Defense Information Systems Agency

**ACAS ESX/ESXi SOAP Credential Guide**

February 18, 2016

v1

Table of Contents

[Change Log 3](#_Toc443573442)

[Introduction 4](#_Toc443573443)

[SOAP Authentication Procedures for SecurityCenter Version 4.x 4](#_Toc443573444)

[SOAP Authentication Procedures for SecurityCenter Version 5.x 7](#_Toc443573445)

[Useful Links 9](#_Toc443573446)

# Change Log

|  |  |  |
| --- | --- | --- |
| Date | Version | Changes |
| 18-Feb-2016 | 1 | * Initial document creation |

# Introduction

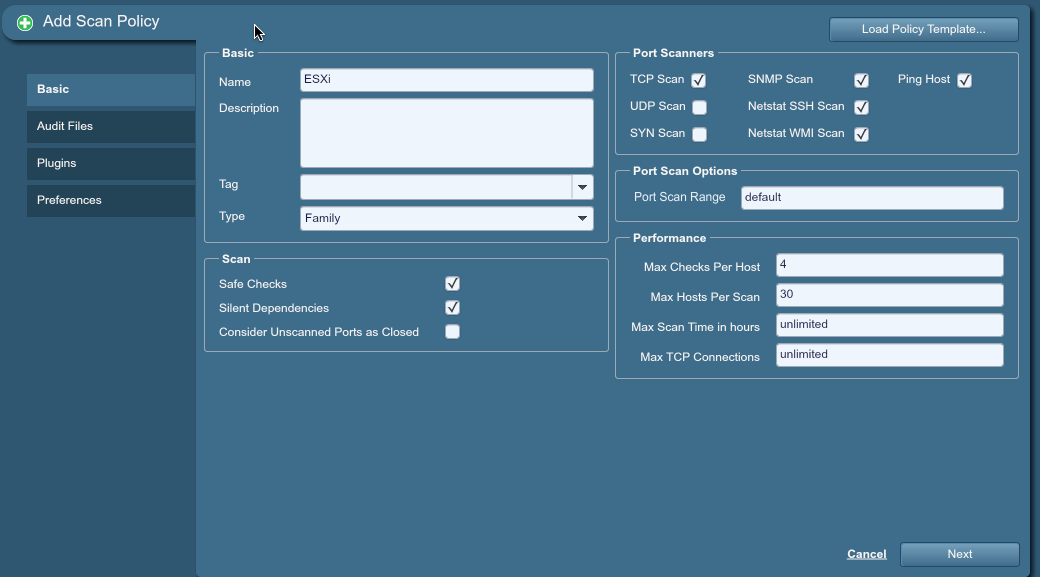
This document describes the step-by-step authentication procedures for both SecurityCenter (SC) 4.x and SC 5.x to scan VMware ESX, ESXi and/or vCenter hosts via the Simple Object Access Protocol (SOAP) Application Programming Interface (API).

