

Create Decryption Policies to Control HTTPS Traffic with the Cisco Web Security Appliance (WSA)

About this document

This document is for Cisco engineers and customers who will deploy HTTPS decryption using the Cisco® Web Security Appliance (WSA) using AsyncOS.

- Introduction to HTTPS decryption
- Certificate overview
- Enabling HTTPS detection on the Web Security Appliance
- HTTPS detection on the Web Security Appliance in action
- Web Security Appliance certificate use for HTTPS decryption

Introduction to HTTPS decryption

The HTTPS proxy engine must be enabled to inspect HTTPS traffic. When enabling the HTTPS proxy, a CA certificate must be generated or uploaded for use by the HTTPS proxy. You may either upload a generated private key and certificate, or generate one using the appliance GUI. This guide will walk through the process of generating a certificate for use by the HTTPS proxy.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Before you begin

When the HTTPS proxy is enabled, HTTPS-specific rules in access policies are disabled. The web proxy will then process decrypted HTTPS traffic using rules for HTTP.

Note: The Cisco Cloud Connector does not support decryption. It passes HTTPS traffic to Cisco Cloud Web Security without decrypting. HTTPS decryption is enabled on the Web Security Appliance only in standalone mode.

HTTPS proxy settings are responsible for the following:

- What private key and certificate to use for decrypted connections
- Whether to decrypt to force proxy authentication
- Whether to decrypt to display end user notifications
- Whether to decrypt for application detection
- How to handle requests that use invalid or revoked security certificates

Decryption policies can handle HTTPS traffic in the following ways. They can:

- Pass through encrypted traffic
- Decrypt traffic and apply content-based access policies defined for HTTP traffic (this process also makes malware scanning possible)
- Drop the HTTPS connection
- Monitor the request (taking no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decryption

Certificate types

Introduction

This section describes the type of certificate that should be used for HTTPS decryption on a Cisco Web Security Appliance.

Certificate overview

The WSA has the ability to use a current certificate and private key with HTTPS decryption. However, not all X.509 certificates work.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

There are two major types of certificates: **server certificates** and **root certificates**. All X.509 certificates contain a Basic Constraints field, which identifies the type of certificate:

- **Subject Type=End Entity** (server certificate)
- **Subject Type=CA** (root certificate)

Note: You must use a root certificate, also referred to as a CA signing certificate, for HTTPS decryption on the WSA.

Root certificates

A root certificate is specifically created for signing server certificates. You can create and operate your own CA and sign your own server certificates.

Note: Since a root certificate signs other certificates only, it cannot be used on a web server to perform HTTPS encryption and decryption.

The WSA must use a root certificate to actively generate server certificates for HTTPS decryption.

Two options are available for root certificate use:

- You can generate a self-signed **root certificate on the WSA**. The WSA creates its own root certificate and private key, and it uses this key pair to sign server certificates.
- You can upload a **current root certificate and its private key into the WSA**. The Common Name (CN) field in a root certificate identifies the entity (typically a corporation name) that trusts any server certificates that contain its signature.

Note: Before a server certificate can be trusted, it must be signed by a root certificate that has a public key present in the web browser.

Server certificates

A server certificate is specifically created to be used in HTTPS encryption and decryption and to verify the authenticity of a specific server. Server certificates are signed by a CA with use of the CA root certificate. Verisign and Global Sign are well-known CAs.

Note: A server certificate cannot be used to sign other certificates. Therefore, HTTPS decryption does not work if a server certificate is installed on the WSA.

The CN field in a server certificate specifies the host for which the certificate is intended to be used. For example, <https://www.verisign.com> uses a server certificate with a CN of www.verisign.com.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Enabling HTTPS decryption on the WSA

Step 1. From **Security Services>HTTPS Proxy**. For the first use you will need to enable HTTPS proxy on the WSA. Click **Enable and Edit Settings**.



Step 2. Now select the check box **Enable HTTPS Proxy**. This will open a few options for you, which we will walk through.

Step 3. For this example, we will use a generated certificate. Select the radio button **Use Generated Certificate and Key**.

Note: The WSA must have a root or intermediate certificate for the HTTPS proxy to work. There are a few options for getting a certificate on the box.

- For this guide, you will generate the certificate and key on the WSA:
 - Click the **Generate New Certificate and Key** button.
 - Fill out the fields for the new certificate and key.
 - Click **Generate** when done.
- Generate a certificate and key and download a certificate signing request to be signed by a Certificate Authority (CA):
 - Follow the steps for generating the certificate and key on the WSA above.
 - Click the link **Download Certificate Signing Request** and save the file in PEM format.
 - Submit changes.
 - Take the file to your CA and have it signed using a subordinate CA template.
 - Ensure that your root signing CA certificate is present in the WSA trusted root authorities before uploading the signed HTTPS certificate.
 - Click **Browse** under the section "Signed Certificate" to upload the signed certificate.

