

Module 10 Mobile Access

Module 10: Mobile Access

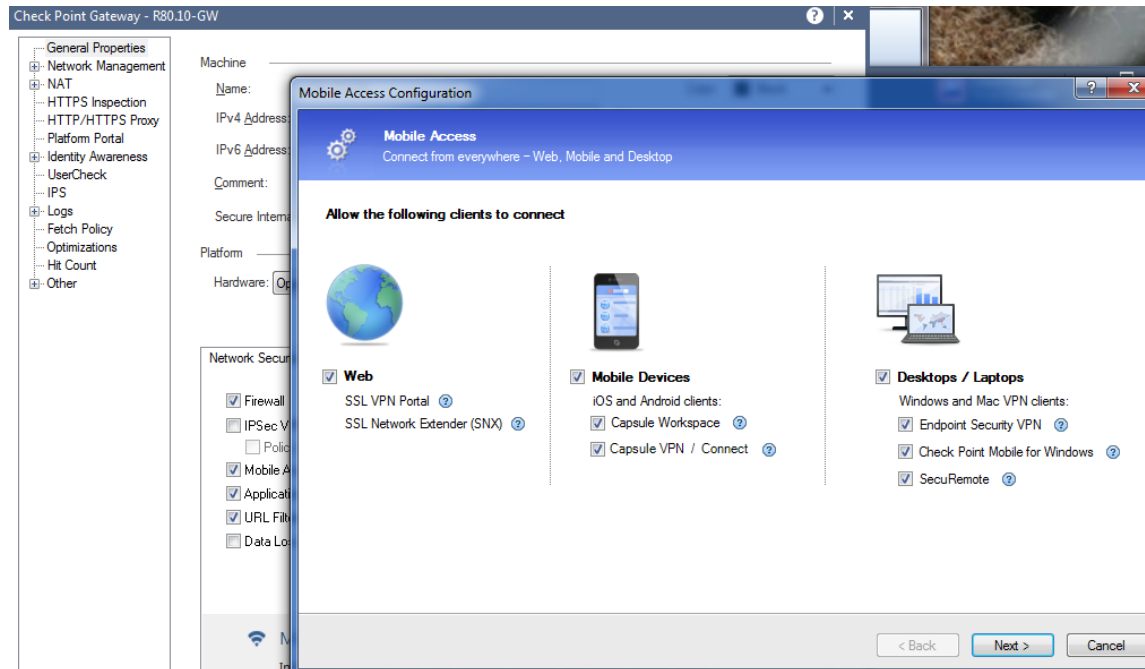
Instructor: Kim Winfield

Objectives

- Administer and implement a Mobile Access solution for SSL VPN
- Apply Secure Workspace to secure, a remote users desktops
- Create access to internal web applications using the Mobile Access Blade