# SOAP Authentication Procedures for SecurityCenter Version 4.x

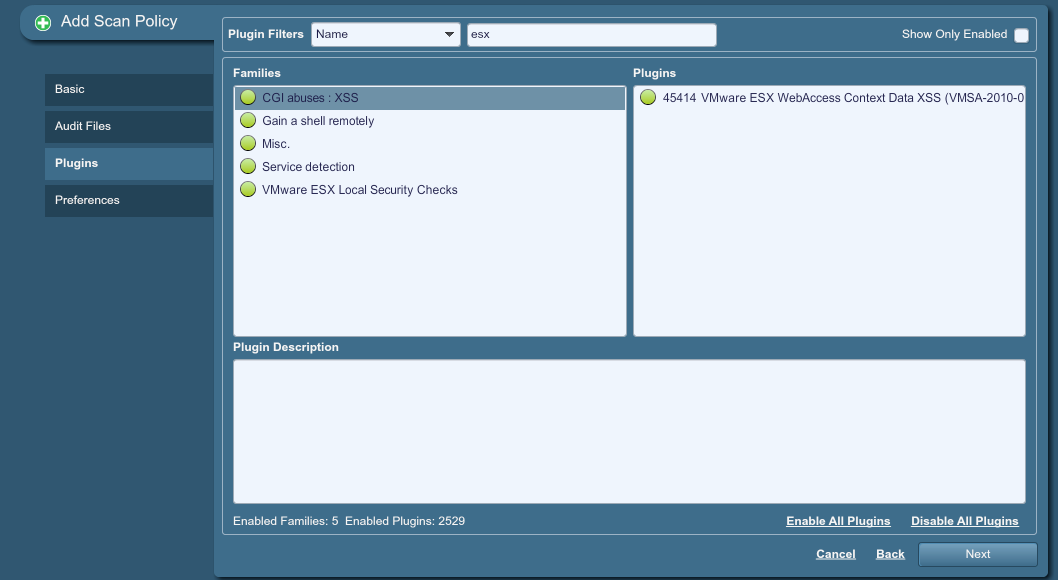
1. Login to SecurityCenter to create a scan policy.
2. From the drop-down menu, click **Support** and select **Scan Policies**.
3. Click on the **Add** button to create a new Scan Policy.



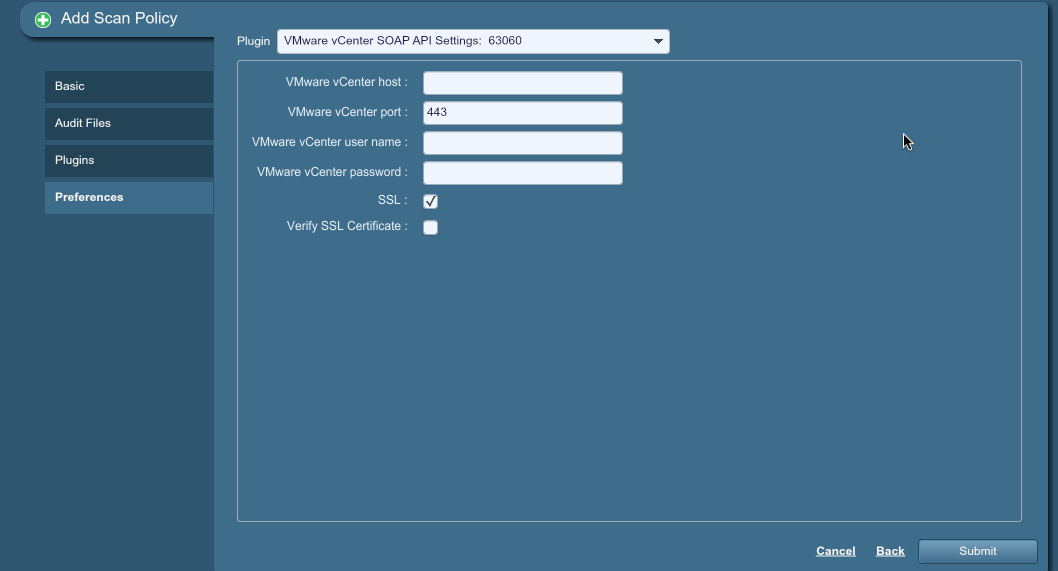
1. Name the policy and select any pertinent options. When done, click **Next** to continue.



1. If you are running a compliance audit, select the appropriate compliance audit file. Otherwise, click **Next** to continue to the vulnerabilities/Plugins tab. **Note**: You need to manually upload any audit files in order for them to show up.
2. In the Plugin Filters search field, type in “ESX” and press Enter to search for all ESX plugins. Select all plugins you wish to run and click **Next** to continue.



