Understanding Admin Access and RBAC Policies on ISE

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Authentication Settings
Configure Admin Groups
Configure Admin Users
Configure Permissions
Configure RBAC policies
Configure Settings for Admin Access

Introduction

This document describes the features on ISE to manage Administrative Access on Identity Service Engine (ISE).

Prerequisites

Requirements

The information in this document is based on Identity Service Engine version 2.1

Components Used

The information in this document is based on these software and hardware versions:

- Identity Service Engine 2.1
- Active Directory Services on Windows Server 2008 R2

Configure

Authentication Settings

Admin Users need to authenticate themselves before accessing any information on ISE. The identity of the admin users can be verified by using the Internal Identity Store or an External Identity Store. The authenticity can be verified by either a password or a certificate. In order to configure these settings, navigate to Administration > Admin Access > Authentication.
Identity Service Engine does not allow to configure the password policy for Command Line Interface (CLI) from the CLI. Password policy for both the Graphical User Interface (GUI) and the CLI can only be configured via the GUI of ISE. In order to configure this, navigate to **Administration > Admin Access > Authentication** and navigate to Password Policy tab.

ISE has a provision to disable an inactive admin user. In order to configure this, navigate to **Administration > Admin Access > Authentication** and navigate to Account Disable Policy tab.
To manage administrative access, there is need for administrative groups, users and various policies, rules to control and manage privileges.

**Configure Admin Groups**

Navigate to Administration > Admin Access > Administrators > Admin Groups to configure administrator groups. There are few groups which are built in by default and cannot be deleted.

Once a group is created, administrative users can be added to that group by selecting the group and clicking on edit. There is provision to map External Identity Groups to the Admin Groups on ISE so that an External Admin user gets the required permissions. In order to configure this, select the type as External while adding the user.

**Configure Admin Users**

In order to configure Admin Users, navigate to Administration > Admin Access > Administrators > Admin Users.
Click **Add**. There are two options to choose from. One is to add a new user altogether. The other one is to make a network user i.e., a user configured as an internal user to access the network/devices, as an admin.

After selecting an option, the required details must be provided and the user group must be selected based on which the permissions and privileges to the user are given.

**Configure Permissions**

There are two kinds of permissions that can be configured for a user group.

1. **Menu Access**
2. Data Access
Menu Access controls the navigational visibility on ISE. There are two options for every tab, Show or Hide, that can be configured. A Menu Access rule can be configured to show or hide selected tabs.

Data Access controls the ability to read/access/modify the Identity Data on ISE. Access permission can be configured only for Admin Groups, Identity Groups, Endpoint Groups and Network Device Groups. There are three options for these entities on ISE which can be configured. They are Full Access, Read Only Access and No Access. A Data Access rule can be configured to choose one of these three options for each tab on ISE.

Menu Access and a Data Access policies must be created before they can be applied to any admin group. There are few policies which are built-in by default but they can always be customized or a new one can be created.

In order to configure a Menu Access policy, navigate to Administration > Admin Access > Authorization > Permissions > Menu Access.

Click Add. Each navigational option in ISE can be configured to be shown/hidden in a policy.
In order to configure Data Access policy, navigate to **Administration > Admin Access > Authorization > Permissions > Data Access.**

Click **Add** to create a new policy to configure permissions to access Admin/Identity/Endpoint/Network Groups.
Configure RBAC policies

RBAC stands for Role Based Access Control. Role (Admin Group) to which a user belongs can be configured to use the desired Menu and Data Access policies. There can be multiple RBAC policies configured for a single role or multiple roles can be configured in a single policy to access Menu and/or data. All of those applicable policies will be evaluated when an admin user tries to perform an action. The final decision will be the aggregate of all the policies applicable for that role. If there are contradictory rules which permit and deny at the same time, permit rule will override the deny rule.
Click **Actions** to Duplicate/Insert/Delete a policy.

**Note**: System-created and default policies cannot be updated, and default policies cannot be deleted.

**Note**: Multiple Menu/Data Access permissions cannot be configured in a single rule.

**Configure Settings for Admin Access**

In addition to the RBAC policies, there are few settings that can be configured which are common to all the admin users.

In order to configure the number of Maximum Sessions Allowed, Pre-login and Post-Login Banners for GUI and CLI, navigate to **Administration > Admin Access > Settings > Access.**
To configure the list of IP Addresses from which the GUI and the CLI can be accessed, navigate to **Administration > Admin Access > Settings > Access** and navigate to the IP Access tab.

In order to configure the timeout due to inactivity for a session, navigate to **Administration > Admin Access > Settings > Session**.
In order to view/invalidate the current active sessions, navigate to **Administration > Admin Access > Settings > Session** and click the Session Info tab.