Cisco Identity Services Engine (ISE) Configuration Guide

Certificate Authentication for Sponsor Portal using Cisco's ASA Auto Login through Self Service feature

Viktor Bobrov
Network Consulting Engineer
Tim Baum
Network Consulting Engineer

Contents

Introduction

The core decisional element of Cisco SecureX is Cisco's innovative policy server: Cisco Identity Services Engine (ISE).
Through an optimized graphical interface, Cisco ISE integrates the full park of solutions for identity and access control. It delivers all the functionalities already consolidated in Cisco ACS, Cisco NAC, Cisco NAC Profiler and Cisco NAC Guest Server and it offers new interactions between all the different authentication, authorization, guest access, profiling and posture assessment options.

- Authentication
- Authorization
- Accounting, Monitoring & Troubleshooting
- Guest Access
- Profiling
- Posture Assessment
- Encryption (MACSec)
- Security Group Access (SGA)

In particular, profiling capabilities support automatic and granular classification for all kinds of endpoints accessing the network. Following from such a classification, it is possible to apply customized authorization policies according to the type of device.
Thanks to posture assessment, customers can verify client's compliancy (installed AV/AS, updates, running services, registry keys, installed applications, etc.) and apply remediation actions before authorizing access to the network.
Data confidentiality is guaranteed through the support and the integration of the IEEE 802.1AE (MACSec) standard and through Cisco Security Group Access, also for what concerns data center and cloud computing architectures.

Cisco ISE Sponsor Process

Overview

One of the key features in ISE for a number of customers is handling of guest and visitor accounts. A very common way to deploy guest services is through the use of Sponsors or Lobby Administrators to create guest account.

The sponsors are company employees who have the permissions to create temporary accounts for visitors. In some cases, only a few employees are entitled to play this role, while in others, all company employees are permitted to register guests. Similarly, it is common that different employees are given different privileges when creating temporary accounts. A Lobby Ambassador may be able to edit all temporary accounts while individual employees may be limited to editing the accounts they create.

Given that Sponsors are typically full time employees with Active Directory (AD) accounts and role based groups, it's quite common to see Sponsor authentication be passed to AD for authentication and authorization. With ISE AD authentication, it is possible for AD users to become sponsors with different rights based on their AD groups.

Authentication Methods

Sponsors Portal supports authentication against most of authentication sources that ISE can integrate with, such as AD, LDAP, RADIUS and Internal DB. However, with the current release of Identity Services Engine (v1.2), the Sponsor portal does not accept all forms of authentication. That is, to gain access to the Sponsor portal, the users must present a valid username and password that the Sponsor Authentication database will accept. The Sponsor portal does not accept a certificate at this time.

Authorization Methods

Sponsor Portal supports most of the common authorization methods that are typically deployed in ISE authorization policy such as Active Directory (AD). And by utilizing user groups from AD, ISE can assign privileges to AD users based on their group assignment. And optionally, RADIUS attributes can be populated based on AD look-up. For example, a pre-defined RADIUS attribute can be checked, by default set to CiscoSecure-Group-Id

Need for Certificate Authentication

A number of customers, notably US Government Agencies, do not utilize password-based authentication databases. The users at these agencies authenticate to their PC and network resources using Smart Cards.

This precludes these customers from utilizing Single Sign-on into the ISE Sponsor portal and forces them to revert to weaker authentication methods by utilizing Internal ISE DB for holding of Sponsor accounts.

Solution

Overview

To get around current limitation of ISE, the solution requires an external system to perform certificate-based authentication to collect credentials from users' Smart Cards. Cisco ASA firewall plays that role in the configuration presented here. The ASA will extract the sponsor's username from the certificate presented from the smartcard. Then by utilizing ISE's flexibility in authentication, that username will be checked against an identity DB to verify it is active as well as retrieve group attributes.

The ASA terminates all connections from Sponsors and passes them through to ISE using Clientless VPN. For authentication, the ASA extract a key attribute from the user certificates and passes that to ISE as a username.

ISE, however, requires that the sponsor's username *and* password to be authenticated against an identity database. To get around this, we "loop" sponsor logins back into ISE as another RADIUS request. To do this we will set Sponsor Authentication source to RADIUS Token server which will point to one or two special use ISE Policy Server Nodes (PSN). ISE will receive this looped request as RADIUS PAP_ASCII. We can use flexibility built-in to ISE to authenticate the request even when an invalid password is specified. In authorization policy, we can cross-reference the username against an external directory group to assign a differentiated policy using the RADIUS attribute CiscoSecure-Group-Id.
When the Sponsor process receives Access-Accept message from RADIUS with the appropriate RADIUS group attribute, it can assign that user to the correct Sponsor Group.

Restricting Sponsor Portal to ASA Only

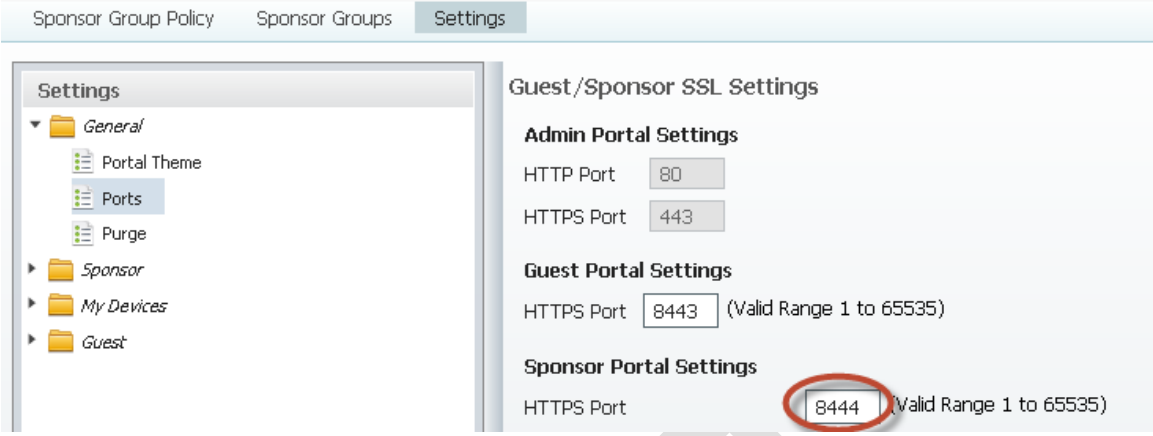
The obvious weakness of this configuration is that Sponsor portal will allow Sponsors to login using just their usernames. This will enable one sponsor to login as another sponsor if they knew each other usernames. This can be secured within ISE to a certain extent by requiring a specific password to be specified for all sponsor users. This password will be configured to match on the ASA and will not be known to typical users.
To completely eliminate the risk of users compromising the security of the Sponsor portal, the TCP port on which the Sponsor Portal resides must be restricted to be accessible from the ASA only. With this restriction, the only way to reach the Sponsor portal is through the ASA which is performing the Clientless VPN function.

ISE Configuration

This deployment guide is intended to assist the administrator with making the necessary changes to an operational system to add the support of the ASA for smartcard authentication for the Sponsor Portal. The assumption is that ISE has the necessary configuration to be fully operational including Guest services, Sponsor portal using normal usernames and passwords for authentication, web services including certificate installation and operations with a Microsoft Active Directory server. Please consult with the ISE administration guides to complete those setup tasks as well as to further explain these configuration settings.

Sponsor Portal TCP port

By default, most of the web portals, including both Guest and Sponsor portals, run on the same port (TCP 8443), so it's impossible to block the Sponsor portal without also blocking the Guest. ISE has the option to change the port number for each. We will change the sponsor port number to an unused value such as 8444. This setting is located under Administration >> Web Portal Management >> Settings >> General >> Ports.

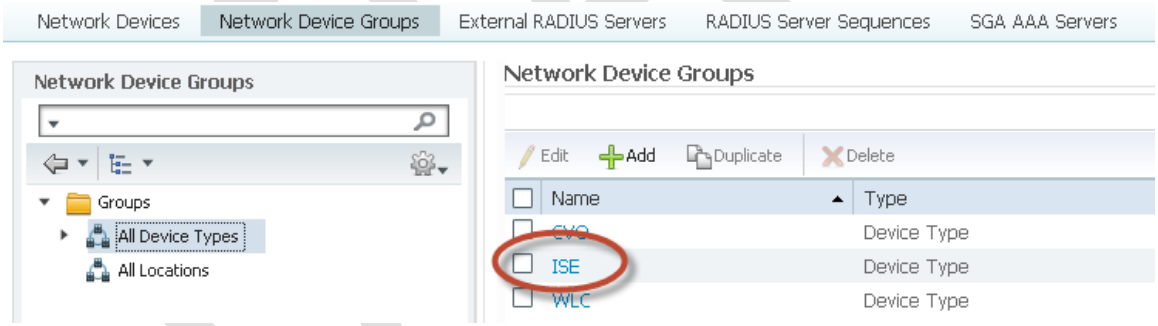


ISE as NAD

Since Sponsor portal will loop the request to ISE, ISE becomes a network access device (NAD) of itself.

