# Table of Contents

**User Guide** .................................................................................................................. 8  
Connect to Tenable.ad ........................................................................................................ 11  
Set Your Profile Preferences ............................................................................................. 13  
Navigate the Interface ........................................................................................................ 16  
Left Navigation Bar ........................................................................................................... 17  
Top Navigation Bar ........................................................................................................... 19  
Interactive Elements ......................................................................................................... 26  
Dashboard and Widgets Overview ....................................................................................... 27  
Create a Dashboard ............................................................................................................ 31  
Working with Widgets .......................................................................................................... 32  
Configure Datasets for Widgets ......................................................................................... 34  
Delete a Dashboard ............................................................................................................ 37  
Topology Graph Overview ................................................................................................. 38  
Filter Forests and Domains ............................................................................................... 42  
Understand Trust Relationships Color Code .................................................................. 43  
Display Trust Relationships Attributes .......................................................................... 44  
Investigate Dangerous Trusts ........................................................................................... 46  
Trail Flow Overview ......................................................................................................... 48  
View the Real-Time Monitoring of Your AD Infrastructures ........................................... 51  
Pause and Restart the Trail Flow ....................................................................................... 55  
Filter the Real-Time Flow of Events ................................................................................ 57  
Run a Search in the Trail Flow ........................................................................................... 58
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Indicators of Exposure</td>
<td>149</td>
</tr>
<tr>
<td>View Indicators of Exposure</td>
<td>156</td>
</tr>
<tr>
<td>Retrieve an IoE from the List</td>
<td>159</td>
</tr>
<tr>
<td>View Indicator Details</td>
<td>164</td>
</tr>
<tr>
<td>Filter Deviant Objects</td>
<td>172</td>
</tr>
<tr>
<td>Retrieve a Deviant Object with the Wizard</td>
<td>173</td>
</tr>
<tr>
<td>Retrieve Deviant Object Manually</td>
<td>180</td>
</tr>
<tr>
<td>Ignore a Deviant Object</td>
<td>183</td>
</tr>
<tr>
<td>View Incriminating Attributes</td>
<td>192</td>
</tr>
<tr>
<td>Export Deviant Objects Report</td>
<td>198</td>
</tr>
<tr>
<td>Administrator Guide</td>
<td>200</td>
</tr>
<tr>
<td>Getting Started</td>
<td>201</td>
</tr>
<tr>
<td>Understand Indicators of Attack</td>
<td>203</td>
</tr>
<tr>
<td>How the IoA Engine Works</td>
<td>204</td>
</tr>
<tr>
<td>Deploy Indicators-of-Attack</td>
<td>205</td>
</tr>
<tr>
<td>ETW Data Retrieval by Tenable.ad</td>
<td>211</td>
</tr>
<tr>
<td>Tenable.ad Indicators of Attack</td>
<td>212</td>
</tr>
<tr>
<td>OS Credential Dumping: LSASS Memory</td>
<td>213</td>
</tr>
<tr>
<td>DCSHadow</td>
<td>214</td>
</tr>
<tr>
<td>DCSync</td>
<td>215</td>
</tr>
<tr>
<td>GoldenTicket</td>
<td>216</td>
</tr>
<tr>
<td>Petit-Potam</td>
<td>217</td>
</tr>
<tr>
<td>Password Guessing</td>
<td>218</td>
</tr>
<tr>
<td>Password Spraying</td>
<td>219</td>
</tr>
</tbody>
</table>
Potential Impacts on your AD Infrastructures .......................................................... 220
Technical Prerequisites .................................................................................................. 221
Install the Tenable.ad IoA Module .................................................................................. 222
Configuration Adaptations .............................................................................................. 224
Limitation and Potential Impacts .................................................................................... 226
Uninstall the Tenable.ad IoA Module .............................................................................. 227
Update the Tenable.ad IoA Module .................................................................................. 228
Microsoft Sysmon ............................................................................................................ 229
MicrosoftSysmonEvents ................................................................................................. 230
Microsoft Sysmon Usage ................................................................................................. 234
Manual Deployment on DCs (optional) ............................................................................ 242
Manage Accounts ........................................................................................................... 244
Manage User Accounts .................................................................................................... 245
Define User Authentication .............................................................................................. 247
Configure LDAP Authentication ....................................................................................... 249
Configure SAML Authentication ....................................................................................... 253
Update SAML Authentication ............................................................................................ 259
Export SAML Metadata .................................................................................................... 260
Lockout Policy .................................................................................................................. 262
Troubleshoot Authentication Issues ................................................................................ 268
Manage Security Profiles ................................................................................................. 270
Create a Security Profile .................................................................................................. 273
Customize a Security Profile ............................................................................................ 275
Refine the Security Profile Customization ....................................................................... 277
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the Severity Level of an Indicator</td>
<td>279</td>
</tr>
<tr>
<td>Save the Customization as Draft</td>
<td>280</td>
</tr>
<tr>
<td>Apply the Customization</td>
<td>281</td>
</tr>
<tr>
<td>Revert a Pending Customization</td>
<td>283</td>
</tr>
<tr>
<td>Restrict Application to Certain Directories</td>
<td>284</td>
</tr>
<tr>
<td>Apply a Security Profile to a Workspace</td>
<td>285</td>
</tr>
<tr>
<td>Manage Access Control</td>
<td>286</td>
</tr>
<tr>
<td>Customize a Role with Permissions</td>
<td>290</td>
</tr>
<tr>
<td>Entity Permissions Type</td>
<td>292</td>
</tr>
<tr>
<td>Example of Changing Interface Entities Settings</td>
<td>297</td>
</tr>
<tr>
<td>Grant or Deauthorize Permissions</td>
<td>303</td>
</tr>
<tr>
<td>Display Only Granted Permissions</td>
<td>307</td>
</tr>
<tr>
<td>Manage Forests</td>
<td>309</td>
</tr>
<tr>
<td>Manage Domains</td>
<td>312</td>
</tr>
<tr>
<td>Add an External Certificate</td>
<td>316</td>
</tr>
<tr>
<td>Define Attack Scenarios</td>
<td>317</td>
</tr>
<tr>
<td>Delete Objects</td>
<td>319</td>
</tr>
<tr>
<td>Configure Alerts</td>
<td>320</td>
</tr>
<tr>
<td>Define the SMTP Configuration</td>
<td>321</td>
</tr>
<tr>
<td>Add New Email Alerts</td>
<td>323</td>
</tr>
<tr>
<td>Manage Email Alerts</td>
<td>328</td>
</tr>
<tr>
<td>Add Syslog Alerts</td>
<td>333</td>
</tr>
<tr>
<td>Manage Syslog Alerts</td>
<td>339</td>
</tr>
<tr>
<td>Understand Syslog and Email Alert Details</td>
<td>342</td>
</tr>
</tbody>
</table>
Introduction to Tenable.ad

