UTD Commands

file-analysis profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file analysis profile, use the **file-analysis profile** command in UTD Multi-Tenancy configuration mode. To delete Cisco AMP file analysis profile, use the **no** form of this command.

file-analysis profile *file-analysis-name* { **alert level** { **critical** | **info** | **warning** } | **file-types** *file-type* }
no file-analysis profile *file-analysis-name* { **alert level** { **critical** | **info** | **warning** } | **file-types** *file-type* }

Table 1: Syntax Description:

file-analysis-name	Specifies the file analysis profile name.
alert level critical |info |warning	Configures alert level as critical, info, or warning.

file-types *file-type*	Configures file types. Possible options are: • flv • mdb • mscab • msole2 • new-office • pdf • rtf • swf • wri • xlw

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

File analysis is the process of submitting an unknown file to Cisco Secure Malware Analytics (formerly Threat Grid) cloud for Cisco IOS XE Catalyst SD-WAN Release 17.2.1v detonation in a sandbox environment. During detonation, the sandbox captures artefacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change the threat response to Clean or Malicious. Findings from Threat Grid are reported back to the Cisco AMP cloud, so that all Cisco AMP customers are protected against newly discovered malware.

Examples

The following example shows how to configure an AMP file analysis profile with critical alerts, and a profile that analyzes flv and pdf files:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-analysis profile file-analysis-profile1
Device(config-utd-mt-file-an-profile)# alert level critical
Device(config-utd-mt-file-an-profile)# file-types
Device(config-utd-mt-file-an-types)# flv
Device(config-utd-mt-file-an-types)# pdf
```

Table 2: Related Commands

Commands	Description
utd multi-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs).
file-inspection profile	Configures a file inspection profile.

file-inspection profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file inspection profile, use the **file-inspection profile** command in UTD Multi-Tenancy configuration mode. To delete Cisco AMP file inspection profile, use the **no** form of this command.

file-inspection profile *file-inspection-profile* { **analysis profile** *file-analysis-name* | **reputation profile** *file-reputation-name* }
no file-inspection profile *file-inspection-profile* { **analysis profile** *file-analysis-name* | **reputation profile** *file-reputation-name* }

Table 3: Syntax Description:

file-inspection-profile	Specifies file inspection profile name.
file-analysis-name	Specifies file analysis profile name.
file-reputation-name	Specifies file reputation profile name.

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **file-inspection profile** command to configure an Cisco Advanced Malware Protection (Cisco AMP) file inspection profile.

Under the file inspection profile, a file reputation profile is required, and a file analysis profile is optional. Both must be configured first before assigning them to the file inspection profile.

Examples

The following example shows how to configure a file inspection profile that calls a file analysis and file reputation profiles:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-inspection profile file-inspection-profile1
Device(config-utd-mt-file-insp)# analysis profile file-analysis-profile1
Device(config-utd-mt-file-insp)# reputation profile file-reputation-profile1
```

After you configure the file-inspection profile, you can call it per VRF:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# policy utd-policy-vrf-1
Device(config-utd-mt-policy)# file-inspection profile file-inspection-profile1
Device(config-utd-mt-policy)# vrf 1
```

Table 4: Related Commands

Commands	Description
utd multi-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).
file-analysis profile	Configures a file analysis profile.
file-reputation profile	Configures a file reputation profile.
policy	Configures a policy under UTD and applies it to a VRF.

file-reputation profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file reputation profile, use the **file-reputation profile** command in UTD Multi-Tenancy configuration mode. To delete a Cisco AMP file reputation profile, use the **no** form of this command.

file-reputation profile *file-reputation-name* [**alert level** { **critical** | **info** | **warning** }]
no file-reputation profile *file-reputation-name* [**alert level** { **critical** | **info** | **warning** }]

Syntax Description

file-reputation-name	Specifies file reputation profile name.
alert level critical | info | warning	Configures alert level as critical, info, or warning.

Command Default

None

Command Modes UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **file-reputation profile** command to configure Cisco AMP file reputation profile, including the alert levels. We recommend configuring alert level info only when used for troubleshooting and not for regular traffic.

Examples

The following example shows how to configure Cisco AMP file reputation with critical alerts:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-reputation profile file-reputation-profile1
Device(config-utd-mt-file-rep-profile)# alert level critical
```

Table 5: Related Commands

Commands	Description
utdmulti-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utdenginestandardmulti-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (AMP) profiles for multi-tenancy (multiple tenants/VRFs).
file-inspectionprofile	Configures a file inspection profile.