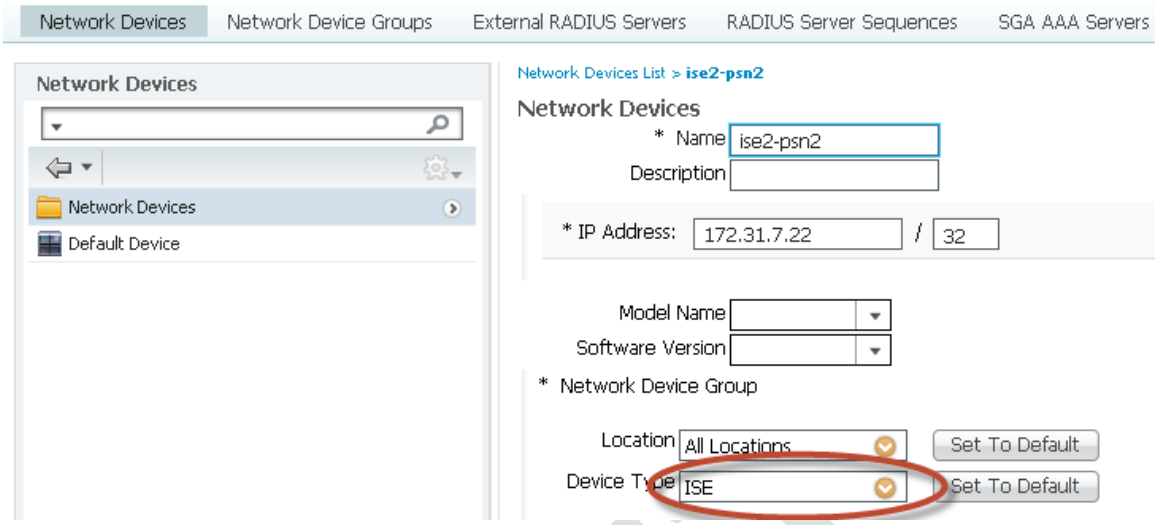
All PSNs that will accept the looped requests must be defined as NADs. To simplify writing rules for looped request, a new Network Device Group (NDG) is recommended. In this example, we will define a new Device Type called *ISE*.

This option is located under Administration >> Network Resources >> Network Device Groups >> Groups >> All Device Types.



Once the device type is created, create entries for each ISE PSN node that will accept the looped RADIUS request. Be sure to set the Network Device Group's Device Type to the newly created *ISE* group.

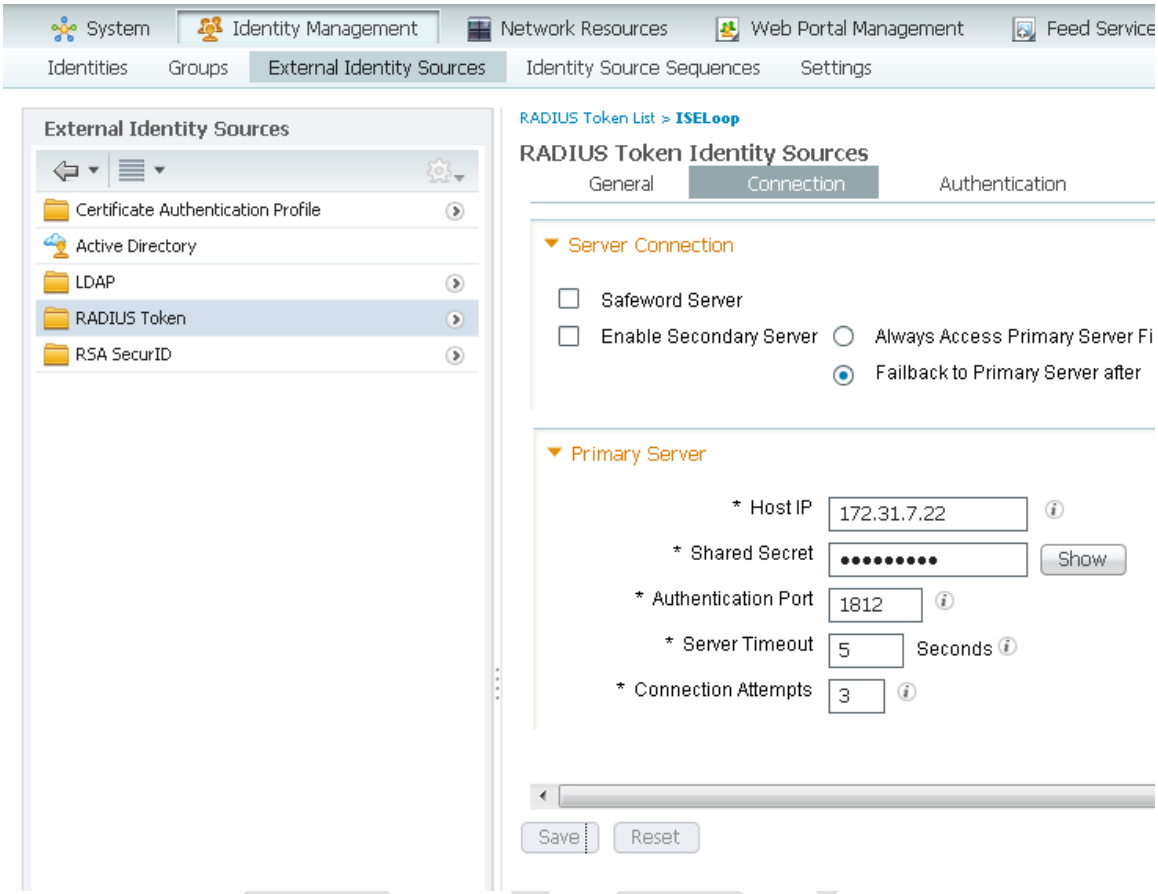
Entries are added from Administration >> Network Resources >> Network Devices.



RADIUS Token Server

Now, we point ISE to itself by creating an entry for a RADIUS Token Server. This entry should match the NAD entry done in the previous step i.e. use the same IP address in both entries since we're defining the same node. In this example, we use ISELoop as the name. Use the default settings including the returning attribute name of CiscoSecure-Group-Id.

The RADIUS Token Server entries are located under Administration >> Identity Management >> External Identity Sources >> RADIUS Token.

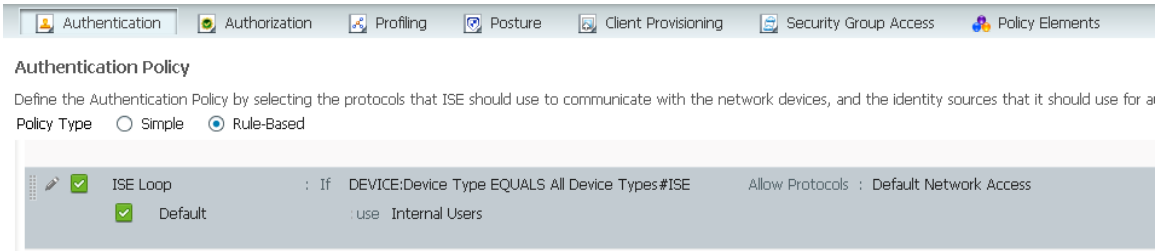


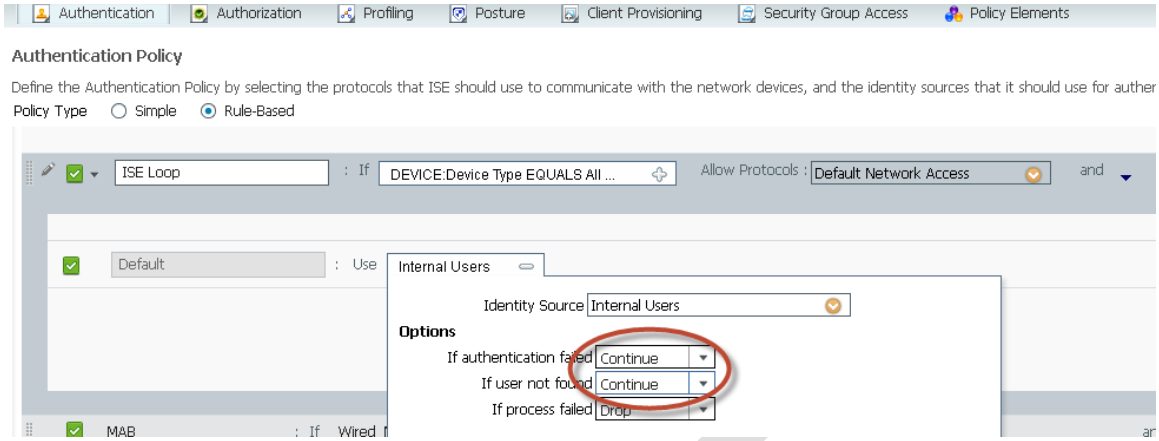
Authentication Policy

In authentication (AuthN) policy, a rule is needed to accept RADIUS requests from ISE itself. We create a rule that has the condition "DeviceType EQUALS ISE". The default protocols can be used. Finally the options for "failed authentication" and "user not found" must be set to *continue*.

Note that this screen may appear differently based on ISE version and if policy sets are enabled. To enter the rule, go to Policy >> Authentication.

Be sure to set authN failure and user not found to continue.



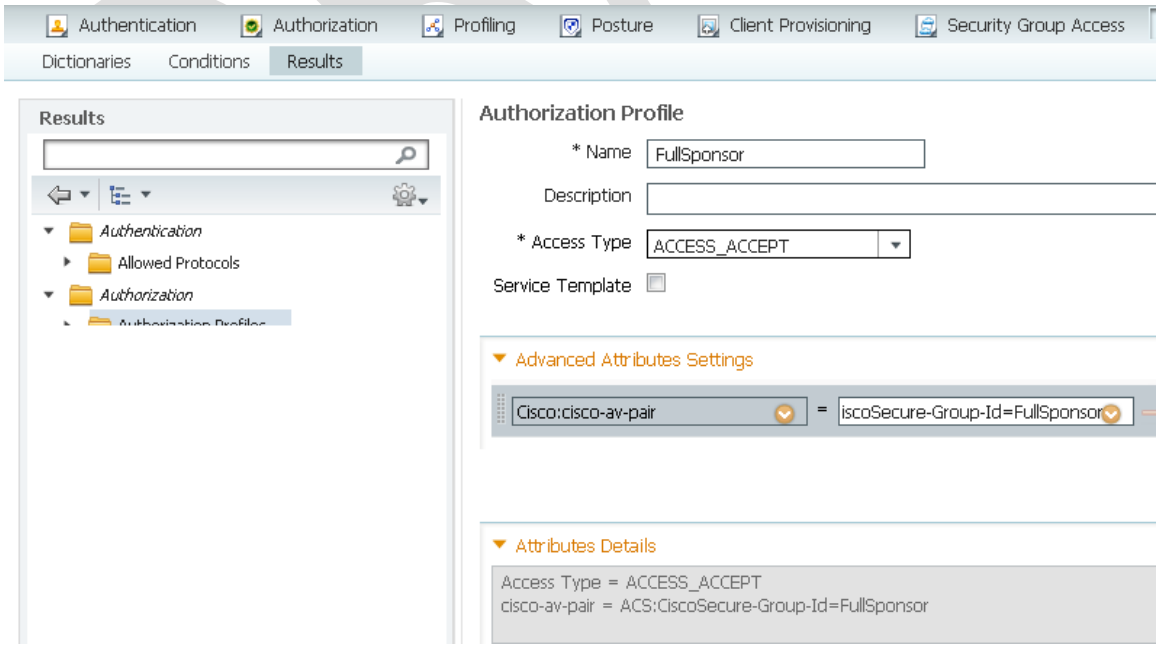


Authorization Profiles

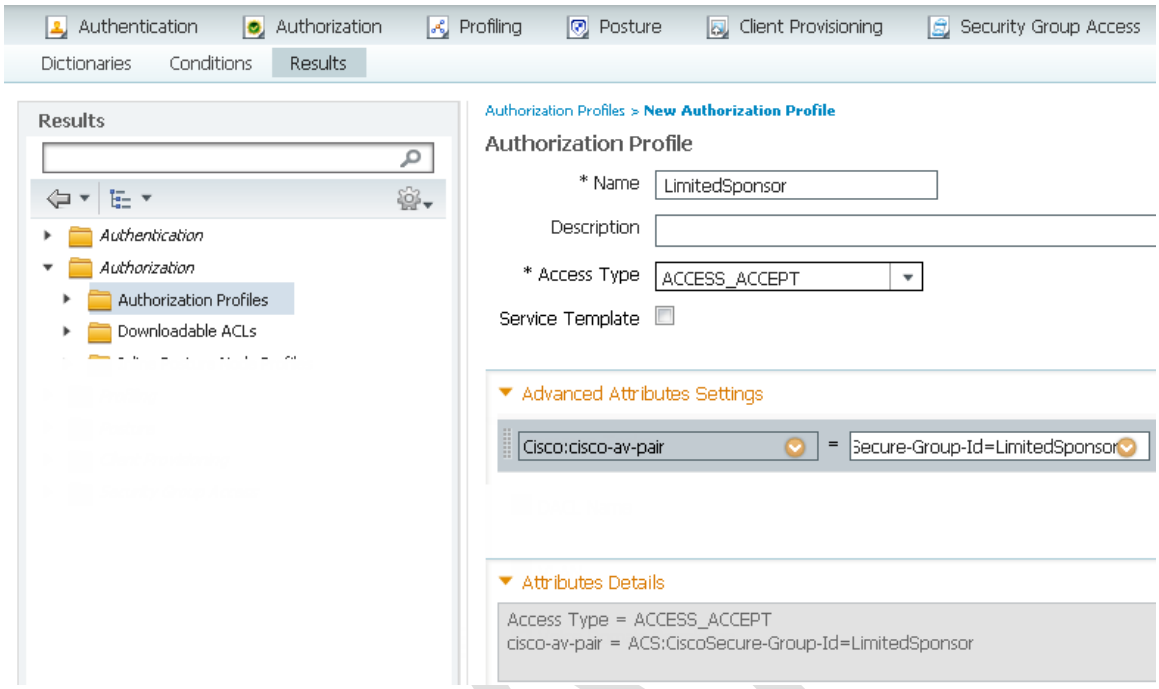
For authorization (AuthZ), we will create two profiles to demonstrate multiple privilege levels for the sponsor accounts. First profile is for limited sponsor. Second is for full sponsor. The profiles will return specific values in CiscoSecure-Group-Id attribute which will later be matched in Sponsor Policy.

For each profile, we need to use the Advanced Attribute Settings. Since we used ISELoop for our RADIUS Token server, this entry will be start with Cisco:cisco-av-pair = ISELoop:CiscoSecure-Group-Id. This can be selected from the 2 pull downs. But since we are nesting variables (av-pair=group-id) we still need an expression to match. Therefore we will manually add the FullSponsor to the end of the string. This will give us Cisco:cisco-av-pair = ISELoop:CiscoSecure-Group-Id=FullSponsor.

AuthZ profiles are created under Policy >> Policy Elements >> Results >> Authorization >> Authorization Profiles.



For the second, limited sponsor account, we do the same settings except the final expression is LimitedSponsor giving us Cisco:cisco-av-pair = ISELoop:CiscoSecure-Group-Id=LimitedSponsor.



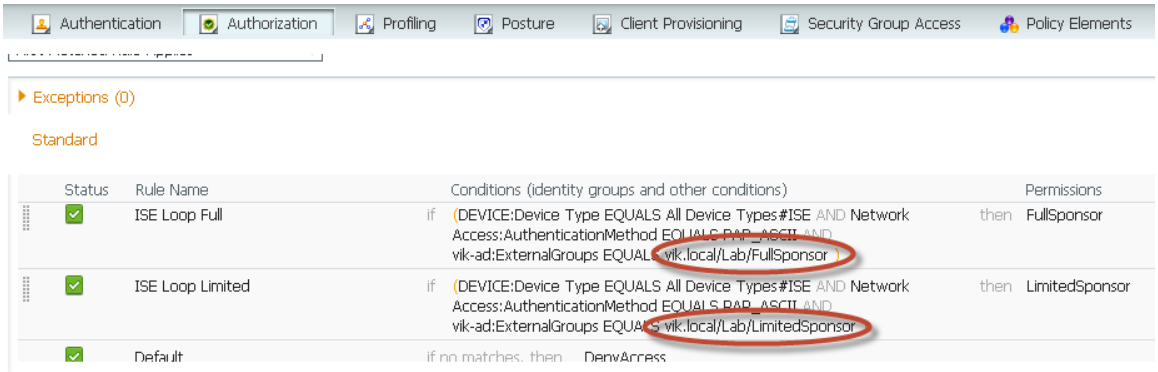
Authorization Policy

In authorization (AuthZ) policy, we return the appropriate profile based on the users' Active Directory group assignments.

The rule should check for the following conditions

1) Device type = ISE. This ensures the rule only applies to the looped RADIUS request. Use the Network device type name entered earlier in this setup.
2) Network Access: Authentication Method = PAP_ASCII. Another check to ensure ISE is processing the looped RADIUS request and not another authN method.
3) AD1:External Groups = FullSponsor. This matches users from the AD:FullSponsor group. Actual group names are configured by the AD administrator and should match the conditional check here for each group being assigned this privilege level.

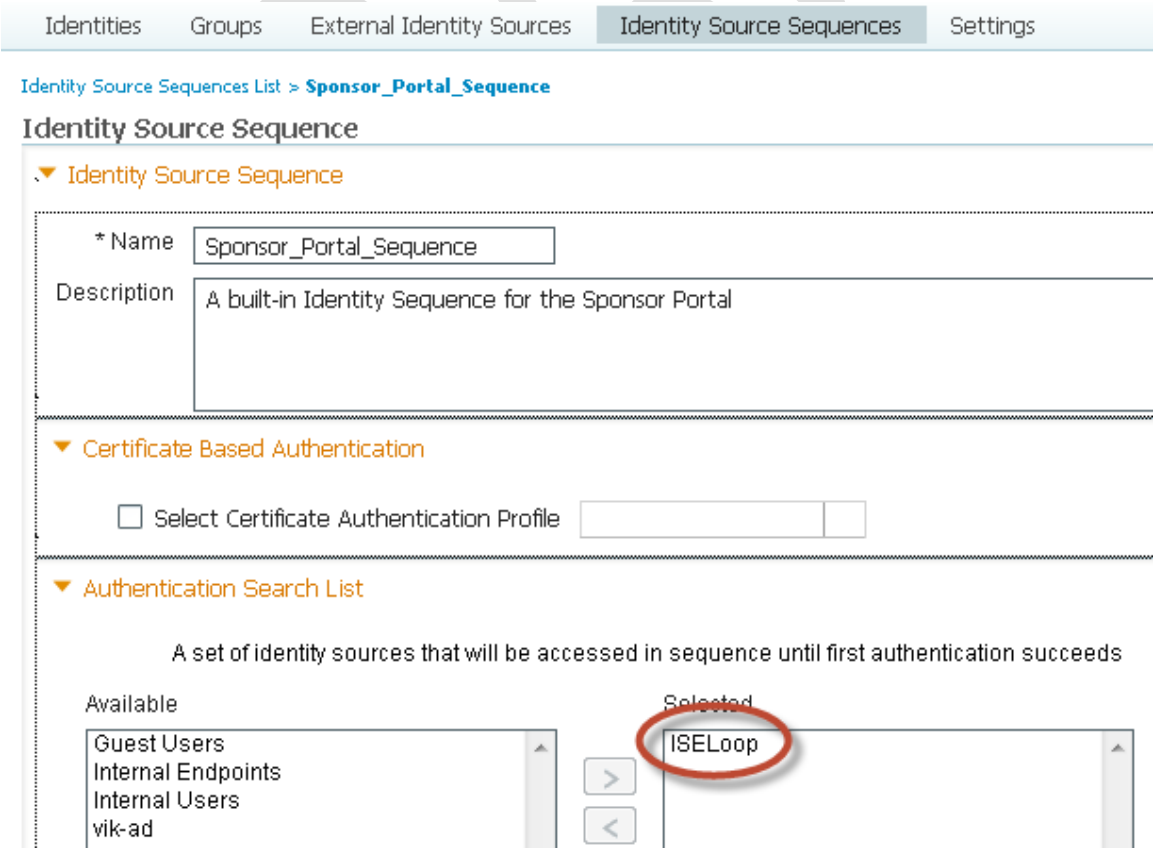
Screens may vary depending on versions and if policy sets are enabled. To enter AuthZ Policy, go to Policy >> Authorizations.



Sponsor Authentication Sequence

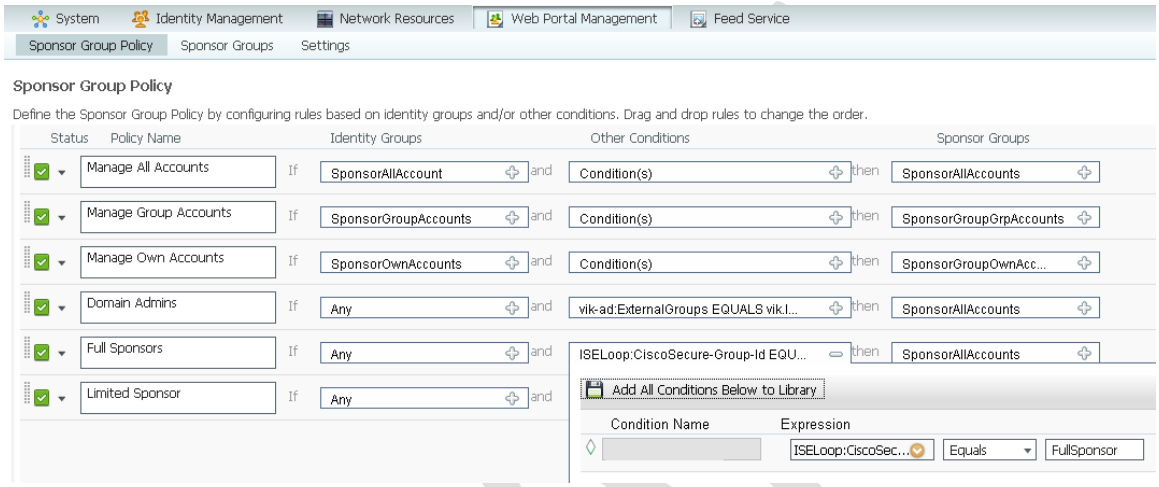
Next, configure a Sponsor authentication source sequence for the ISE servers. This can be done with the default Sponsor_Portal_Sequence or using a new sequence name. In this configuration, we use the default name and set it to the RADIUS Token server created above, ISELoop. If you do use another name for the source sequence, be sure to change the Sponsor Authentication Servers setting to match.

To update the source sequence, go to Administration >> Identity Management >> Identity Source Sequences.



Sponsor Policy

Finally, in Sponsor Policy, we create two new entries to key off CiscoSecure-Group-Id to assign users to a specific Sponsor Group. The condition to match for each is the ISELoop:CiscoSecure-Group-Id EQUALS FullSponsor or LimitedSponsor. Assign a Sponsor Group with the appropriate privileges to each condtion.
This is done under Administration >> Web Portal Management >> Sponsor Group Policy.



ASA Setup

ASA Configuration

ISE Sponsor Portal uses a security feature which prevents it from being accessed via a simple POST or GET bookmarks defined on the ASA.
HTTP form auto-submit type of bookmark must be used on the ASA to transmit SSO credentials to the ISE Sponsor page. This bookmark functions by preloading the login form with all of its contents and hidden fields and then submitting SSO credentials into that form. This feature was introduced in ASA version 9.0
This section assumes that the ASA has some basic Clientless VPN configuration and the certificate roots for the issuing CA are already pre-loaded.

APCF

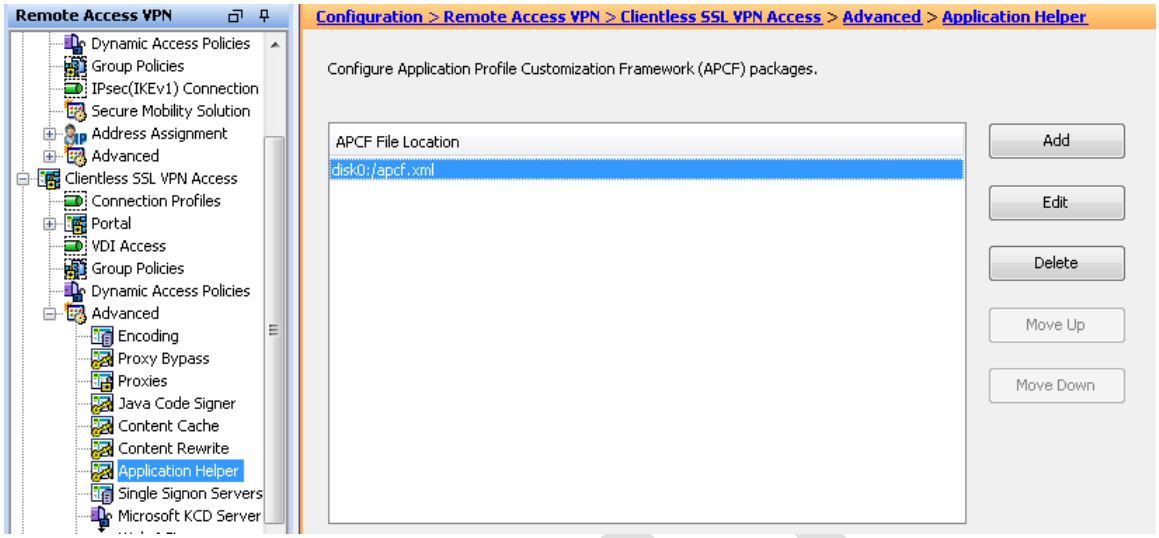
With sponsor portal in ISE 1.1.x, ASA auto-submit feature is not able to properly handle the login form. APCF framework must be used to modify the login page on the fly to make it compatible with ASA.

Additionally, to prevent the users from manually attempting to login to the sponsor portal, APCF is used to change username and password fields from being text fields to being hidden.
The following APCF file will perform these changes.

File apcf.xml

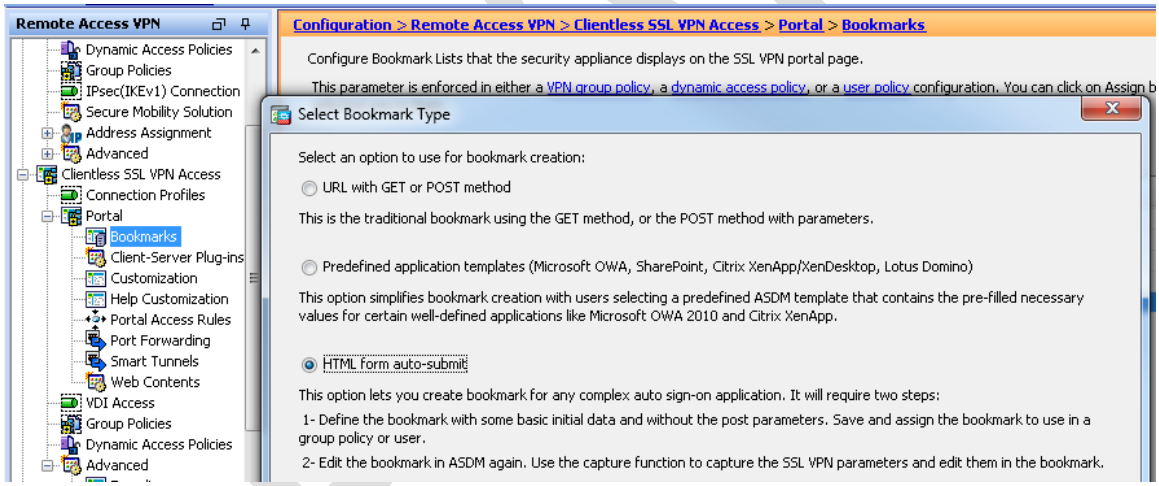
```
<APCF>
<version>1.0</version>
<application>
  <id>ISE 1.1 Sponsor Portal Login</id>
  <apcf-entities>
      <preprocess-response-body>
        <conditions>
            <request-uri-regexp>/sponsorportal/$</request-uri-regexp>
        </conditions>
        <action>
<sed-script>s|&lt;form id="timeoutForm" name="timeoutForm">||g
s|&lt;script>|&lt;script>/*|g
s|&lt;script type="text/javascript">|&lt;script>/*|g
s|&lt;/script>|*/&lt;/script>|g
s|onsubmit="cuesShowLoginProgressMessage();"||g
s|action=""|action="LoginCheck.action"|g
s|name="sponsorUser.name" id="username" type="text"|name="sponsorUser.name" id="username" type="hidden"|g
s|name="sponsorUser.password" id="password" type="password"|name="sponsorUser.password" id="password" type="hidden"|g
s|type="text" name="sponsorUser.loginUsername"|type="hidden" name="sponsorUser.loginUsername"|g
s|type="password" name="sponsorUser.password"|type="hidden" name="sponsorUser.password"|g
</sed-script>
        </action>
      </preprocess-response-body>
      <preprocess-response-body>
        <conditions>
            <request-uri-fnmatch>/sponsorportal/*</request-uri-fnmatch>
        </conditions>
        <action>
<sed-script>s|name="sponsorUser.name" id="username" type="text"|name="sponsorUser.name" id="username" type="hidden"|g
s|name="sponsorUser.password" id="password" type="password"|name="sponsorUser.password" id="password" type="hidden"|g
s|type="text" name="sponsorUser.loginUsername"|type="hidden" name="sponsorUser.loginUsername"|g
s|type="password" name="sponsorUser.password"|type="hidden" name="sponsorUser.password"|g
</sed-script>
        </action>
      </preprocess-response-body>
  </apcf-entities>
</application>
</APCF>
```

The file should be uploaded to the ASA flash using a transfer method such as File Upload in ASDM. Then the file is added globally to the ASA configuration for Client SSL VPN Access using the following configuration screen (Configuration >> Clientless SSL VPN Access >> Advanced >> Application Helper).



Bookmark

The bookmark is created with an HTML form auto-submit entry. Begin by adding a bookmark list. (Configuration >> Clientless SSL VPN Access >> Portal >> Bookmarks). This example uses *ISE-SponsorPortal* for a name. Next we enter a bookmark by clicking Add and selecting "HTML form auto-submit" from the options.



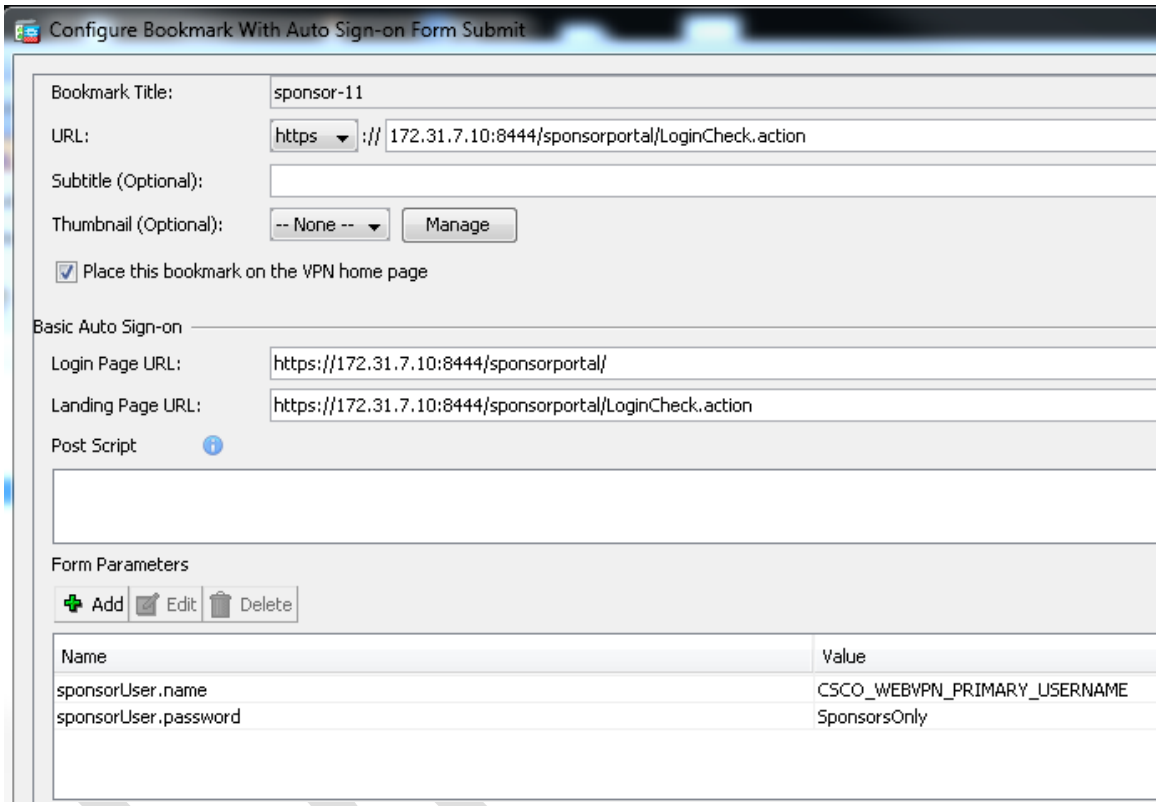
The bookmark configuration screen will now appear. Complete the following sections.

1) Enter a bookmark title. Example: sponsor-11
2) Enter the URL for the ISE server Sponsor Portal page. This is made up of the ISE server's IP address, the port used for sponsor portal and use of https. This example uses: https://172.31.7.10:8444/sponsorportal/LoginCheck.action
3) Complete the Basic Auto Sign-in information for both Login Page and Landing Page. Again, use the data from the ISE server when configuring the URL.
4) Finally enter the Form Parameters for username and password. Username should use sponsorUser.name set to CSCO_WEBVPN_PRIMARY_USERNAME

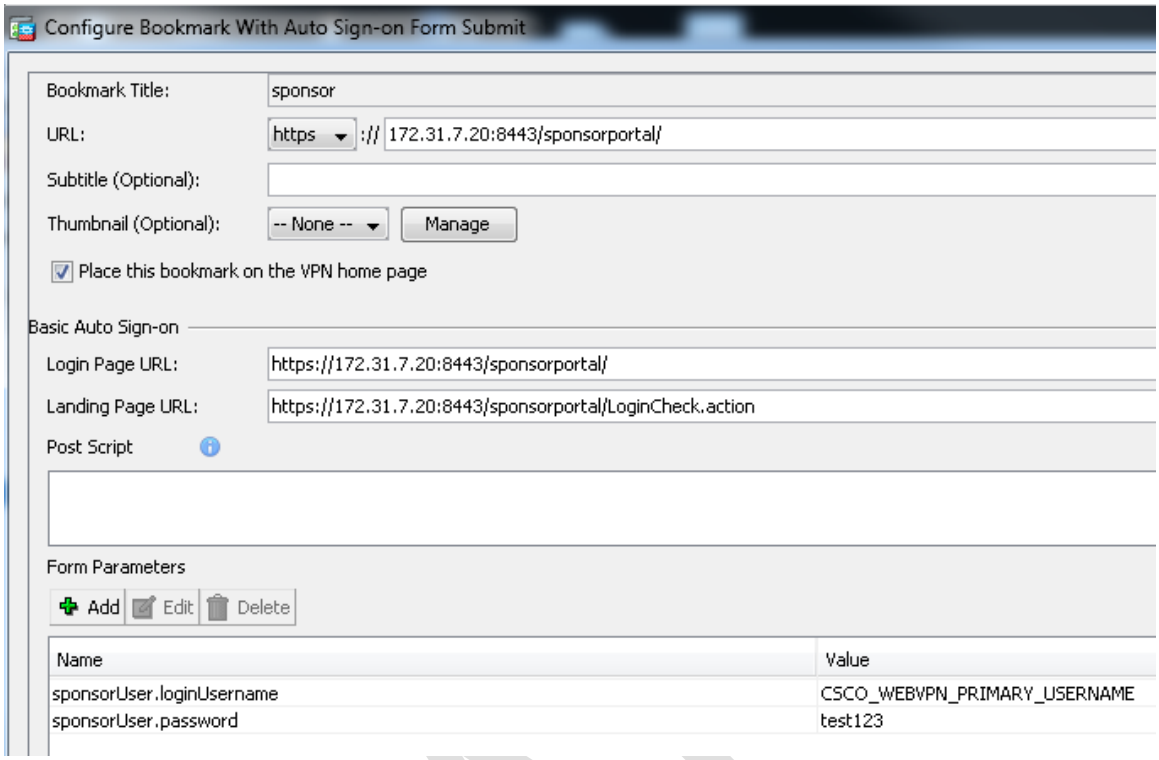
And Password should use sponsorUser.password set to any non-blank value such as test123.

Since ISE is configured to accept any passwords, the value of the password field is not important. Enter any non-blank value.

ISE 1.1 bookmark

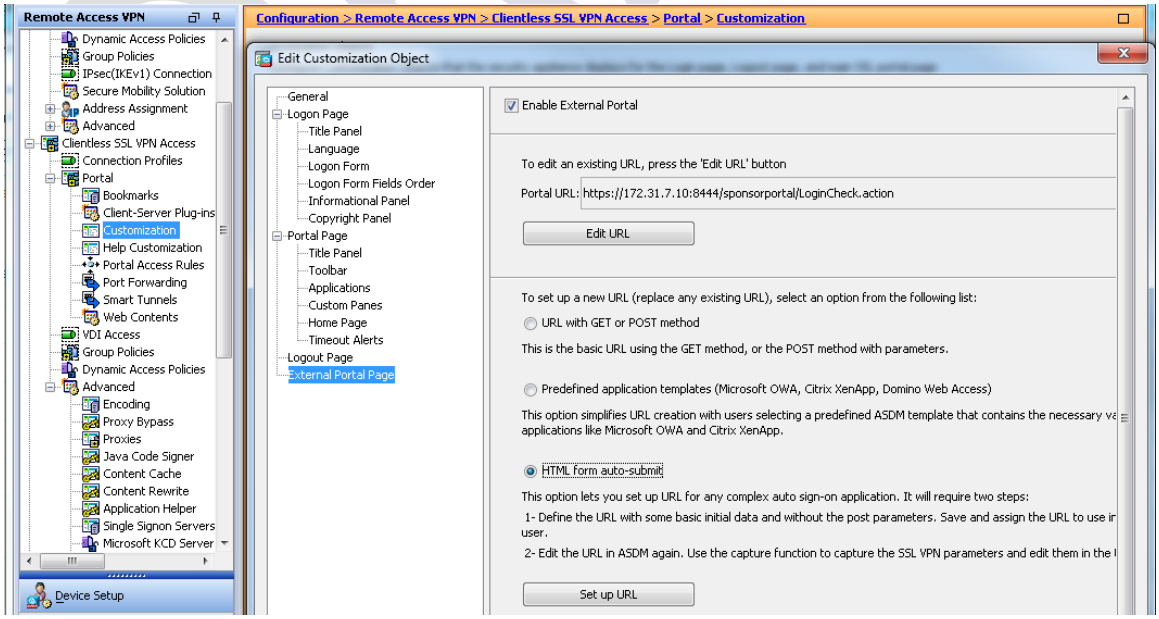


The name of the login field was changed from ISE 1.1 to 1.2, so the bookmark setup will differ slightly from version to version. Below is an example of entries needed for ISE 1.2.



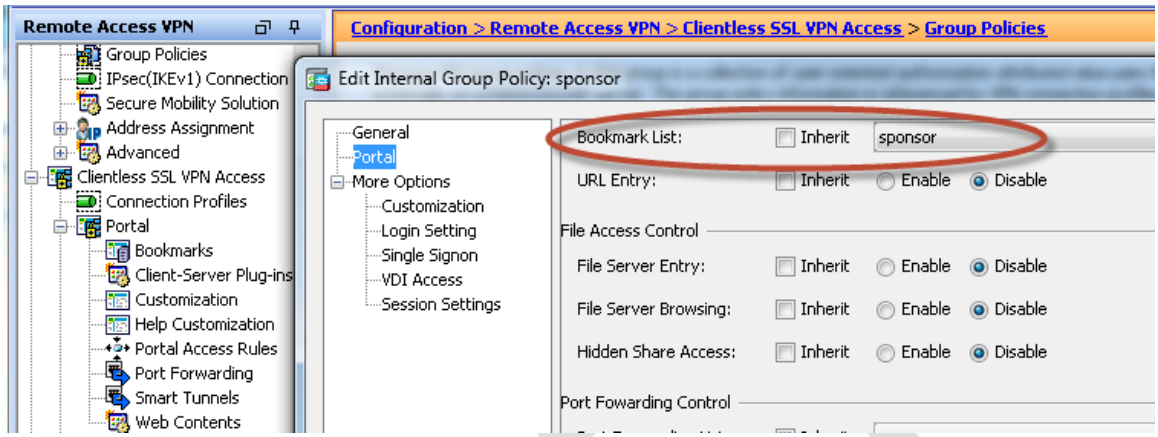
Customization

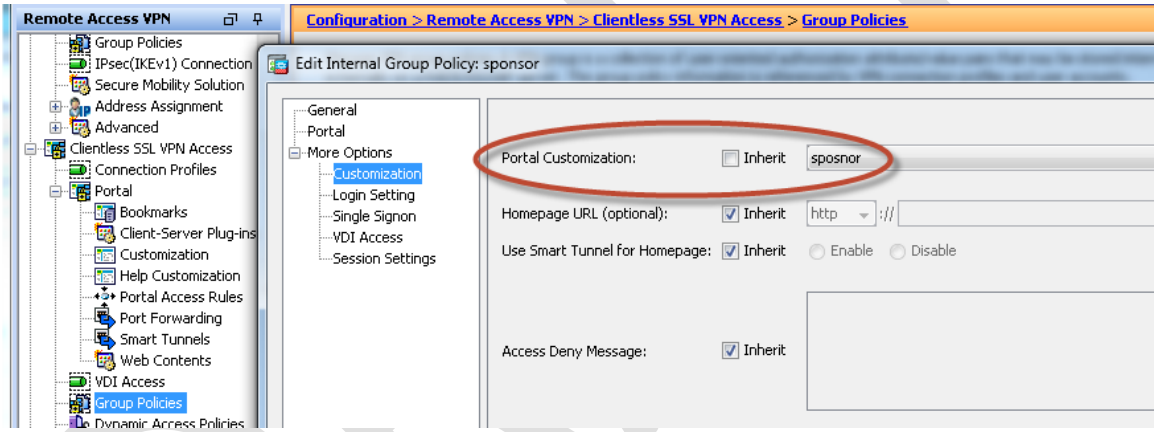
It is possible to send the users directly to the sponsor portal without going through ASA Clientless portal page and the bookmark.
To do that, a customization can be create that performs HTTP auto-submit as the initial page.



Group Policy

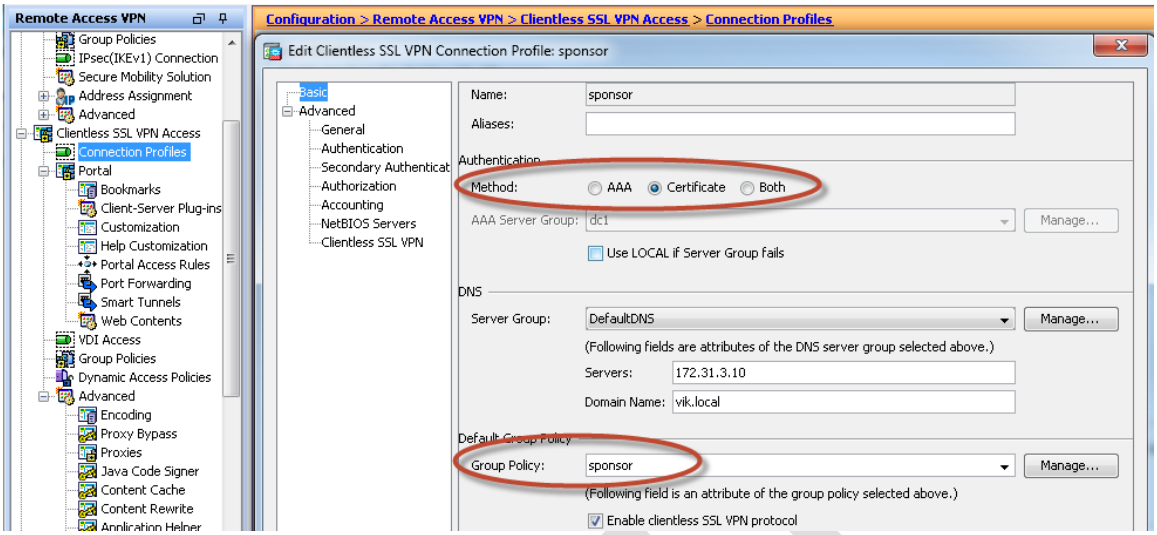
Group Policy can point to the bookmark or the customization depending on the requirements.



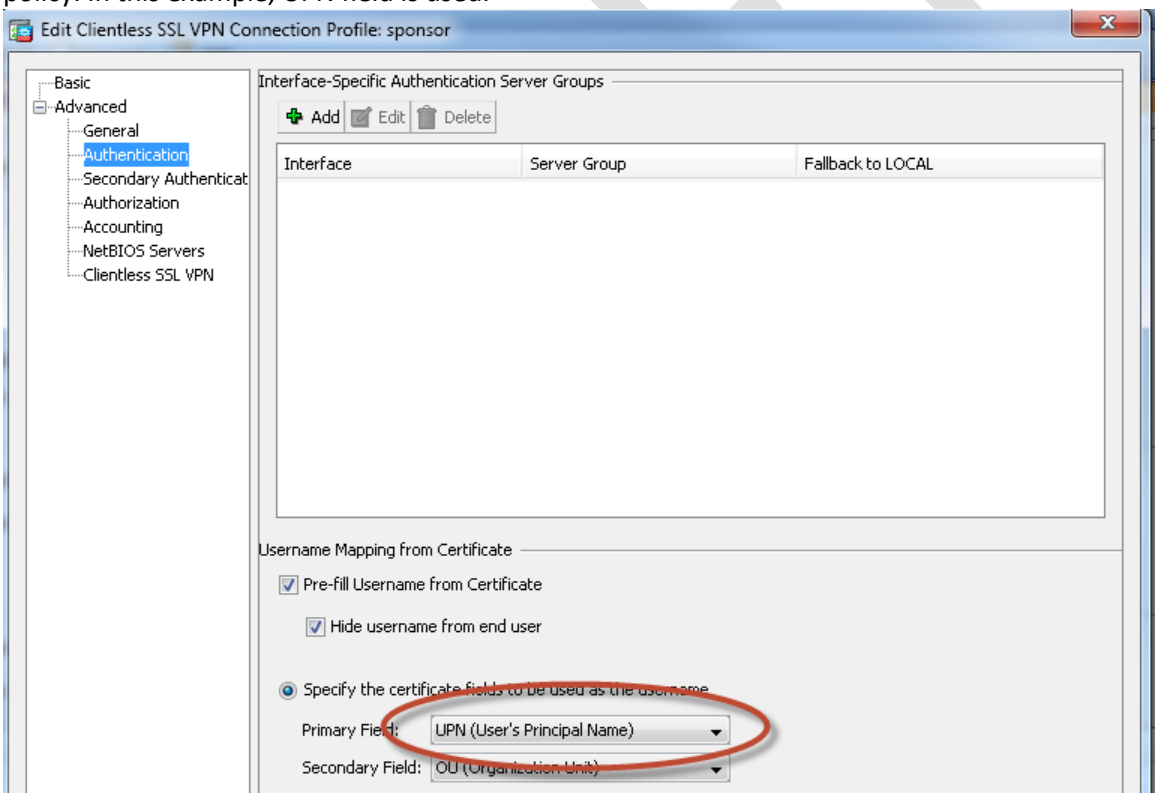


Connection Profile/Tunnel Group

Tunnel Group is configured to perform Certificate authentication only.



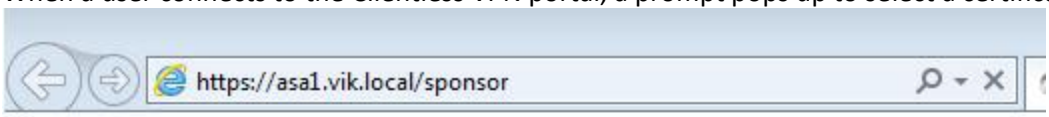
It is important to use the correct field on the certificate as a username. This username will be transmitted to the Sponsor portal and ISE will in turn need to authorize it through the AuthZ policy. In this example, UPN field is used.



Sample Flow

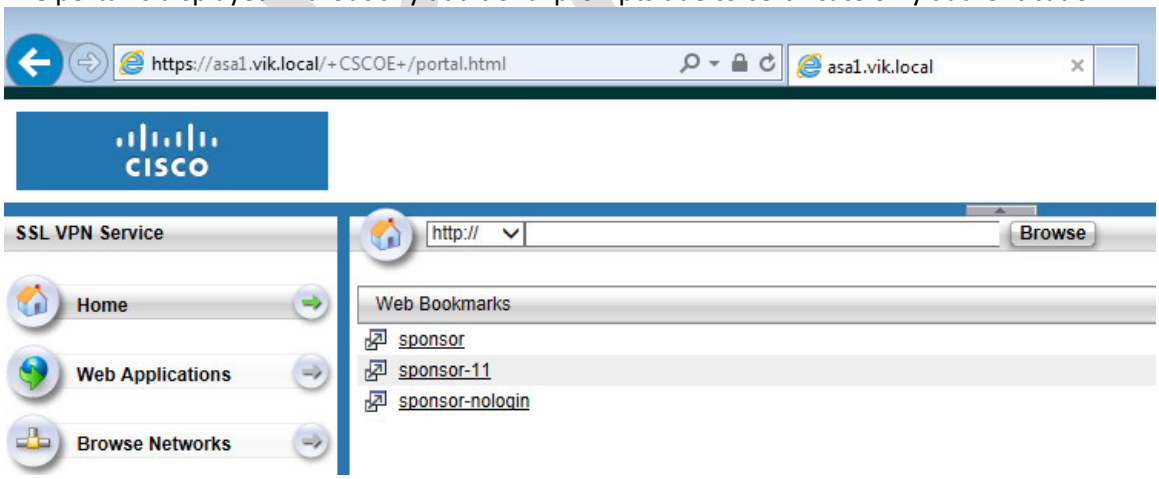
User Logon

When a user connects to the Clientless VPN portal, a prompt pops up to select a certificate.



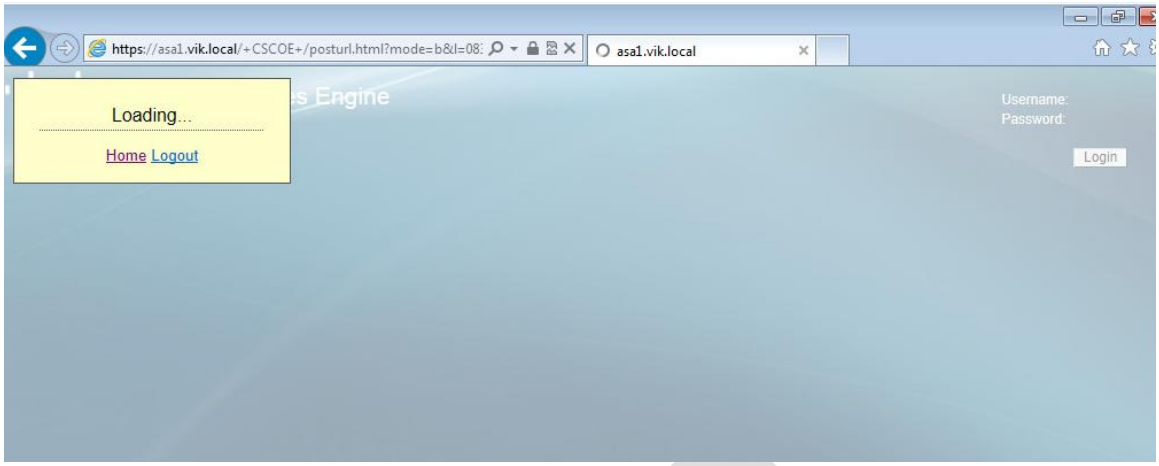
Clientless Portal

The portal is displayed without any additional prompts due to certificate only authentication

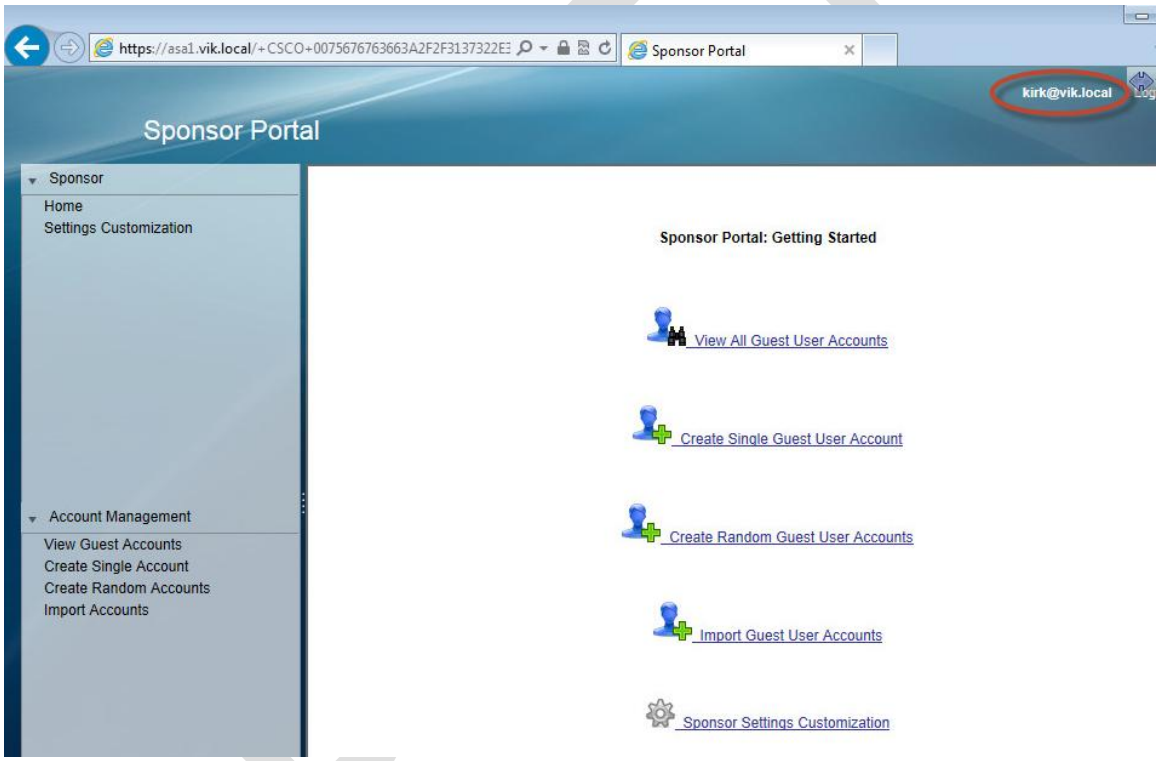


ISE 1.1 Sponsor Portal

Due to APCF file pre-loaded on the ASA, the login page looks different than it normally does when accessed directly. This does not affect the logon process.

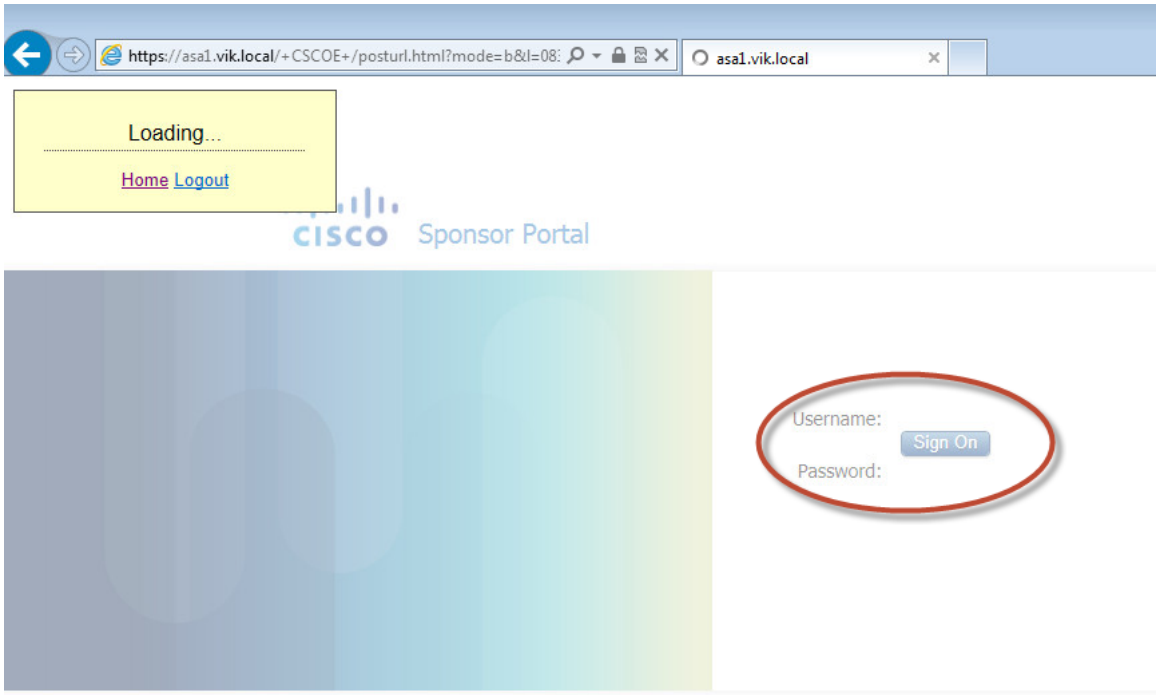


The logon succeeds as the username extracted from the certificate

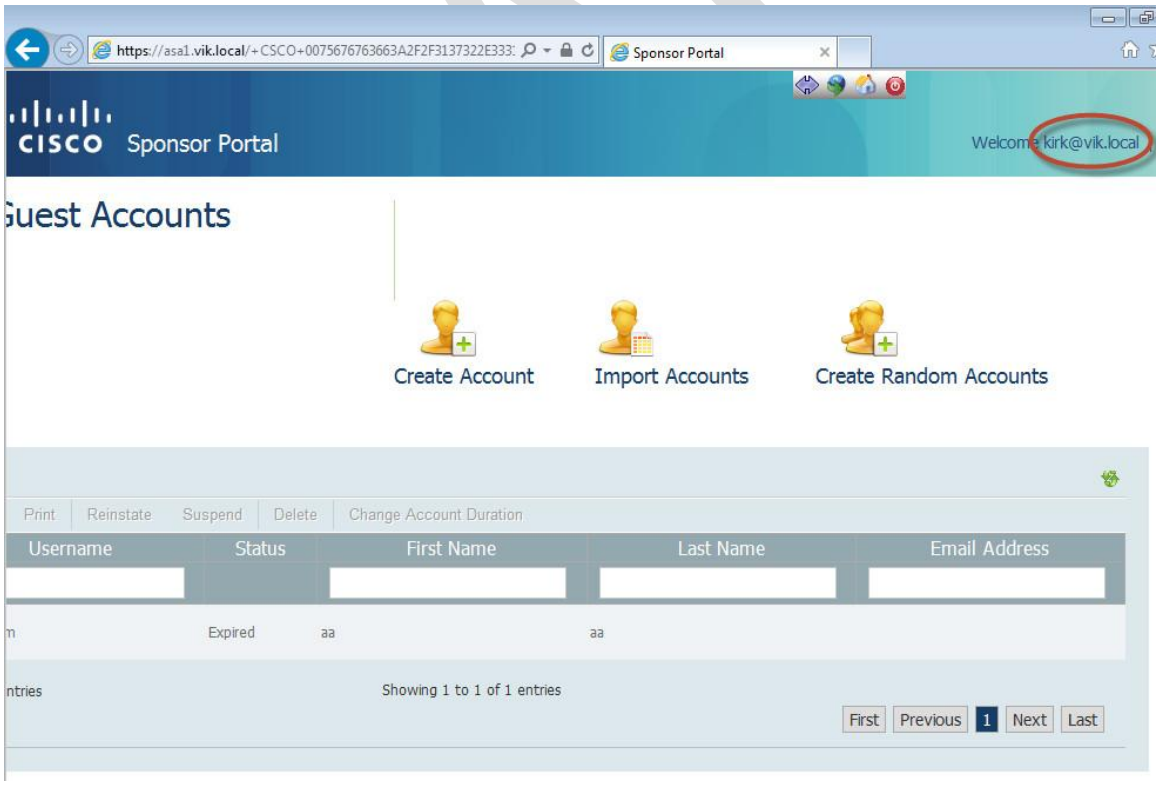


ISE 1.2 Sponsor Portal

Due to APCF file pre-loaded on the ASA, the username and password fields are not displayed. This does not affect the logon process.



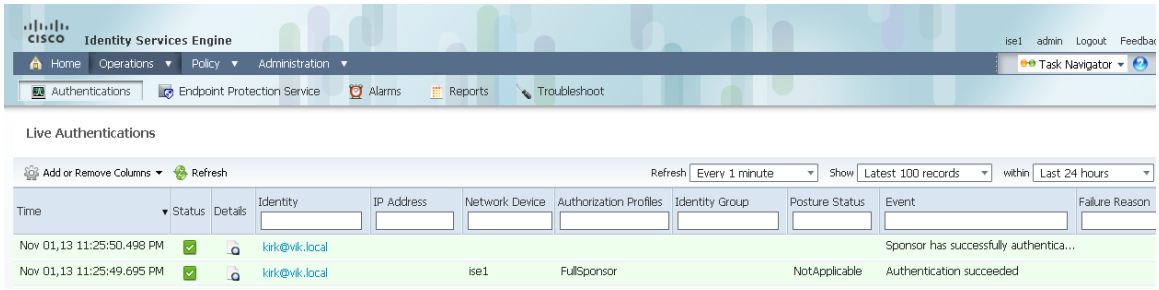
After a couple of seconds, ISE Sponsor portal is displayed



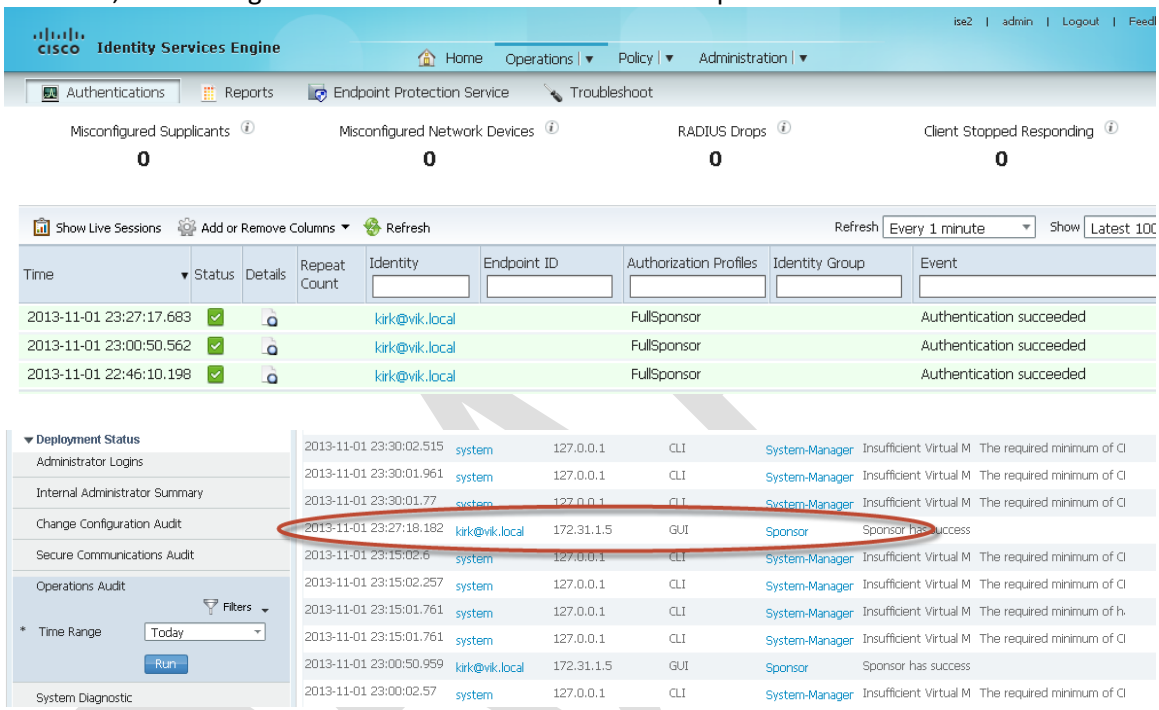
ISE Logs

The logs show the logins.

In ISE 1.1, two login entries are displayed in the main log, one for looped RADIUS request and the second for successful sponsor authentication.



In ISE 1.2, the two log entries are located in two different reports.



Disclaimer

Cisco's policy is one of continuous improvement and the specifications and information regarding the products in this presentation are subject to change without notice. All statements, information, and recommendations in this presentation are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products. The software license and limited warranty terms are set forth in the information pack shipped with the products and are incorporated herein by this reference.