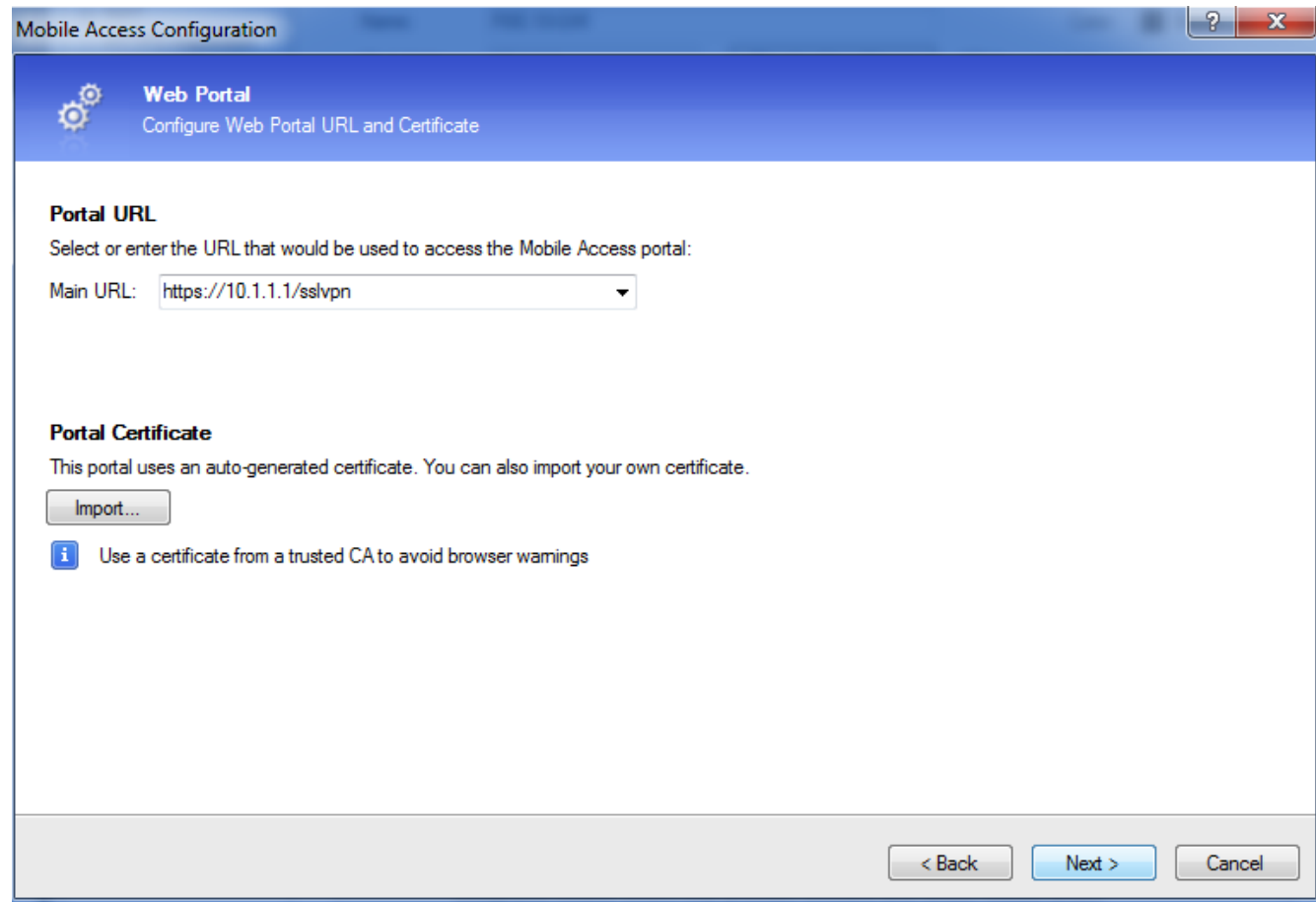
Mobile Access an SSL VPN Solution

- Mobile Access Blade Wizard
 - Web
 - Mobile Devices
 - Desktops
 - Laptops



Mobile Access Web Portal

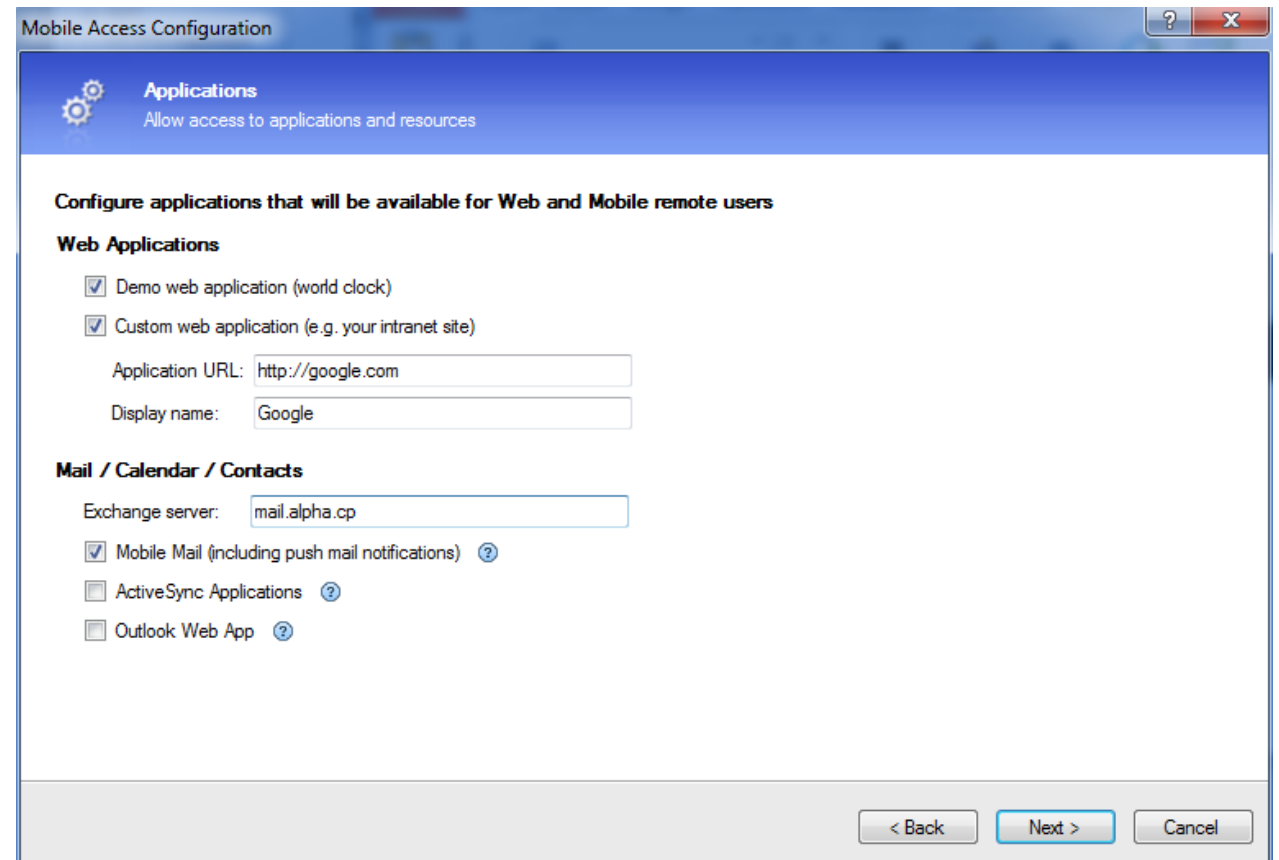
- Portal URL
- Portal Certificate



The screenshot shows a Windows-style window titled "Mobile Access Configuration". Inside, there's a tab labeled "Web Portal" with a subtitle "Configure Web Portal URL and Certificate". The "Portal URL" section has a dropdown menu for "Main URL" currently set to "https://10.1.1.1/sslvpn". The "Portal Certificate" section states that the portal uses an auto-generated certificate but allows importing a custom one, with an "Import..." button. An information icon and text advise using a certificate from a trusted CA to avoid browser warnings. Navigation buttons at the bottom include "< Back", "Next >", and "Cancel".