Tenable.ad packs a solid set of features to allow you to anticipate threats, detect breaches, and respond to incidents and attacks.

These protections are available depending on the license that you have purchased.

Trail Flow
Your new Active Directory (AD) security solution continuously monitors your infrastructure and detects regressions as they happen.

Using an intuitive dashboard, you identify at a glance the most critical vulnerabilities and their recommended courses of remediation.

**Indicators of Attack**

Tenable.ad 3.x User and Administrator Guide Indicators of Attack (IoA) help your Blue Team detect and take immediate action when the most advanced techniques attempt to compromise your AD infrastructures.

These IoAs need your infrastructures to share information with Tenable.ad in a seamless and non-intrusive way. There is no third-party software deployed, and the setup process only requires a one-time administrative action.

From a security standpoint, IoAs aim to:

- Uncover major security incident in your Active Directory infrastructure
- Visualize each threat from an accurate attack timeline
- Consolidate attack distribution in a single view
- Make the link between AD changes and malicious actions
- Analyze in-depth details of an AD attack
- Explore MITRE ATT&CK® description directly from the incident

Tenable.ad's features are based on the license type. Your license may or may not include Indicators of Attack.

**Indicators of Exposure**

Our Indicators of Exposure (IoE) are behavioral detection indicators. Tenable.ad builds IoEs from technical indicators (IOCs) and tactics, techniques, and procedures (commonly referred as TTPs), and disseminate them to your platforms transparently to ensure an up-to-date detection capability.

From a security standpoint, IoEs aim to:
• Harden your AD, so that it becomes more resilient to potential attacks.

• Detect breaches in real time, so that your teams can react to them as soon as humanly possible.

• Accelerate remediation of AD incidents to contain your attackers before they succeed.

From a usability point of view, Tenable.ad's product design ensures that:

• Roll-out efforts and management overheads are negligible.

• Tenable.ad does not create any additional risks for your infrastructure because of its operations or access levels.

• Tenable.ad ensures full transparency on the actions conducted by our solution.

