

CISCO WEB SECURITY

- Setting up Identification Profiles



Handy Putra

October 2017

WHAT IS IDENTIFICATION PROFILE

Identification Profiles let you classify users and user agents (client software) for these purposes:

- Group transaction requests for the application of policies (except SaaS)
- Specification of identification and authentication requirements

AsyncOS assigns an Identification Profile to every transaction:

- Custom Identification Profiles — AsyncOS assigns a custom profile based on that identity's criteria.
- The Global Identification Profile — AsyncOS assigns the global profile to transactions that do not meet the criteria for any custom profile. By default, the global profile does not require authentication.

AsyncOS processes Identification Profiles sequentially, beginning with the first. The global profile is the last profile.

An Identification Profile may include only one criterion. Alternately, Identification Profiles that include multiple criteria require that all the criteria are met ("AND" conditions).



IDENTIFICATION PROFILE BEST PRACTICES

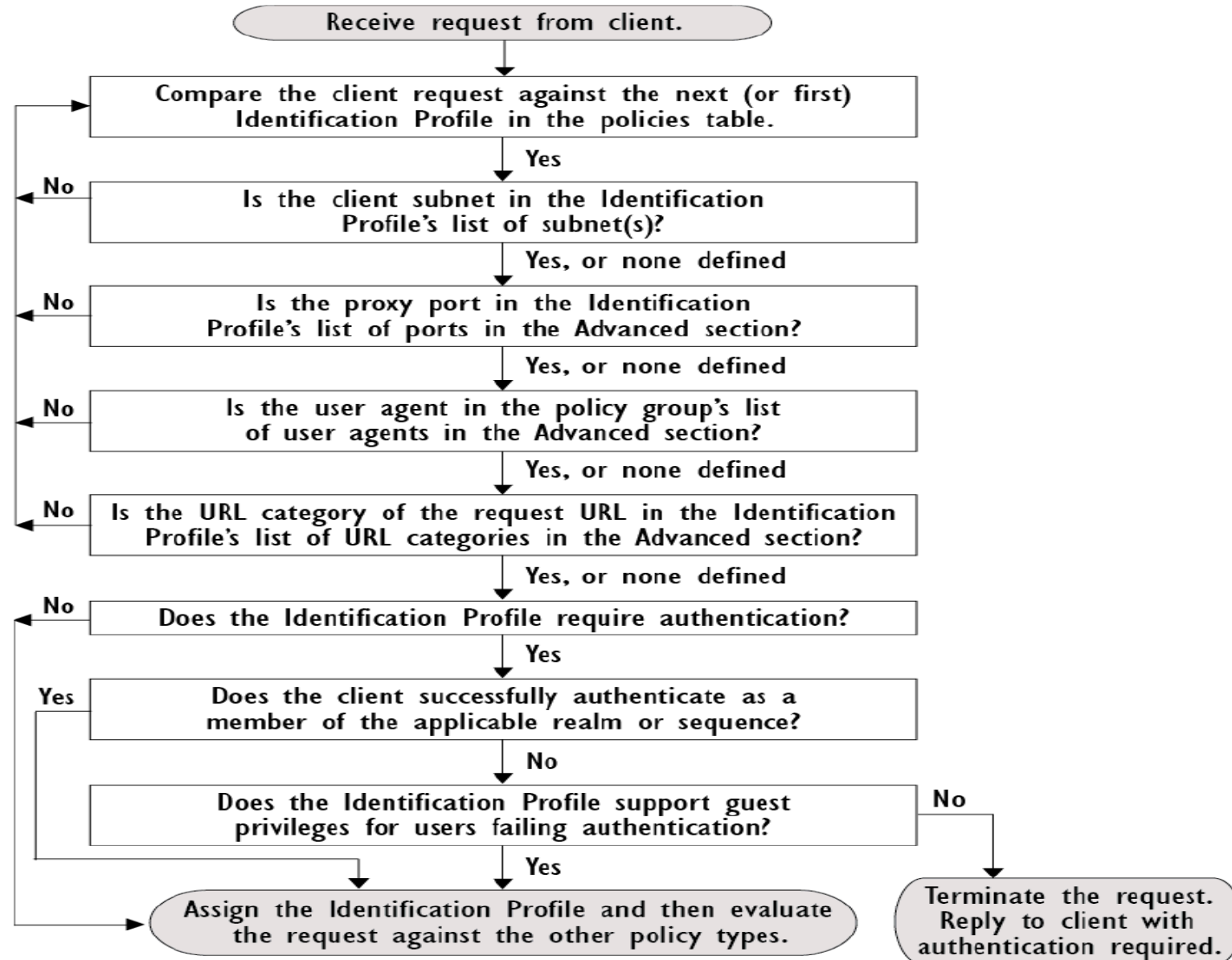
- Create fewer, more general Identification Profiles that apply to all users or fewer, larger groups of users.
- Use policies, rather than profiles, for more granular management.
- Create Identification Profiles with unique criteria.
- Place Identification Profiles with unique criteria on the top of general Identification Profile (read from top to bottom manner)
- Not more than 25-30 Identification Profiles to avoid performance issue.

