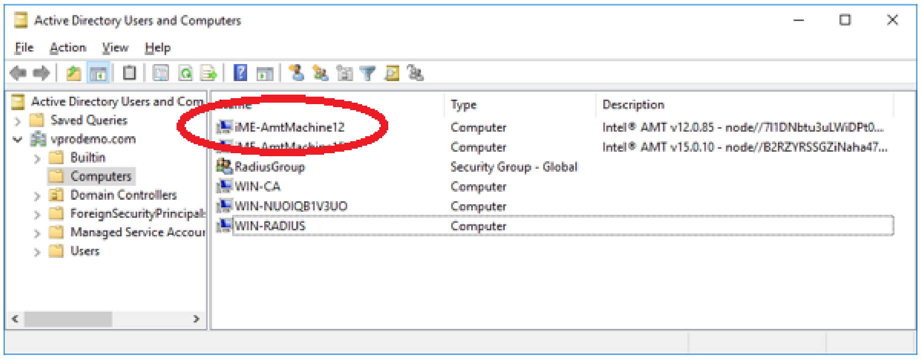
```
> amtconfig
Enabled live view of Intel AMT configuration events, "amtevents off" to disable.
17:25:30, LMS tunnel start.
17:25:31, Checking Intel AMT state...
17:25:32, Intel AMT connected with TLS.
17:25:36, Changing WIFI profiles, adding 1, removing 0.
17:25:36, Requesting 802.1x credentials for eap-tls from MeshCentral Satellite...
17:25:36, Generated a RSA key pair.
17:25:38, Generated a signed certificate request.
17:25:38, Setting up new 802.1x root certificate...
17:25:39, Setting up new 802.1x client certificate...
17:25:40, Setting MeshCentral Satellite 802.1x profile...
17:25:40, Enabled WIFI.
17:25:42, Done.
17:25:42, LMS tunnel closed.
```

MeshCentral is adding a new WIFI profile, setting up 802.1x and issuing a new Intel AMT certificate from the domain CA. This was all done in a few seconds. On the MeshCentral Satellite side, we see this:



```
5:24:54 PM - Started up.
5:24:54 PM - Contacted certificate authority: vprodemo-WIN-CA-CA-1
5:24:54 PM - MeshCentralSatelliteServer - Start();
5:24:54 PM - Connecting to: 192.168.2.147, user: admin
5:24:55 PM - Connected
5:25:36 PM - MeshCentralSatelliteServer - AmtMachine12 - 802.1x eap-tls request.
5:25:36 PM - MeshCentralSatelliteServer - AmtMachine12 - Requesting key pair generation...
5:25:37 PM - MeshCentralSatelliteServer - AmtMachine12 - Requesting CSR signature...
5:25:38 PM - Reset computer: AmtMachine12
5:25:38 PM - MeshCentralSatelliteServer - AmtMachine12 - Sent response.
```

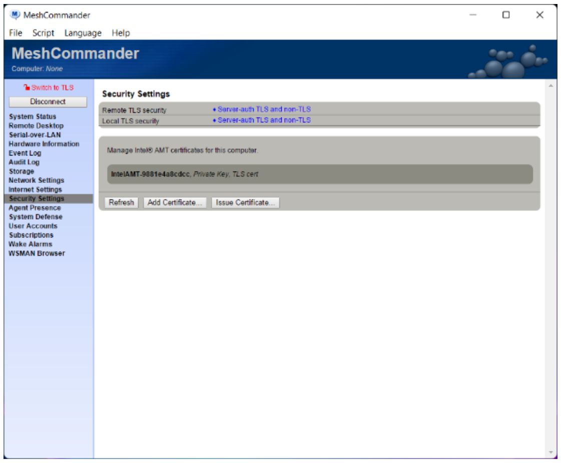
The MeshCentral Satellite received an 802.1x EAP-TLS request. It asked Intel AMT to generate a RSA key pair, to sign a certificate request, forwarded the request to the domain CA for signature and finally returned the final certificate to Intel AMT. The computer account in the domain was also updated and looks like this:



Name	Type	Description
iME-AmtMachine12	Computer	Intel® AMT v12.0.85 - node//7I1DNbtu3uLWiDPt0...
iME-AmtMachi[illegible]	Computer	Intel® AMT v15.0.10 - node//B2RZYRSSGZiNaha47...
RadiusGroup	Security Group - Global	
WIN-CA	Computer	
WIN-NUOIQB1V3UO	Computer	
WIN-RADIUS	Computer	

The new Intel AMT device was added to the domain along with the Intel AMT version and node identifier in the description. If “Node Identifier” was selected as the computer name in MeshCentral Satellite settings, the friendly name would be in the description and the node identifier would be used as the device name.

Finally, it’s worth taking a look at how Intel AMT was configured before and after this operation. Before setting up the 802.1x profile, Intel AMT looked like this:

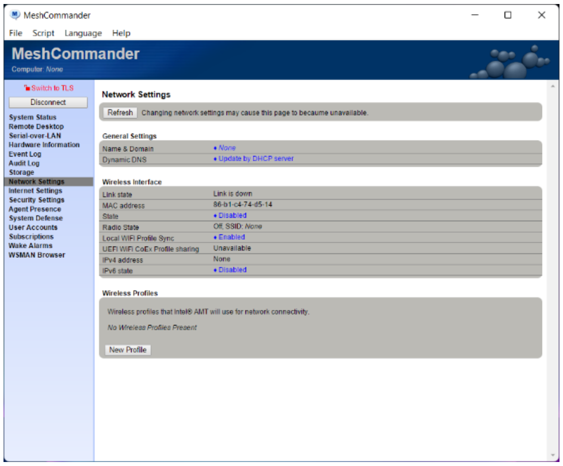


Security Settings

Remote TLS security	• Server-auth TLS and non-TLS
Local TLS security	• Server-auth TLS and non-TLS

Manage Intel® AMT certificates for this computer.

IntelAMT-9881e4a8cdcc, *Private Key, TLS cert*



Network Settings

Changing network settings may cause this page to becaume unavailable.

General Settings

Name & Domain	• *None*
Dynamic DNS	• Update by DHCP server

Wireless Interface

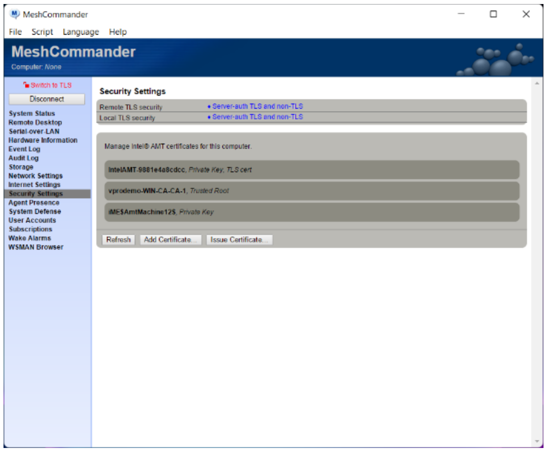
Link state	Link is down
MAC address	86-b1-c4-74-d5-14
State	• Disabled
Radio State	Off, SSID: *None*
Local WIFI Profile Sync	• Enabled
UEFI WiFi CoEx Profile sharing	Unavailable
IPv4 address	None
IPv6 state	• Disabled

Wireless Profiles

Wireless profiles that Intel® AMT will use for network connectivity.

