TMWS Best Practices

Version 1.3

Contents

Tables

How to set up the Authentication of your company?

1 How to set up the Authentication of your company?

1.1 General Description

TMWS provides many authentication methods to adapt company's authentication system. TMWS also provides some add-on methods to co-work with these authentication methods. You can balance your choice according to the company's present situation.

The following table shows the available authentication methods. The "Requirements & Guides" column gives the basic requirements and available guides for setting the corresponding authentication method.

Table 1 Authentication Methods

AUTH Method	***Description***	***Requirements & Guides***
Direct	Communicate with the AD server directly User Authentication & Synchronization	▪ A public IP of your AD Service is required. Your AD services need expose the LDAP/LDAPS ports to Internet. ▪ Allow Trend Micro public IPs to access your AD services. Network Diagram: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-dir/direct-authenticatio.aspx Setup Guide: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-dir.aspx
AD FS	Communicate with the AD FS Service for User Authentication. Install Sync Agent to synchronize AD users to TMWS.	▪ AD FS should be setup for the AD. ▪ A public IP of your AD FS is required if you want to use the TMWS Cloud proxy outside your company's office. ▪ Sync Agent is required to synchronize the user information. Network Diagram: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-fed/port-configuration-f.aspx Setup Guide: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-fed.aspx
Agent	Communicate with the AUTH Agent for User Authentication. Install Sync Agent to synchronize AD users to TMWS.	▪ AUTH Agent is required to authenticate users. ▪ A public IP of your AUTH Agent is required if you want to use the TMWS Cloud proxy outside your company's office. ▪ Sync Agent is required to synchronize the user information. Network Diagram: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-fed/port-configuration-f.aspx

		Setup Guide: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/active-directory-age.aspx
Okta	Communicate with Okta for User Authentication & Synchronization	▪ Okta account is required for setup. ▪ SAML and SCIM Apps of Okta are required for setup. Setup Guide: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/azure-active-directo.aspx
Azure AD	Communicate with Azure AD for User Authentication & Synchronization	▪ Azure AD account is required for setup. Setup Guide: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services/okta-authentication.aspx

The following table shows the available addon methods to co-work with authentication methods.

Table 2 Addon authentications

Addon Methods	***Description***	***Requirements & Guides***
Kerberos	Communicate with AD with Kerberos for User Authentication. Kerberos should co-work with one of the following company authentication method: ▪ Direct ▪ AD FS ▪ Agent ▪ Okta ▪ Azure AD	▪ Kerberos authentication is only available for On-premises. ▪ Users should be synchronized by the chosen company authentication method. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/editing-an-on-premis/configuring-user-aut_001/configuring-kerberos.aspx
Hosted Users	Administrator can create TMWS local users in the service for user authentications.	▪ Hosted users only work under of the following authentication ways: ○ Direct ○ AD FS ○ Agent Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/hosted-users.aspx

1.2 Allow to visit the external dependent services.

TMWS has dependencies on some external services. Make sure your company's network allows the users to access these external services.
Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/introduction-and-get_001/task-overview-for-ne.aspx for the external services used by the system.

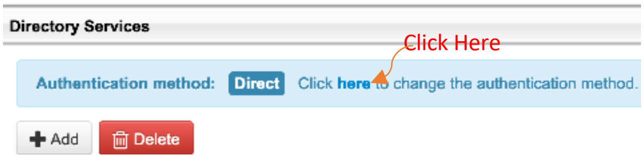
1.3 Setup Authentications of your Company

1.3.1 Logon your admin console.

1.3.2 Customize your company's authentication methods

1.3.2.1 Go to Administration -> Directories Services

1.3.2.2 Click the "**here**" to choose your company's authentication methods.



Directory Services

Authentication method: Direct Click **here** to change the authentication method.

1.3.3 Manage your AD domain

1.3.3.1 Go to Administration -> Directory Services

1.3.3.2 Add/Delete your AD domains
Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/directory-services.aspx

1.3.4 Setup your Authentication settings according to your chosen authentication method.

1.3.4.1 For Direct/AD FS/Agent authentication method, please go to each domain setting page to customize the detail settings.
How to visit the domain setting page:

- Go to Administration -> Directory Services.
- Find your AD domain.
- Click the edit button in the column "AD Integration" of your AD domain.

1.3.4.2 For Okta/Azure AD authentication method, please go to the authentication method page to customize the detail settings.
How to visit the authentication method setting page:

- Go to Administration -> Directory Services.
- Click the "**here**" to go to your authentication method page.

How to set up the Authentication of TMWS on-premises?

2 How to set up the Authentication of TMWS on-premises?

2.1 General Description

TMWS On-premises authentication is decided by the authentication method settings plus the on-premises self-settings.

2.2 Setup your company-level authentication method

Refer to best practice **How to set up the Authentication of your company?**

2.3 Setup Authentications of your On-premises Gateway

2.3.1 Go to Gateways page.

2.3.2 Find your on-premises gateway

2.3.3 Click the gateway name. It will show your on-premises gateway page.

2.3.4 Click the Authentication menu of your on-premises authentication setting page.

2.3.5 Setup Kerberos if you need it.

2.4 Setup Hosted Users

Go to Administration -> USERS & AUTHENTICATIONS -> Hosted Users

Manage your hosted users on this page. Hosted users work in some authentication methods only.

Refer to **How to set up the Authentication of your company?** For the detail introduction of Hosted Users.

2.5 Setup Guest User

TMWS provides 2 ways for Guest User's: Use Guest Port or Enable Guest User account.