Note: The CA cannot be a third-party trusted CA, such as Verisign or Global Sign, because they will not sign an intermediate or root certificate.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

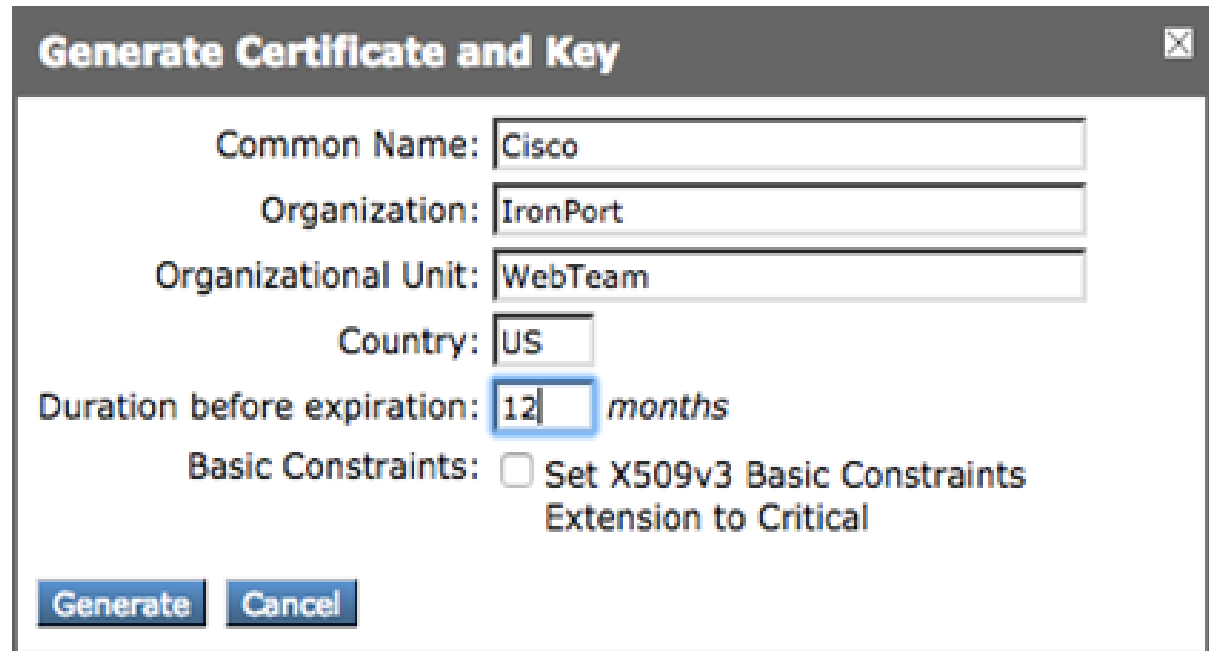
Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

- Upload an existing certificate and key:
 - Ensure that your root signing CA certificate is present in the WSA trusted root authorities before uploading the signed HTTPS certificate.
 - Select the box next to **Use Uploaded Certificate and Key**.
 - Select **Browse** to search for the certificate and key (as stated, a private key must be unencrypted).
 - Click **Upload Files** to upload the certificate and key.

Step 4. Continue from Step 3. Click **Generate New Certificate and Key**. You will need to populate the fields as shown in the example below. Click the **Generate** button.



Generate Certificate and Key

Common Name: Cisco

Organization: IronPort

Organizational Unit: WebTeam

Country: US

Duration before expiration: 12 months

Basic Constraints: Set X509v3 Basic Constraints Extension to Critical

Generate **Cancel**

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 5. Click **Submit** and **Commit** all changes to save them.



Use Generated Certificate and Key Generate New Certificate and Key

Common name: Cisco
Organization: IronPort
Organizational Unit: WebTeam
Country: US
Expiration Date: Dec 24 18:17:25 2017 GMT
Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Step 6. Select **Download Certificate**.

You can now download the PEM file and distribute it to web clients. Remember, it needs to be imported into the trusted root certificate store in your operating system and/or browser.

HTTPS decryption on the WSA in action

After the Web Security Appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection.

Step 1. Select **Web Security Manager>Decryption Policies**.

Step 2. You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Filtering column for the policy group you want to configure.

Note: If you want to block (with end-user notification) a particular URL category for HTTPS requests instead of dropping it (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group. Then choose to block the same URL category in the Access Policy group. The URLs will be chosen in Step 3.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 3. Select the URL categories you would like to decrypt. In the following example, Social Networking is among those selected.

