# Trust Visitor Permission Model

Trust visor should use a Role Based Permission Model. RBAC more easily maps onto a well understood set of functions compared to Discretionally Access Control and Attribute Based Access Control. RBAC allows for both a broad and granular levels of what administrators and users can do. RBAC has the dimensions

## Tasks

The main building block for composing roles are tasks. Tasks are an elemental discreet function which cannot be further sub-divided.

## Role Definition

An RBAC role is the identity given to one or more tasks a role is allowed to execute.

## Role Assignment

User have to be assigned to roles. The role assignment can be static or dynamic.

## Role Scope

Role scope defines the set of objects the role can function over.

# Trust Manager V1

## Role Definition

For Version 1, a fixed set of roles will be defined. TV tasks will be assigned to one or more roles as appropriate. The v1 roles are as follows

* **Administrator.** Able to perform any Task on the TV. Add\remove physical node definitions
* **PACS Administrator** Able to perform Tasks necessary to the maintenance and operation of the connections to the PACS. Able to update existing nodes, not add or remove.
* **Approver** Able to approve visitors access to a PACS security zone
* **User** FTE or long term contingent staff of the organization who operates the instance of TV. Able to submit visitor requests.
* **Visitor.** Short term contingent staff or ad hoc visitor. Able to manage their own details

## Role Assignment

For v1, role assignment to administrator, operator and approver roles will be via AD group membership. The AD group names will be configured in TV

User is anybody with an active user account in AD

Visitor will be the accounts directly registered with TM.

## Role Scope

The administrator, operator and approver roles can be scoped to one or more nodes in the physical hierarchy (global\region\location\building\floor\zone). Scoped roles will have discreet AD group membership.

# Visitor Request and Approval Access Scope

By default, a user can only request or approve a visitor to access a location they themselves have access to. A physical location will also have an AD group which will allow for exceptions to the default behavior for both requests and approvals.