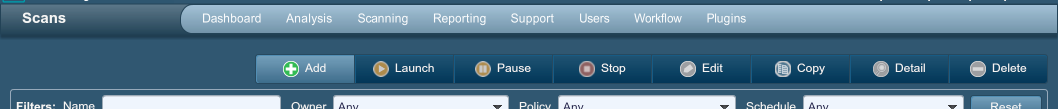
1. On the **Preferences** tab use the **Plugin** drop-down, select the version of ESX server you are running (i.e., vCenter, ESX or ESXi) and how you wish to authenticate (i.e., SOAP). You will need to enter the host Internet Protocol (IP) address, port, username and password for the host. Once you fill in the fields, click **Submit** to create the policy.



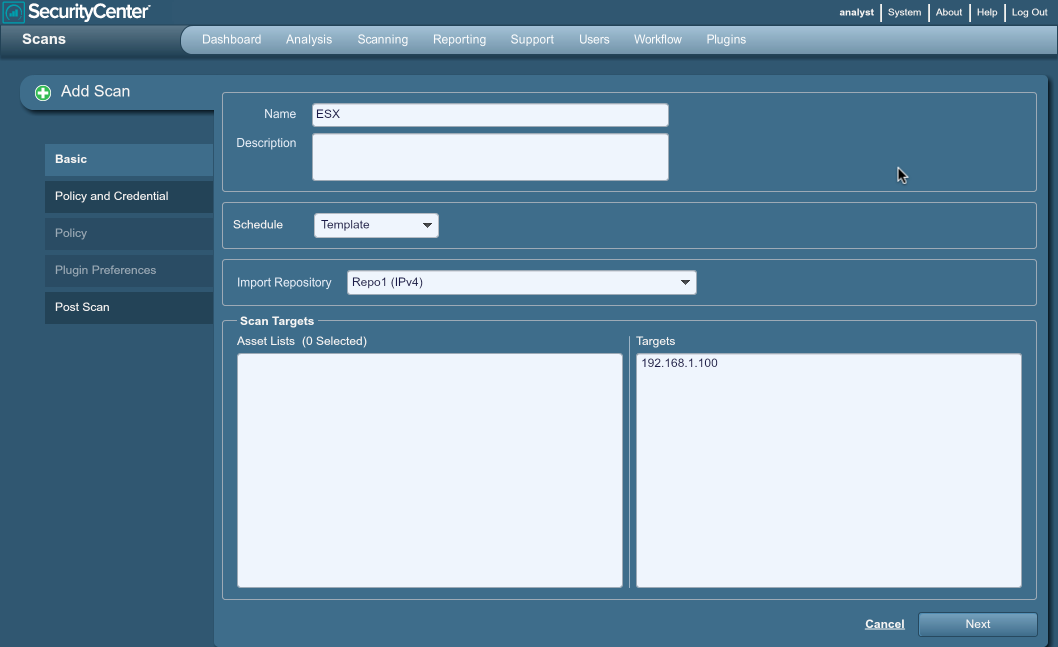
1. From the drop-down menu, click **Scanning** and then **Scans** to create a scan job.



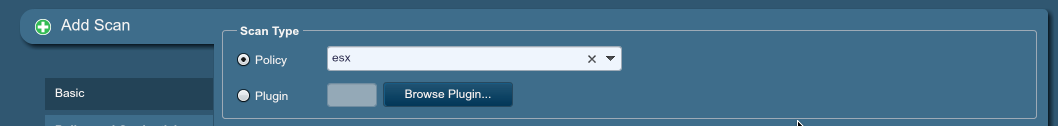
1. Click the **Add** button to create a new scan job.