Mobile Access Application

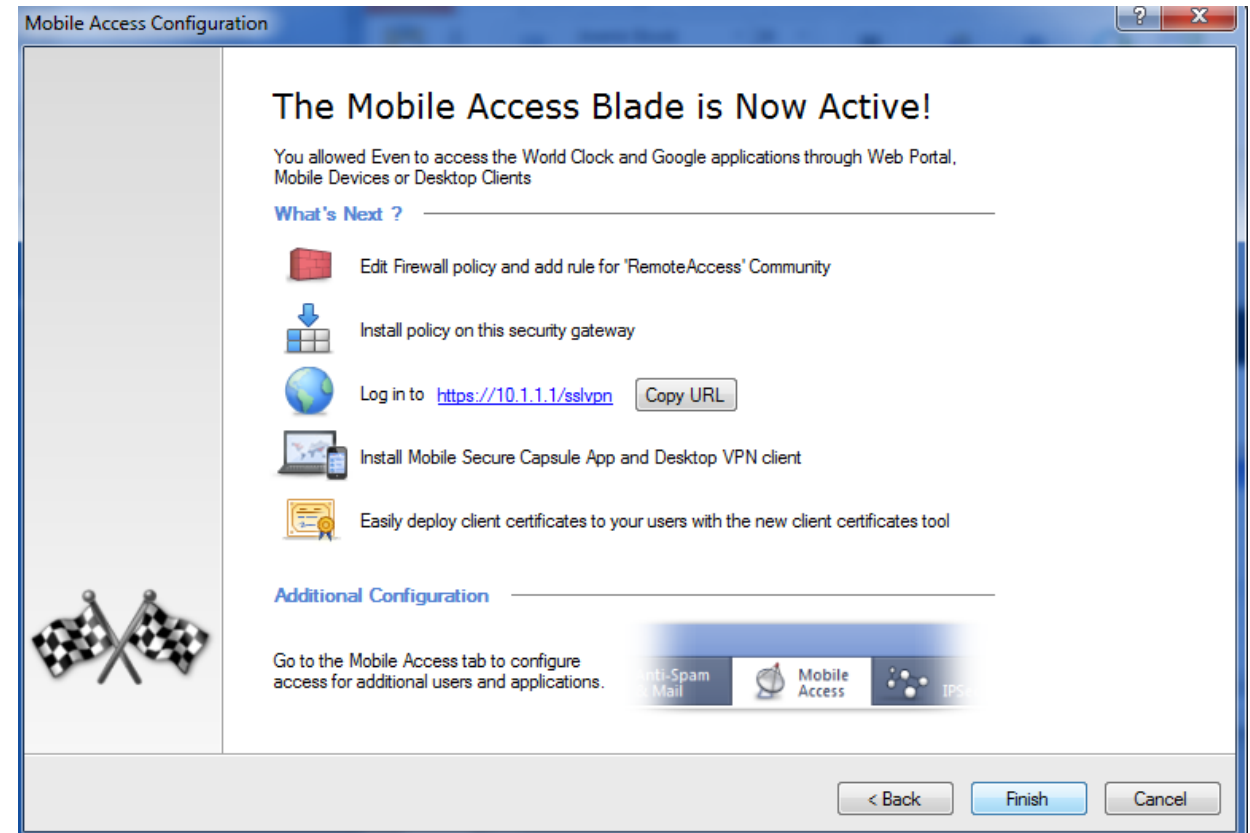
- Application Wizard
- E-Mail Configuration
- Integration with Active Directory
- Users Per Application



The screenshot shows the 'Mobile Access Configuration' window with the 'Applications' tab selected. The window title is 'Mobile Access Configuration'. The tab header is 'Applications' with a subtitle 'Allow access to applications and resources'. Below this, a section titled 'Configure applications that will be available for Web and Mobile remote users' contains two main categories: 'Web Applications' and 'Mail / Calendar / Contacts'. Under 'Web Applications', there are two checked checkboxes: 'Demo web application (world clock)' and 'Custom web application (e.g. your intranet site)'. Below these, there are text input fields for 'Application URL' (containing 'http://google.com') and 'Display name' (containing 'Google'). Under 'Mail / Calendar / Contacts', there is an 'Exchange server' text input field (containing 'mail.alpha.cp') and three unchecked checkboxes: 'Mobile Mail (including push mail notifications)', 'ActiveSync Applications', and 'Outlook Web App'. Each checkbox has a help icon (question mark in a circle) next to it. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

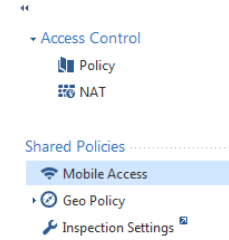
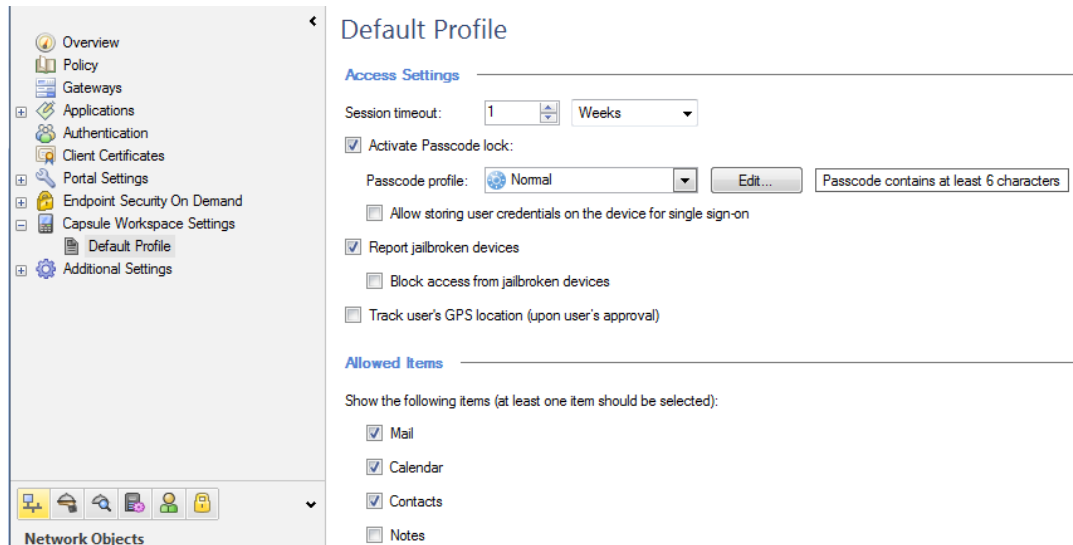
Mobile Access Wizard Completion