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Nature		<input checked="" type="checkbox"/>			--	--
News	<input checked="" type="checkbox"/>				--	--
Non-governmental Organizations	<input checked="" type="checkbox"/>				--	--
Non-sexual Nudity			<input checked="" type="checkbox"/>		--	--
Online Communities		<input checked="" type="checkbox"/>			--	--
Online Storage and Backup	<input checked="" type="checkbox"/>				--	--
Online Trading	<input checked="" type="checkbox"/>				--	--
Organizational Email			<input checked="" type="checkbox"/>		--	--
Parked Domains			<input checked="" type="checkbox"/>		--	--
Peer File Transfer			<input checked="" type="checkbox"/>		--	--
Personal Sites	<input checked="" type="checkbox"/>				--	--
Photo Search and Images	<input checked="" type="checkbox"/>				--	--
Politics		<input checked="" type="checkbox"/>			--	--
Pornography			<input checked="" type="checkbox"/>		--	--
Professional Networking	<input checked="" type="checkbox"/>				--	--
Real Estate		<input checked="" type="checkbox"/>			--	--
Reference	<input checked="" type="checkbox"/>				--	--
Religion			<input checked="" type="checkbox"/>		--	--
SaaS and B2B	<input checked="" type="checkbox"/>				--	--
Safe for Kids		<input checked="" type="checkbox"/>			--	--
Science and Technology		<input checked="" type="checkbox"/>			--	--
Search Engines and Portals	<input checked="" type="checkbox"/>				--	--
Sex Education		<input checked="" type="checkbox"/>			--	--
Shopping	<input checked="" type="checkbox"/>				--	--
Social Networking			<input checked="" type="checkbox"/>		--	--
Social Science		<input checked="" type="checkbox"/>			--	--
Society and Culture	<input checked="" type="checkbox"/>				--	--

Cancel Submit

Note: You can create decryption policies to handle HTTPS traffic in the following ways: pass through, decrypt, drop, or monitor.

Step 4. When the URL categories are selected, click **Submit** and then **Commit** all changes to save them.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 5. Select **Web Security Manager > Access Policies**, and select the policy you would like to modify. In the following example, Global Policy has been selected.

Access Policies

Policies							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Office365 Identification Profile: O365 All identified users	(global policy)	Monitor: 1	(global policy)	(global policy)	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	
	Global Policy Identification Profile: All	No blocked items	Block: 4 Monitor: 75	Monitor: 365	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Disabled Anti-Malware Scanning: Enabled	

Step 6. Click the text within the URL Filtering cell.

Step 7. Select **Social Networking** as a category to block.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Block	Monitor	Warn	Quota-Based	Time-Based
	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Real Estate		✓		--	--
Reference		✓		--	--
Religion		✓		--	--
SaaS and B2B		✓		--	--
Safe for Kids		✓		--	--
Science and Technology		✓		--	--
Search Engines and Portals		✓		--	--
Sex Education		✓		--	--
Shopping		✓		--	--
Social Networking	✓			--	--
Social Science		✓		--	--
Society and Culture		✓		--	--
Software Updates		✓		--	--
Sports and Recreation		✓		--	--
Streaming Audio		✓		--	--

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

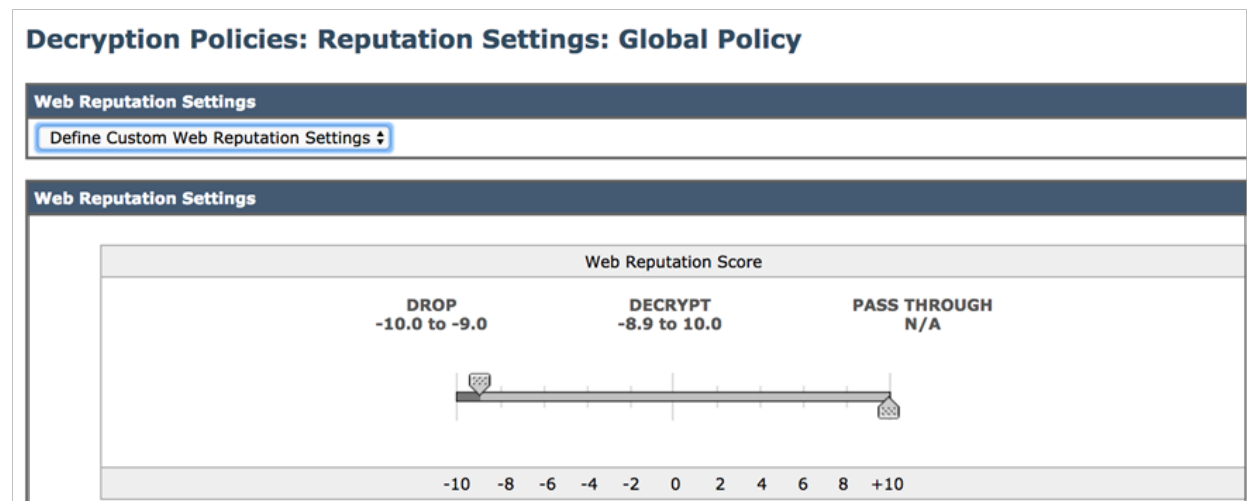
Adding WSA self-signed certificate to Firefox certificate store

Step 8. Click **Submit** and **Commit** all changes.