For Example:

- Position Identification Profiles that do not require authentication above the first Identification Profile that requires authentication.
- Position Identification Profiles that have specific subnets, URL categories, User Agents above the more general Identification Profile



Identification Profile workflow





Setting up Identification Profiles

Identification Profile with define members by
Subnet



Identification Profile with define members by
Protocol



Identification Profile with define members by
Machine ID (Connector Mode Only)



Identification Profile with define members by
User Location



Identification Profile with **Authentication**





Setting up Identification Profiles Cont.

Identification Profile based on **Proxy Ports**



Identification Profile based on **URL Categories**
and **Custom Categories**



Identification Profile based on **User Agents**





Identification Profile with define members by Subnet

- Enter the addresses to which this Identification Profile should apply.
- You can use IP addresses, CIDR blocks, and subnets.
- If nothing is entered, the Identification Profile applies to all IP addresses.





Identification Profile with define members by Subnet cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Identification Profiles'

The screenshot shows the Cisco S100V Web Security Virtual Appliance GUI. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The 'Web Security Manager' tab is selected, and a red arrow points to it. Below this, a dropdown menu is open, showing various policy categories. A red arrow points to the 'Identification Profiles' option under the 'Authentication' section. The main content area displays the 'Identification Profiles' configuration page, which includes a table for 'Client / User Identification' and a table for 'Authentication / Identification Decision'.

Order	Transaction C	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Ident	Exempt from Authentication / User Identification	Not Available	

User Identification Method: Authentication Transparent Identification

Copyright © 2003-2016





Identification Profile with define members by Subnet cont.

- Click on “Add Identification Profile” button.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes a home icon, a search icon, and the text "Cisco S100V Web Security Virtual Appliance". Below this is a menu bar with tabs: Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Identification Profiles" and contains a section for "Client / User Identification Profiles". This section has a table with columns: Order, Transaction Criteria, Authentication / Identification Decision, End-User Acknowledgement, and Delete. A red arrow points to the "Add Identification Profile..." button located above the table. The table contains one row for the "Global Identification Profile" with the transaction criteria "Exempt from Authentication / User Identification" and "Not Available" for the End-User Acknowledgement. Below the table is an "Edit Order..." button. At the bottom right, there is a "User Identification Method" section with radio buttons for "Authentication" and "Transparent Identification". The footer contains the copyright notice: "Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | Privacy Statement".

Cisco S100V Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Edit Order...

User Identification Method: ☒ Authentication ☐ Transparent Identification

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Identification Profile with define members by Subnet cont.

- Give the new Identification Profile a Name
- Give the new Identification Profile a Description
- Set the position of the new Identification Profile – “Insert Above”
- On “Define Members by Subnet”, enter your IP addresses, CIDR blocks, and subnets
- Click on “Submit”
- Then “Commit”





Identification Profile with define members by Subnet cont.

Cisco S100V
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

Name:
(e.g. my IT Profile)

Description:

Insert Above: 1 (Global Profile)

User Identification Method

Identification and Authentication: For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: ☒ HTTP/HTTPS
☐ Native FTP

Define additional group membership criteria.



Identification Profile with define members by Subnet cont.

Cisco S100V Web Security Virtual Appliance

Logged in as: admin on vWSA100.apac.lab

My Favorites Options Support and Help

Reporting Web Security Manager Security Services Network System Administration

Commit Changes »

Identification Profiles

Success — Settings have been saved.

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	subnetMember.id Subnets: 1.1.1.1 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Edit Order...

