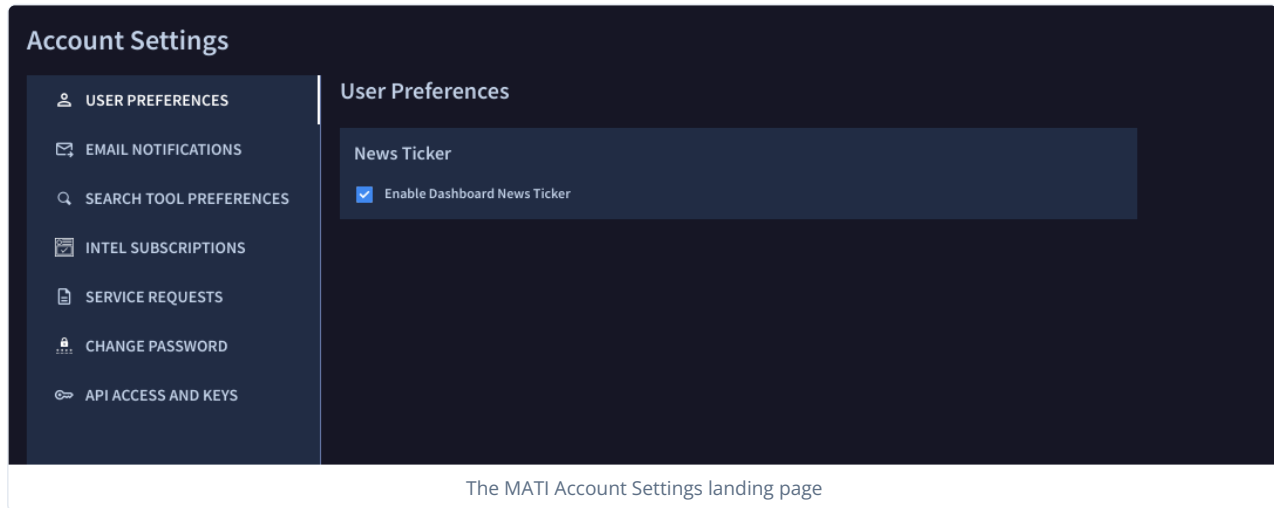


## MANAGE THREAT INTELLIGENCE ACCOUNT SETTINGS

Click **Account Settings** to manage your account settings in Mandiant Advantage Threat Intelligence (MATI). Scroll to the desired section or select it from the navigation bar.



### User Preferences

The Enable Dashboard News Ticker checkbox is checked by default to display the latest Threat Activity Alerts released by Mandiant. To disable this feature, deselect the checkbox.

### Email Notifications

Click **Email notifications > Add Email Notifications** to configure your email delivery preferences. You can choose to receive the specific notifications that are important to you.

The following settings are available in each of the email notification options:

- **Name:** Required free-text field for the digest name.
- **Frequency:** Optional **Daily** or **Hourly** delivery.
- **Mailing To:** Autopopulated with the email address used to log into MATI.
- **Daily Delivery Preferences:** Select days of the week, **Delivery Time**, and **Timezone** for delivery.

The other settings you configure depend on the notification type that you choose:

- **Report Digest:** Sign up for our email digest to get the latest news analysis and reports in your inbox
  - **Report Type:** Choose any of the following report types that you want included in the digest, or select **All** to include all of them:
    - **Actor Overview**
    - **Actor Profile**
    - **Country Profile**
    - **Event Coverage/Implication**
    - **Executive Perspective**
    - **ICS Security Roadmap**
    - **Industry Reporting**
    - **Malware Overview**
    - **Malware Profile**

- **Network Activity reports**
  - **News Analysis**
  - **Patch Report**
  - **Tactical Threat Report**
  - **Threat Activity Report**
  - **Trends and Forecasting**
  - **TTP Deep Dive**
  - **Weekly Vulnerability Exploitation Report**
- **Threat Profile Digest:** Sign up for our threat profile digest to get the latest, personalized threat updates in your inbox. This option is only available if you've created at least one Threat Profile.
    - **Threat Profile:** Choose a threat profile to include in the digest. For more information about configuration threat profiles, see **Build a Personalized Threat Landscape** (<https://docs.mandiant.com/home/mati-threat-profiles>).
  - **Vulnerability Digest:** Sign up to get the latest vulnerability updates in your inbox.
    - **Risk Rating:** Choose a risk rating or select **All** to include all of them:
      - **Critical**
      - **High**
      - **Medium**
      - **Low**



- The Vulnerability Digest notifications focus on new vulnerabilities and risk rating changes, excluding minor vulnerability updates.
- See **Vulnerability Intelligence Reporting Overview** (<https://docs.mandiant.com/home/vulnerability-intelligence-reporting-overview>) for more information on risk ratings.