Step 9. All social networking sites will now be decrypted and blocked.

Web Reputation Score Custom setting

The decrypt policy matches the WBRS rating for the HTTPS website against the predefined web reputation score and determines the action accordingly. **(As show in the figure)**



The administrators can define custom web reputation setting for drop, decrypt and pass through action.

NOTE: We Recommend that you do not make changes to the Web reputation Score settings and keep it as default in order to prevent any unforeseen and unintended actions on the web transactions.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 1. From **Web security manager >Decryption policies** -> **Click** under the **Web reputation** column.

Decryption Policies					
Policies					
Add Policy...					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	Decrypt News traffic Identification Profile: Global All identified users	(global policy)	Enabled	(global policy)	

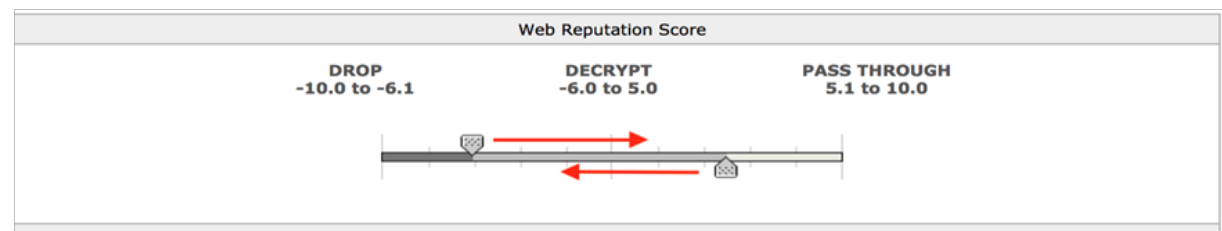
Step 2. Under the **Web reputation Settings** drop down menu select **Define Custom Web reputation Settings**.

Decryption Policies: Reputation Settings: Decrypt News traffic

- Use Global Web Reputation Settings
- Define Custom Web Reputation Settings
- Disable Web Reputation for this Policy

Web Reputation Settings

Step 3. Move the Slider to set the appropriate settings for **Drop, Decrypt or pass through** action.



Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 4. Save and Commit Changes.

The URL categories under the specific decryption policies that are set to **Monitor** Action, will run through the WBSR custom settings and will action on the Web request accordingly.

Importing WSA server certificate on end clients

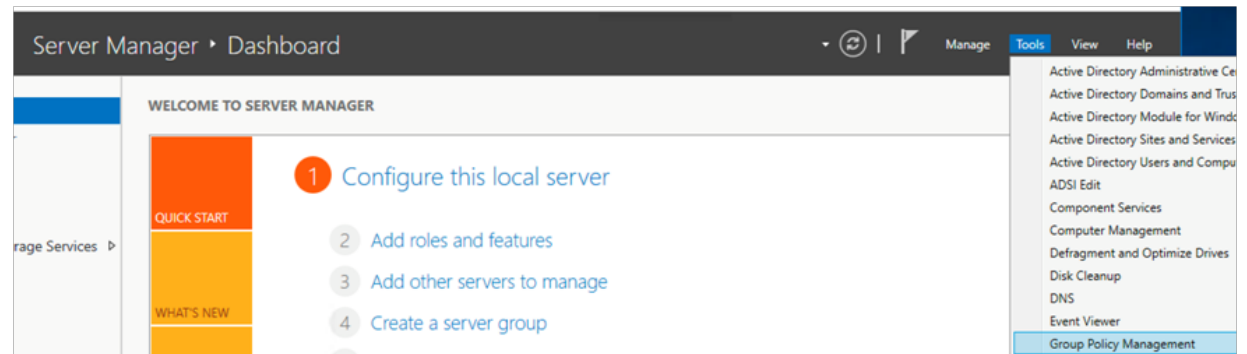
The WSA HTTPS Proxy Certificate can either be manually installed on clients or deployed via group policy.

Applying Certificates at the enterprise level

This section describes the WSA self-signed certificate applied using active directory group policy.

Step 1: Login to active directory domain controller.

Step 2: On your active directory server, select **Start > Server Manager > Tools > Group Policy management**.