User Identification Method: Authentication Transparent Identification



Identification Profile with define members by Protocol

- Select the protocols to which this Identification Profile should apply;
- Select all that apply:
 - *HTTP/HTTPS* – Applies to all requests that use HTTP or HTTPS as the underlying protocol, including FTP over HTTP, and any other protocol tunneled using HTTP CONNECT.
 - *Native FTP* – Applies to native FTP requests only.
 - *SOCKS* – Applies to SOCKS Policies only (SOCKS Proxy will need to be enabled on Security Services -> SOCKS Proxy).





Identification Profile with define members by Protocol cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Identification Profiles'

The screenshot shows the Cisco S100V Web Security Virtual Appliance GUI. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The 'Web Security Manager' tab is selected, and a red arrow points to it. Below the tabs, a dropdown menu is open, showing various policy categories. The 'Identification Profiles' option under the 'Authentication' section is highlighted with a red arrow. The main content area displays a table with columns for Order, Transaction C, and Global Ident. The table contains one row with the value 'Not Available' in the 'Global Ident' column. At the bottom, the 'User Identification Method' is set to 'Authentication'.

Order	Transaction C	Global Ident
		Not Available





Identification Profile with define members by Protocol cont.

- Click on “Add Identification Profile” button.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes links for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Identification Profiles" and contains a section for "Client / User Identification Profiles". Within this section, there is a table with the following data:

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Below the table, there is an "Edit Order..." button. A red arrow points to the "Add Identification Profile..." button located above the table. At the bottom of the interface, the "User Identification Method" is set to "Authentication".

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)





Identification Profile with define members by **Protocol** cont.

- Give the new Identification Profile a Name
- Give the new Identification Profile a Description
- Set the position of the new Identification Profile – “Insert Above”
- On “Define Members by Protocol”, select the protocol to which this Identification Profile should apply.
- Click on “Submit”
- Then “Commit”





Identification Profile with define members by Protocol cont.

Cisco S100V
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

Name:
(e.g. my IT Profile)

Description:

Insert Above:

User Identification Method

Identification and Authentication:
For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).

Membership Definition


Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol:

- ☒ HTTP/HTTPS
- ☐ Native FTP
- ☐ SOCKS

Advanced Define additional group membership criteria.

Cancel  Submit





Identification Profile with define members by Protocol cont.

Cisco S100V Web Security Virtual Appliance

Logged in as: admin on vWSA100.apac.lab

My Favorites Options Support and Help

Reporting Web Security Manager Security Services Network System Administration

Commit Changes »

Identification Profiles

Success — Item was successfully deleted.

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	ProtocolMember.id Protocols: Native FTP, HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Edit Order...

User Identification Method: Authentication Transparent Identification



Identification Profile with define members by Machine ID

Requirements:

- The WSA mode has to be in Cloud Web Security Connector Mode.
- The WSA AsyncOS version need to be 10.1.x and above.
- Authentication need to be enabled and has joined the domain.
- Machine ID Service need to be enabled.





Identification Profile with define members by Machine ID cont.

- Enabled Authentication (Network -> Authentication)

The screenshot shows the Cisco S690 Web Security Appliance configuration interface. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. A red arrow points to the Network tab. Below the navigation bar, the Authentication section is expanded, showing a list of services including Interfaces, Transparent Redirection, Routes, DNS, High Availability, Internal SMTP Relay, External DLP Servers, Certificate Management, Identification Services, and Authentication. A red arrow points to the Authentication service. The Authentication service is configured with the following settings:

Realm Name	Server Type	Scheme(s)	Server
ntlm	Active Directory	Kerberos, NTLMSSP, Basic	10.66.66.66

Global Authentication Settings:

Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600





Identification Profile with define members by Machine ID cont.

- Enabled Machine ID Service (Network -> Machine ID Service)

The screenshot shows the Cisco S690 Web Security Appliance configuration interface. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The 'Network' tab is selected, and a red arrow points to it. A dropdown menu is open under 'Network', showing options like Interfaces, Transparent Redirection, Routes, DNS, High Availability, Internal SMTP Relay, External DLP Servers, Certificate Management, Identification Services, Machine ID Service, and Cloud Connector. A red arrow points to 'Machine ID Service'. The 'Machine Identification' section is visible on the left, showing configuration details for the Machine Identification Service, including the Service (NetBios), Realm (ntlm), and Failure Handling (Continue (apply policies wh)). An 'Edit Settings...' button is located to the right of the configuration table.