1. Enter a name and target(s) for the job. And click **Next** to continue.



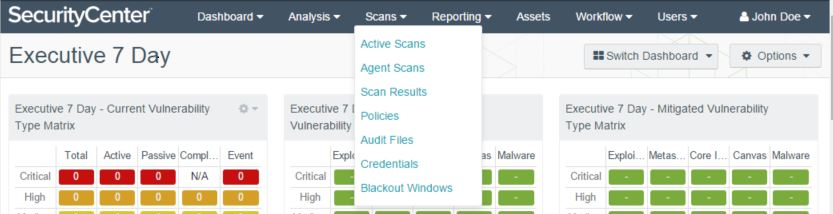
1. From the Scan Type window, select the Policy you created when logged in as Admin and click **Next** to continue.



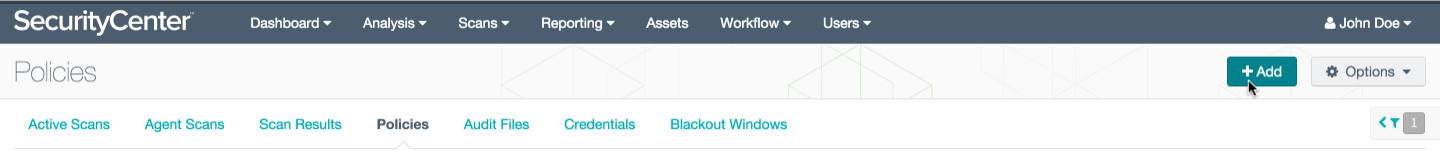
1. Select any pertinent Post Scan actions and click **Submit** to create the job. Once created, you will be able to scan ESX, ESXi and/or vCenter hosts via the SOAP API.

# SOAP Authentication Procedures for SecurityCenter Version 5.x

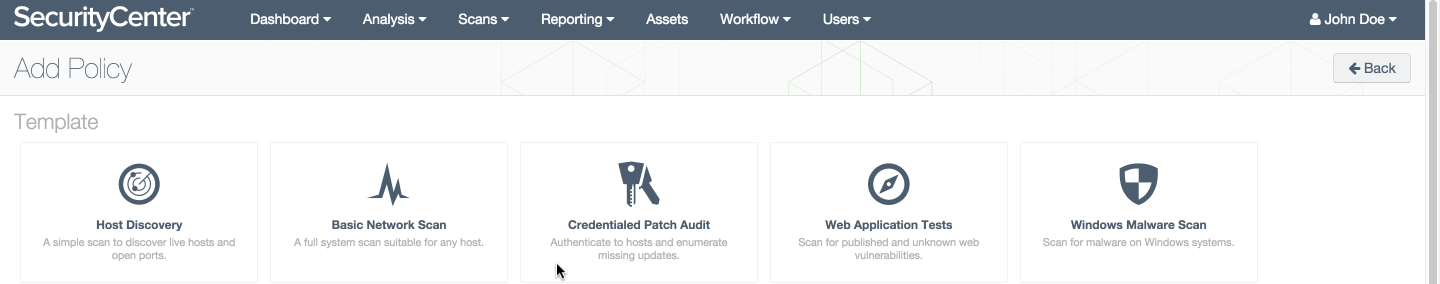
1. Login as a regular user to SecurityCenter.
2. From the drop-down menu, click **Scans** and select **Policies**.



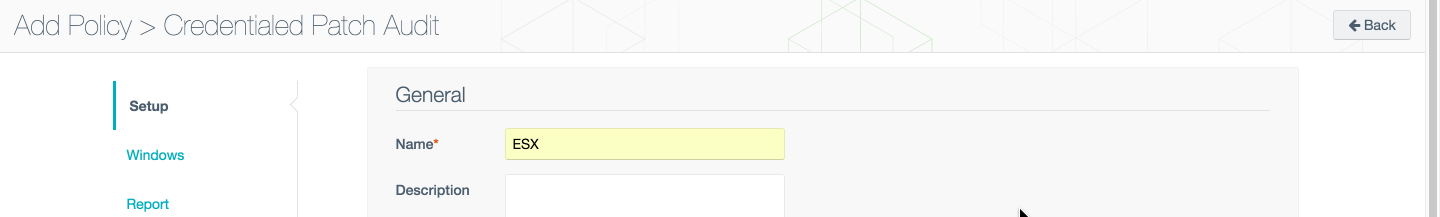
1. Click on the **Add** button to create a new Policy for your scan.