- Edit Firewall Policy
- Install Policy
- Login Information for Users
- User Application
- Client Certificate if desired



Capsule Workspace

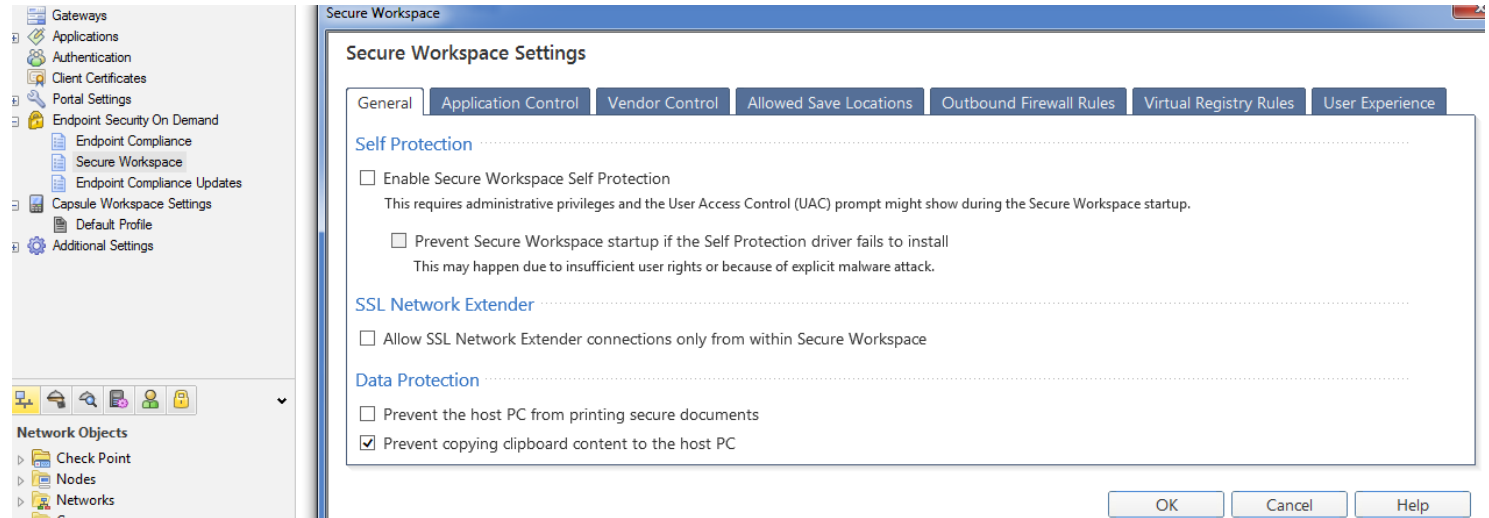
- Open Legacy SmartDashboard
- Create Capsule Workspace Policy



[Open Mobile Access Policy in SmartDashboard...](#)