Remediation tactics

Tenable.ad tightly integrates into your defensive workflows. Most notably, alerts automatically populate your IT Service Management (ITSM) tool to give your response team informative notifications in real time. If you also use a response orchestrator, Tenable.ad provides remediation playbooks and triggers them dynamically according to the detected incident.
Connect to Tenable.ad

You can access Tenable.ad's web application through a URL of the type CLIENT_URL.tenable.ad.app.

To launch Tenable.ad's web interface:

- Enter Tenable.ad 3.x User and Administrator Guide's IP address or host name in the address bar of any web browser.

Sign In

There are three ways to log into Tenable.ad. To select your login mode, click on any blade (also called tab) in the authentication window.

Via a Tenable.ad account

To sign in with your Tenable.ad account:

1. Select the Tenable.ad tab.
2. Enter your email address.
3. Enter your password.
4. Click Login.

Via an LDAP account

To sign in with LDAP:
1. Select the **LDAP** tab.
2. Enter your LDAP account name.
3. Enter your LDAP password.
4. Click Login.

Via SAML authentication

To sign in with SAML:
1. Select the **SAML** tab.
2. Enter your email address.
3. Enter your password. You will leave Tenable.ad and be redirected to your SAML server for authentication.
4. Click Login.

Caution: After repeated failed login attempts, Tenable.ad displays the following message to users: "Your account is blocked due to too many failed authentication attempts. You have to contact an administrator."

Sign Out

To sign out of your account:
1. Click the User icon button at the bottom of the left navigation bar.
2. Select **Logout** from the submenu.
Set Your Profile Preferences

To set your preferences:

1. Click on the User icon at the bottom of the page under My Settings, and select Preferences from the submenu.

2. You can do any of the following:

Select your language:

a. In Preferences, select the language from the drop-down list.

b. Click Save.

Select your profile:

Profiles allow you to create and customize your own view of risks affecting AD infrastructures:

Each profile can load a different IoE configuration with different exclusions. For instance, an IT administrator team's requirements for monitoring potential risks are less stringent than those of the Security team, which requires a comprehensive view of all the risks that AD infrastructures face.
a. In Preferences, select Profiles from the secondary left menu.

b. Select the profile to apply from the drop-down list.

c. Click Save.

For more information on security profiles, see Manage Security Profiles.

Change Your Password

a. In Preferences, select Credentials from the secondary left menu.

b. Enter your old password.

c. Create a new password.

d. Confirm the new password and Save.

Manage Your API Key

a. In Preferences, select API key from the secondary left menu.

Your access token displays in the Current API key field.

b. Click on Refresh API key to generate a new access token.

c. Click on the File icon to copy the new API key to your clipboard and paste it into your tool.
For more details, see Use Public API.
Navigate the Interface

The interface of Tenable.ad provides a view of the events and risks affecting your AD infrastructures.

It is fully responsive and you can access it from any device (computers and tablets).

The interface comprises:

- A left navigation bar displayed on all pages.
- A top navigation bar on each page.
- Pages including interactive elements.
Left Navigation Bar

The left navigation bar provides access to the following pages.

Tenable.ad's features are based on the license type. Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack.

<table>
<thead>
<tr>
<th>Page</th>
<th>Page Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Allows you to create customized dashboards including graphical widgets. Dashboards display your data on interactive charts and counters.</td>
</tr>
<tr>
<td>Trail Flow</td>
<td>Shows the real-time monitoring and analysis of events affecting your AD infrastructures.</td>
</tr>
<tr>
<td>Indicators of Exposure</td>
<td>Provides a summary view of the risks affecting your AD infrastructures. Indicators of Exposure are displayed in the form of tiles on the right side of the screen.</td>
</tr>
<tr>
<td>Indicators of Attack</td>
<td>Provides a summary view of the attacks affecting your AD infrastructures. Indicators of Attack are displayed in the form of a timeline with key inform-</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accounts</td>
<td>Manages Tenable.ad users, their roles and security profiles.</td>
</tr>
<tr>
<td>System</td>
<td>Manages forests and domains and configures Tenable.ad for AD's alerting system.</td>
</tr>
<tr>
<td>User</td>
<td>Allows you to set your language and profile preferences, and to log out.</td>
</tr>
</tbody>
</table>
Top Navigation Bar

The top bar displays the following elements on each page.

Bell

A bell icon and its badge counts notify the user that he/she has received notifications waiting for user's acknowledgement. On receiving new alerts, the notification badge counts will be incremented.