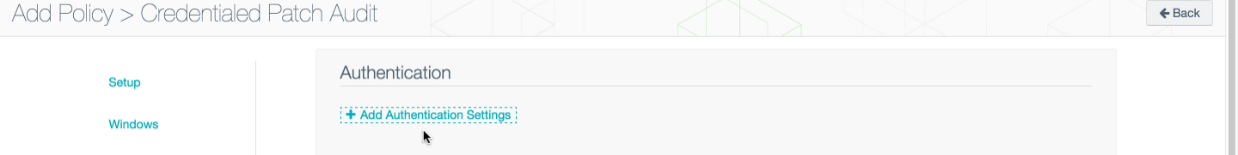
1. Select the type of Policy template you wish to conduct. For this example, we selected the “Credentialed Patch Audit” policy template.



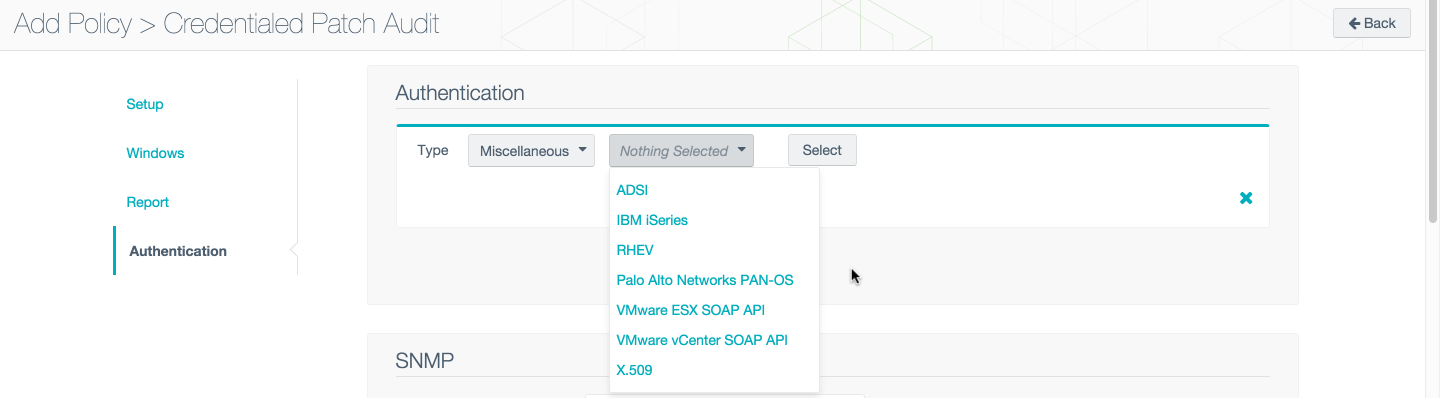
1. Name the policy and specify any configuration settings needed for the policy.



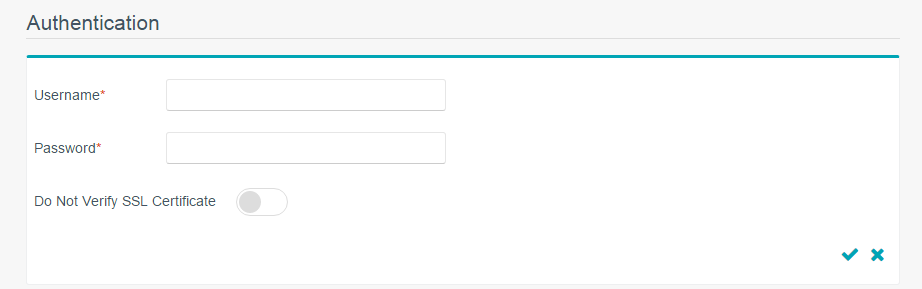
1. Under the Authentication tab, select “**Add Authentication Settings**”.