Machine Identification

Machine Identification	
Machine Identification Service:	NetBios
Realm:	ntlm
Failure Handling:	Continue (apply policies wh

Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement





Identification Profile with define members by Machine ID cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Identification Profiles'

Cisco S690 Web Security Appliance

Reporting Web Security Manager Security Services Network System Administration

Authentication
Identification Profiles
Web Policies
Data Transfer Policies
Custom Policy Elements

Cloud Routing Policies
External Data Loss Prevention
Custom and External URL Categories

Client / User Identification

Add Identification Profile

Order	Transaction Category	Identification Profile	Authentication / Identification Decision	Delete
		Global Identification	Exempt from Authentication / User Identification	

Edit Order...

User Identification Method: Authentication Transparent Identification





Identification Profile with define members by Machine ID cont.

- Click on “Add Identification Profile” button.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes links for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Identification Profiles" and contains a section for "Client / User Identification Profiles". Within this section, there is a table with the following data:

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Below the table, there is an "Edit Order..." button. A red arrow points to the "Add Identification Profile..." button located above the table. At the bottom of the interface, there is a "User Identification Method" section with radio buttons for "Authentication" and "Transparent Identification". The footer contains the copyright notice: "Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | Privacy Statement".





Identification Profile with define members by **Machine ID** cont.

- Give the new Identification Profile a Name
- Give the new Identification Profile a Description
- Set the position of the new Identification Profile – “Insert Above”
- On “Define Members by Machine ID”, click the drop down box
 - **Do Not Use Machine ID in This Policy** – The user is not identified by machine ID.
 - **Define User Authentication Policy Based on Machine ID** – The user is identified primarily by machine ID.
- Click the **Machine Groups** area to display the Authorized Machine Groups page.
 - For each group you want to add, in the Directory Search field, start typing the name of the group to add and then click Add.
 - You can select a group and click Remove to remove it from the list.
 - Click Done to return to the previous page.
- Click the **Machine IDs** area to display the Authorized Machines page.
 - In the Authorized Machines, field, enter the machine IDs to associate with the policy then click Done.





Identification Profile with define members by Machine ID cont.

Cisco S690 Web Security Appliance

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

Name:
(e.g. my IT Profile)

Description:

Insert Above:

User Identification Method

Identification and Authentication:
This option may not be valid if any preceding Identity Profile requires authentication on all subnets.

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Machine ID:

Machine Groups: No machine groups entered

Machine IDs: No machine IDs entered



Identification Profile with define members by Machine ID cont.

Cisco S690
Web Security Appliance

Logged in as: admin on 28.1ab
My Favorites - Options - Support and Help -

Reporting Web Security Manager Security Services Network System Administration

Commit Changes »

Identification Profiles

Success — Settings have been saved.

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	Delete
1	MachineID.id Machine ID: Required	Exempt from Authentication / User Identification	
	Global Identification Profile	Exempt from Authentication / User Identification	

Edit Order...

User Identification Method: Authentication Transparent Identification





Identification Profile with define members by User Location

- Configure this Identification Profile to apply to:
Local Users Only, Remote Users Only , or Both.
- This selection affects the available authentication settings for this Identification Profile.

Requirements:

- Require feature key of “Cisco AnyConnect Secure Mobility” to be valid
- AnyConnect Secure Mobility service need to be enabled





Identification Profile with define members by User Location cont.

- Verifying your feature key for Cisco AnyConnect Secure Mobility is valid (System Administration -> Feature Keys)

Description	Status	Time Remaining	Expiration Date
Cisco L4 Traffic Monitor	Dormant	Expired	Wed Sep 13 23:59:59 2017
Cisco HTTPS Proxy	Dormant	89 days	Fri Jan 5 01:41:47 2018
File Reputation	Dormant	89 days	Fri Jan 5 01:42:05 2018
Sophos	Dormant	89 days	Fri Jan 5 01:40:50 2018
File Analysis	Dormant	89 days	Fri Jan 5 01:42:15 2018
McAfee	Dormant	89 days	Fri Jan 5 01:41:04 2018
Webroot	Dormant	89 days	Fri Jan 5 01:41:33 2018
Cisco Web Proxy & DVS Engine	Dormant	156 days	Tue Mar 13 01:33:27 2018
Cisco AnyConnect Secure Mobility	Active	89 days	Fri Jan 5 04:46:17 2018
Cisco Web Reputation Filters	Dormant	89 days	Fri Jan 5 01:45:09 2018
Pending Activation			
<i>No feature key activations are pending.</i>			
Check for New Keys			
Feature Activation			
Feature Key: <input type="text"/>			
Submit Key			





Identification Profile with define members by User Location cont.