2.5.1 Go to Gateways page.

2.5.2 Find your on-premises gateway

2.5.3 Click the gateway name. It will show your on-premises gateway page.

2.5.4 Click the Authentication menu of your on-premises authentication setting page.

2.5.5 Customize the Guest User settings under the section "Guest User Logon Settings"

2.5.5.1 Go to Administration -> USERS & AUTHENTICATIONS -> Hosted Users

2.5.6 Click "Guest User Account" to configure the Guest to configure the Guest User Account information

Available Helps:

Deployment Setup	***Helps***
On-premises Gateway Management Guide	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/editing-an-on-premis.aspx
On-premises Gateway Authentication Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/editing-an-on-premis/configuring-user-aut_001.aspx
Transparent Authentication	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/managing-internet-ga/transparent-authenti.aspx
Kerberos Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/editing-an-on-premis/configuring-user-aut_001/configuring-kerberos.aspx
Hosted User Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/hosted-users.aspx
Guest User Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/hosted-users/guest-user-account.aspx

How to set up the Authentication of TMWS virtual gateway?

3 How to set up the Authentication of TMWS virtual gateway?

3.1 General Description

TMWS virtual gateway authentication is decided by the authentication method settings plus the virtual gateway self-settings.

3.2 Setup your company-level authentication method

Refer to best practice **How to set up the Authentication of your company?**

3.3 Setup Authentications of your Virtual Gateway

3.3.1 Go to Administration -> Gateways page.

3.3.2 Find your virtual gateway

3.3.3 Click the gateway name. It will go to the virtual gateway page.

3.3.4 Click the Authentication menu of your virtual gateway authentication setting page.

3.4 Setup Hosted Users

Go to Administration -> USERS & AUTHENTICATIONS -> Hosted Users

Manage your hosted users on this page. Hosted users work in some authentication methods only.

Refer to **How to set up the Authentication of your company?** For the detail introduction of Hosted Users.

3.5 Setup Guest User

TMWS provides 2 ways for Guest User's: Use Guest Port or Enable Guest User account.

3.5.1 Go to Gateways page.

3.5.2 Find your virtual gateway

3.5.3 Click the gateway name. It will show your virtual gateway page.

3.5.4 Click the Authentication menu of your gateway authentication setting page.

3.5.5 Customize the Guest User settings under the section "Guest User Logon Settings"

3.5.5.1 Go to Administration -> USERS & AUTHENTICATIONS -> Hosted Users

3.5.6 Click "Guest User Account" to configure the Guest to configure the Guest User Account information

Available Helps:

Deployment Setup	***Helps***
Virtual Gateway Management Guide	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/managing-internet-ga.aspx
Virtual Gateway Authentication Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/managing-internet-ga/user-authentications.aspx
Transparent Authentication	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/gateways_001/managing-internet-ga/transparent-authenti.aspx
Hosted User Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/hosted-users.aspx
Guest User Setup	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/hosted-users/guest-user-account.aspx

How to get threat protection for your Cloud Access Rule?

4 How to get the threat protection for your Cloud Access Rule?

4.1 General Description

By default, TMWS provides a default cloud access rule with default threat template. Default threat template has default threat protection settings. Different cloud access rule can share the same threat template. The default cloud access rule has no DLP template.

The cloud access rule without threat/DLP template has no threat protection. Please choose threat/DLP template for your cloud access rule to get the threat protection ability.

4.2 Manage your threat templates

4.2.1 Logon your admin console.

4.2.2 Go to Policies -> SECURITY TEMPLATES -> Threat Protection
You can add/edit/delete your threat/DLP templates here.

4.3 Customize your threat template in your Cloud Access Rule

4.3.1 Go to Policies -> Cloud Access Rules

4.3.2 Find your rule name

4.3.3 Click your rule name and go to the rule setting page.

4.3.4 Find the Action section
If you choose “Block” action with option “Block with no more actions”, you cannot choose the threat template for your rule.
“Block with no more actions” means to directly block the traffic and it does not need take further threat scanning.

4.3.5 Find the Security Templates section

4.3.6 Change the threat protection to your preferred threat template.

4.3.7 Change the data loss prevention to your preferred DLP template.

Available Helps:

Topic	***Available Helps***
Threat Protection Management Guide	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/security-templates/threat-protection.aspx
Data Loss Prevention Management Guide	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/security-templates/data-loss-prevention.aspx
Cloud Access Rule Configuration Guide	https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/cloud-access-rules/configuring-a-cloud-.aspx

What's the scanning order of the scanning policies?

5 What's the scanning order of the scanning policies?

5.1 General Description

TMWS provides rich policy types to scan the web traffic step by step. HTTP traffic and HTTPS traffic have different scanning steps.

5.2 Policy Types

The available policy types are listed in the following table. The online help documents for them are provided in the Description columns.

Table 3 Scanning Policy Types

Policy Type	***Description***
Approved URLs	Approved URLs are used to allow trustworthy web traffic. Traffic matching the Approved URLs will be allowed immediately without further scanning. Trusted web sites can be added into the Approved URLs. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/approved_blocked-url.aspx
Blocked URLs	Blocked URLs are used to block the unwanted web traffic. Traffic matching the Blocked URLs will be blocked immediately. Forbidden web sites can be added into the Blocked URLs. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/approved_blocked-url.aspx
Decryption Rules	Decryption Rules are used to decide what kind of HTTPS traffic should be decrypted for content scanning. Traffic matching the Decryption Rules will be decrypted. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/decryption-rules.aspx
HTTPS Tunnels	HTTPS Tunnels are used to decide what kind of HTTPS traffic should be bypassed directly. Traffic matches the HTTPS Tunnels will be allowed immediately without further scanning. Manually added tunneled list will never expire. System auto-added tunneled list will expire in 24 hours. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/https-tunnels.aspx
CA Certificates	CA Certificates are used to manage the trust status of CAs. Traffic matching the distrusted CAs will be blocked directly; Traffic matching the inactive CAs will be warned immediately except the user decide to continue to access the traffic; Traffic matching the trusted CAs will continue to scan other policy types. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/digital-certificates.aspx
Server Certificate Exceptions	Server Certificate Exceptions are used to manage the trust status of Server certificates. Traffic matching the blocked common names will be blocked directly; Traffic matching the warning common names will be warned immediately except the user decide to continue to access the traffic; Traffic matching the allowed common names will bypass scanning CA Certificates and continue to scan other policy types. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/digital-certificates.aspx
Cloud Access Rules	TMWS provides the uniformed cloud access rule to manage and control the company's web traffic. The cloud access rule can match the web traffic with one or more conditions to adapt the company's requirements. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/cloud-access-rules/configuring-a-cloud-.aspx.

5.3 Scan HTTP Traffic

Scanning HTTP Traffic is more straightforward as the following table shows. The HTTP traffic will be scanned by the scan-steps in order. If the scan step matches the traffic, it will take the action or go to next scan-step in the “Match” column; if it does not match the traffic, it will take the action or go to next scan-step in the “Not Match” column.

Table 4 Scanning Steps and Actions for HTTP Traffic

Scan Phases	*Scan Steps (By Order)*	*Match*	*Not Match*
Scan HTTP Content	1. URL Matches **Approved URLs**	Allow	Go to Scan Step 2. URL Matches **Blocked URLs**
	2. URL Matches **Blocked URLs**	Block	Go to Scan Step 3. Match **Cloud Access Rules** (Full)
	3. Match **Cloud Access Rules** (Full)	Refer to Table 5 Scanning Actions for Cloud Access Rules	

The following table shows how to decide the scan action of the Cloud Access Rule according to the Rule-action and the threat detection result. If the threat is detected, the system will take the action in the “Threat detected” column for the matched rules with the action in the “***Cloud Access Rule Actions”*** column; If the threat is not detected, the system will take the action in the “No threat detected” column for the matched rules with the action in the “***Cloud Access Rule Actions”*** column.

Table 5 Scanning Actions for Cloud Access Rules

Policy Match Status	*Cloud Access Rule Actions*		*Threat detected*	*No threat detected*
Matched	Allow		Block	Allow
	Block	Block with no more actions	NA	Block
		Enable warning	Block	Show warning page with “Continue” button. Allow after clicking “Continue” button.
		Enable password override	Block	Show password-required page. Allow after input correct password.
Not Matched			NA	Allow

Threat detection is not mandatory for the cloud access rule. Refer to **How to get the threat protection for your Cloud Access Rule?** For how to enable the threat detections for your Cloud Access Rules.

5.4 Scan HTTPS Traffic

Scanning HTTPS traffic is complicated than scanning HTTP traffic. It includes 5 Scanning Phases as show in the following table. The HTTPS traffic will be scanned by the scan-steps in order. If the scan step matches the traffic, it will take the action or go to next scan-step in the “Match” column; if it does not match the traffic, it will take the action or go to next scan-step in the “Not Match” column.

Table 6 Scanning Steps, Conditions and Actions for HTTPS Traffic

Scan Phases	*Scan Steps (By Order)*	*Match*	*Not Match*
Scan SNI	1. SNI Matches **Approved URLs**	Allow	Go to Scan Step 2. SNI Matches **Blocked URLs**
	2. SNI Matches **Blocked URLs**	Block	Go to Scan Step 3. SNI Matches **HTTPS Tunnels**
	3. SNI Matches **HTTPS Tunnels**	Allow	Go to Scan Step 4. CA Matches **CA Certificates**
Scan Certificates	4. CA Matches **CA Certificates**	Go to Scan Step 6. Match **Decryption Rules** if it matches the Trusted CAs; Block if it matches the Untrusted CAs;	Show warning page with “Continue” button. Go to Scan Step 6. Match **Decryption Rules** after clicking Continue;
	5. Matches **Server Certificate Exceptions**	Block for Matching Blocked Exceptions; Show warning message for matching Warn-Exceptions with “Continue” button;	Go to Scan Step 6. Match **Decryption Rules**

		Go to Scan Step 6. Match **Decryption Rules** for matching Allow- Exceptions; Go to Scan Step 6. Match **Decryption Rules** after clicking "Continue" button.	
Decryption	6. Match **Decryption Rules**	Go to Scan Step 7. URL Matches **Approved URLs**	Go to Scan Step 10. Match **Cloud Access Rules** (Conditional)
Scan Decrypted Content (Scan HTTP Content)	7. URL Matches **Approved URLs**	Allow	Go to Scan Step 8. URL Matches **Blocked URLs**
	8. URL Matches **Blocked URLs**	Block	Go to Scan Step 9. Match **Cloud Access Rules** (Full)
	9. Match **Cloud Access Rul**es (Full)	Take actions according to rule settings. Refer to Table 5 Scanning Actions for Cloud Access Rules.	
Scan Undecrypted Content	10. Match **Cloud Access Rules** (Conditional)	Take actions according to rule settings. Refer to Table 5 Scanning Actions for Cloud Access Rules.	

Match Cloud Access Rules (Conditional) means to match the WRS Score, URL Categories, Application Categories and Cloud Applications. For Application Categories, the system may not identify the Application Categories correctly if it does not decrypt the https traffic.

How to customize the Cloud Applications in the cloud access rules?

6 How to customize the Cloud Applications in the Cloud Access Rules?

6.1 General Description

Users can customize the Cloud Applications for your company. The customized Cloud Applications will work together as the part of Cloud Access Rules to match the web traffic.

6.2 Manage your Cloud App Access Sets

Manage your Cloud App Access Sets on page Policies -> OBJECTS -> Cloud App Access Sets.

Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/objects/cloud-application-ac.aspx.

6.3 Apply the Cloud Applications in your Cloud Access Rules

Choose your Cloud App Access Sets in the Traffic Types section of your Cloud Access Rules to apply them.

Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/cloud-access-rules/configuring-a-cloud-.aspx

How to allow the specific traffic in TMWS?

7 How to allow the specific traffic in TMWS?

There are some different ways to allow the specific traffic in TMWS. Read the description column in the following table to get know how to use it.

Table 7 Methods to allow specific traffic in TMWS

Method	Description
Use the **PAC file**	You add the websites into the skip-host list of the PAC file to not forward your related web traffic to TMWS. In this way, your traffic will not be blocked by TMWS. TMWS provides the function to manage your PAC files on TMWS. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/pac-files.aspx for how to manage your PAC files on TMWS.
Use the **Approved URLs**	You can add the websites into the Approved URLs of TMWS policies to directly allow the web traffic. TMWS provides the guide to manage your Approved URLs. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/approved_blocked-url.aspx
Use the **HTTPS Tunnels**	You can add the https websites into the HTTPS tunnels of TMWS policies to directly allow the web traffic. TMWS provides the guide to manage your HTTPS Tunnels. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/https-tunnels.aspx
Use the **Cloud Access Rules**	You can customize the Cloud Access Rules to directly allow the web traffic. TMWS provides the guide to manage your Cloud Access Rules. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/cloud-access-rules/configuring-a-cloud-.aspx.
Not match any policy	If your traffic does not match any policy, it will be allowed. You can focus on the policies to block the traffic and leave the other traffic allowed. Refer to **What's the scanning order of the scanning policies?** For all the available scanning policies and their scanning orders.

How to use the Customized URL Categories in the cloud access rules?

8 How to use the Customized URL Categories in the Cloud Access Rules?

8.1 General Description

Users can customize the Categories for your company. The customized URL Categories will work together with URL Categories as the part of Decryption Rules or Cloud Access Rules to match the web traffic.

8.2 Customized URL Categories.

Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/objects/customized-url-categ/configuring-a-custom.aspx

8.3 Apply the customized URL Categories in your Decryption Rules

Choose your Customized URL Categories in the Certificate section of your Decryption Rules to apply them.

Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/decryption-rules/configuring-a-decryp.aspx

8.4 Apply the customized URL Categories in your Cloud Access Rules

Choose your Customized URL Categories in the Traffic Types section of your Cloud Access Rules to apply them.

Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/cloud-access-rules/configuring-a-cloud-.aspx.

What’s the mapping relations from BC URL Categories to TMWS URL Categories? *(Internal Only, should not publish).*

9 What’s the mapping relations from BC URL Categories to TMWS URL Categories**?**
Refer to the following table for the mapping relations. Some category has no mapping while some has 2 mapping categories.

Table 8 The mapping relations between BC and TM URL Categories

Bluecoat Category	***TM Category1***	***TM Category2***
Abortion	Abortion	
Adult/Mature Content	Adult / Mature Content	
Alcohol	Alcohol / Tobacco	
Alternative Spirituality/Belief	Cult / Occult	
Art/Culture	Arts	Cultural Institutions
Auctions	Auctions	
Audio/Video Clips	Streaming Media / MP3	
Brokerage/Trading	Brokerages / Trading	
Business/Economy	Business / Economy	
Charitable Organizations	Politics	
Chat (IM)/SMS	Chat / Instant Messaging	
Child Pornography	Illegal or Prohibited Content	
Computer/Information Security	Computers / Internet	
Content Servers	Computers / Internet	
Controlled Substances	#N/A	
Dynamic DNS Host	Dynamic DNS	
E-Card/Invitations	Computers / Internet	Society / Lifestyle
Education	Education	
Email	Email	
Entertainment	Entertainment	
Extreme	Tasteless	Violence / Hate / Racism
File Storage/Sharing	Sharing Services	
Financial Services	Financial Services	
For Kids	For Kids	
Gambling	Gambling	
Games	Games	
Government/Legal	Government / Legal	
Hacking	Disease Vector	
Health	Health	
Humor/Jokes	Humor	
Informational	#N/A	
Internet Connected Devices	Computers / Internet	
Internet Telephony	Internet Telephony	
Intimate Apparel/Swimsuit	Intimate Apparel / Swimsuit	
Job Search/Careers	Job Search / Careers	

Malicious Outbound Data/Botnets	Disease Vector	
Malicious Sources/Malnets	Disease Vector	
Marijuana	Marijuana	
Media Sharing	Photo Searches	Streaming Media / MP3
Military	Military	
Mixed Content/Potentially Adult	#N/A	
News/Media	News / Media	
Newsgroups/Forums	Newsgroups / Forum	
Non-Viewable/Infrastructure	Internet Infrastructure	
Nudity	Nudity	
Office/Business Applications	Computers / Internet	
Online Meetings	Computers / Internet	
Peer-to-Peer (P2P)	Peer-to-peer	
Personal Sites	Personal Sites	
Personals/Dating	Personals / Dating	
Phishing	Phishing	
Piracy/Copyright Concerns	Illegal / Questionable	
Placeholders	#N/A	
Political/Social Advocacy	Politics	
Pornography	Pornography	
Potentially Unwanted Software	#N/A	
Proxy Avoidance	Proxy Avoidance and Anonymizers	
Radio/Audio Streams	Internet Radio and TV	Streaming Media / MP3
Real Estate	Real Estate	
Reference	Reference	
Religion	Religion	
Remote Access Tools	Computers / Internet	
Restaurants/Dining/Food	Restaurants / Food	
Scam/Questionable/Illegal	Scam	
Search Engines/Portals	Search Engines / Portals	
Sex Education	Sex Education	
Sexual Expression	#N/A	
Shopping	Shopping	
Social Networking	Social Networking	
Society/Daily Living	Society / Lifestyle	
Software Downloads	Ringtones / Mobile Phone Downloads	Software Downloads
Spam	Spam	
Sports/Recreation	Recreation / Hobbies	Sports
Suspicious	#N/A	
TV/Video Streams	Internet Radio and TV	Streaming Media / MP3
Technology/Internet	Computers / Internet	

Tobacco	Alcohol / Tobacco	
Translation	Translators / Cached Pages	
Travel	Travel	
Vehicles	Vehicles	
Violence/Hate/Racism	Violence / Hate / Racism	
Weapons	Weapons	
Web Ads/Analytics	Web Advertisements	
Web Hosting	Web Hosting	

How to chain TMWS decryption CA into your company’s trust CAs?

10 How to chain TMWS decryption CA into your company’s trust CAs?

10.1 General Description

TMWS provides the default CA for HTTPS decryption. By default, the decrypted traffic’s server certificate will be signed by the TMWS default CA.

You can cross sign your TMWS CA to chain our CA as the subordinary CA of your company trust CAs. With this way your clients, which installs your company’s trust CAs, can trust TMWS CA without deploying TMWS CA into your system.

10.2 Cross sign TMWS default CA

TMWS provides the helps to guide you how to cross sign TMWS default CA with your company’s CA.
Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/decryption-rules/configuring-a-decryp/cross-signing-the-ca.aspx

10.3 Customize the CA in your Decryption Rules

Configure your decryption policy and replace the CA. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/decryption-rules/configuring-a-decryp.aspx

How to manage HTTPS Tunnels?

11 How to manage HTTPS Tunnels?

11.1 General Description

TMWS provides several ways to allow specific web traffic. HTTPS Tunnels is one way to allow the HTTPS traffic. Refer to **How to allow the specific traffic in TMWS?** for the complete description of ways to allow your web traffic.

TMWS provides the guide to manage your HTTPS Tunnels. Refer to https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/policies_001/https-inspection/https-tunnels.aspx

Refer to **What's the scanning order of the scanning policies?** For all the available scanning policies and their scanning orders.

11.2 How to turn on Auto Tunnel

The system can automatically add the websites into the HTTPS Tunnels to get the better business continuity if you turn on Auto Tunnel.

11.2.1 Go to Policies -> Global Settings -> HTTPS Inspection
Enable HTTPS Inspection.
Enable HTTPS Tunneling.

11.2.2 Policies -> HTTPS INSPECTION -> HTTPS Tunnels -> Failed HTTPS Access
Enable auto tunneling for fatal failures

How to implement the HA of TMWS on-premises?

12 General Description

Here provide several ways to implement TMWS on-premises failover or load balance, including DNS round robin, Intelligent DNS, Multiple on-premises in PAC file and use "Load Balance Device".

Table 9 HA Methods

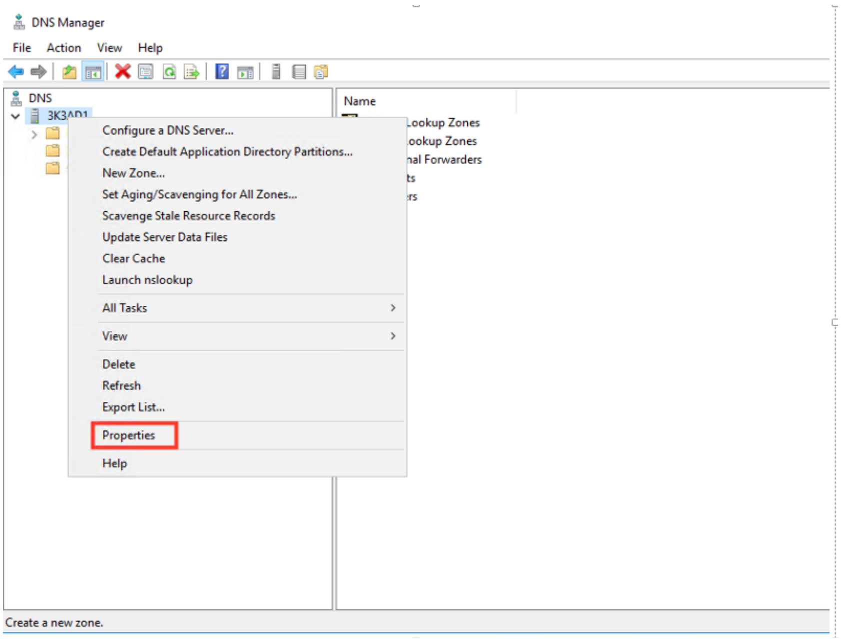
HA Method	*Description*	*Supported deployment modes*
DNS round robin	Simply provide a method of distributing to different on-premises based on the result of hostname resolution.	1. Forward Proxy Mode 2. ICAP Mode
Intelligent DNS	Provide a method to return different DNS resolution results based on different IP address segments.	1. Forward Proxy Mode 2. ICAP Mode
Multiple on-premises in PAC file	Based on standard PAC files, realize TMWS on-premises failover and simple IP address-based traffic distribution.	1. Forward Proxy Mode
Load Balance Device	Load balancing of TMWS on-premises based on Load Balance Devices	1. Forward Proxy Mode 2. ICAP Mode

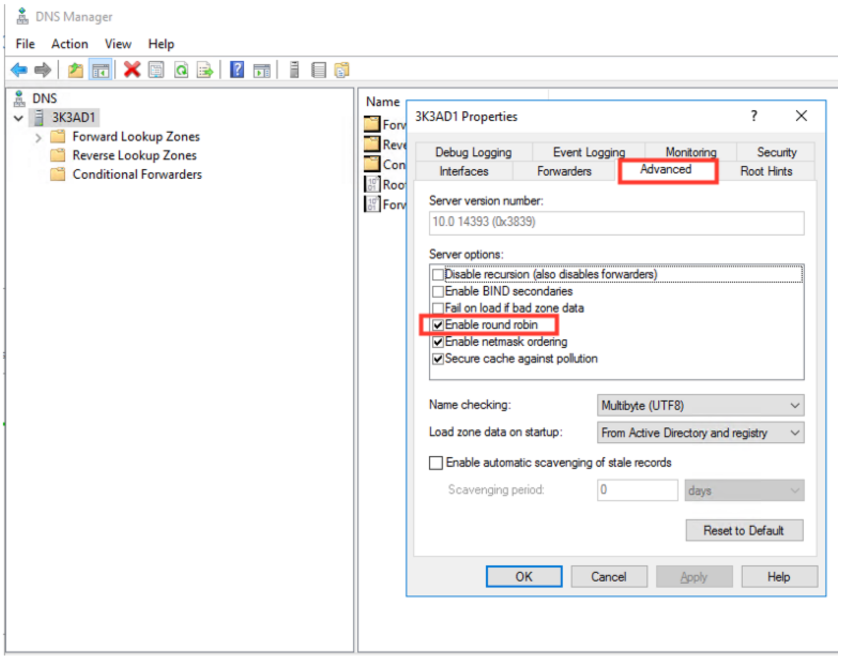
Before implementing HA, you need to ensure that the configuration of each TMWS on-premises are consistent.

12.1 How to Enable DNS round robin on your DNS server?

This chapter introduces how to configure DNS round robin on the DNS server, taking windows server 2016 as an example. Please note that you must be a member of the Domain Admins, Enterprise Admins, or the DNS Admins group to complete this procedure.

12.1.1 Login on the windows server 2016, which the DNS server has already been installed.
12.1.2 Click Start, point to Administrative Tools, and click DNS.
12.1.3 Right click on DNS zone and go to properties, Enable round robin.





Server version number: 10.0 14393 (0x3839)

Server options:

- ☐ Disable recursion (also disables forwarders)
- ☐ Enable BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

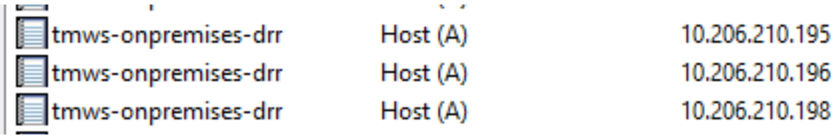
Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

12.1.4 Add each TMWS on-premises address record in the DNS Forward Lookup Zone, each record has the same hostname and different IP address.



tmws-onpremises-drr	Host (A)	10.206.210.195
tmws-onpremises-drr	Host (A)	10.206.210.196
tmws-onpremises-drr	Host (A)	10.206.210.198

12.2 How to Enable Intelligent DNS on your DNS server?

This chapter introduces how to configure Intelligent DNS on the windows server 2016, and return resolution address information based on the requested IP address segment. According to the official Microsoft documentation, Intelligent DNS is only supported in windows server 2016 and later versions.

12.2.1 Planning address range and server information, example:

ENV	DNS zone	Hostname	IP	Location	Clients Subnet

TMWS on-premises 1	3k3alpha.com	tmws-onpremises-195.3k3alpha.com	10.206.210.195	1st Floor	10.206.210.0/24
TMWS on-premises 2		tmws-onpremises-196.3k3alpha.com	10.206.210.196	2nd Floor	10.206.199.0/24
...					
TMWS on-premises N		tmws-onpremises-xxx.3k3alpha.com	x1.x2.x3.x4	Nth Floor	a.b.c.d/x

12.2.2 Login on the windows server 2016, which the DNS server has already been installed.

12.2.3 Open the windows PowerShell, run the following commands:

12.2.3.1 Create and check the subnet for all the floors

```
Add-DnsServerClientSubnet -Name "1stFloorSubnet" -IPv4Subnet "10.206.210.0/24"
Add-DnsServerClientSubnet -Name "2ndFloorSubnet" -IPv4Subnet "10.206.199.0/24"
… Change parameters, repeat configuration
Add-DnsServerClientSubnet -Name "NthFloorSubnet" -IPv4Subnet "a.b.c.d/x"
```

12.2.3.2 Create and check dns server zone scope

```
Add-DnsServerZoneScope -ZoneName "3k3alpha.com" -Name "1stFloor"
Add-DnsServerZoneScope -ZoneName "3k3alpha.com" -Name "2ndFloor"
… Change parameters, repeat configuration
Add-DnsServerZoneScope -ZoneName "3k3alpha.com" -Name "NthFloor"
```

12.2.3.3 Create host records for the scopes

```
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "10.206.210.195" -ZoneScope "1stFloor"
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "10.206.210.196" -ZoneScope "2ndFloor"
… Change parameters, repeat configuration
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "x1.x2.x3.x4" -ZoneScope "NthFloor"
```

12.2.3.4 Create host records for default scope

```
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "10.206.210.195"
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "10.206.210.196"
… Change parameters, repeat configuration
Add-DnsServerResourceRecord -ZoneName "3k3alpha.com" -A -Name "tmws-onpremises" -IPv4Address "x1.x2.x3.x4"
```

12.2.3.5 Create and check DNS return policy

```
Add-DnsServerQueryResolutionPolicy -Name "1stFloorPolicy" -Action ALLOW -ClientSubnet "eq,1stFloorSubnet" -ZoneScope "1stFloor,1" -ZoneName "3k3alpha.com"
Add-DnsServerQueryResolutionPolicy -Name "2ndFloorPolicy" -Action ALLOW -ClientSubnet "eq,2ndFloorSubnet" -ZoneScope "2ndFloor,1" -ZoneName "3k3alpha.com"
… Change parameters, repeat configuration
Add-DnsServerQueryResolutionPolicy -Name "NthFloorPolicy" -Action ALLOW -ClientSubnet "eq,NthFloorSubnet" -ZoneScope "NthFloor,1" -ZoneName "3k3alpha.com"
```

12.2.4 Try to resolve the Hostname of TMWS on-premises on different clients, you can see that the addresses obtained by clients belonging to different subnets are inconsistent

12.3 How to add Multiple on-premises in PAC file?

This chapter introduces how to add multiple TMWS on-premises to the PAC file to achieve failover or load balancing based on IP address segments.

Before you start, you must read the TMWS online help, and be familiar with the use of PAC files. Refer to: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/pac-files.aspx

12.3.1 Multiple on-premises in PAC file implementation TMWS on-premises failover.

12.3.1.1 Planning TMWS on-premises hostname

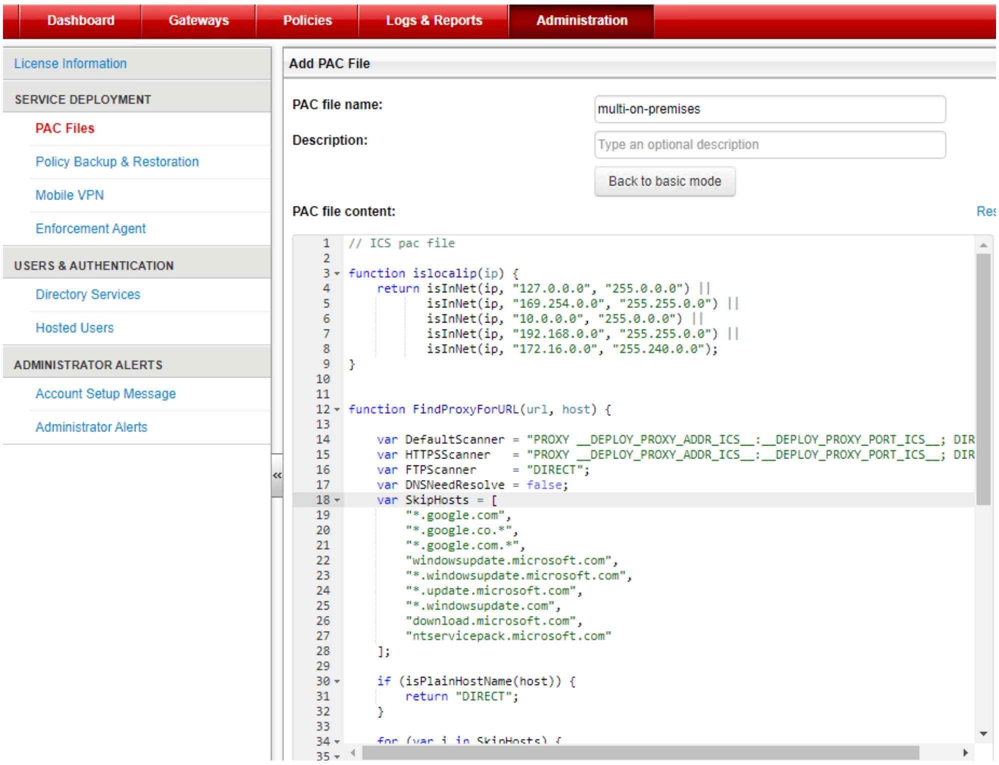
TMWS on-premises	Host Name
on-premises 1	tmws-onpremises-195.3k3alpha.com
on-premises 2	tmws-onpremises-196.3k3alpha.com
…	
on-premises N	xxx.3k3alpha.com

12.3.1.2 Logon your admin console.

12.3.1.3 Go to Administration ->SERVICE DEPLOYMENT ->PAC Files

12.3.1.4 Add a new PAC file.

12.3.1.5 Edit the PAC file in advanced mode



Add PAC File

PAC file name: multi-on-premises

Description: Type an optional description

PAC file content:

```
// ICS pac file

function islocalip(ip) {
    return isInNet(ip, "127.0.0.0", "255.0.0.0") ||
           isInNet(ip, "169.254.0.0", "255.255.0.0") ||
           isInNet(ip, "10.0.0.0", "255.0.0.0") ||
           isInNet(ip, "192.168.0.0", "255.255.0.0") ||
           isInNet(ip, "172.16.0.0", "255.240.0.0");
}


function FindProxyForURL(url, host) {

    var DefaultScanner = "PROXY __DEPLOY_PROXY_ADDR_ICS__:__DEPLOY_PROXY_PORT_ICS__; DIR
    var HTTPSScanner   = "PROXY __DEPLOY_PROXY_ADDR_ICS__:__DEPLOY_PROXY_PORT_ICS__; DIR
    var FTPScanner     = "DIRECT";
    var DNSNeedResolve = false;
    var SkipHosts = [
        "*.google.com",
        "*.google.co.*",
        "*.google.com.*",
        "windowsupdate.microsoft.com",
        "*.windowsupdate.microsoft.com",
        "*.update.microsoft.com",
        "*.windowsupdate.com",
        "download.microsoft.com",
        "ntservicepack.microsoft.com"
    ];

    if (isPlainHostName(host)) {
        return "DIRECT";
    }

    for (var i in SkipHosts) {
```

12.3.1.6 Replace the "DefaultScanner" and "HTTPSScanner" with the following

"PROXY tmws-onpremises-1.3k3alpha.com:8080; tmws-onpremises-2.3k3alpha.com:8080; DIRECT"

12.3.1.7 Edit other configurations as needed.

12.3.1.8 Save the new PAC file.

12.3.1.9 Refer to this section of the online help: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/pac-files/traffic-forwarding-u.aspx, To deploy PAC file.

12.3.2 Multiple on-premises in PAC file to achieve load balancing based on source IP.

12.3.2.1 Plan the correspondence between TMWS on-premises and client IP addresses

TMWS on-premises	Host Name	IP segment

on-premises 1	tmws-onpremises-1.3k3alpha.com	189.190.1.0/24
on-premises 2	tmws-onpremises-2.3k3alpha.com	189.190.2.0/24
…		
on-premises N	xxxxxx-N.3k3alpha.com	x.x.x.x/y

12.3.2.2 Logon your admin console.

12.3.2.3 Go to Administration ->SERVICE DEPLOYMENT ->PAC Files

12.3.2.4 Add a new PAC file.

12.3.2.5 Edit the PAC file in advanced mode.

12.3.2.6 Replace the “DefaultScanner” and “HTTPSScanner” with the following:

```
if (isInNet(myIpAddress(), "189.190.1.0", "255.255.255.0"))
    var DefaultScanner = "PROXY tmws-onpremises-1.3k3alpha.com:8080; tmws-onpremises-2.3k3alpha.com:8080; DIRECT";
    var HTTPSScanner   = "PROXY tmws-onpremises-1.3k3alpha.com:8080; tmws-onpremises-2.3k3alpha.com:8080; DIRECT";
if (isInNet(myIpAddress(), "189.190.2.0", "255.255.255.0"))
    var DefaultScanner = "PROXY tmws-onpremises-2.3k3alpha.com:8080; tmws-onpremises-1.3k3alpha.com:8080; DIRECT";
    var HTTPSScanner   = "PROXY tmws-onpremises-2.3k3alpha.com:8080; tmws-onpremises-1.3k3alpha.com:8080; DIRECT";
```

12.3.2.7 Edit other configurations as needed.

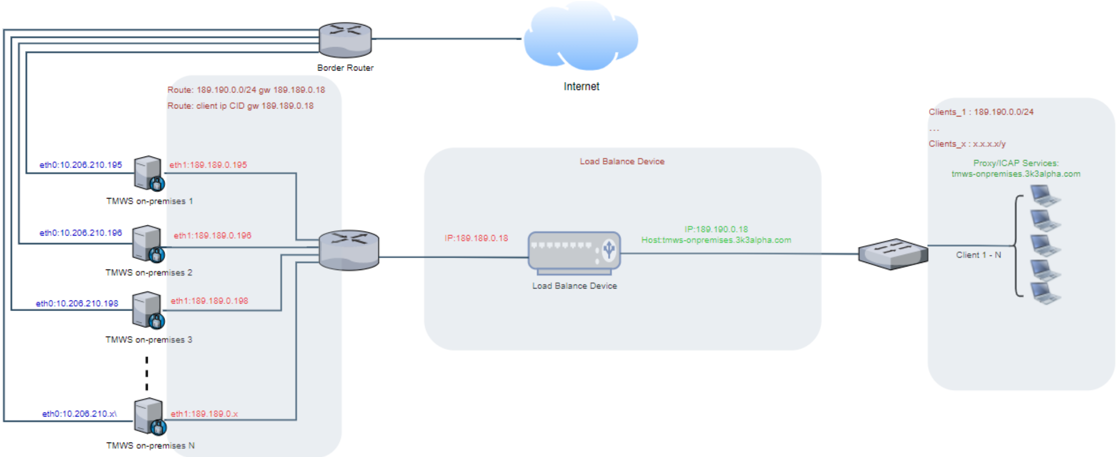
12.3.2.8 Save the new PAC file.

12.3.2.9 Refer to this section of the online help: https://docs.trendmicro.com/en-us/enterprise/trend-micro-web-security-online-help/administration_001/pac-files/traffic-forwarding-u.aspx, To deploy PAC file.

12.4 How to Enable Load Balance with Load Balance Device?

Customers can use some load balanc device to achieve TMWS on-premises load balancing. load balance devices like: LVS+keeplived, HAProxy, ext.

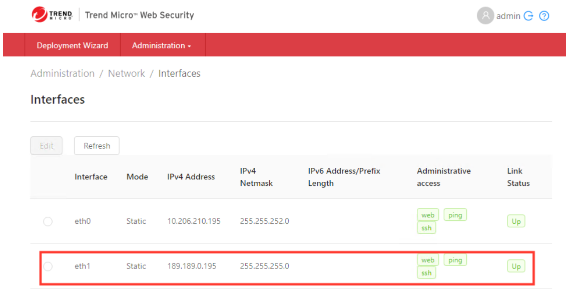
12.4.1 Network logic topology



12.4.2 Add a new network adapter for each TMWS on-premises.

12.4.3 Login on each TMWS on-premises admin portal.

12.4.4 Go to Administration->Network->Interfaces, set the IP address of the new NIC

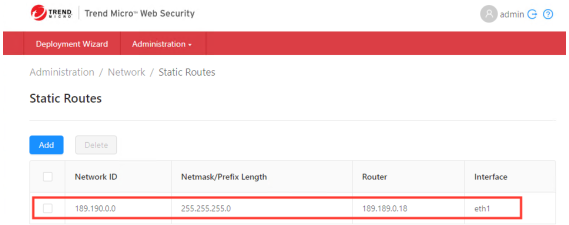


Administration / Network / Interfaces

Interfaces

	Interface	Mode	IPv4 Address	IPv4 Netmask	IPv6 Address/Prefix Length	Administrative access	Link Status
○	eth0	Static	10.206.210.195	255.255.252.0		web ping ssh	Up
○	eth1	Static	189.189.0.195	255.255.255.0		web ping ssh	Up

12.4.5 Go to Administrator->Network->Static Routes, add the static routes to clients


Trend Micro™ Web Security
admin
Deployment Wizard
Administration
Administration / Network / Static Routes
Add
Delete

Static Routes

□	Network ID	Netmask/Prefix Length	Router	Interface
□	189.190.0.0	255.255.255.0	189.189.0.18	eth1

12.4.6 Repeat the above steps, set all the TMWS on-premises.

12.4.7 Configure the load balance device, add the load balancing strategy, and provide the service address to the client as the Proxy/ICAP services address.