No Wireless Profiles Present

Note that there is no 802.1x profiles or WIFI profiles. After the new configuration, MeshCommander shows Intel AMT looking like this:



Security Settings

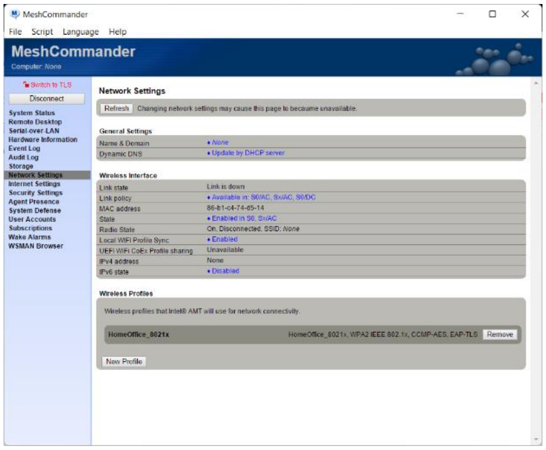
Remote TLS security	• Server-auth TLS and non-TLS
Local TLS security	• Server-auth TLS and non-TLS

Manage Intel® AMT certificates for this computer.

IntelAMT-9881e4a8cdcc, *Private Key, TLS cert*

vprodemo-WIN-CA-CA-1, *Trusted Root*

iME$AmtMachine12$, *Private Key*



Network Settings

Changing network settings may cause this page to becaume unavailable.

General Settings

Name & Domain	• *None*
Dynamic DNS	• Update by DHCP server

Wireless Interface

Link state	Link is down
Link policy	• Available in: S0/AC, Sx/AC, S0/DC
MAC address	86-b1-c4-74-d5-14
State	• Enabled in S0, Sx/AC
Radio State	On, Disconnected, SSID: *None*
Local WIFI Profile Sync	• Enabled
UEFI WiFi CoEx Profile sharing	Unavailable
IPv4 address	None
IPv6 state	• Disabled

Wireless Profiles

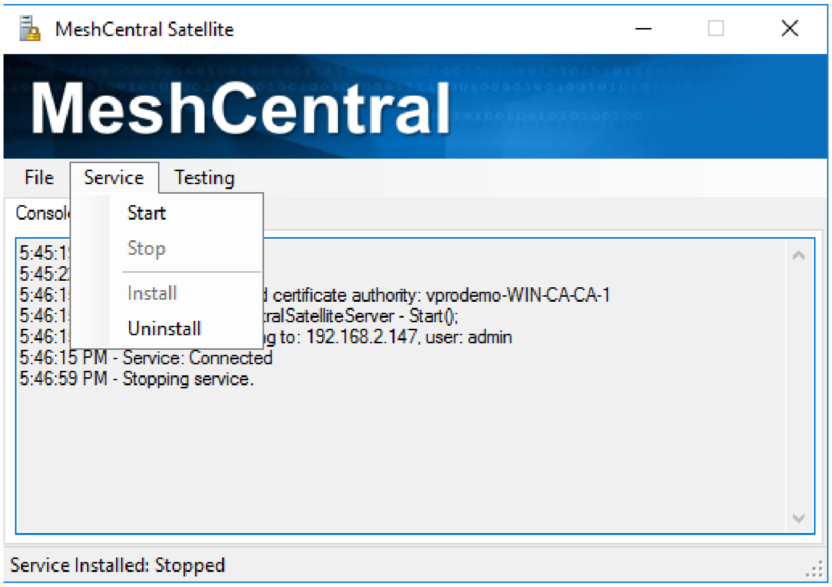
Wireless profiles that Intel® AMT will use for network connectivity.

HomeOffice_8021x	HomeOffice_8021x, WPA2 IEEE 802.1x, CCMP-AES, EAP-TLS

There are now two new certificates in the “Security” tab. One if the root of the domain CA, the other is the certificate assigned to the Intel AMT device by the CA. You also see the WIFI 802.1x profile. In this example, the device did not have a wired network interface, but if it did, 802.1x would also be setup for the wired interface.