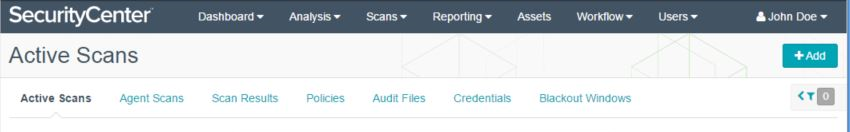
1. Under type, select **Miscellaneous**, under the next drop-box, select the type of ESX host you are connecting to (i.e., ESX or vCenter), and hit **Select** when finished



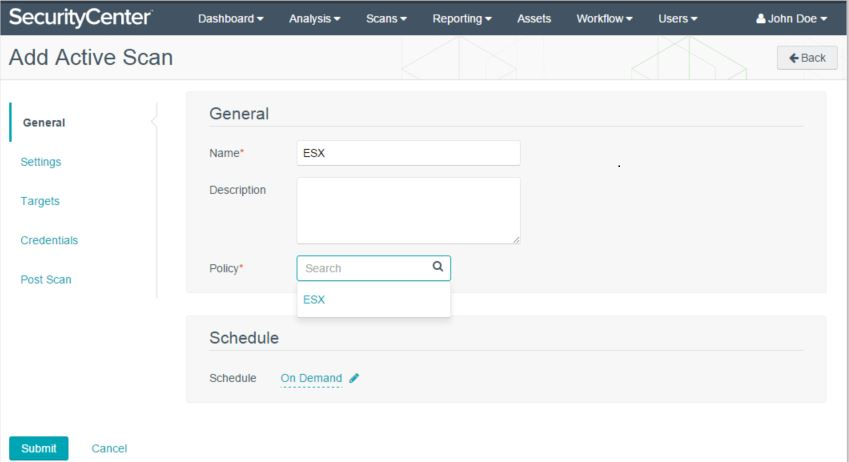
1. Enter the proper credentials and select the check box in the lower, right-hand corner. Save the policy by clicking on **Submit** at the bottom of the screen.



1. Click on **Active Scans** and select the **Add** button to create a new scan job.



1. Enter a name and select the **Policy** you created previously for the job. You must also select an **Import Repository** under the Settings tab and provide **Target(s)** under the Targets tab. Select any pertinent Post Scan actions and click **Submit** to create the job. Once created, you will be able to scan ESX, ESXi and/or vCenter hosts via the SOAP API.



# Useful Links

## ACAS Homepage

<https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/Home.aspx>

Contains access to the following: ACAS License Request Portal, ACAS Build 1 Request Portal, ACAS Working Group information, ACAS Training, and other important ACAS related information.

## Approved documentation/binaries are located on DoD Patch Repository

Posted at: <https://patches.csd.disa.mil/CollectionInfo.aspx?id=442>

(CAC is required for access). Click on ACAS > ACAS Software > then whichever application you need. All of our latest Plugins files and Red Hat patches can be found here also.

## ACAS Customer Support/OKC Helpdesk

* Toll-free: 844-347-2457 (Select options 1,5, and 4)
* DSN: 850-0032 (Select options 1,5, and 4)
* Email: [disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil](mailto:disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil)

## SoftwareForge

<https://software.forge.mil/sf/projects/acas>

All of our test and development efforts are located here and do not represent the approved baselines.

## Certification and Accreditation Artifacts

Posted at ACAS SIPR Wiki: <https://www.intelink.sgov.gov/wiki/ACAS>

## ACAS Front Door

<http://www.disa.mil/Cybersecurity/Network-Defense/ACAS>

## ACAS TTP

Posted at: <https://powhatan.iiie.disa.mil/ttp/capability/capability.html>