IncMan and Cisco ISE integration configuration

Contents

Version 1

Information.....1

Executive

Summary.....2-5

Executive Summary

This document describes the configuration for Cisco ISE

Procedure

IncMan and Cisco ISE integration configuration

Summary:

Utilize Cisco ISE Session, Policy, and Security Group information during an investigation

Supported Versions: 2.7

Actions:

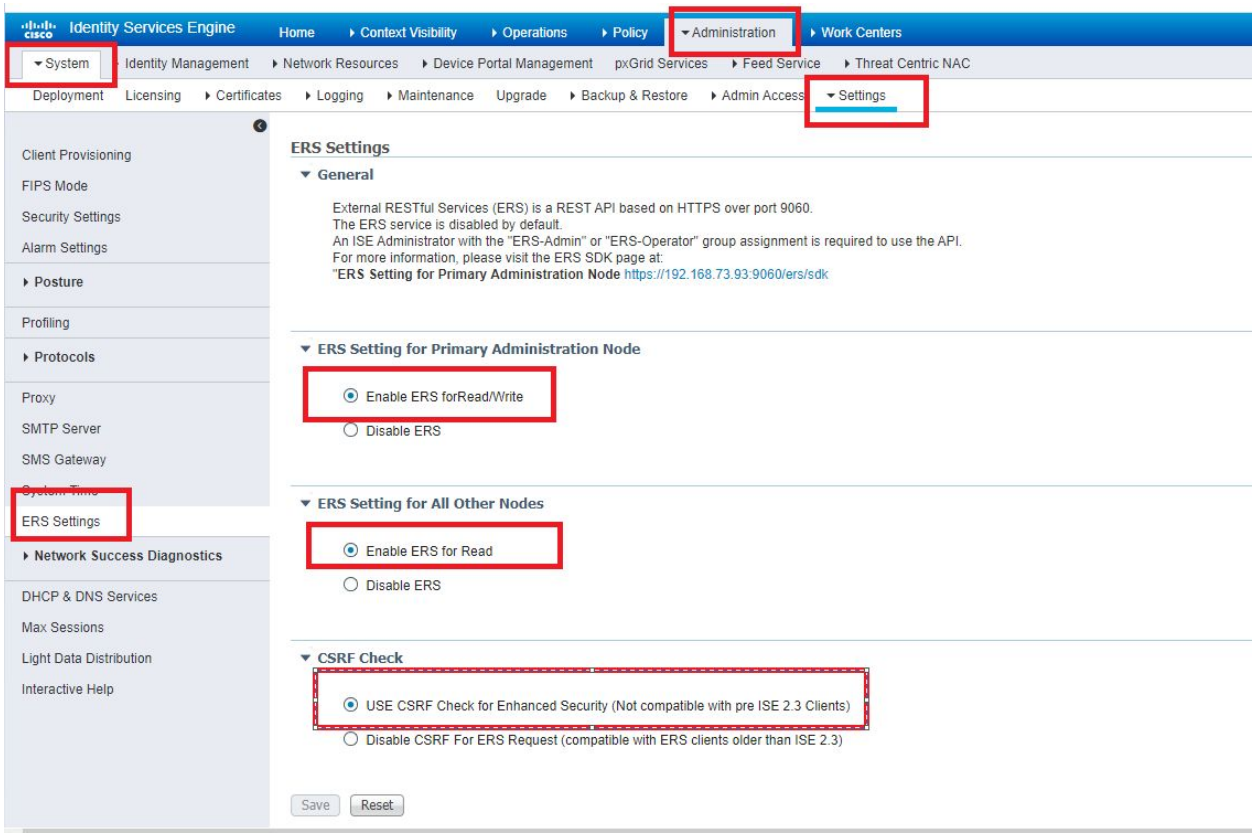
Get Sessions (*Enrichment*) - Gather session information from Cisco ISE
List Policies (*Enrichment*) - List all available ISE policies
List Security Groups (*Enrichment*) - List all available security groups
Get Policies Endpoints (*Enrichment*) - List endpoints associated with policies
Apply Policy (*Containment*) - Create a new policy
Clear Policy (*Containment*) - Remove an existing policy
Get Endpoints (*Enrichment*) - List all available endpoints
Get Endpoint Identity Groups (*Enrichment*) - List all available endpoint identity groups
Get Internal Users (*Enrichment*) - List all available internal user
Deployment Info (*Enrichment*) - To check if ISE primary node is up or not

Cisco ISE configuration:

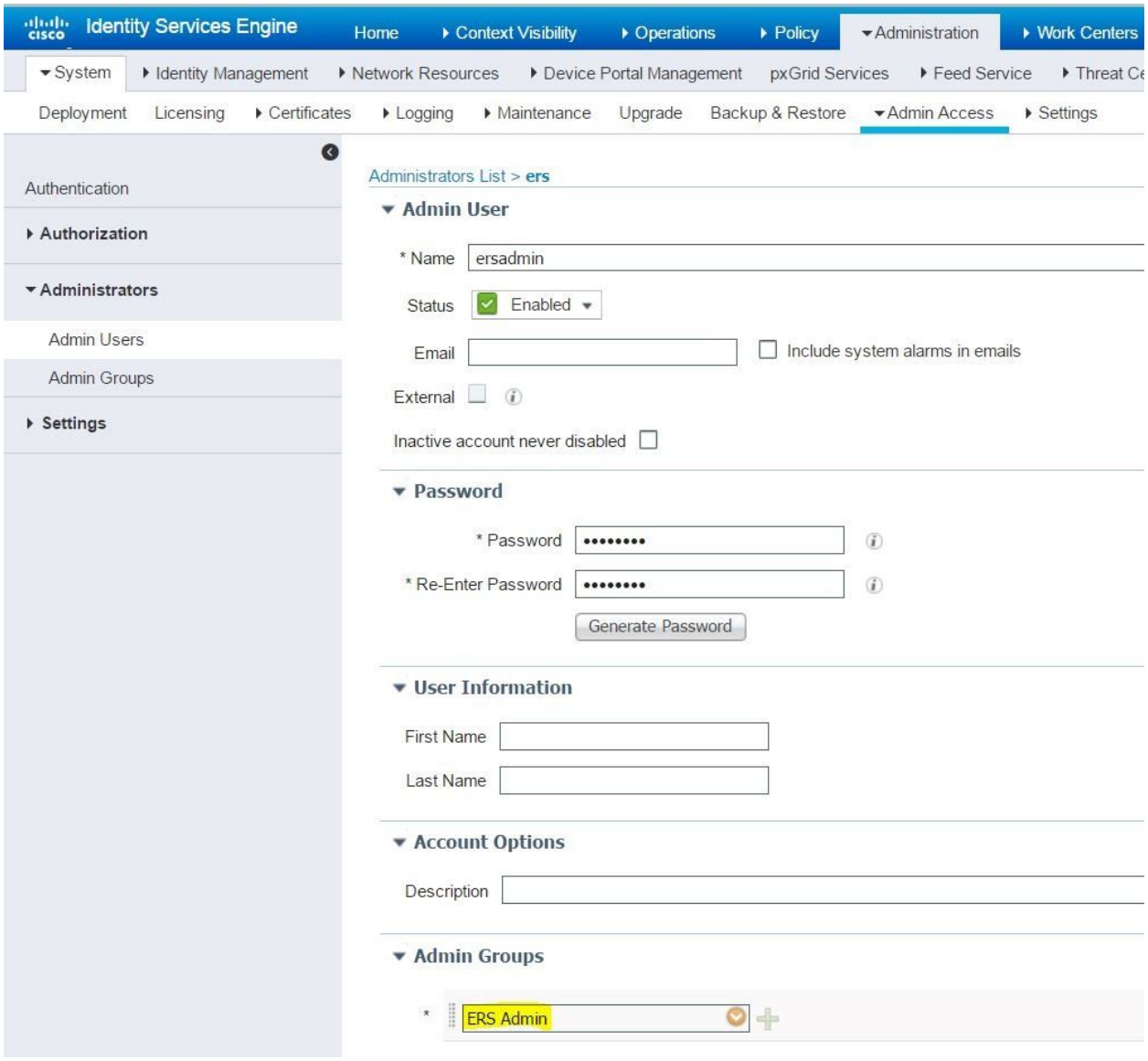
Cisco ISE is configured in a way that you'll need to specify the resource together with the URL and port in the following manner:

URL:port **The default port used is port 9060** that will need to be enabled.

ERS uses HTTPS port 9060 which is by default closed. Clients trying to access this port without enabling ERS first, will face a timeout from the server. Therefore, the first requirement is to enable ERS from the ISE admin UI.
Go to Administration -> Settings -> ERS Settings. check the 'Enable ERS for Read/Write' radio button as shown in the screenshot below.



The second requirement is to create an ISE Administrator with the ERS Admin group as shown in the following screenshot:



The following ISE Administrator Groups allow REST API access:

ISE Admin Group	Permissions
SuperAdmin	Read/Write
ERSAdmin	Read/Write
ERSOperator	Read Only

To perform **Get Sessions** action, the users must be assigned to one of the following Admin Groups and must be authenticated against the credentials stored in the Cisco ISE internal database (internal admin users):

- Super Admin
- System Admin
- MnT Admin

So you have to use both Admins Groups together to use all the actions inside the IncMan.