



IncMan and Cisco ISE integration configuration

Copying of this document is strictly prohibited without the express written consent of DFLabs, S.p.A.

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

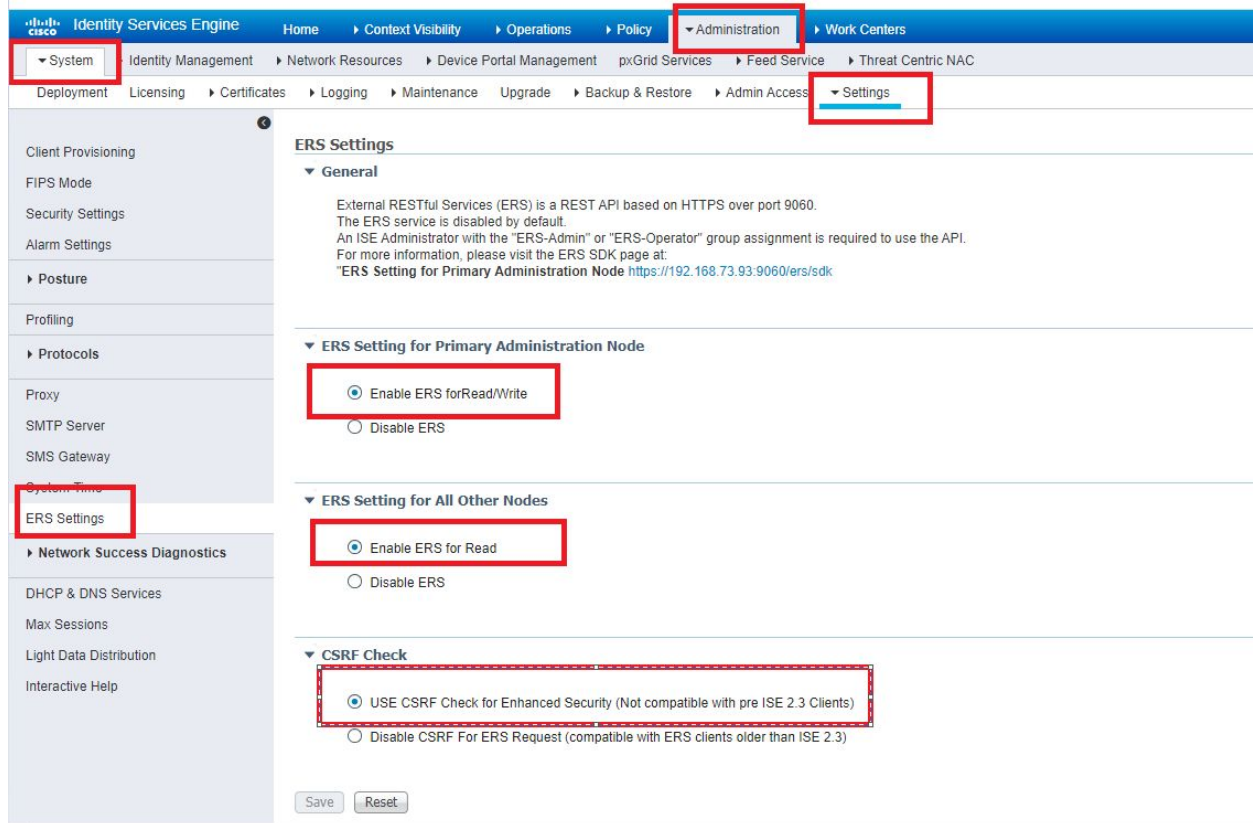
Cisco ISE configuration:

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 screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Center > Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings.

The left sidebar contains the following navigation items: Authentication, Authorization, Administrators (selected), Admin Users, Admin Groups, and Settings.

The main content area is titled "Administrators List > ers" and shows the configuration for the "Admin User".

- Admin User**
 - * Name: ersadmin
 - Status: Enabled
 - Email: Include system alarms in emails
 - External: [?](#)
 - Inactive account never disabled:
- Password**
 - * Password: [?](#)
 - * Re-Enter Password: [?](#)
 -
- User Information**
 - First Name:
 - Last Name:
- Account Options**
 - Description:
- Admin Groups**
 - *

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.

The screenshot shows the Cisco ISE configuration interface for an Admin User. The breadcrumb trail is: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Admin Access > Settings. The left sidebar shows the navigation menu with 'Administrators' selected. The main content area is titled 'Administrators List > api_admin' and contains the following sections:

- Admin User**
 - * Name: api_admin
 - Status: Enabled
 - Email: Include system alarms in emails
 - External: *i*
 - Read Only:
 - Inactive account never disabled:
- Password**
 - * Password: *i*
 - * Re-Enter Password: *i*
 -
- User Information**
 - First Name:
 - Last Name:
- Account Options**
 - Description:
- Admin Groups** (highlighted with a red box)
 - * MnT Admin
 - * ERS Admin