Blessed Subnets

Introduction

Beginning with Open-AudIT 1.12.6 we have a new feature called Blessed Subnets.

A blessed subnet is a network that Open-AudIT will accept audit results from. Each network you wish to post data to Open-AudIT from HAS to be in this list to use this feature.

The feature is enabled by default. We **highly** recommend you use this feature as a security precaution.

When an audit result is accepted the first thing checked is the sending IP address and a test is run to determine if that IP iis in one of the blessed subnets. If it is not (and the feature is enabled), then audit result is discarded and a log entry created.

Use

When a user goes to the login page, the networks local to the Open-AudIT server are added to the list (if they're not already in the list).

When a Discovery is run from the web interface that specified network (if a network is actually specified) is added to the list.

When an Active Directory Discovery is run (from the web interface), Active Directory is queried for all it's networks and they are added to the list.

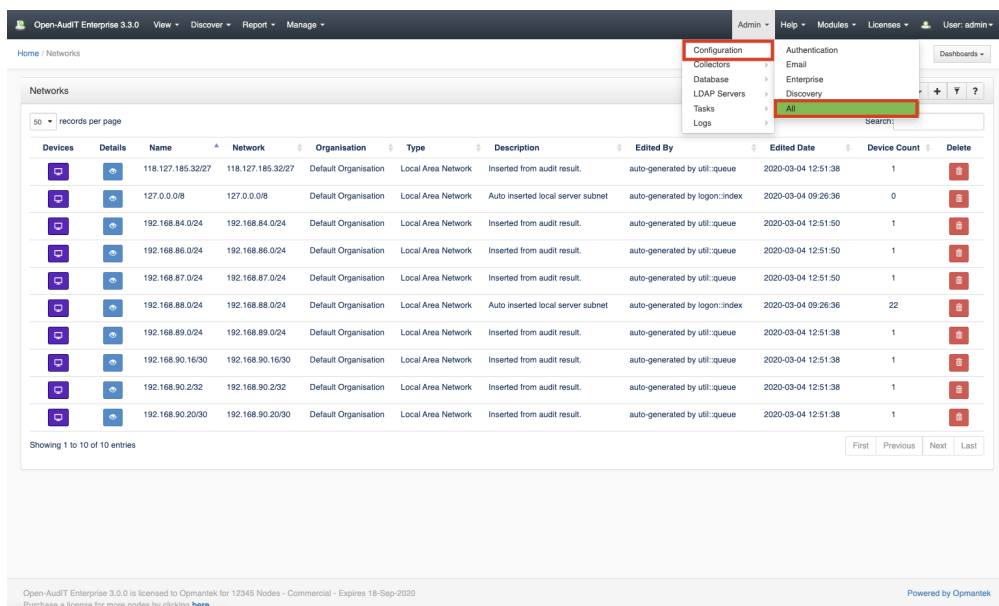The list can be viewed at menu -> Manage -> Networks -> List Networks.

Networks can be added to the list at menu -> Manage -> Networks -> Create Networks.

Networks can have a description added by clicking the Edit Network link on the View Network page.

You can disable the feature in the config (menu -> Admin -> Configuration -> All) by changing the value of blessed_subnets_use to 'n' (sans quotes).

New Installs

On a new install, the feature is enabled and the typical user should see nothing different. Running discovery will work as normal.

Upgraded Installs

Installs that have been upgraded from a previous version of Open-AudIT will have the network list populated based on the existing devices already present in Open-AudIT. Because these lists have been populated, the user should see no difference and things should work as normal.

Running with audit_subnet

You may need to populate the networks in advance is you are using the audit_subnet scripts (which you really shouldn't be - they're deprecated) on a new install.

Running with Remote Open-AudIT audit hosts

You may need to populate the networks in advance if you are running remote audit hosts (other Open-AudIT instances) that submit back to the main instance. This is an unusual setup and Opmantek are only too happy to help with support if required.