Step 3: Expand your domain settings > **Default Domain Policy** > Right-click > **Default Domain Policy** and click **Edit**. If you have other domain policies configured for the users, apply the settings to the

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

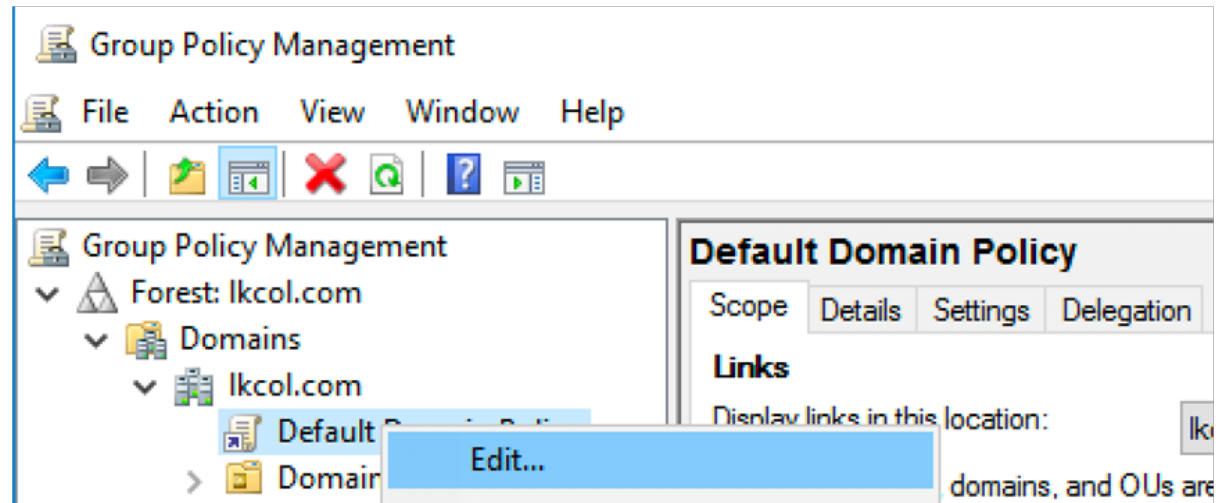
Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

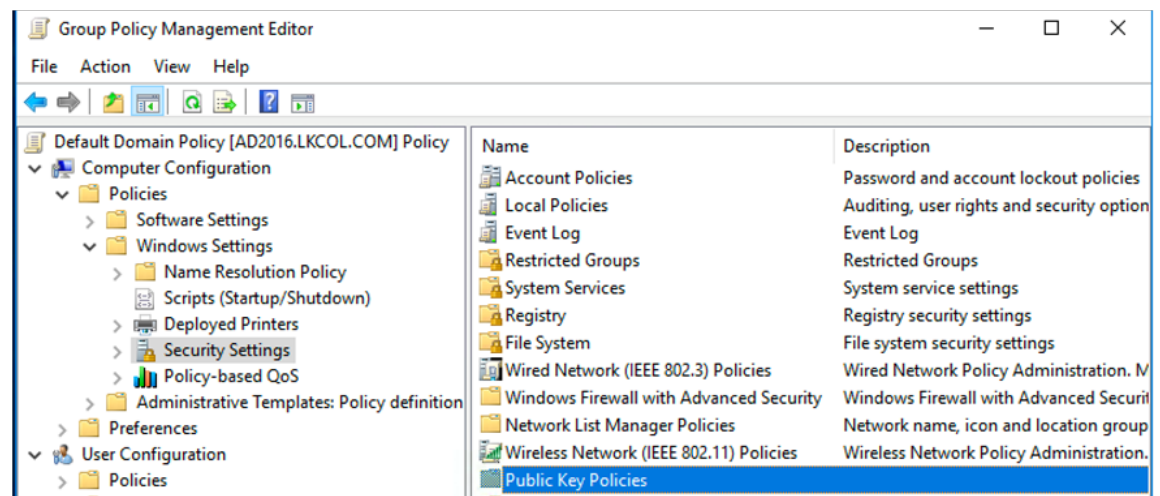
Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

specific policy associated with the users.



Step 4: Expand the **Computer Configuration** section>**Policies** and open **Windows Settings**\Security Settings\Public Key.



Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

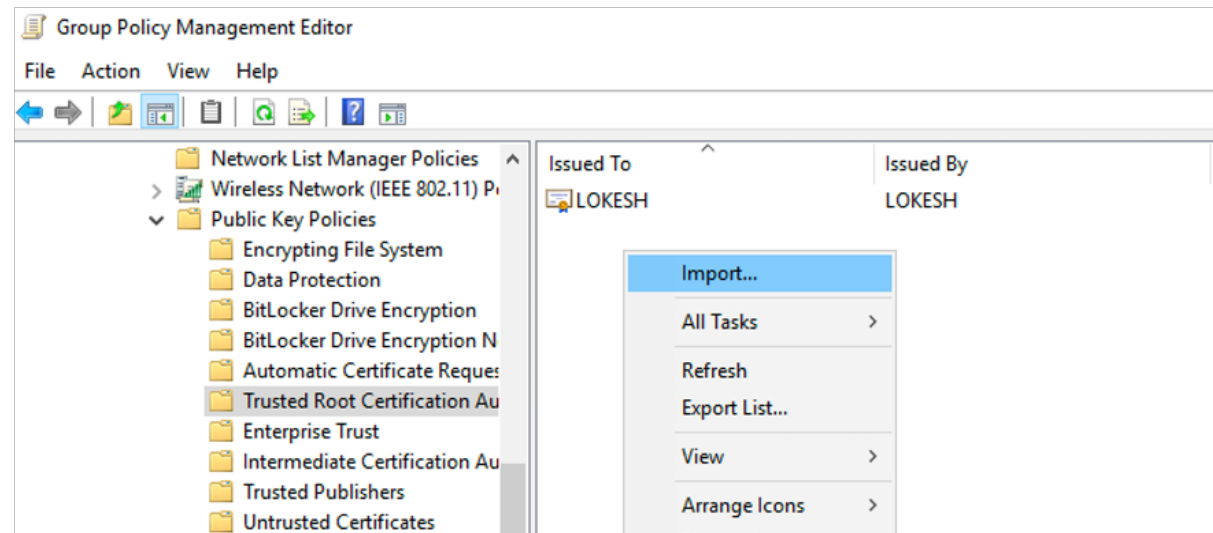
Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 5: Double-click **Public Key Policies** and go to **Trusted Root Certification Authorities**. Right-click and select **Import**.



Step 6: Follow the prompts in the wizard to import the WSA self-signed certificate. Reboot all the client machines for the changes to take effect.

All of the systems in the domain will now have a copy of the root certificate in their trusted root store. The next time client machines reboot, it will have the WSA certificate.

Contents

[About this document](#)

[Introduction to HTTPS decryption](#)

Before you begin

[Certificate Types](#)

Introduction

Certificate overview

Root certificates

Server certificates

[Enabling HTTPS decryption on the WSA](#)

[HTTPS decryption on the WSA in action](#)

[Web Reputation Score Custom setting](#)

[Importing WSA server certificate on end clients](#)

[Applying Certificates at the enterprise level](#)

[Applying certificates at the client level](#)

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

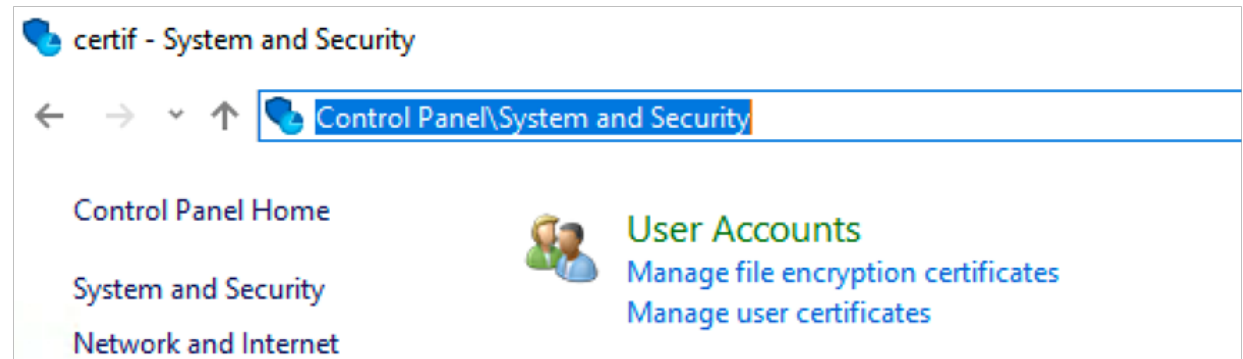
Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

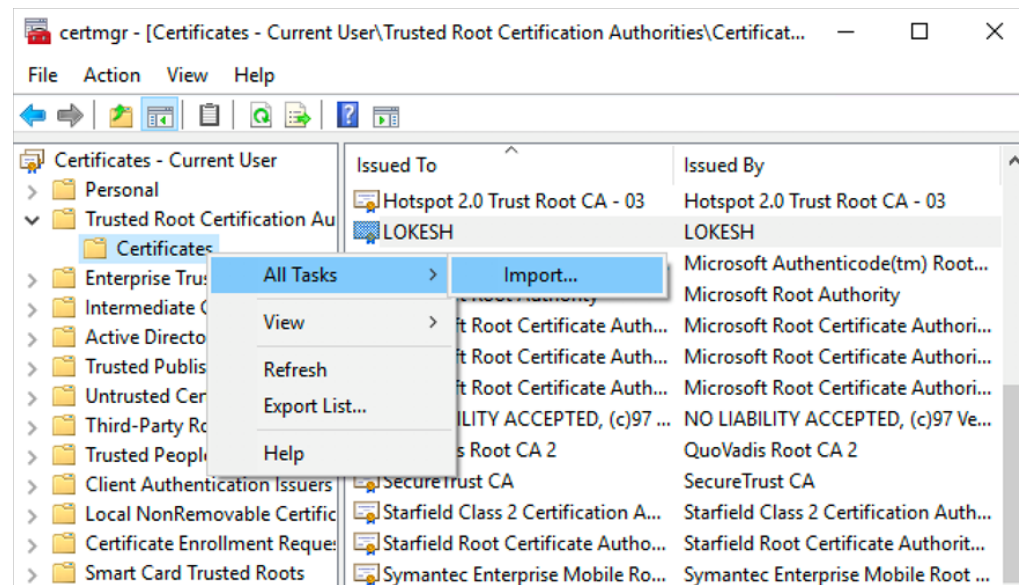
Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Step 1: Go to **Control Panel/System and Security**, and click on **Manage user certificates**.



Step 2: Expand **Trusted Root Certificate Authorities>Certificate>Right-click >All Tasks**, and **Import** the WSA self-signed certificate.



Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

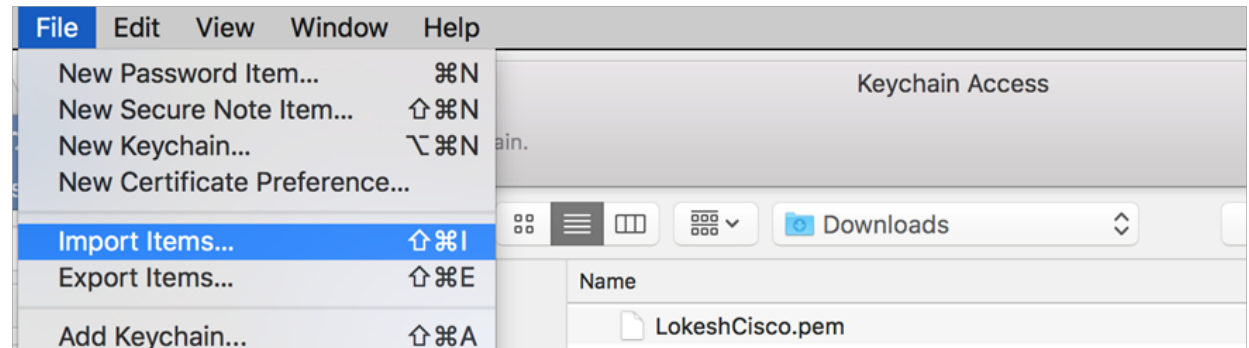
Adding the WSA self-signed certificate to a MAC client

Step 1: Open the **Keychain Access** utility (**Applications > Utilities**).

Step 2: Choose **File > Import Items**.

Step 3: Browse to the location of your WSA certificate file, and click **Open**. You will be prompted for your key pair's export password.

Step 4: You may also be prompted whether to automatically trust certificates issued by your CA. To trust and install your certificate, click **Always Trust**.



Once imported, your certificate-key pair will appear under both the **Certificates** and **Keys** categories in the **Keychain Access** utility.

Making changes to Firefox browser

Firefox maintains its own certificate store. In order to install the WSA self-signed certificate, we can either add the certificate to the Firefox certificate store, or if we are using the active directory to apply the certificates, we need to enable the “**security.enterprise_roots.enabled**” to **true**.

Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

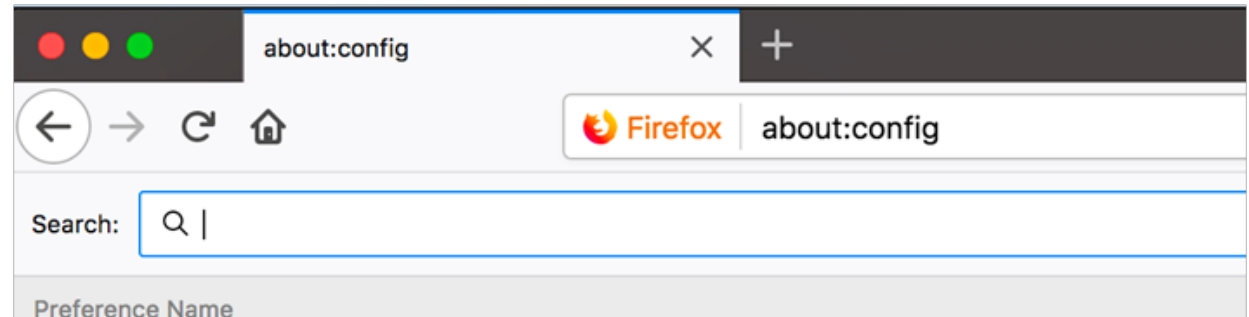
Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