flow-logging

To enable unified logging for UTD features use the **flow-logging** command in UTD Multi-Tenancy and unified-policy global configuration mode. To disable unified logging, use the **no** form of this command.

flow-logging [{ **all** | **file-inspection** | **threat-inspection** | **tls-decryption** | **web-filter** }]

Command Default None

Command Modes UTD Multi-Tenancy and unified-policy global configuration (config-utd-mt-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure UTD logging in a unified security policy:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all
```

logging host

To log UTD syslog messages to a remote host, use the **logging host** command in UTD Multi-Tenancy and unified-policy global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host *host_name* [{ **source-interface** *interface-name* }]

Syntax Description

host-name	Host name or IP address of the host that will receive the UTD syslog messages.
interface-name	The interface from which the UTD syslog originates.

Command Default

None

Command Modes

UTD Multi-Tenancy and unified-policy global configuration (config-utd-mt-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure UTD logging in a unified security policy:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# logging host 10.1.1.1
Device(config-utd-mt-global)# logging host 10.2.2.2 source-interface GigabitEthernet3
```

threat-inspection profile

To configure threat-inspection profile and optionally specify the name of a custom signature profile, use the **threat-inspection profile** command in UTD unified policy configuration mode. To delete threat-inspection profile, use the **no** form of this command.

threat-inspection profile *threat-inspection-profile-name* **{custom-signature profile** *custom-signature-profile-name* **}**
no threat-inspection profile

Syntax Description

threat-inspection-profile-name	Specifies the threat-inspection profile name.
custom-signature profile *custom-signature-profile-name*	(Optional) Specifies the custom signature profile name.

Command Default

This command is not configured, and the IPS/IDS (Intrusion Prevention System and Intrusion Detection System) feature is not applied to traffic.

Command Modes

UTD unified policy configuration (config-utd-unified-policy)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added support for specifying a custom-signature profile name.

Examples

The following example shows how to configure a threat-inspection profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# threat-inspection profile IPS_UNIFIED_1
Device(config-utd-mt-threat)# custom-signature profile global
```

threat-inspection custom-signature profile

To add a custom signature profile to a threat-inspection profile, use the **threat inspection custom-signature profile** command in UTD unified policy configuration mode. To delete the custom signature file, use the **no** form of this command.

threat-inspection custom-signature profile *custom-signature-profile-name* **file** *path-to-custom-signature-file*
no threat-inspection custom-signature profile

Syntax Description

custom-signature profile name	Specifies the custom-signature profile name.
file *path to custom signature file*	Specifies the path to the custom-signature file.

Command Default

Custom signature profile is not added to threat inspection profile.

Command Modes

UTD unified policy configuration (config-utd-unified-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines If the custom signature profile does not exist in the designated path, an empty file is created on that path.

Examples The following example shows how to add a custom signature profile to a signature package:

```
utd engine standard unified-policy
  threat-inspection custom-signature profile global
    file bootflash:GLOBAL_CUSTOM_SIG.txt
  threat-inspection profile IPS_UNIFIED_1
     threat protection
     policy security
     custom-signature profile global
```

tls-decryption profile

To configure tls-decryption profile, use the **tls-decryption profile** command in UTD unified policy configuration mode. To delete tls-decryption profile, use the **no** form of this command.

tls-decryption profile *tls-decryption profile name*
no tls-decryption profile

tls-decryption profile name	Specifies tls-decryption profile name.

Command Default None

Command Modes UTD unified policy configuration (config-utd-unified-policy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a tls-decryption profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# tls-decryption profile tls
```

utd engine standard multi-tenancy

To configure UTD policies, web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs), use the **utd engine standard multi-tenancy** command in global configuration mode. To remove them, use the **no** form of this command.

utd engine standard multi-tenancy

Syntax Description

(none)	You enter a sub-mode UTD engine standard multi-tenancy and configure UTD policies, web filtering, threat-inspection, and Advanced Malware Protection (AMP) profiles. After exiting the UTD engine standard multi-tenancy sub-mode, the UTD policies are applied.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **utd engine standard multi-tenancy** command to configure UTD policies, web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).

Before you begin, remove any existing single-tenancy UTD configuration, using the **no utd engine standard** command, and you must have previously configured a VRF for each tenant. Once you have done that, you can start configuring the policies that should be enforced for each tenant.

Examples

The following example shows how to configure UTD policies, web filtering, threat-inspection, and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs):

```
Device(config)# utd multi-tenancy
Device(config)# utd engine standard multi-tenancy
```

Table 6: Related Commands

Command	Description
utd multi-tenancy	Enables UTD policies for multi-tenancy (multiple tenants/VRFs).

utd engine standard unified-policy

To configure a unified security policy that includes firewall and other UTD profiles such as web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP), TLS decryption, use the **utd engine standard unified-policy** command in global configuration mode. To remove them, use the **no** form of this command.

utd engine standard unified-policy

Syntax Description

(none)	Enter a sub-mode UTD engine standard unified-policy and configure a unified security policy. After exiting the UTD engine standard unified-policy sub-mode, the unified security policies are applied.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **utd engine standard unified-policy** command to configure unified security policy, web filtering, threat-inspection, Cisco Advanced Malware Protection (Cisco AMP) profiles, and TLS decryption.

Examples

The following example shows how to configure a unified policy with web filtering, threat-inspection, Cisco AMP profiles, and TLS decryption.

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# policy aip-policy
Device(config-utd-mt-policy)# threat-inspection profile ips
Device(config-utd-mt-policy)# web-filter url profile url
Device(config-utd-mt-policy)# file-inspection profile fs
Device(config-utd-mt-policy)# tls-decryption profile tls
```

utd global

To configure settings that apply to all configured Unified Threat Defense (UTD) policies, use the **utd global** command in UTD Multi-Tenancy configuration mode. To remove the setting, use the **no** form of this command.

utd global { **file-analysis** [**apikey 0** *string*] | **cloud-server** *string* | **file-reputation** { **cloud-server** *string* | **est-server** *string* | **query-interval** *time* } }
no utd global { **file-analysis** [**apikey 0** *string*] | **cloud-server** *string* | **file-reputation** { **cloud-server** *string* | **est-server** *string* | **query-interval** *time* } }

Table 7: Syntax Description

(none)	Applies UTD policies to all tenants/VRFs. Multiple settings can be configured once the command is applied.
file-analysis	Configures Cisco AMP Threat Grid File analysis settings.
apikey 0 *string*	Specifies Cisco AMP Threat Grid API Key.
cloud-server *string*	Specifies Cisco AMP Threat Grid file analysis server. Example: cloud-isr-asn.amp.cisco.com
file-reputation	Specifies Cisco AMP File reputation settings.

cloud-server *string*	Specifies Cisco AMP Cloud server. Example: cloud-isr-asn.amp.cisco.com
est-server *string*	Specifies Cisco AMP EST server. Example: cloud-isr-est.amp.cisco.com
query-interval *time*	Specifies the query interval in seconds.

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure settings that apply to all configured UTD policies, use the **utd global** command in UTD Multi-Tenancy configuration mode.

Examples

The following example shows how to configure global AMP settings:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# utd global
Device(config-utd-mt-global)# file-analysis
Device(config-utd-mt-file-an-global)# apikey 0 0123456789abcdef
Device(config-utd-mt-file-an-global)# cloud-server cloud-isr-asn.amp.cisco.com
Device(config-utd-mt-file-an-global)# file-reputation
Device(config-utd-mt-file-rep-global)# cloud-server cloud-isr-asn.amp.cisco.com
Device(config-utd-mt-file-rep-global)# est-server cloud-isr-est.amp.cisco.com
Device(config-utd-mt-file-rep-global)# query-interval 900
```

Table 8: Related Commands

Commands	Description
utd multi-tenancy	Enables UTD for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs).

utd multi-tenancy

To enable Unified Threat Defense (UTD) for multi-tenancy (multiple tenants/VRFs), use the **utd multi-tenancy** command in global configuration mode. To disable UTD for multi-tenancy, use the **no** form of this command.

utd multi-tenancy [**engine standard multi-tenancy**]

Syntax Description

(none)	Enables UTD for multi-tenancy (multiple tenants/VRFs).

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **utd multi-tenancy** command to enable UTD multi-tenancy mode. Single-tenancy mode is the default.

Examples

The following example shows how to enable UTD for multi-tenancy (multiple tenants/VRFs):

```
Device(config)# utd multi-tenancy
```

Table 9: Related Commands

Command	Description
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).

web-filter url profile

To configure web-filter url profile, use the **web-filter url profile** command in UTD unified policy configuration mode. To delete web-filter url profile, use the **no** form of this command.

web-filter url profile *web-filter-profile-id*
no web-filter url profile

web-filter-profile-id	Specifies web filter url profile name.

Command Default

None

Command Modes

UTD unified policy configuration (config-utd-unified-policy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a web filter url profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# web-filter url profile url
```