The blue badge indicates the number of exposure alerts, whereas the red badge shows the number of attack alerts to be acknowledged by the user.

You can click on the Bell icon to display the Alerts side panel. The last blade (Exposure alerts or Attack alerts) previously opened by the user will appear on the screen.

When the Show archived toggle switch has been flipped to the right, the user will be able to see all notifications, including those that have been archived before. Archived notifications are displayed in light gray.

The user can hover the mouse over the information displayed within the alert rectangle to display the information about the forest and domain affected by the deviance or the attack.
In short, **three actions** are available from the side panel:

- **Archive** or **unarchive** alert notifications either **individually** or in **bulk**.
- **See the deviance** associated with the notification selected from the **Exposure alerts** blade. Then, the **Event details** blade will be displayed.
- Get more information on the notification selected from the **Attack alerts** blade. Then, the **Indicators of Attack** page will be displayed.
Link

A link icon that indicates if your AD infrastructure is properly connected to Tenable.ad.

When your AD is disconnected, the link icon becomes red.

Profile

A profile status that displays your team profile.

Profiles are used to fine-tune the security analysis performed by Tenable.ad according to the configuration parameters specific to a profile. Let’s take the example of A and B who have the same profile:

- When A places certain deviant accounts on allow lists, this also impacts B.
- On the other hand, C, who has his own profile, gets results that are not be affected by this filter.
Interactive Elements

When you click on or hover over interactive elements, they display more information and enable more actions.

Types of interactive elements

The interface of Tenable.ad includes a wide range of interactive elements such as:

- Action buttons
- Blades (also called tabs)
- Check boxes
- Clickable areas
- Contextual menus
- Date pickers
- Hovers
- Hyperlinks
- Icon buttons
- Search fields
- Toggle switches

For more details, see Use The Trail Flow and Use Indicators of Exposure.
Dashboard and Widgets Overview

Dashboards allow users to manage and monitor efficiently and in a visual way security in an Active Directory infrastructure.

Dashboards are designed to enhance and visualize data and trends at a glance. They are populated with widgets containing bar charts, line charts, and counters. Widgets can be customized according to your requirements.

Dashboards vs. Widgets: Do not confuse dashboards with widgets. Dashboards include widgets and not the other way around!
Interactive Elements

Elements common to all widgets

In the upper-right corner of each widget, three icons are displayed standing for Refresh, Modify, and Delete. Click any icon to run it.

In the lower-left corner of each widget, hover the black triangle to display the names of the domains supervised by Tenable.ad.

On the lower-right corner of each widget, drag and drop the corner to resize the widget frame.

Bar chart elements

Simply hover the various bars on the chart to display the action date/time and values in percentage.
Line chart elements

Simply hover the line to display the action date/time and number of events detected by Tenable.ad.

Draggable widgets
You can drag and drop widgets to change their position on the dashboard.
Create a Dashboard

To create a new dashboard:

1. Click on Dashboards below the GENERAL section on the left navigation bar.
2. Click on the Add icon in the upper-right corner of the screen.
3. Enter the name of the dashboard and click OK to validate your changes.

To rename of your dashboard:

1. Click on Dashboards below the GENERAL section on the left navigation bar.
2. Click on the Configure icon in the upper-right corner of the screen and select Configure the dashboard.
3. Enter its new name and click OK to validate your changes.
Working with Widgets

To add widgets to your dashboard:

There are two ways to add a widget to your dashboard:

- Either, after creating your first dashboard, click **Add a new widget on this dashboard** which is an action button displayed by default at the bottom of the window.

- Or, when a dashboard is already available on the screen, click on the **Add** icon in the upper-right corner and select **Add a new widget on this dashboard**.

In both cases, the **MAIN INFORMATION** window is displayed to configure the widget.

![Dashboard Image]

To define a new widget:

1. Select the following:
   - The widget type
   - The widget name
   - The type of data displayed via the widget
• Some context-sensitive information (for more details, see Configure your data sets in your widget in Set up Dashboards).

2. **Configure datasets.**

To modify a widget:

• Click on the **Pencil** icon in the upper-right corner of the widget.

To refresh a widget

• Click on the **Refresh** icon in the upper-right corner of the widget. By default, the widget content is updated every minute.

To delete a widget

• Click on the **Bin** icon in the upper-right corner of the widget. You will be prompted to confirm your changes.
Configure Datasets for Widgets

You will have to define some context-sensitive information to set up your widget.

Let us consider several examples such as Bar chart, Line chart and Counter. Depending on the widget type selected, different fields will be displayed.