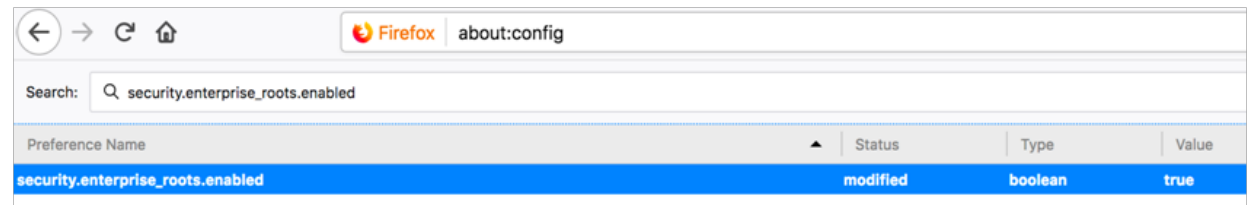
Applying active directory certificate to Firefox

Step 1: Ensure that you are running the latest version of Firefox.

Step 2: Open the Firefox browser and type “**about:config**.”

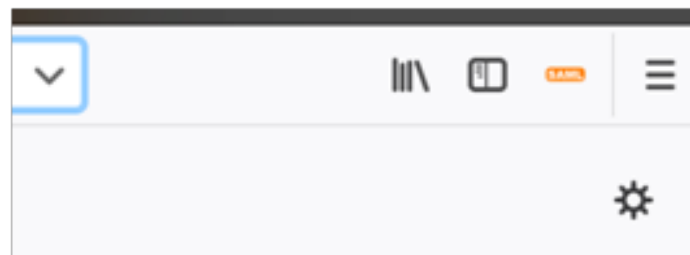


Step 3: Search for “**security.enterprise_roots.enabled**,” and toggle it to **true**.



Adding WSA self-signed certificate to Firefox certificate store

Step 1: Open Firefox and click on the gear icon on the top-right corner.



Contents

About this document

Introduction to HTTPS decryption

Before you begin

Certificate Types

Introduction

Certificate overview

Root certificates

Server certificates

Enabling HTTPS decryption on the WSA

HTTPS decryption on the WSA in action

Web Reputation Score Custom setting

Importing WSA server certificate on end clients

Applying Certificates at the enterprise level

Applying certificates at the client level

Adding the WSA self-signed certificate to windows machine

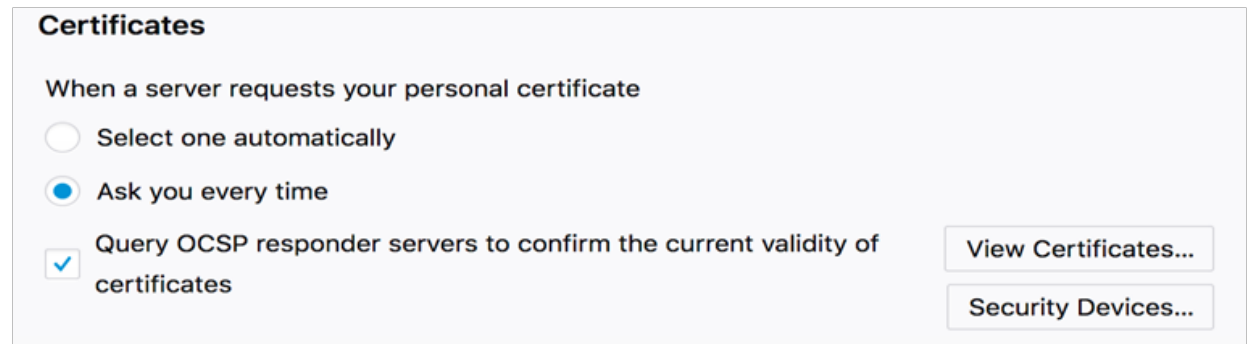
Adding the WSA self-signed certificate to a MAC client

Making changes to Firefox browser

Applying active directory certificate to Firefox

Adding WSA self-signed certificate to Firefox certificate store

Step 2: Go to **Privacy and Security** tab, and click on **View Certificates**.



Step 3: Click on the Import icon and upload the certificate.