7. Running as a Background Service

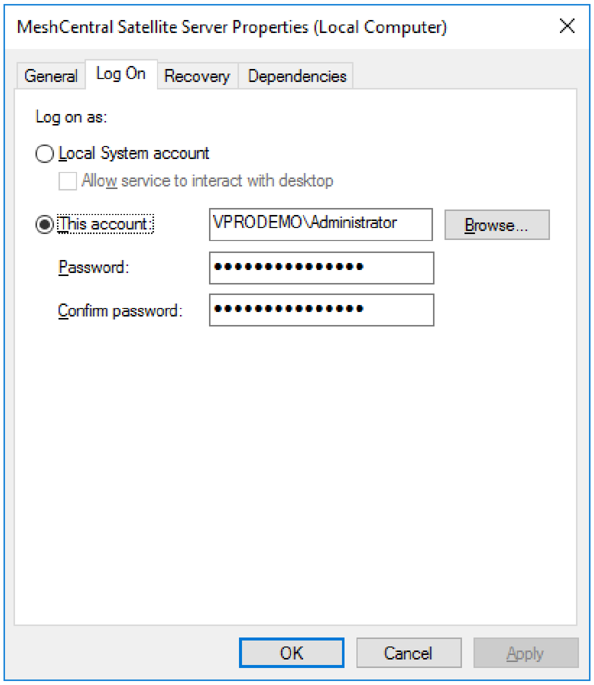
MeshCentral Satellite can be run as a background service. This is useful when running for lang periods on a domain server. You can use the “Service” menu in MeshCentral Satellite to install, start, stop and uninstall the Windows service. Make sure to come and run “MeshCentralSatellite.exe” from the correct location you want to install the Windows Service from.



```
5:45:1
5:45:2
5:46:1                     certificate authority: vprodemo-WIN-CA-CA-1
5:46:1                    ralSatelliteServer - Start();
5:46:1                    g to: 192.168.2.147, user: admin
5:46:15 PM - Service: Connected
5:46:59 PM - Stopping service.
```

Service Installed: Stopped

Since MeshCentral Satellite need to have domain rights to add and remove computer objects from the active directory and to have certificate authority (CA) rights, you may want to install the service, go in the service manager and change the “Log On” account to one with the proper rights.



Log on as:

○ Local System account

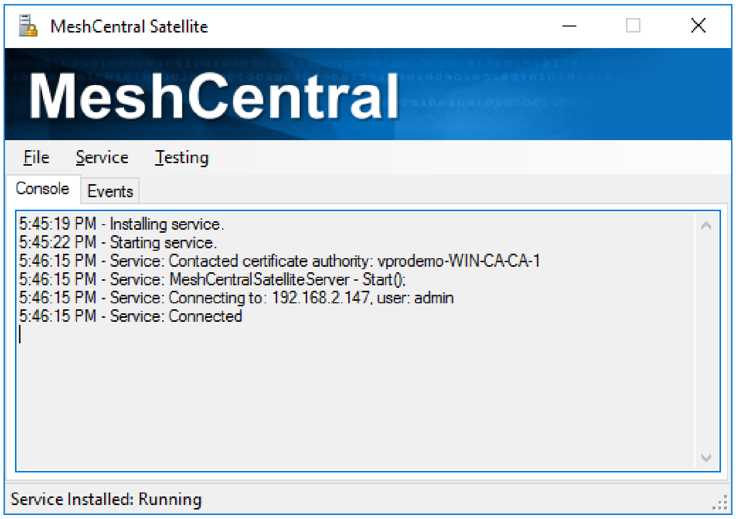
□ Allow service to interact with desktop

● This account: VPRODEMO\Administrator

Password: •••••••••••••••

Confirm password: •••••••••••••••

Once set, you can start the service from within MeshCentral Satellite. Once the service is started, there is a communication channel that will be create with the local application so you can still monitor what the service is doing.



```
5:45:19 PM - Installing service.
5:45:22 PM - Starting service.
5:46:15 PM - Service: Contacted certificate authority: vprodemo-WIN-CA-CA-1
5:46:15 PM - Service: MeshCentralSatelliteServer - Start();
5:46:15 PM - Service: Connecting to: 192.168.2.147, user: admin
5:46:15 PM - Service: Connected
```

The lines starting with “Service:“ are coming from the background service. At this point, you can close the local application and the service will keep running in the background.

8. License

MeshCentral, MeshCentral Satellite and this document are both opens source and licensed using Apache 2.0, the full license can be found at https://www.apache.org/licenses/LICENSE-2.0.