- Enabled AnyConnect Secure Mobility Settings (Security Services -> AnyConnect Secure Mobility). Either specifying IP range or Integrate with Cisco ASA.

AnyConnect Secure Mobility Settings

When AnyConnect Secure Mobility is enabled, a policy can be created based on whether the user is physically in the corporate network or logged in through a VPN.

☒ **Enable AnyConnect Secure Mobility**

Define Remote Users by:

☐ IP Range

1.1.1.1

(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

☒ Cisco ASA Integration

ASA Hostname or IP Address	Port	Add Row
test.ASA	443	

The values below will be applicable to all ASAs configured above.

ASA Access Passphrase: ?

[Start Test](#)





Identification Profile with define members by User Location cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Identification Profiles'

The screenshot shows the Cisco S100V Web Security Virtual Appliance GUI. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The 'Web Security Manager' tab is selected, and a red arrow points to it. Below the navigation bar, a dropdown menu is open, showing various policy categories. The 'Identification Profiles' option is highlighted with a red arrow. The main content area displays a table with columns for Order, Transaction C, and a table row for 'Global Ident'. The table row shows 'Authentication / Identification Decision' and 'End-User Acknowledgement' with a 'Delete' button. The bottom of the screen shows the 'User Identification Method' set to 'Authentication' and 'Transparent Identification'.

Order	Transaction C	End-User Acknowledgement	Delete
	Global Ident	Authentication / Identification Decision	Not Available





Identification Profile with define members by **User Location** cont.

- Click on “Add Identification Profile” button.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes links for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Identification Profiles" and contains a section for "Client / User Identification Profiles". Within this section, there is a table with the following data:

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Below the table, there is an "Edit Order..." button. A red arrow points to the "Add Identification Profile..." button located above the table. At the bottom of the interface, the "User Identification Method" is set to "Authentication".

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)





Identification Profile with define members by **User Location** cont.

- Give the new Identification Profile a Name
- Give the new Identification Profile a Description
- Set the position of the new Identification Profile – “Insert Above”
- On “Define Members by User Location” select the location of the users

Local Users Only - these users are connected to the network either physically or wirelessly.

Remote Users Only - These users are connected to the network from a remote location using VPN (virtual private network). Users might be located in a home office, coffee shop, or hotel, for example. The Web Security appliance automatically identifies remote users when both the Cisco ASA and Cisco AnyConnect Client are used for VPN access. Otherwise, the Web Security appliance administrator must specify remote users by configuring a range of IP addresses.

- Click on “Submit”
- Then “Commit”





Identification Profile with define members by User Location cont.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

Name: (e.g. my IT Profile)

Description:

Insert Above:

User Identification Method

Identification and Authentication: For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by User Location: ☐ Local Users Only ☒ Remote Users Only ☐ Both

Define Members by Subnet: (examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: ☒ HTTP/HTTPS ☐ Native FTP ☐ SOCKS



Identification Profile with define members by User Location cont.

Cisco S100V
Web Security Virtual Appliance

Logged in as: **admin** on **vWSA100.apac.lab**
My Favorites ▾ Options ▾ Support and Help ▾

Reporting Web Security Manager Security Services Network System Administration

Commit Changes »

Identification Profiles

Success — Settings have been saved.

Client / User Identification Profiles

[Add Identification Profile...](#)

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	UserLocation.id User Location: Remote Users Only Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

[Edit Order...](#)

User Identification Method: Authentication Transparent Identification



Identification Profile with Authentication

Requirement:

- Authentication service will need to be enabled (Network -> Authentication)

