



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

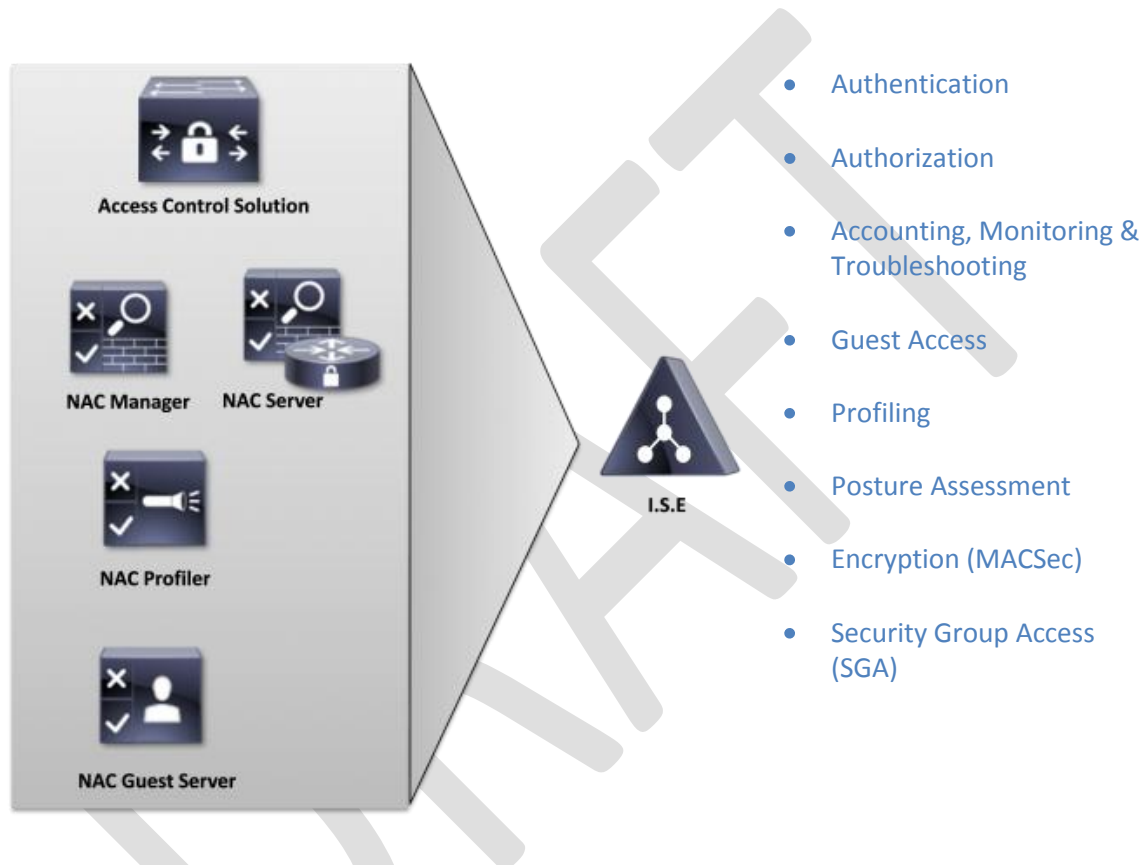
Contents

Introduction	3
Cisco ISE Sponsor Process	3
Overview.....	4
Authentication Methods	4
Authorization Methods	4
Need for Certificate Authentication.....	4
Solution	4
Overview.....	4
Restricting Sponsor Portal to ASA Only.....	5
ISE Configuration	5
Sponsor Portal TCP port	5
ISE as NAD.....	6
RADIUS Token Server	7
Authentication Policy	8
Authorization Profiles.....	9
Authorization Policy	10
Sponsor Authentication Sequence.....	11
Sponsor Policy	12
ASA Setup	12
ASA Configuration	12
APCF.....	12
Bookmark	14
Customization.....	16
Group Policy	17
Connection Profile/Tunnel Group.....	17
Sample Flow	19
<i>User Logon</i>	19
<i>Clientless Portal</i>	19
<i>ISE 1.1 Sponsor Portal</i>	19
<i>ISE 1.2 Sponsor Portal</i>	20
<i>ISE Logs</i>	21
Disclaimer	23

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.



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

Cisco Systems, Inc.

All contents are covered by copyright © 2013, Cisco Systems, Inc. All rights reserved.
Important notes and declaration of confidentiality.

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.

Sponsor Group Policy Sponsor Groups **Settings**

Settings

- ▼ General
 - Portal Theme
 - Ports
 - Purge
- ▶ Sponsor
- ▶ My Devices
- ▶ Guest

Guest/Sponsor SSL Settings

Admin Portal Settings

HTTP Port

HTTPS Port

Guest Portal Settings

HTTPS Port (Valid Range 1 to 65535)

Sponsor Portal Settings

HTTPS Port (Valid Range 1 to 65535)

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.

Network Devices **Network Device Groups** External RADIUS Servers RADIUS Server Sequences SGA AAA Servers

Network Device Groups

Groups

- ▶ All Device Types
- ▶ All Locations

Network Device Groups

Edit + Add Duplicate Delete

Name	Type
<input type="checkbox"/> CVD	Device Type
<input style="border: 2px solid red;" type="checkbox"/> ISE	Device Type
<input type="checkbox"/> WLC	Device Type

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.

Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers

Network Devices List > ise2-psn2

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type

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.

The screenshot displays the Cisco ISE web interface for configuring RADIUS Token Identity Sources. The navigation menu includes System, Identity Management, Network Resources, Web Portal Management, and Feed Service. The current page is 'External Identity Sources', with 'RADIUS Token' selected. The configuration is for 'RADIUS Token Identity Sources' under the 'ISELoop' token list, specifically in the 'Connection' tab. The 'Server Connection' section has 'Safeword Server' and 'Enable Secondary Server' unchecked. The 'Primary Server' section has the following settings: Host IP (172.31.7.22), Shared Secret (masked), Authentication Port (1812), Server Timeout (5 seconds), and Connection Attempts (3). The 'Always Access Primary Server First' radio button is selected, and 'Failback to Primary Server after' is also selected. 'Save' and 'Reset' buttons are at the bottom.

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.

The screenshot displays the Cisco ISE web interface for configuring an Authentication Policy. The navigation menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The current page is 'Authentication Policy', with 'Rule-Based' selected. The policy is defined with the condition "If DEVICE:Device Type EQUALS All Device Types#ISE" and "Allow Protocols : Default Network Access". The 'Default' protocol is checked.

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

ISE Loop : If DEVICE:Device Type EQUALS All ... Allow Protocols: Default Network Access and

Default : Use Internal Users

Identity Source: Internal Users

Options

- If authentication failed: Continue
- If user not found: Continue
- If process failed: Drop

MAB : If Wired

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.

Authorization Profile

* Name: FullSponsor

Description:

* Access Type: ACCESS_ACCEPT

Service Template:

Advanced Attributes Settings

Cisco:cisco-av-pair = iscoSecure-Group-Id=FullSponsor

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = ACS: CiscoSecure-Group-Id=FullSponsor

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.

The screenshot displays the Cisco ISE configuration interface for creating a new authorization profile. The top navigation bar includes tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. Below this, there are sub-tabs for Dictionaries, Conditions, and Results. The main content area is titled 'Authorization Profiles > New Authorization Profile' and contains the following configuration details:

- Name:** LimitedSponsor
- Description:** (Empty field)
- Access Type:** ACCESS_ACCEPT
- Service Template:** (Unchecked checkbox)
- Advanced Attributes Settings:**
 - Attribute: Cisco:cisco-av-pair = Value: Secure-Group-Id=LimitedSponsor
- Attributes Details:**
 - Access Type = ACCESS_ACCEPT
 - cisco-av-pair = ACS: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.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	ISE Loop Full	if (DEVICE:Device Type EQUALS All Device Types#ISE AND Network Access:AuthenticationMethod EQUALS RAR_ASCII AND vik-ad:ExternalGroups EQUALS vik.local/Lab/FullSponsor)	then FullSponsor
✓	ISE Loop Limited	if (DEVICE:Device Type EQUALS All Device Types#ISE AND Network Access:AuthenticationMethod EQUALS RAR_ASCII AND vik-ad:ExternalGroups EQUALS vik.local/Lab/LimitedSponsor)	then LimitedSponsor
✓	Default	if no matches, then DenyAccess	

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.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > **Sponsor_Portal_Sequence**

Identity Source Sequence

▼ Identity Source Sequence

* Name:

Description: A built-in Identity Sequence for the Sponsor Portal

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
<ul style="list-style-type: none"> Guest Users Internal Endpoints Internal Users vik-ad 	<ul style="list-style-type: none"> ISELoop

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 condition.

This is done under Administration >> Web Portal Management >> Sponsor Group Policy.

The screenshot shows the 'Sponsor Group Policy' configuration page in the Cisco ISE Administration console. The page has a navigation bar with tabs for System, Identity Management, Network Resources, Web Portal Management, and Feed Service. Below the navigation bar, there are sub-tabs for Sponsor Group Policy, Sponsor Groups, and Settings. The main content area is titled 'Sponsor Group Policy' and includes a sub-header: 'Define the Sponsor Group Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.'

Status	Policy Name	Identity Groups	Other Conditions	Sponsor Groups
✓	Manage All Accounts	If SponsorAllAccount and Condition(s) then		SponsorAllAccounts
✓	Manage Group Accounts	If SponsorGroupAccounts and Condition(s) then		SponsorGroupGrpAccounts
✓	Manage Own Accounts	If SponsorOwnAccounts and Condition(s) then		SponsorGroupOwnAcc...
✓	Domain Admins	If Any and vik-ad:ExternalGroups EQUALS vik.I...		SponsorAllAccounts
✓	Full Sponsors	If Any and ISELoop: CiscoSecure-Group-Id EQU...		SponsorAllAccounts
✓	Limited Sponsor	If Any and Add All Conditions Below to Library		

A pop-up window titled 'Add All Conditions Below to Library' is open, showing a table for defining conditions:

Condition Name	Expression
	ISELoop: CiscoSec... Equals FullSponsor

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

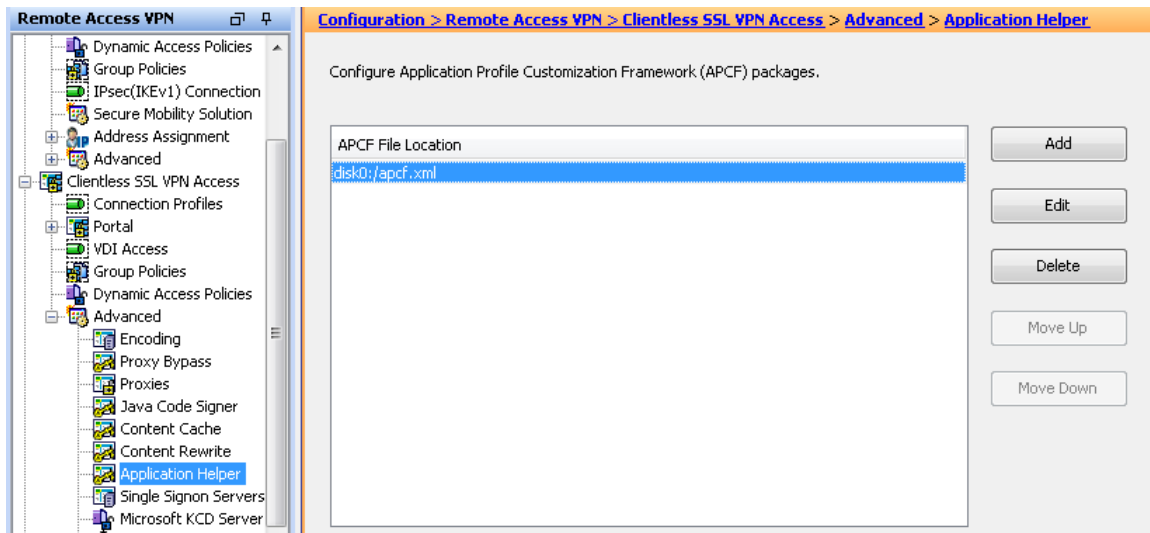
With sponsor portal in ISE 1.1.x, ASA auto-submit feature is not able to properly handle the login form. APCF framework must be used to modify the login page on the fly to make it compatible with ASA.

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

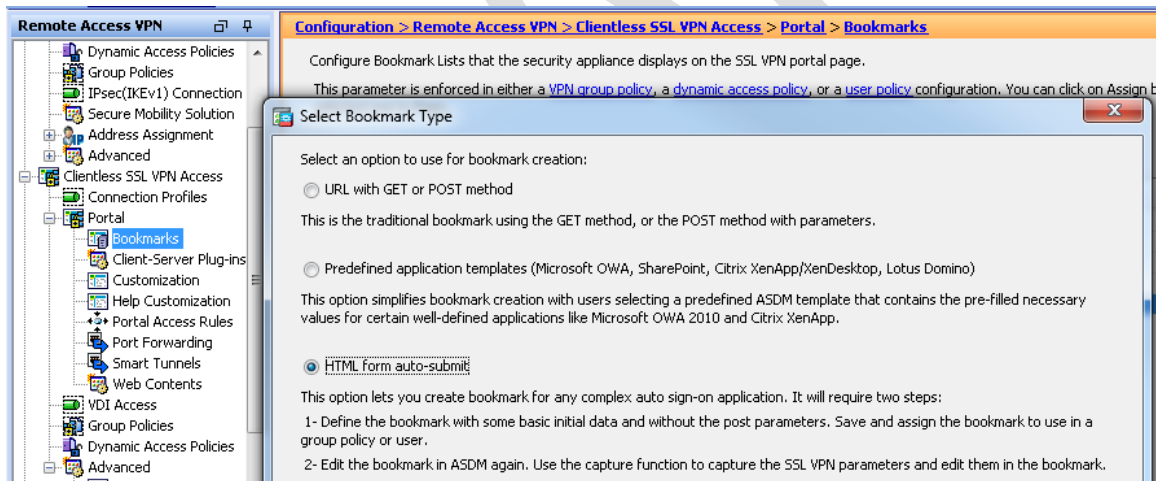
```
<APCF>
<version>1.0</version>
<application>
  <id>ISE 1.1 Sponsor Portal Login</id>
  <apcf-entities>
    <preprocess-response-body>
      <conditions>
        <request-uri-regexp>/sponsorportal/$</request-uri-regexp>
      </conditions>
      <action>
<sed-script>s|&lt;form id="timeoutForm" name="timeoutForm">||g
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 screenshot shows the 'Configure Bookmark With Auto Sign-on Form Submit' window. The 'Bookmark Title' is 'sponsor-11'. The 'URL' is 'https://172.31.7.10:8444/sponsorportal/LoginCheck.action'. The 'Thumbnail (Optional)' is set to '-- None --'. The checkbox 'Place this bookmark on the VPN home page' is checked. Under 'Basic Auto Sign-on', the 'Login Page URL' is 'https://172.31.7.10:8444/sponsorportal/' and the 'Landing Page URL' is 'https://172.31.7.10:8444/sponsorportal/LoginCheck.action'. The 'Post Script' field is empty. The 'Form Parameters' section contains a table with two entries:

Name	Value
sponsorUser.name	CSCO_WEBVPN_PRIMARY_USERNAME
sponsorUser.password	SponsorsOnly

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.

Configure Bookmark With Auto Sign-on Form Submit

Bookmark Title:

URL:

Subtitle (Optional):

Thumbnail (Optional):

Place this bookmark on the VPN home page

Basic Auto Sign-on

Login Page URL:

Landing Page URL:

Post Script

Form Parameters

Name	Value
sponsorUser.loginUsername	CSCO_WEBVPN_PRIMARY_USERNAME
sponsorUser.password	test123

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.

The screenshot shows the Cisco ISE configuration interface. The left pane displays the configuration tree with 'Remote Access VPN > Clientless SSL VPN Access > Portal > Customization' selected. The right pane shows the 'Edit Customization Object' dialog for the 'External Portal Page' object.

General

- Enable External Portal

To edit an existing URL, press the 'Edit URL' button

Portal URL:

To set up a new URL (replace any existing URL), select an option from the following list:

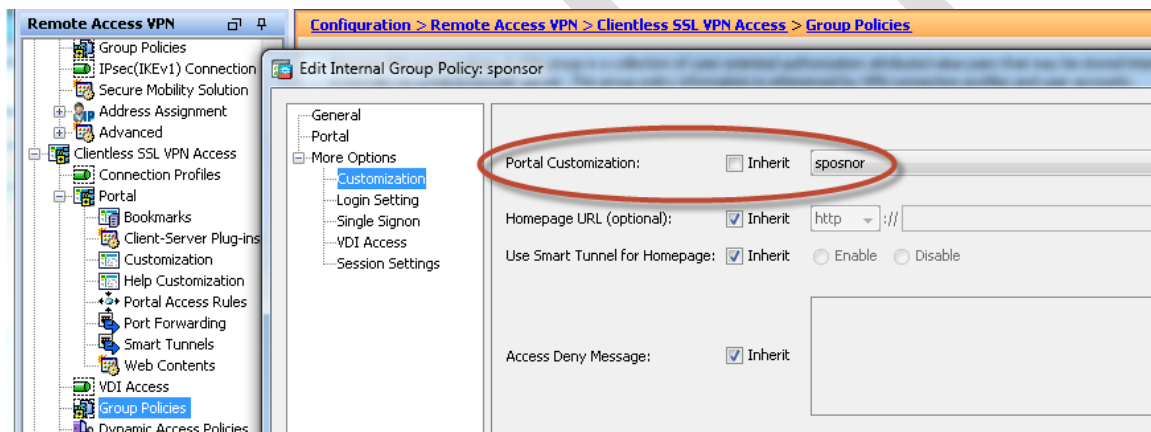
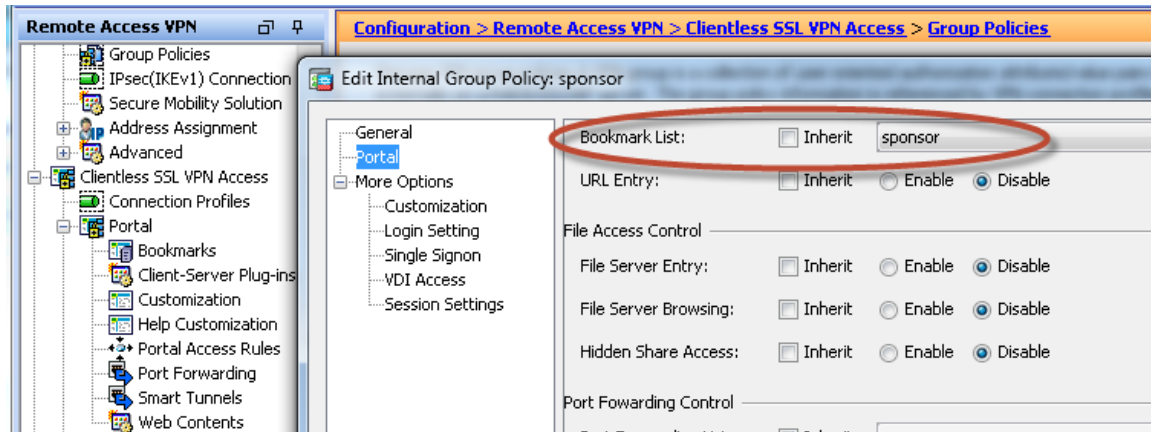
- URL with GET or POST method
This is the basic URL using the GET method, or the POST method with parameters.
- Predefined application templates (Microsoft OWA, Citrix XenApp, Domino Web Access)
This option simplifies URL creation with users selecting a predefined ASDM template that contains the necessary variables for applications like Microsoft OWA and Citrix XenApp.
- HTML form auto-submit
This option lets you set up URL for any complex auto sign-on application. It will require two steps:
1- Define the URL with some basic initial data and without the post parameters. Save and assign the URL to use in user.
2- Edit the URL in ASDM again. Use the capture function to capture the SSL VPN parameters and edit them in the ISE.

Cisco Systems, Inc.

All contents are covered by copyright © 2013, Cisco Systems, Inc. All rights reserved.
Important notes and declaration of confidentiality.

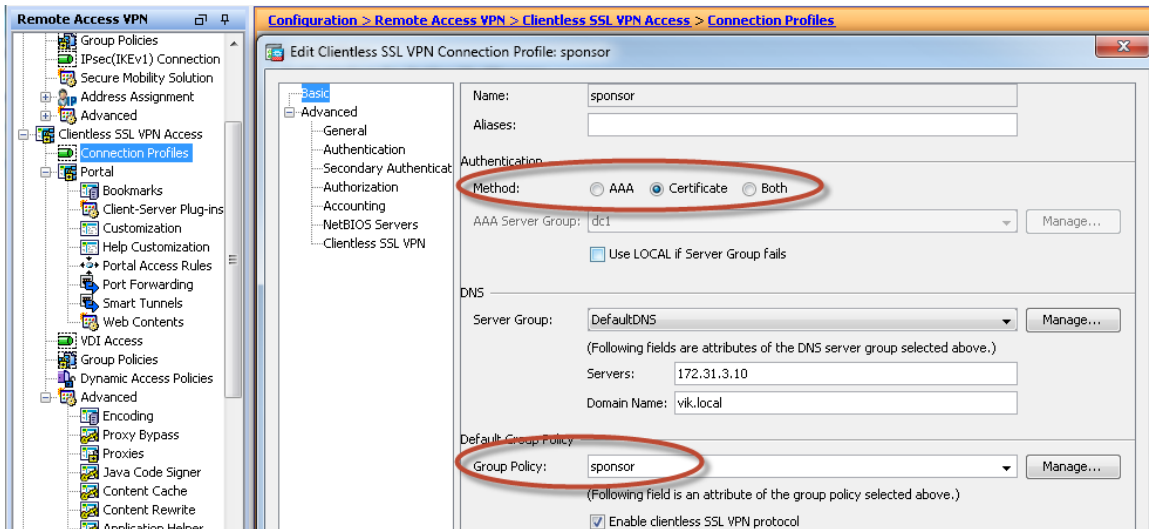
Group Policy

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

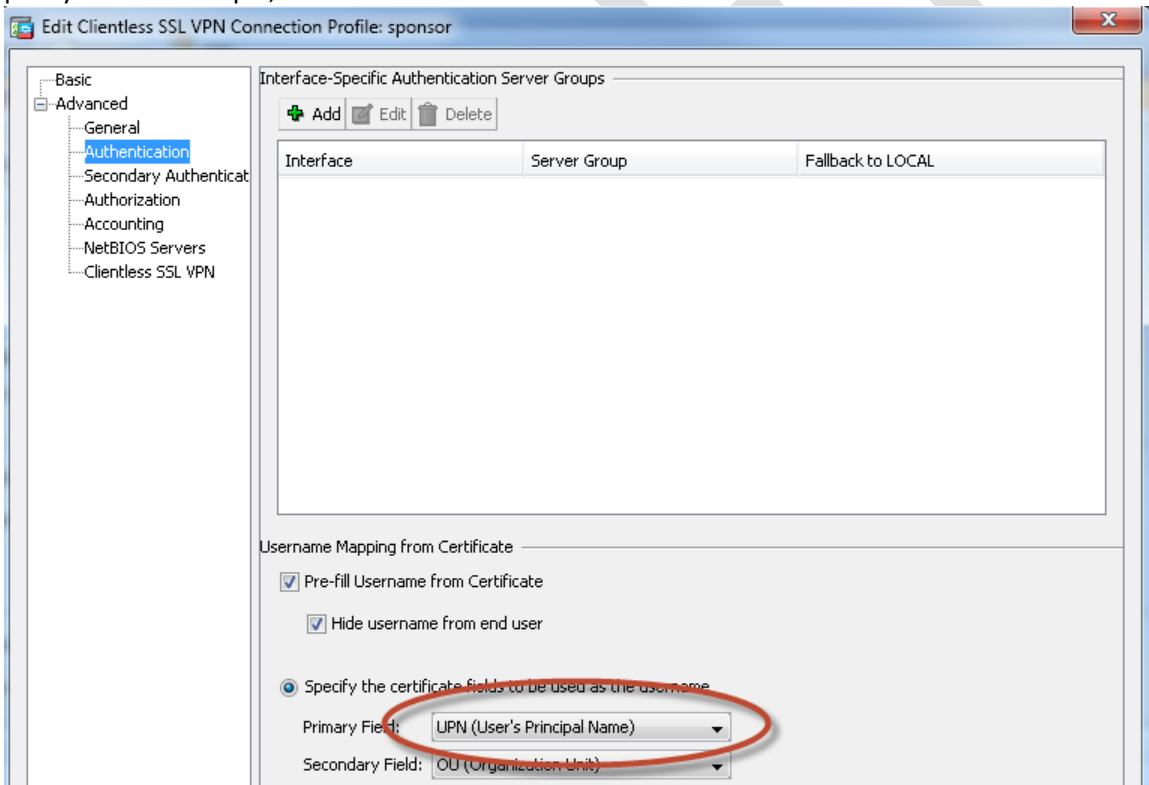


Connection Profile/Tunnel Group

Tunnel Group is configured to perform Certificate authentication only.



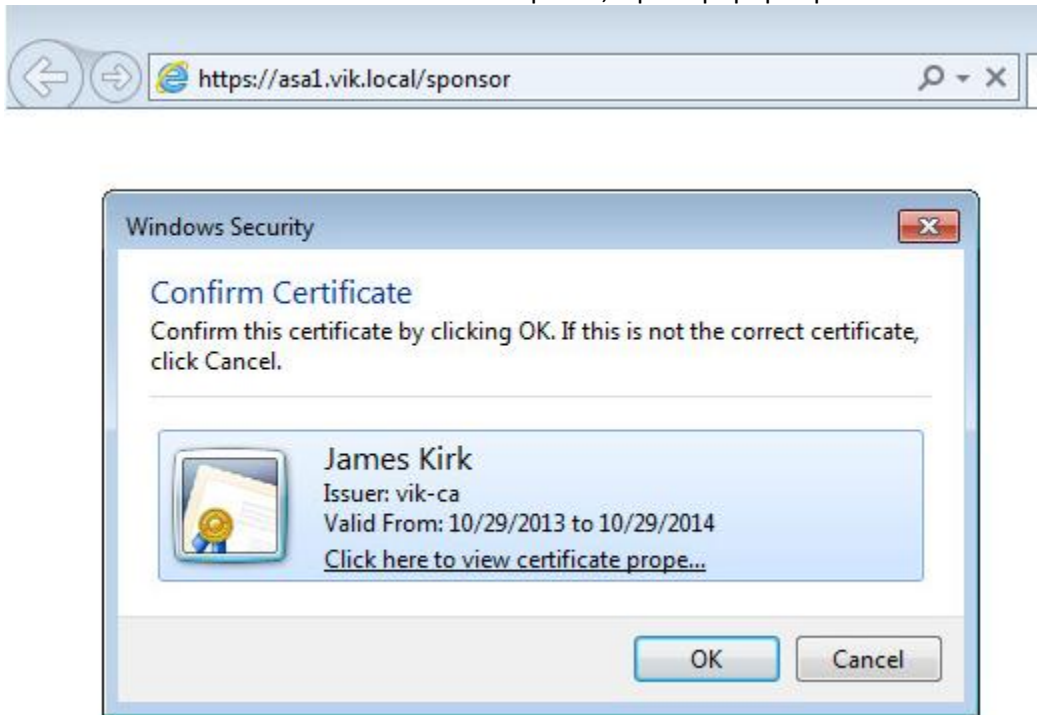
It is important to use the correct field on the certificate as a username. This username will be transmitted to the Sponsor portal and ISE will in turn need to authorize it through the AuthZ policy. In this example, UPN field is used.



Sample Flow

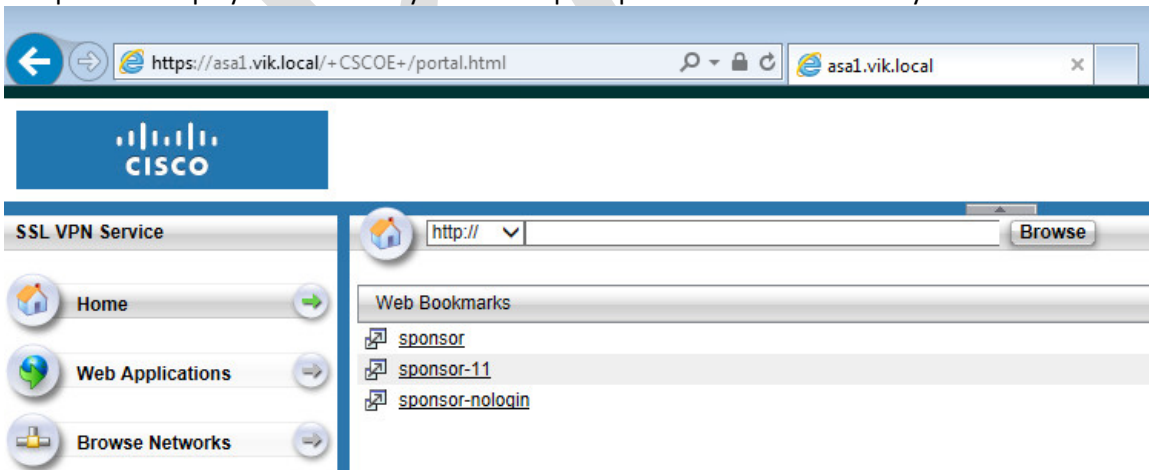
User Logon

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



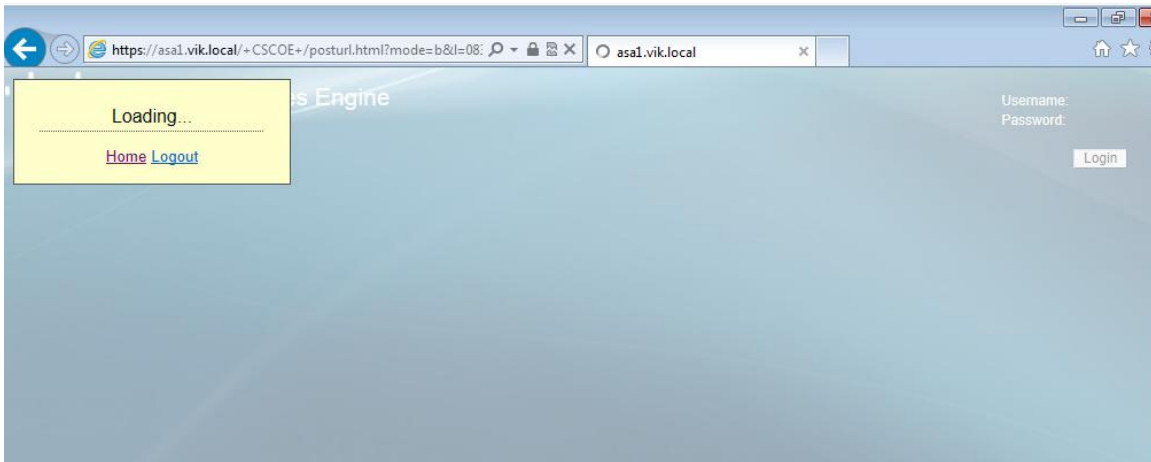
Clientless Portal

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

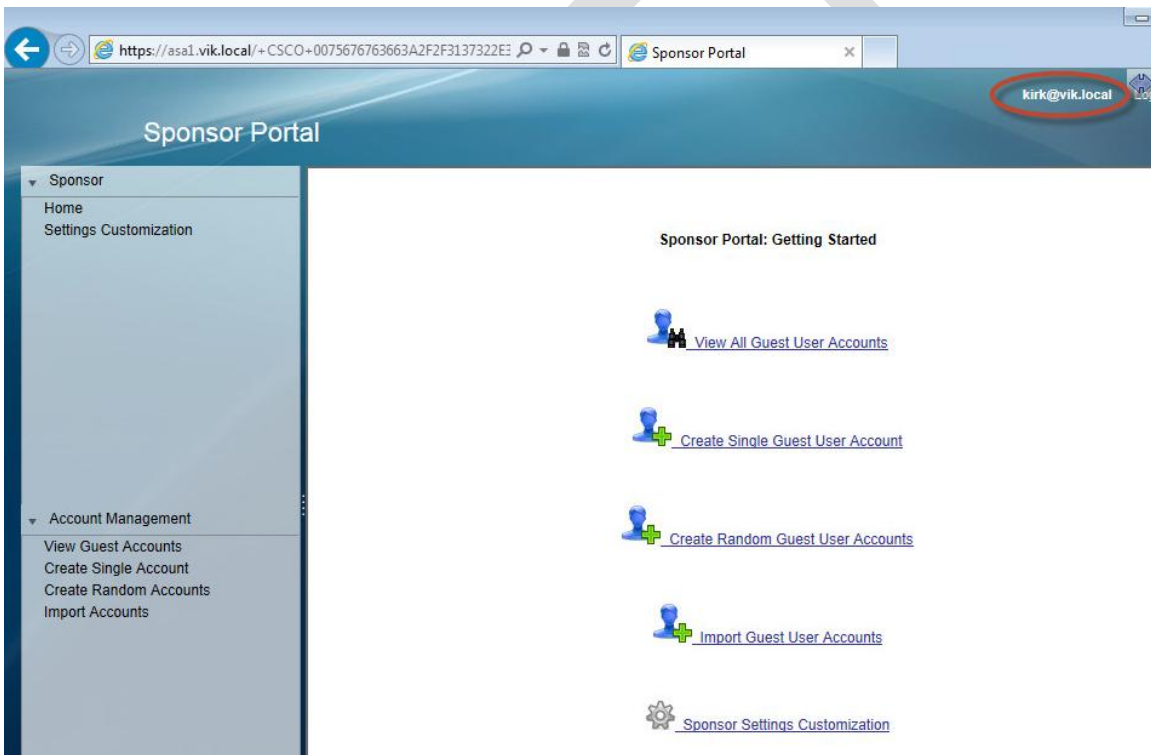


ISE 1.1 Sponsor Portal

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.

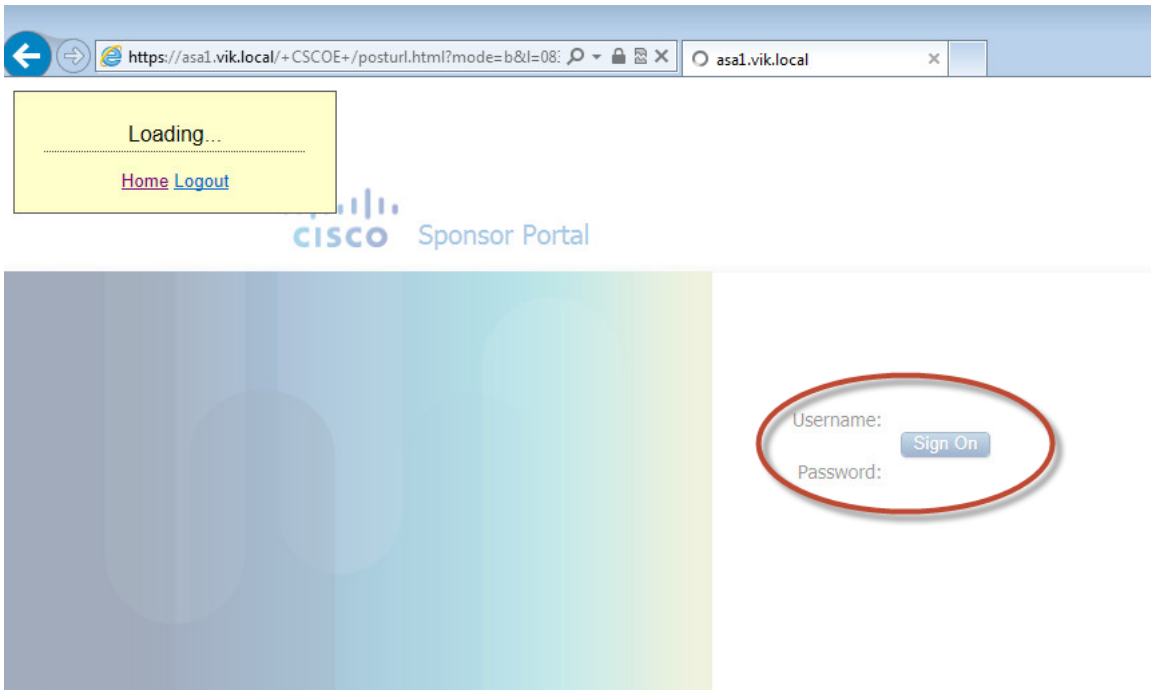


The logon succeeds as the username extracted from the certificate

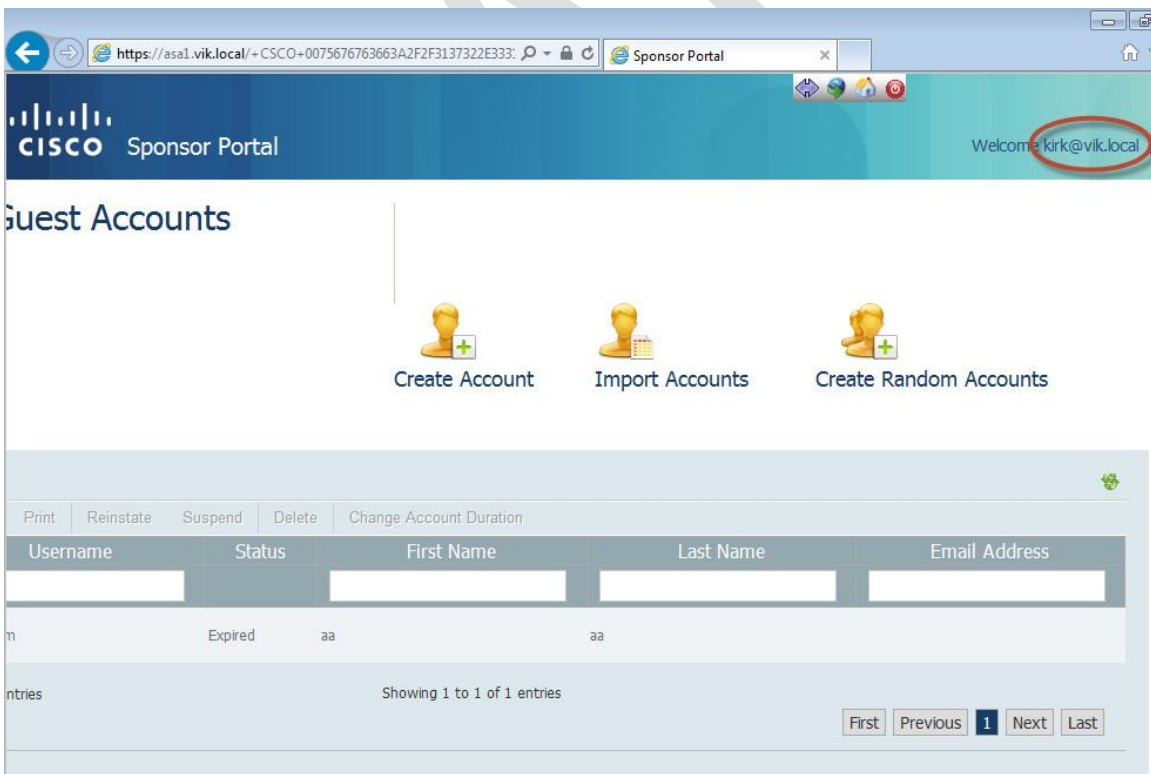


ISE 1.2 Sponsor Portal

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.

Live Authentications

Refresh: Every 1 minute | Show: Latest 100 records | within: Last 24 hours

Time	Status	Details	Identity	IP Address	Network Device	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason
Nov 01, 13 11:25:50.498 PM	✓		kirk@vik.local						Sponsor has successfully authentica...	
Nov 01, 13 11:25:49.695 PM	✓		kirk@vik.local		ise1	FullSponsor		NotApplicable	Authentication succeeded	

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

Reports

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0 | Client Stopped Responding: 0

Show Live Sessions

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Authorization Profiles	Identity Group	Event
2013-11-01 23:27:17.683	✓			kirk@vik.local		FullSponsor		Authentication succeeded
2013-11-01 23:00:50.562	✓			kirk@vik.local		FullSponsor		Authentication succeeded
2013-11-01 22:46:10.198	✓			kirk@vik.local		FullSponsor		Authentication succeeded

Operations Audit

Time Range: Today | Run

2013-11-01 23:30:02.515	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:30:01.961	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:30:01.77	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:27:18.182	kirk@vik.local	172.31.1.5	GUI	Sponsor	Sponsor has success	
2013-11-01 23:15:02.6	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:15:02.257	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:15:01.761	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of h
2013-11-01 23:15:01.761	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C
2013-11-01 23:00:50.959	kirk@vik.local	172.31.1.5	GUI	Sponsor	Sponsor has success	
2013-11-01 23:00:02.57	system	127.0.0.1	CLI	System-Manager	Insufficient Virtual M	The required minimum of C

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.

DRAFT