Configure Umbrella VA to Receive User-IP Mappings

Contents

Introduction

This document describes how to configure the Cisco Umbrella Virtual Appliance (VA) to receive user-IP mappings over a secure channel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Private key creation, certificate creation, certificate signing and management are out of scope for the Umbrella components. This must be done external to these components.
- You must create one certificate with a unique Common Name per Virtual Appliance.
- You must also add an A record in your internal DNS server, pointing this Common Name to the IP address of the Virtual Appliance.
- If the IP address of a Virtual Appliance needs to be changed, this A record must also be correspondingly changed.
- The FQDN corresponding to the certificate must be configured as a local domain on the Umbrella dashboard so that the VA recognizes this as a local domain.
- Private key and certificates need to be created in the .key and .cer format respectively.

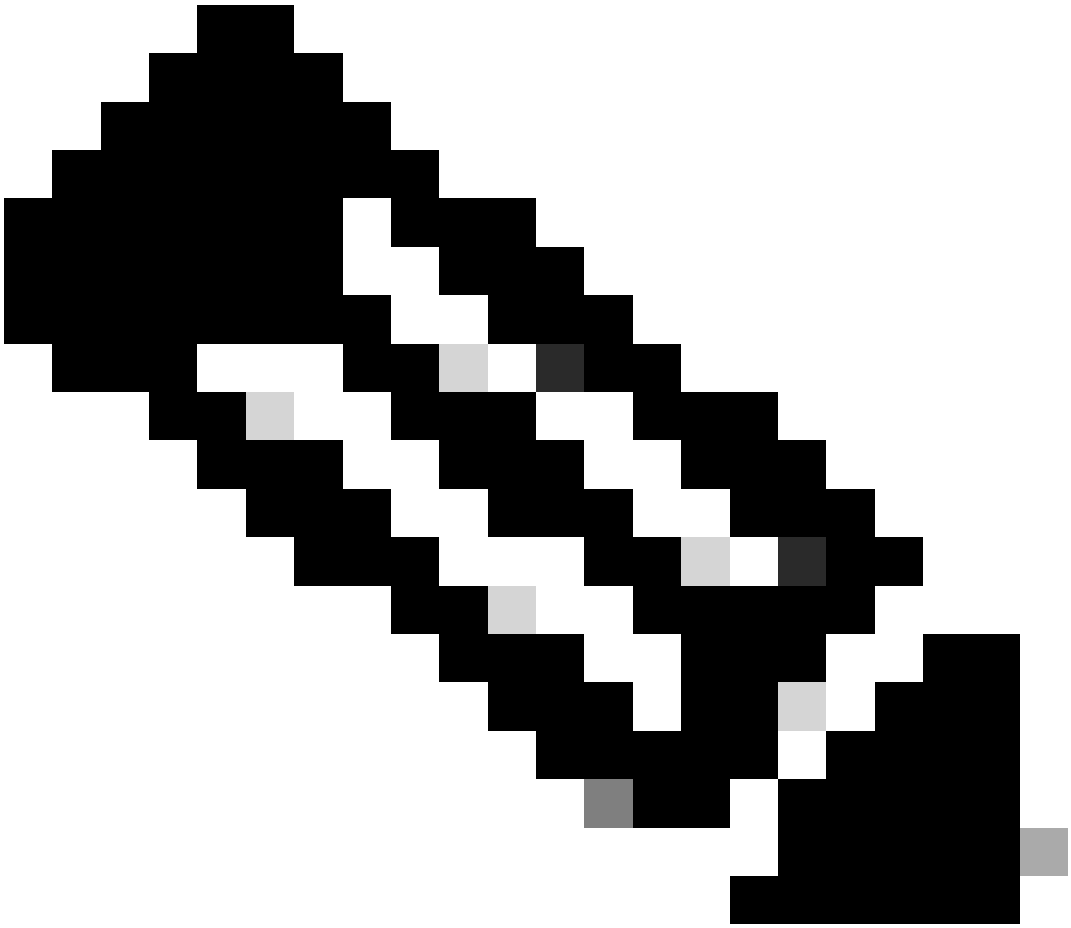
- You can use either self-signed certificates or CA-signed certificates for this purpose.

Components Used

The information in this document is based on these software and hardware versions:

- Virtual Appliance running version 2.7 or later
- Umbrella AD Connector must be running version 1.5 or later
- Umbrella Chromebook Clients must be running version 1.3.3 or higher

---



Note: If your VA or AD Connector are running previous versions, you can open a support ticket with Umbrella to get them upgraded to the respective supported versions.

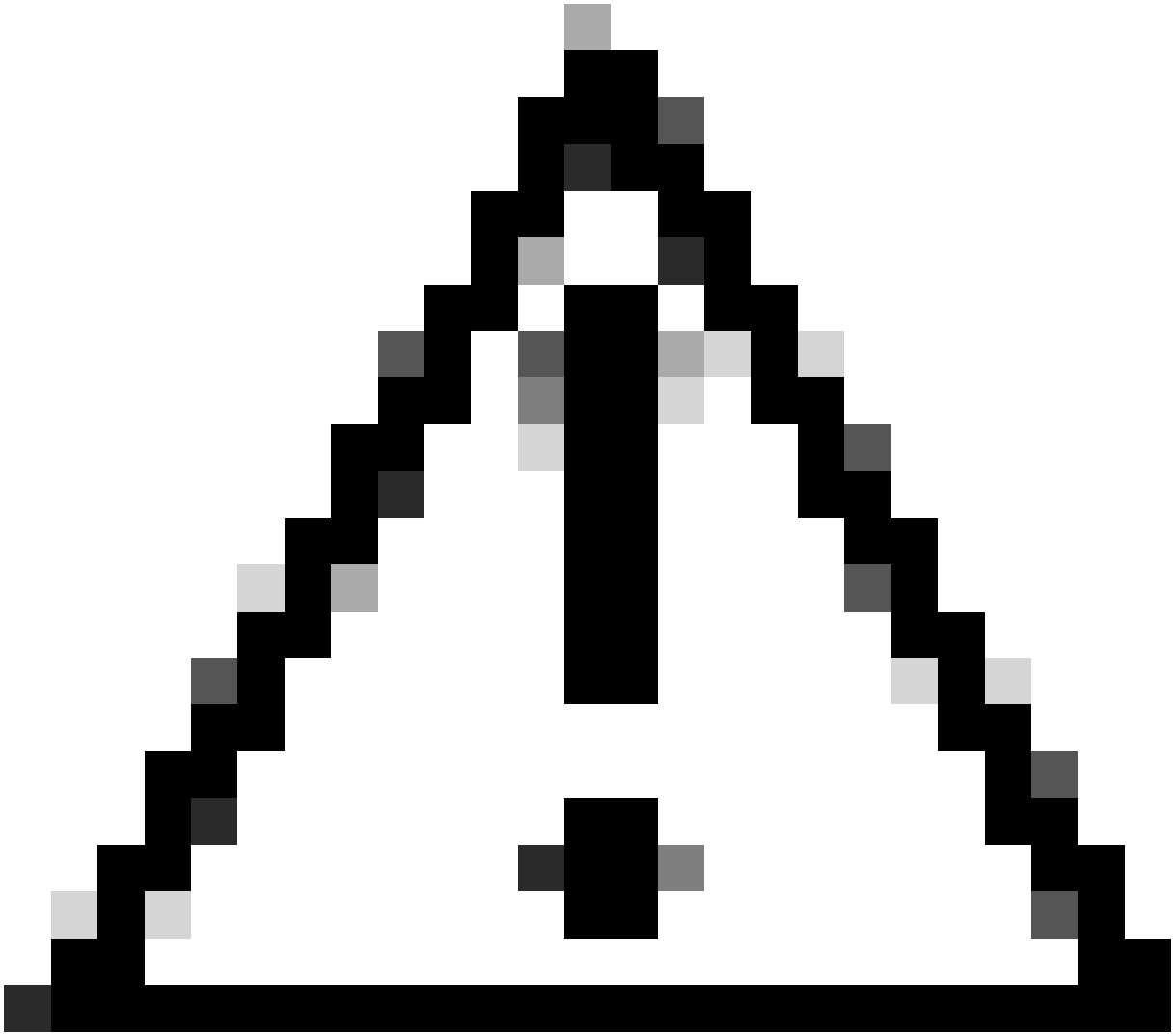
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Umbrella Virtual Appliances, running version 2.6 or prior, support receiving user-IP mappings from the Umbrella Active Directory (AD) Connector and the Umbrella Chromebook Clients only in unencrypted form on port 443. As a result, a mandatory prerequisite for deployment has been that the AD Connector and VA or Chromebook Clients and VA communicate over a trusted network only.

Starting in version 2.7, Umbrella Virtual Appliances can now receive AD user-IP mappings from the AD Connector over HTTPS, and similarly GSuite user-IP mappings from each Umbrella Chromebook Client over HTTPS.

This article details the configuration steps on each component to enable HTTPS communication. By default, HTTPS communication is disabled and the AD Connector and Chromebook Clients communicate to the VA over HTTP only.



Caution: Turning on this feature can increase the CPU and memory utilization on the VA and the Umbrella AD Connector and can result in reduced DNS throughput for the VA. As a result, it is recommended to turn on this feature only if mandated by any compliance requirements for your organization.

Virtual Appliance

Add Private Key and Certificate to the VA

To add the private key and certificate to the VA:
1. Open the private key file via text editor.

2. Select all, copy, and then paste in the double quotes for this command:

```
config va ssl key "paste the contents of the .key file here"
```

Add Certificate to the VA

To add the certificate to the VA:
1. Open the certificate file via text editor.

2. Select all, copy, and then paste in the double quotes for the command below:

```
config va ssl cert "paste the contents of the .crt file here"
```

Enable HTTPS on the VA

Enable HTTPS on the VA using this command:

```
config va ssl enable
```

Verify HTTPS Enablement

Verify that HTTPS is enabled using the command:

```
config va show
```

Output of this command can include the HTTPS status as well as the SSL certificate details.

Example output:

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

It can take up to 20 minutes for the VA to start receiving events over HTTPS. You can check after around 20 minutes using the `config va status` command. The AD Connector status is in yellow (stalled) state in the intermediate period and moves to green state once the VA starts receiving events over HTTPS.

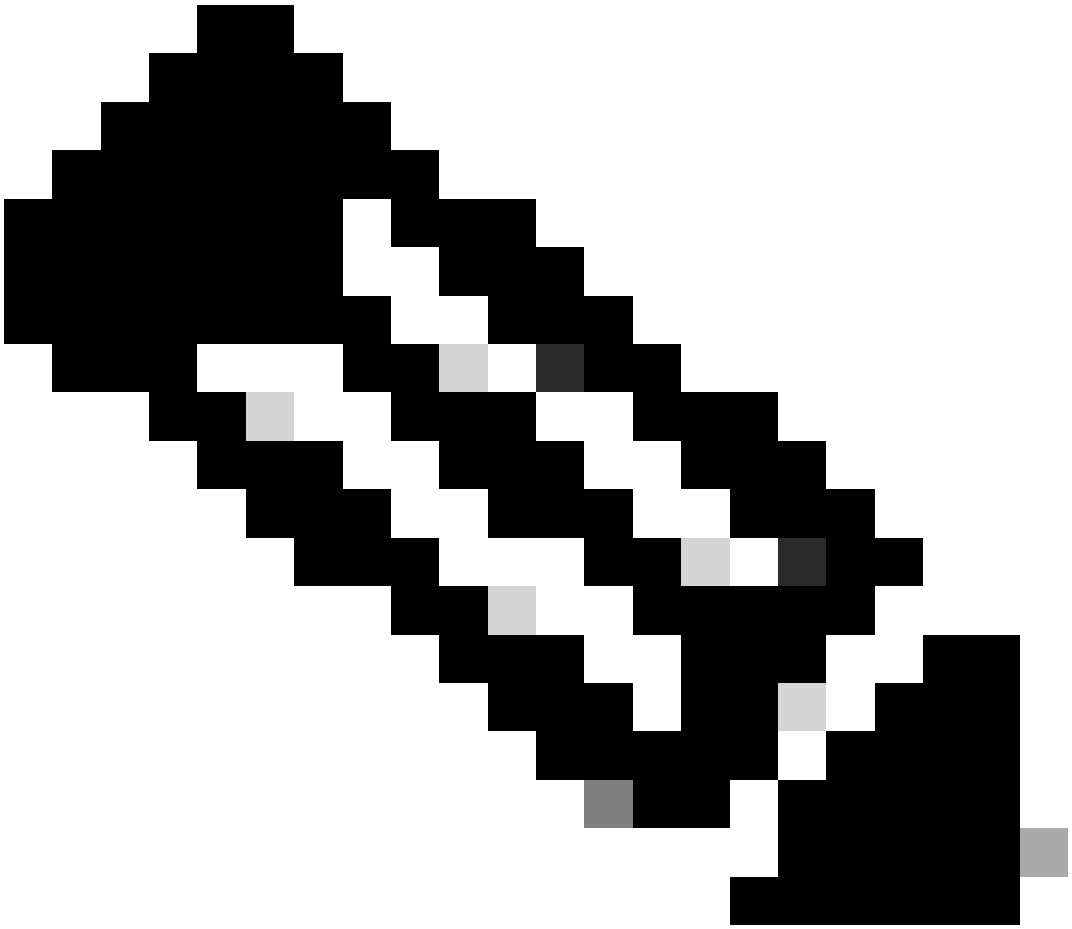
If you wish to disable HTTPS and revert to HTTP, use the command `config va ssl disable`.

If you want to re-enable HTTPS, you must add the private key and certificate again and then use the `config va enable` command.

Active Directory

If you are using a CA-signed certificate for each VA, make sure the root certificate and issuing CA certificates for each VA certificate are installed on each system running the AD Connector in the same site as the VA.

If you are using self-signed certificate for each VA, make sure each VA certificate is installed on each system running the AD Connector in the same Umbrella site as the VA.



Note: Only certificates for VAs in the same Umbrella site as the AD Connector need to be installed on the AD Connector.

It can take up to 20 minutes for the VA to sync the HTTPS status to Umbrella, which is then synced to the AD Connector. As a result, it can take up to 20 minutes for the Connector to start sending data to the VA over HTTPS. Any user-IP mappings sent during this period is discarded by the VA. It is therefore recommended to make the configuration change on the VA only during downtime hours when no user logins are expected.

Umbrella Android Client

If you are using CA-signed certificates for VAs, make sure the root certificate and issuing CA certificates for each VA certificate are pushed to and installed on each Android device.

If you are using self-signed certificates for VAs, make sure each VA certificate is pushed to and installed on each Android device.

Once the certificate is available, the Umbrella Android Client can start using this certificate to set up an HTTPS channel with the VA.

Umbrella Chromebook Client

If you are using CA-signed certificates for VAs, make sure the root certificate and issuing CA certificates for each VA certificate are pushed to and installed on each Chromebook.

If you are using self-signed certificates for VAs, make sure each VA certificate is pushed to and installed on each Chromebook.

Once the certificate is available, the Umbrella Chromebook Client can start using this certificate to set up an HTTPS channel with the VA.

For more information, refer to the article Umbrella Chromebook Client: Sending user-IP mappings over a secure channel to the Umbrella Virtual Appliance.

Configuration Sequence

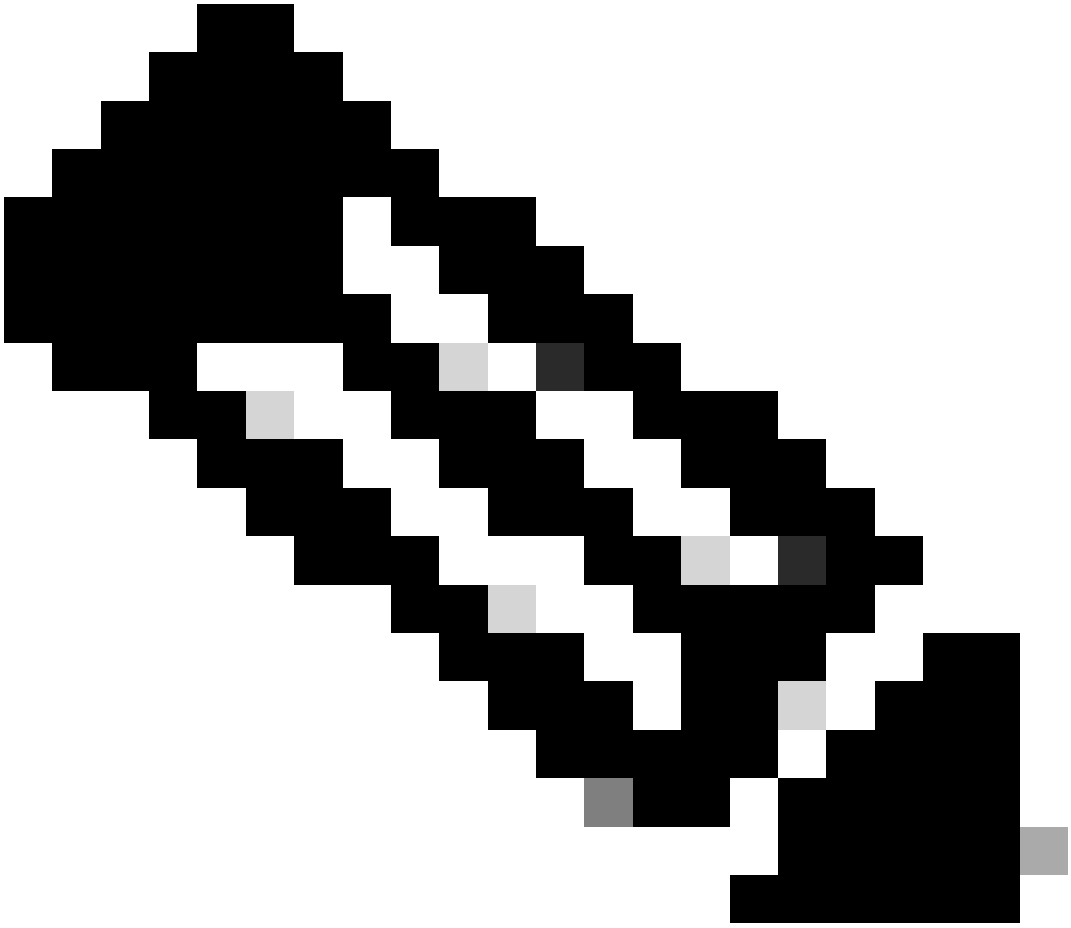
Once HTTPS is enabled on the VA, the VA does not accept user-IP mappings sent in plaintext over HTTP. As a result, any user logins sent over HTTP are discarded, and user attribution for DNS requests from these users are not available. It is therefore recommended to configure these components in this order:

1. Create the certificate and private key for each VA based on a CA signed or self-signed certificate.

2. Add the certificate and private key to each VA respectively.

3. Make sure the root certificate and intermediate parent certificates for each VA certificate (or VA self-signed certificate) are installed on each system running the AD Connector in the same site as the VA, and on each Chromebook.

4. During downtime hours, enable HTTPS on the VA.



Note: The certificate on the VA must be replaced before it expires, and the intermediate parent and root certificates must be installed on the AD Connector and Umbrella Chromebook Clients. If this is not done, the AD Connector and Umbrella Chromebook Clients are not able to communicate with the VA.