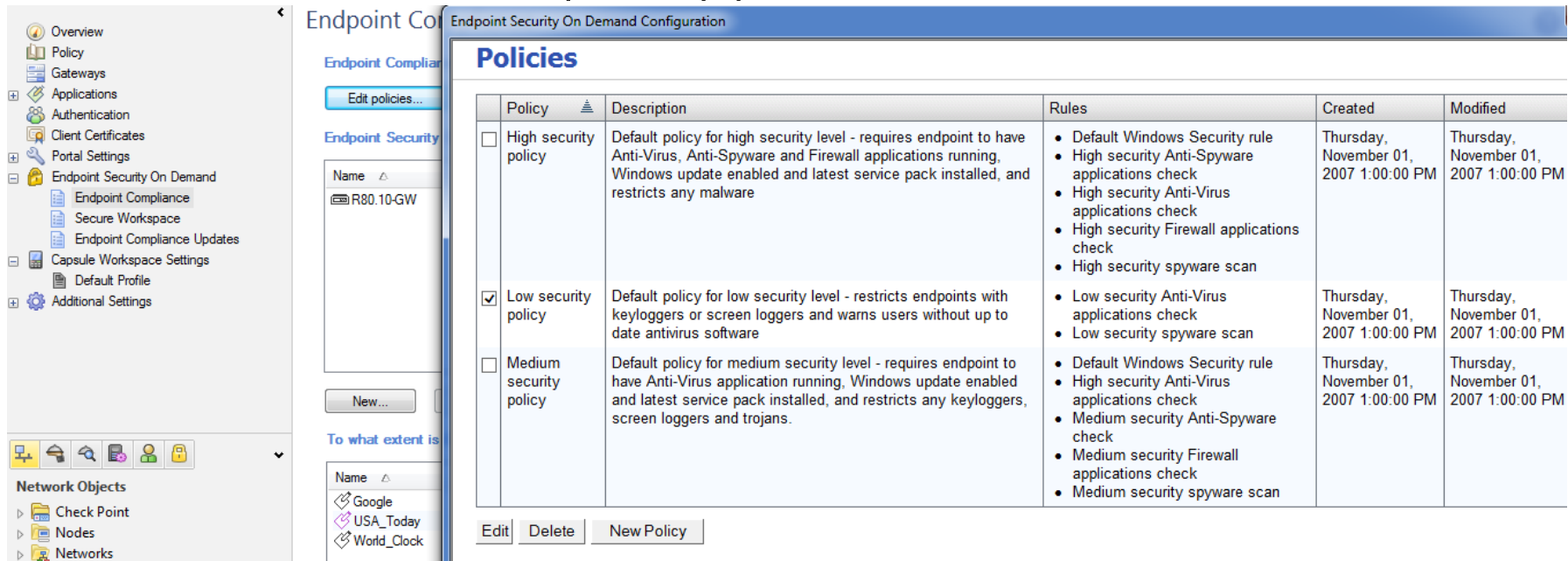
Endpoint Security on Demand

- Secure Workspace
 - Application Control
 - Vendor Control
 - Allowed Saved Locations
 - Outbound Firewall Rules
 - Virtual Registry Rules
 - User Experience



Endpoint Compliance

- Policy
- Policy Enforcement per Application

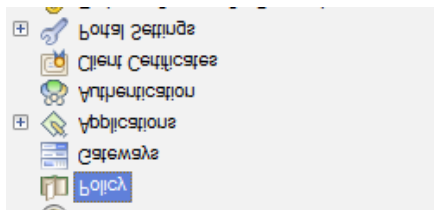






The screenshot displays the 'Endpoint Security On Demand Configuration' window. On the left is a navigation pane with categories like Overview, Policy, Gateways, Applications, Authentication, Client Certificates, Portal Settings, Endpoint Security On Demand (selected), Capsule Workspace Settings, and Additional Settings. Under 'Endpoint Security On Demand', 'Endpoint Compliance' is highlighted. The main area shows the 'Policies' section with a table of three policies: High security, Low security (selected), and Medium security. Each policy has a description, a list of rules, and creation/modification timestamps. At the bottom, there are 'Edit', 'Delete', and 'New Policy' buttons.

Policy	Description	Rules	Created	Modified
<input type="checkbox"/> High security policy	Default policy for high security level - requires endpoint to have Anti-Virus, Anti-Spyware and Firewall applications running, Windows update enabled and latest service pack installed, and restricts any malware	<ul style="list-style-type: none"> Default Windows Security rule High security Anti-Spyware applications check High security Anti-Virus applications check High security Firewall applications check High security spyware scan 	Thursday, November 01, 2007 1:00:00 PM	Thursday, November 01, 2007 1:00:00 PM
<input checked="" type="checkbox"/> Low security policy	Default policy for low security level - restricts endpoints with keyloggers or screen loggers and warns users without up to date antivirus software	<ul style="list-style-type: none"> Low security Anti-Virus applications check Low security spyware scan 	Thursday, November 01, 2007 1:00:00 PM	Thursday, November 01, 2007 1:00:00 PM
<input type="checkbox"/> Medium security policy	Default policy for medium security level - requires endpoint to have Anti-Virus application running, Windows update enabled and latest service pack installed, and restricts any keyloggers, screen loggers and trojans.	<ul style="list-style-type: none"> Default Windows Security rule High security Anti-Virus applications check Medium security Anti-Spyware check Medium security Firewall applications check Medium security spyware scan 	Thursday, November 01, 2007 1:00:00 PM	Thursday, November 01, 2007 1:00:00 PM

Access to Internal Applications

- Policy Based
 - Users and User Groups
 - Applications (Internal or Internet Based)



1	 EVEN	 Work Clock  Google	 R80.10-CW	Rule created automatically by Mobile Access wizard.
No.	User	Applications	Install On	Comment

Access to Internal Applications

- Access is based on Application
 - IP Address
 - Domain Name
 - Multiple Servers
 - Directories on those Servers
 - Specific Services

No.	Users	Applications	Install On	Comment
1	Even	Google World_Clo	Web Application - Google	

General Properties

Authorized Locations

Link in Portal

Additional Settings

Allow access to these locations only:

Servers

☒ Host or DNS name:

☐ Multiple servers

Directories

☒ Allow access to any directory

☐ Allow access to specific directories

☐ Application directories are case sensitive

Services

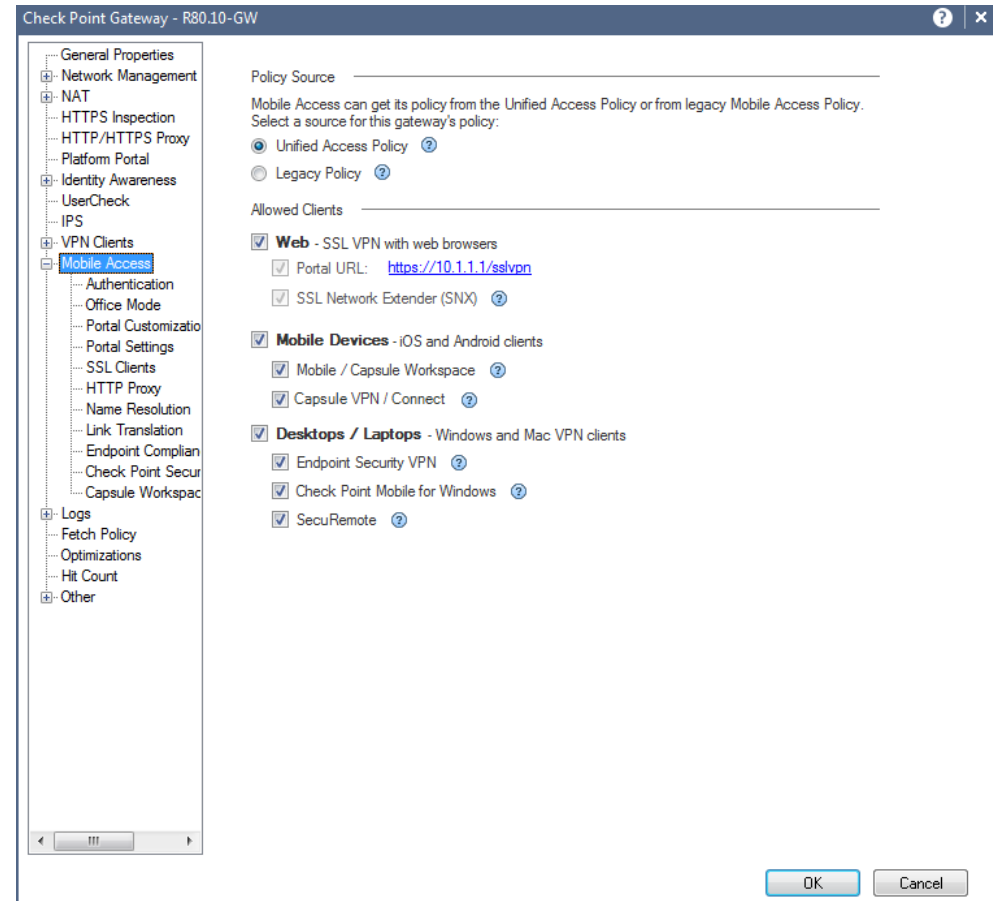
☒ Default:

☒ http

☒ https

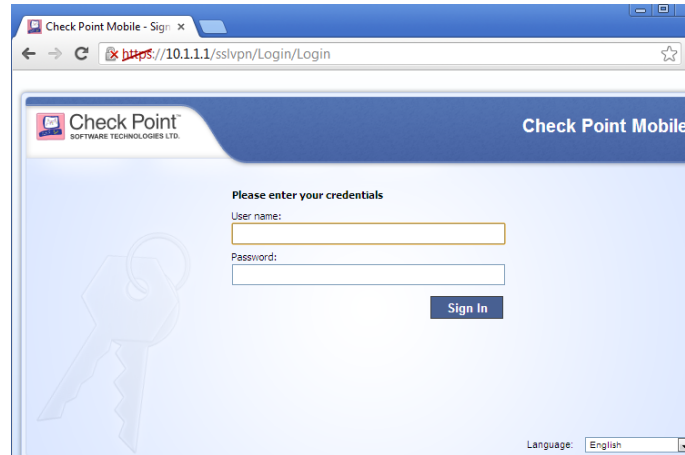
SmartConsole Mobile Access

- Mobile Access
 - Policy Source
 - Allowed Clients
 - Authentication
 - Office Mode
 - Portal Customization
 - Portal Settings
 - SSL Clients
 - HTTP Proxy
 - Name Resolution
 - Link Translation
 - Endpoint Compliance
 - Check Point Secure Workspace
 - Capsule Workspace

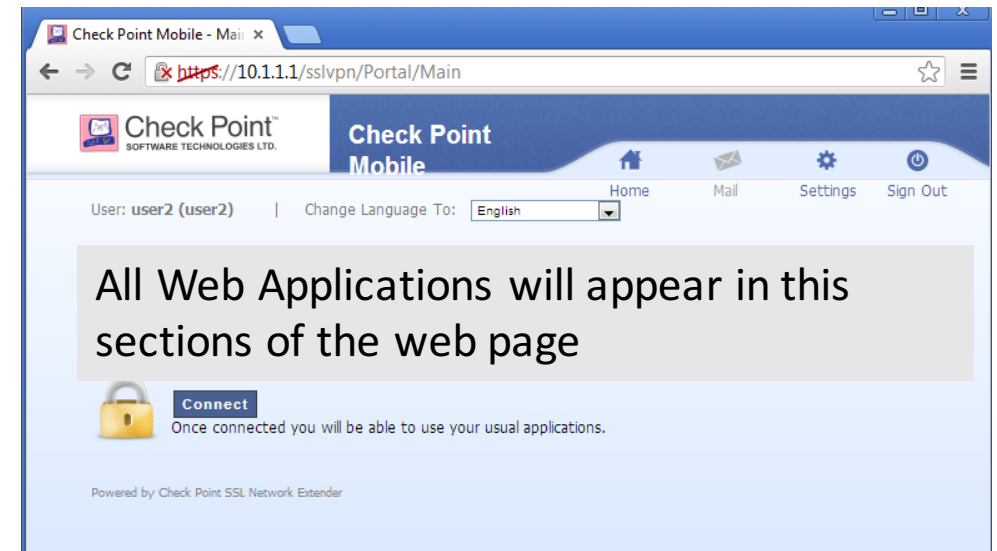


Access to Internal Applications Client Side

- User Login



- User Portal



Summary

- Administered and implemented a Mobile Access solution for SSL VPN
- Applied SecureWorkspace to secure, a remote users desktop or laptop
- Created access to internal web applications using the Mobile Access Blade

Bibliography

Check Point R80.10 Mobile Access Admin Guide California: USA