To choose a bar chart display:

1. Select severity levels and associated indicators-of-exposure (IoEs) from dropdown lists.
2. Select the AD domains supervised by Tenable.ad.
3. Give a name to the data set that you have created.
4. Click Add a new series to add another data set for comparison purposes. Indeed, when using bar or line charts, you will be able to display several data sets inside the same widget.
5. To delete the last data set that you have created, click Remove the last series.
6. Click Add to validate your changes.
The Compliance Score bar chart used for illustration purposes in Set up Dashboards corresponds to a score on 100 computed by Tenable.ad, taking into account the number of deviances detected and their severity levels. The bar chart reflects the global security maturity of an Active Directory and allows you to compare this level with that of other infrastructures.

For more details on IoEs, see Use Indicators of Exposure.

To choose a line chart display:

1. Repeat the procedure for a bar chart display.

2. Select the time span for which the results will be displayed (ranging from one hour to one month).
The **Deviance Count** line chart used for illustration purposes in *Set up Dashboards* represents the number of deviances, or in other words, the number of security breaches detected by Tenable.ad.

For more details on deviances, see Use Indicators of Exposure and View Indicator Details.

To choose a counter display:

1. Repeat the procedure detailed above in If you choose a bar chart display.

2. Select the **Users count** data type in the **MAIN INFORMATION** window, the data set configuration will also include statuses such as **Active**, **Inactive**, and **All users**.
Delete a Dashboard

To delete a dashboard:

1. Click on Dashboards below the GENERAL section on the left navigation bar.
2. Select the dashboard blade to be deleted.
3. Click on the Configure icon in the upper-right corner of the screen.
4. Select Delete the dashboard.
5. Click Delete to confirm your changes.
Topology Graph Overview

This page provides an interactive graph visualization of your AD infrastructures. The **Topology Graph** displays the forests, domains and trust relationships that exist between them.

To Access the Topology Graph:

---

**Topology Graph overview**

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective

• Click on **Topology Graph** on the left navigation menu to open the page.

Interactive Elements
Hover Areas

The hover areas include:

- Forests (circles)
- Domains (triangles)
- Trust relationships (curved arrows)

You can hover forests and domains to highlight trust relationships. The user can also hover trust relationships to view their attributes.

Toggle switch

You can activate or deactivate the display of internal trust relationships within a forest on the graph.
Zoom slider
You can drag the zoom slider to the right to increase the size of the graph.

Search box
You can enter the name associated with a domain or a forest to run a search.
Filter Forests and Domains

The search box is mainly designed to point to **forests** (represented as circles). If there is only one forest matching the name entered by the user, the graph will immediately focus on this forest. If several forests match the name entered by the user, the graph will zoom out to get a better look at the whole graph. Each forest will be highlighted in blue.

The search performed can also return results that include **domains** (represented as triangles). If the search finds a match or if the matching forest(s) include(s) inter-domain relationships, the graph will highlight the forest(s), their domains and their trust relationships.
Understand Trust Relationships Color Code

The color of a trust relationship depends on its threat level:

- **Red** for dangerous trusts
- **Orange** for regular trusts
- **Blue** for unknown trusts

**Dangerous Trusts**

Dangerous trusts are clickable. They will reveal a blade displaying the same configuration options and object information as the Deviant object view of the Indicator details blade.
Display Trust Relationships Attributes

When hovered, trust relationships (represented as curved arrows) will display specific attributes.

A trust attribute window includes two sections. The top section indicates the trust direction: uni-directional or bidirectional (incoming/outgoing). The lower section displays one of the following values:

- **Non-transitive**: by default, intra-forest trusts are transitive trusts. This flag is used to convert them into non-transitive trusts. On the other hand, inter-forest trusts are non-transitive by default, hence the presence of the forest transitive flag. This value is displayed if an intra-forest inter-domain trust exists. The trust grants no access and delegates no authority to interconnected domains beyond the forest.

- **Forest transitive**: indicates that a transitive trust between two forests exists. The trust granted to another domain can be passed to the trusted forest.

- **Within forest**: indicates that an inter-domain trust exists within the same forest. If WITHIN_FOREST and QUARANTINED_DOMAIN are both present, the trust is referred to as QuarantinedWithinForest.

- **Uplevel only**: indicates that the trust can be used only by clients running Windows 2000 and later operating systems.

- **Treat as external**: indicates (only when FOREST_TRANSITIVE is set) that the trust is of the external type. The SID filtering on the trust is then modified and authorizes the SIDs whose RID is greater than or equal to 1000 to pass across the forest.