## Search Tool Preferences

You can specify your default search tool for MATI:

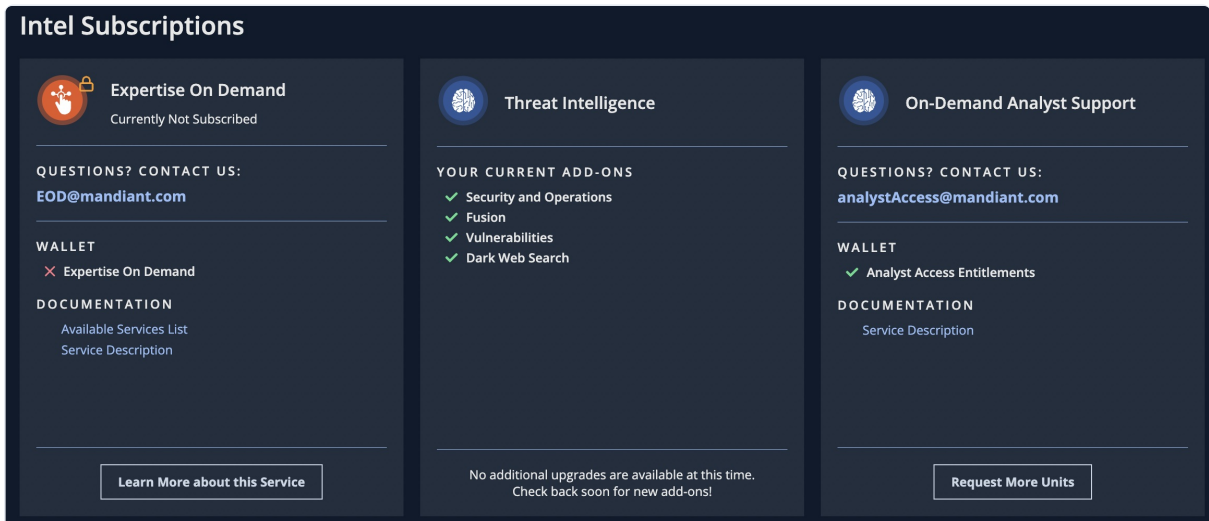
- **Keyword Search:** This is the default, keyword-based search option for MATI.
- **Gemini Search:** Gemini in Threat Intelligence gives you natural language searches, LLM-generated summaries, and follow-up questions to narrow down relevant information.

## Intel Subscriptions

Subscribe to additional Threat Intelligence services including the following:

- **Expertise On Demand** (<https://docs.mandiant.com/home/eod-service-description>): Access to a range of Mandiant expertise, including Threat Intelligence data, technical analysis, Mandiant Incident Response, consulting services, and training courses led by our subject-matter experts.
  - May include an Incident Response Retainer with a Service-Level Agreement (SLA) for expedited response and Mandiant's Incident Response Preparedness Service (IRPS).
- **Threat Intelligence** (<https://docs.mandiant.com/home/intelligence-subscriptions>):
  - **Security and Operations:** Aligned to the needs of a Security Operations Center (SOC) with common use cases related to monitoring and detection of cyber threats. It provides access to finished intelligence reporting and threat data relevant to those use cases and adversary tactics, techniques, and procedures (TTPs).
  - **Fusion:** Provides full access to all available Mandiant Threat Intelligence, delivering analysis and visibility into ongoing, past, and predictive threat activity.

- **Vulnerabilities:** Provides access to Mandiant Threat Intelligence reporting and near real-time intelligence related to vulnerabilities and their exploitation.
- **Dark Web Search** (also called Digital Threat Monitoring (DTM)): Provides enhanced situational awareness of your digital footprint to help identify breaches, exposures, and digital threats across the deep and dark web. Offered as a standalone subscription, Managed Service, or a Digital Threat Assessment delivered as a one-time report after 30 days of monitoring.
- **OnDemand Analyst Support** (<https://docs.mandiant.com/home/on-demand-intelligence-access-service-description>): Remotely delivered service for which our expert analyst team provides subscribing customers with succinct, tailored artifacts that answer their questions related to cyber threats.



**Intel Subscriptions**

**Expertise On Demand**  
Currently Not Subscribed

QUESTIONS? CONTACT US:  
[EOD@mandiant.com](mailto:EOD@mandiant.com)

WALLET  
✗ Expertise On Demand

DOCUMENTATION  
[Available Services List](#)  
[Service Description](#)

[Learn More about this Service](#)

**Threat Intelligence**

YOUR CURRENT ADD-ONS

- ✓ Security and Operations
- ✓ Fusion
- ✓ Vulnerabilities
- ✓ Dark Web Search

No additional upgrades are available at this time.  
Check back soon for new add-ons!

**On-Demand Analyst Support**

QUESTIONS? CONTACT US:  
[analystAccess@mandiant.com](mailto:analystAccess@mandiant.com)

WALLET  
✓ Analyst Access Entitlements

DOCUMENTATION  
[Service Description](#)

[Request More Units](#)

Threat Intelligence subscriptions and add-ons

## Service Requests

If your subscription includes access to Expertise on Demand (EOD) or On-Demand Analyst Support (Ask an Analyst), any support requests associated with those services will be displayed here.



Please click on the case number to add comments and view case details.

Service Requested	Summary	Case Number	Date Requested	Date Completed	Status
Analyst Investigation	TESTAAFORM NAD_AI	00171784	Sep 25, 2023	---	In Progress
Query	TESTAAFORM AI_NAD2	00156551	Dec 7, 2022	---	In Progress
Query	TESTAAFORM AI_NAD	00156550	Dec 7, 2022	---	In Progress

Service Requests table

## Change Password

To reset your password, perform the following:

1. Click the provided hyperlink to <https://login.mandiant.com/settings>.
2. Enter your current password.
3. Enter and re-enter your new password, adhering to the password requirements.
4. Click **Update**.

**Change Password**

Current Password:

New Password:

Retype New Password:

**Passwords:**  
must contain at least one uppercase letter  
must contain at least one lowercase letter  
must contain at least one number  
must be a minimum of 10 and maximum of 64 characters  
must contain special characters (such as @, !, #, %, \$, etc)

## API Access and Keys



To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support** (<https://www.mandiant.com/support>).

To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.