The screenshot shows the Cisco S690 Web Security Appliance configuration interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Network' menu is expanded, showing options like 'Interfaces', 'Transparent Redirection', 'Routes', 'DNS', 'High Availability', 'Internal SMTP Relay', 'External DLP Servers', 'Certificate Management', 'Identification Services', 'Machine ID Service', and 'Cloud Connector'. The 'Authentication' option under 'Identification Services' is highlighted with a red arrow. The main content area is titled 'Authentication' and contains two sections: 'Authentication Realms' and 'Global Authentication Settings'. In the 'Authentication Realms' section, the 'Add Realm...' button is highlighted with a red arrow. Below it is a table with columns 'Realm Name', 'Server Type', 'Scheme(s)', and 'Server'. The first row shows 'ntlm', 'Active Directory', 'Kerberos, NTLMSSP, Basic', and '10.66.1.10'. In the 'Global Authentication Settings' section, there are four rows of settings: 'Action if Authentication Service Unavailable' (Block all traffic if authentication fails), 'Failed Authentication Handling' (Log Guest User by: IP Address), 'Re-authentication' (Disabled), and 'Basic Authentication Token TTL' (3600).

Cisco S690 Web Security Appliance

Reporting Web Security Manager Security Services **Network** System Administration

Authentication

Authentication Realms

Add Realm...

Realm Name	Server Type	Scheme(s)	Server
ntlm	Active Directory	Kerberos, NTLMSSP, Basic	10.66.1.10

Global Authentication Settings

Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600

Base DN or NetBIOS Domain: Domain not joined

Delete



Identification Profile with define members by Authentication cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Identification Profiles'

Cisco S100V Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

Identification

Client / User Identification

Add Identification Profile

Order	Transaction C	Global Ident	End-User Acknowledgement	Delete
			Not Available	

User Identification Method: Authentication Transparent Identification

Copyright © 2003-2016





Identification Profile with define members by Authentication cont.

- Click on “Add Identification Profile” button.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes links for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Identification Profiles" and contains a section for "Client / User Identification Profiles". Within this section, there is a table with the following data:

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Below the table, there is an "Edit Order..." button. A red arrow points to the "Add Identification Profile..." button located above the table. At the bottom of the interface, the "User Identification Method" is set to "Authentication".

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)





Identification Profile with Authentication cont.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

Name: ?

(e.g. my IT Profile)

Description:

Insert Above:

1 (Global Profile) ⌵

User Identification Method

Identification and Authentication: ?

Authenticate Users ⌵

Authentication Realm:

Select a Realm or Sequence: ?

ntlm ⌵

Select a Scheme:

Use Kerberos ⌵

Scheme setting applies to HTTP/HTTPS only.

If a user fails authentication:

☐ Support Guest privileges ?

Authorization of specific users and groups is defined in subsequent policy layers
(see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Authentication Surrogates: ?

☒ IP Address

☐ Persistent Cookie

☐ Session Cookie

☒ Apply same surrogate settings to explicit forward requests

If this option is not selected, no surrogates will be used with HTTP/HTTPS
explicit forward requests, and NTLM credential caching will not be available to
these requests. In addition, re-authentication will not be available for Kerberos.



Identification Profile with Authentication cont.

Choose an identification method from the User Identification Method drop-down list.

- Exempt from authentication/identification

Users are identified primarily by IP address. No additional parameters are required.

- Authenticate users

Users are identified by the authentication credentials they enter.

- Transparently identify users with ISE

Available when the ISE service is enabled (Network > Identity Services Engine). For these transactions, the user name and associated Secure Group Tags will be obtained from the Identity Services Engine

- Transparently identify users with ASA

Users are identified by the current IP address-to-user name mapping received from a Cisco Adaptive Security Appliance (for remote users only). This option appears when Secure Mobility is enabled and integrated with an ASA. The user name will be obtained from the ASA, and associated directory groups will be obtained from the selected authentication realm or sequence.

- Transparently identify users with authentication realm

This option is available when one or more authentication realms are configured to support transparent identification.





Identification Profile with **Authentication** cont.

Authentication Realm:

- **Select a Realm or Sequence** – choose a defined authentication realm or sequence
- **Select a Scheme** – Choose an authentication scheme:
 - **Kerberos** – The client is transparently authenticated by means of Kerberos tickets.
 - **Basic** – The client always prompts users for credentials. After the user enters credentials, browsers typically offer a check box to remember the provided credentials. Each time the user opens the browser, the client either prompts for credentials or resends the previously saved credentials. Credentials are sent unsecured as clear text (Base64). A packet capture between the client and Web Security appliance can reveal the user name and passphrase.
 - **NTLMSSP** – The client transparently authenticates using its Windows login credentials. The user is not prompted for credentials. However, the client prompts the user for credentials under the following circumstances:
 - The Windows credentials failed.
 - The client does not trust the Web Security appliance because of browser security settings. Credentials are sent securely using a three-way handshake (digest style authentication). The passphrase is never sent across the connection.