- **Quarantined**: indicates that the filtering of the SIDs whose RID is greater than or equal to 1000 is enabled for the trust (by default, it is only enabled for an external trust but can also be applied to a parent-child trust or a forest trust.

- **Cross-organization authentication**: indicates that selective authentication is enabled and can be used across domain or forest trusts.

- **Selective authentication**: see details on Cross-organization authentication.

- **Cross-organization without TGT delegation**: is displayed if the delegation on a trusted domain is fully disabled (never sets the ok-as-delegate option in the issued service tickets).
• **RC4 encryption**: indicates that the trust supports RC4-encryption keys for Kerberos exchanges. This flag is present only if the trustType is set to TRUST_TYPE_MIT.

• **AES keys**: indicates that the trust supports AES-encryption keys for Kerberos exchanges.

• **PIM trust**: if the FOREST_TRANSITIVE and TREAT_AS_EXTERNAL flags are set and the QUARANTINED_DOMAIN flag has not been enabled, the PIM trust flag indicates that the trusted forest manages privileged identities (Privileged Identity Management) regarding SID filtering (local SIDs can pass across this trust). PIM trust is used to implement bastion forests.

• **Tree parent** (deprecated): is displayed if the transitive and bidirectional parent-child trust has been implicitly created when adding a domain.

• **Tree root** (deprecated): is displayed if the transitive and bidirectional trust has been implicitly created when adding a root domain to the forest.

• **No attribute**: indicates that the external trust has no specific attribute.
Investigate Dangerous Trusts

When you hover over them, dangerous trusts (represented as red curved arrows) display a specific mouse pointer indicating that you can click on.

When you hover over and click on a dangerous trust, a blade appears to display the same configuration options (Filter, Ignore, View, Export) and object information as the Deviant object view of the Indicator details blade.
In the same way as on the **Deviant Objects** blade, you can view the incriminating attributes. For more information, see **View Incriminating Attributes**.

**Dangerous Trust deviant objects**
The objects, the incriminating attributes, the reasons, and the details of the events displayed on the dangerous trust relationships blade are all linked to the **Dangerous Trust Relationship** IoE which you also find in the **Indicators of exposure** menu.
Trail Flow Overview

This landing page displays the real-time monitoring and analysis of events affecting your AD infrastructure.

The **Trail Flow** page provides you with the ability to load previous events in order to go back in time. You can also use the search box at the top of this page to perform threat hunting and detect malicious patterns.

Interactive Elements

Clickable entries
You can click on every single entry in the table displayed. The details on the event selected will appear in the form of a blade.

- These details include what attributes have changed value, with a blue dot as an indicator of this change. Hovering over the blue dot will show the user the attribute value before and after the modification.
- If a red diamond appears next to a clickable entry, it means that a potential exploit exists within this event.

Toggle switches

You can activate or deactivate the display of deviant events in the table.
Action buttons

You can load previous events. The trail flow will automatically stop to allow the user to search for an event which occurred within a specific time frame.

Check boxes

You can select the forests and domains to be included in the search or in the display.

Search box
View the Real-Time Monitoring of Your AD Infrastructures

The Trail Flow page is the default landing page you will be taken to after a successful login. It shows the real-time monitoring and analysis of events affecting your AD infrastructures.

Understand the Trail Flow Table

The Trail Flow table includes the following columns.

Source

This column indicates the origin of any security-related change in your AD infrastructures.

There are two possible sources:
• The Lightweight Directory Access Protocol (LDAP) which is used to communicate with your AD infrastructure.

• The Server Message Block (SMB) protocol which is used to share files, printers, etc.

**Group Policy Objects**

Active Directory allows administrators to create group policies which control settings deployed on user and machine accounts. These settings are stored in a Group Policy Object (GPO). GPO files are stored in the sysvol folder on the domain controller. Monitoring the content of GPOs is key for the security of your AD as they will be applied or executed by each member of the domain with a huge level of privileges. The SMB (Server Message Block) protocol is used to retrieve these GPO files from the sysvol folder.

**Tenable.ad** analyzes thoroughly LDAP and SMB traffic over your network in order to detect anomalies and potential threats.

**Type**

This column is used to enhance characteristic elements which may be of interest for users such as entering a group, creating a new user account, etc.

The type list includes the following event types:

• ACL changed
• SPN changed
• Member removed
• New member
• New trust
• Unknown file type added
• New object
• