Mandiant

EMAIL THEATER

Email Theater Overview

The Mandiant Advantage Security Validation (MA-SV) Email Theater is an advanced feature that extends the capabilities of the platform. Email Theater lets you validate and tune email security tools, such as Office 365, Proofpoint, Symantec, Mimecast, and Cisco Email Security Appliance (ESA) or Cloud Email Security (CES).

This may be licensed separately from the main Security Validation platform. If you are uncertain if you have it available, contact your administrator, TSC, or **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.

Your email controls are designed to stop inbound phishing, emails containing malware, and data leaving the production IT environment. Email Theater uses a dedicated email account to send threats, like malware and spearphishing links, into the enterprise and send sensitive information, like PII and PCI data, out of the enterprise to test your email controls using a Network Actor.

Setting up Email Theater comprises the following steps:

1. Configure and test Email settings for the Director (see **Email Settings (https://docs.mandiant.com/home/email-settings)**).
2. Add at least one Email Profile (see **Email Profiles (https://docs.mandiant.com/home/msv-email-actions-settings#profiles)**).
3. Add at least one Email Rule (see **Email Rules (https://docs.mandiant.com/home/msv-email-actions-settings#profiles)**).
4. Add Email Actions (see **Creating Email Actions (https://docs.mandiant.com/home/msv-adding-email-actions)**).
5. Run Email Actions (see **Running Email Actions (https://docs.mandiant.com/home/msv-running-email-actions)**).

Supported Protocols

Email Theater Before You Begin

Before you begin to configure Email Theater, gather the following information. You will need these values when setting up email profiles in the Director.

NOTE: The email settings also must be configured and could use the same outgoing email server or Microsoft Office 365 Graph API. For more information, see **Configuring Email Settings for Office 365 with Graph API (https://docs.mandiant.com/home/msv-email-settings-for-common-email-providers#Configur2)**.

Description	Value
Email Theater license	**Location of license file:**

Description	Value
Director host information	**Hostname:** **IP address:**
Email account to be used for sending email and notifications from Director	**Email address:**
Outgoing email server (not applicable to Microsoft Office 365 Graph API)	**Server address:** **Server port:** **Use Encryption?: If yes, tls or ssl?** **Use Authentication?:** yes or no **Authentication Type:** (Plain or NTLM)
Incoming email server (not applicable to Microsoft Office 365 Graph API)	**Server address** **Server port:** **Authentication type:** Plain or NTLM
Account (must be the same on both the incoming and outgoing email servers; not applicable to Microsoft Office 365 Graph API)	**Username:** **Password:** **NOTE:** If you are using two-factor authentication, you may need an application-specific password from your email provider, instead of the regular password for the email address.See **Email Settings for Common Email Providers (https://docs.mandiant.com/home/msv-email-settings-for-common-email-providers)** for more information.
Email addresses to be used for Email Actions	**Email address:** **Email address:** **Email address:**

The following parameters are required for the Microsoft Office 365 Graph API security protocol:

- **Tenant ID** - Unique ID assigned to the Azure AD tenant the email account/profile belongs to
- **Client ID** - Unique ID assigned to the application that must be created in Azure. Represents the Email Theater

application in the Azure tenant

- **Client Secret** (as created for the application) - Expiring value that is created in the Azure UI
  For more information, see **Email Settings for Common Email Providers** **(https://docs.mandiant.com/home/msv-email-settings-for-common-email-providers)**.

If you want to test the effectiveness of DNS-based email security controls, you may have to configure DKIM, SPF, and DMARC records for the email source domain. Some scenarios include:

Email Setup to Test	Required Configuration
SPF blocking	Requires an email domain without SPF records
DKIM blocking	Requires an email domain without DKIM
DMARC blocking	Requires an email domain with SPF, DKIM, and DMARC
Combination of the 3 above	Requires SPF, DKIM, and DMARC to be configured
Malware is stopped	If there's a combination of SPF/DKIM blocking enabled, may require SPF and DKIM to be configured for email to flow correctly

There are many different ways to complete the above configurations, so refer to either your email provider or your email software's documentation.