Identification Profile with **Authentication** cont.

Authentication Surrogates:


Specify how transactions will be associated with a user after successful authentication (options vary depending on Web Proxy deployment mode):

- **IP Address** – The Web Proxy tracks an authenticated user at a particular IP address. For transparent user identification, select this option.
- **Persistent Cookie** – The Web Proxy tracks an authenticated user on a particular application by generating a persistent cookie for each user per application. Closing the application does not remove the cookie.
- **Session Cookie** – The Web Proxy tracks an authenticated user on a particular application by generating a session cookie for each user per domain per application. (However, when a user provides different credentials for the same domain from the same application, the cookie is overwritten.) Closing the application removes the cookie.
- **No Surrogate** – The Web Proxy does not use a surrogate to cache the credentials, and it tracks an authenticated user for every new TCP connection. When you choose this option, the web interface disables other settings that no longer apply. This option is available only in explicit forward mode and when you disable credential encryption on the Network > Authentication page.
- **Apply same surrogate** settings to explicit forward requests – Check to apply the surrogate used for transparent requests to explicit requests; enables credential encryption automatically. This option appears only when the Web Proxy is deployed in transparent mode.






Identification Profile with Authentication cont.

 Cisco S100V
Web Security Virtual Appliance

Logged in as: **admin** on **vWSA100.apac.lab**
[My Favorites](#) - [Options](#) - [Support and Help](#)

[Home](#) | [Reporting](#) | [Web Security Manager](#) | [Security Services](#) | [Network](#) | [System Administration](#)



[Commit Changes »](#)



Identification Profiles

Warning — The policy group "Authentication.id" was added.



Groups that do not require authentication should typically be ordered above authentication-based groups in the policy table for effective evaluation. Changing this order may require users to authenticate, regardless of policy group settings.

Client / User Identification Profiles

[Add Identification Profile...](#)

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Authentication.id Protocols: HTTP/HTTPS	 Authenticate: Realm: ntlm (Scheme: Kerberos)	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

[Edit Order...](#)

User Identification Method:  Authentication  Transparent Identification



Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents)

Proxy Ports – Specify one or more proxy ports used to access the Web Proxy. Enter port numbers separated by commas.

For explicit forward connections, the proxy port is configured in the browser.

For transparent connections, this is the same as the destination port.

Defining identities by port works best when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. Defining identities by port when

client requests are transparently redirected to the appliance may result in some requests being denied.






Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

- Click on “Advanced” link in the new Identification Profile
- Click on the Proxy Port – “None Selected” link
- Enter the ports separated by commas

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by User Location:	<input type="radio"/> Local Users Only ? <input type="radio"/> Remote Users Only ? <input checked="" type="radio"/> Both
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP <input type="checkbox"/> SOCKS
 Advanced	<p>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Proxy Ports: None Selected</p> <p>URL Categories: No URL Categories Available (see Security Services > Acceptable Use Controls or Web Security Manager > Custom Categories)</p> <p>User Agents: None Selected</p> <p><small>The advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories, are not applicable for transparent HTTPS (unless decrypted). When advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.</small></p>



Identification Profile based on **Advanced Settings** **(Proxy Ports, URL Categories, User Agents)** cont.

URL Categories – Select user-defined or predefined URL categories.

Membership for both is excluded by default, meaning the Web Proxy ignores all categories unless they are selected in the Add column.

If you need to define membership by URL category, only define it in the Identity group when you need to exempt from authentication requests to that category.






Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

- Click on “Advanced” link in the new Identification Profile
- Click on the **URL Categories** – “None Selected” link

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by User Location:	<input type="radio"/> Local Users Only ? <input type="radio"/> Remote Users Only ? <input checked="" type="radio"/> Both						
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>						
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP <input type="checkbox"/> SOCKS						
 Advanced	<p>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <table><tr><td>Proxy Ports:</td><td>None Selected</td></tr><tr><td>URL Categories:</td><td>No URL Categories Available (see Security Services > Acceptable Use Controls or Web Security Manager > Custom Categories)</td></tr><tr><td>User Agents:</td><td>None Selected</td></tr></table> <p><small>The advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories, are not applicable for transparent HTTPS (unless decrypted). When advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.</small></p>	Proxy Ports:	None Selected	URL Categories:	No URL Categories Available (see Security Services > Acceptable Use Controls or Web Security Manager > Custom Categories)	User Agents:	None Selected
Proxy Ports:	None Selected						
URL Categories:	No URL Categories Available (see Security Services > Acceptable Use Controls or Web Security Manager > Custom Categories)						
User Agents:	None Selected						

[Cancel](#) [Submit](#)





Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

- Tick the URL Categories that you want to include in the new Identification Profile then click “Done” (Scroll to the bottom)

Identity Profiles: Policy "New Policy": Membership by URL Categories

Advanced Membership Definition: URL Category

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

Custom URL Categories

No Custom Categories are defined. See Web Security Manager > Custom URL Categories.

Predefined URL Categories

Category	Add Select all
Adult	
Advertisements	
Alcohol	
Arts	<input checked="" type="checkbox"/>
Astrology	
Auctions	
Business and Industry	
Chat and Instant Messaging	
Cheating and Plagiarism	
Child Abuse Content	
Computer Security	
Computers and Internet	
DIY Projects	
Dating	
Digital Postcards	
Dining and Drinking	
Dynamic and Residential	
Education	



Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

User Agents – Defines policy group membership by the user agents found in the client request. You can select some commonly defined agents, or define your own using regular expressions.

Also specify whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents






Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

- Click on “Advanced” link in the new Identification Profile
- Click on the **User Agents** – “None Selected” link

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by User Location:	<input type="radio"/> Local Users Only ? <input type="radio"/> Remote Users Only ? <input checked="" type="radio"/> Both
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP <input type="checkbox"/> SOCKS
 Advanced	<p>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Proxy Ports: None Selected</p> <p>URL Categories: No URL Categories Available (see Security Services > Acceptable Use Controls or Web Security Manager > Custom Categories)</p> <p>User Agents: None Selected</p> <p><small>The advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories, are not applicable for transparent HTTPS (unless decrypted). When advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.</small></p>

[Cancel](#) [Submit](#)





Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

- Enter the **Custom User Agents**. For example: iPhone, iPad, Android, etc
- Enter **Common User Agents** for IE browsers or Firefox or Windows Update or Adobe Updater.
- Select to match the selected user agent or match all “except”
- Then click “**Done**”





Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

Identity Profiles: Policy "New Policy": Membership by User Agent

Advanced Membership Definition: User Agents

Common User Agents: **Browsers**

Internet Explorer

- ☐ Version 10.X MSIE 10
- ☐ Version 9.X MSIE 9
- ☐ Version 8.X MSIE 8
- ☐ Version 7.X MSIE 7
- ☐ Version 6.X MSIE 6
- ☐ Version 5.X or earlier MSIE [54321]
- ☐ Internet Explorer Any Versions MSIE

Firefox

- ☐ Version 3.X Firefox/3
- ☐ Version 2.X Firefox/2
- ☐ Version 1.X or earlier Firefox/1
- ☐ Firefox Any Versions Firefox

Others

- ☐ Microsoft Windows Update ^Windows-Update-Agent\$
- ☐ Adobe Acrobat Updater Adobe Update Manager\Acrobat SOAP

Custom User Agents:

Enter any regular expression, one regular expression per line, to specify user agents. Use a pound sign (#) to start a comment; comments are any text added after a pound sign up to a newline and can be on the same line as the regular expression.

Example User Agent Patterns

Match User Agents:

- ☒ Match the selected user agent definitions
- ☐ Match all **except** the selected user agent definitions

Cancel **Done**





Identification Profile based on Advanced Settings (Proxy Ports, URL Categories, User Agents) cont.

Example User Agent Patterns

Example Patterns	
Regular Expressions	Matches
Mozilla/* Gecko/* Firefox/	All Firefox versions
Mozilla/* Gecko/* Firefox/1\\.5	Firefox versions 1.5.x
Mozilla/*compatible; MSIE	All Internet Explorer versions
Mozilla/*compatible; MSIE 5\\.5	Internet Explorer version 5.5
Mozilla/4.0 \\(compatible; MSIE 5.5;\\)	Specific user agent: Mozilla/4.0 (compatible; MSIE 5.5;)

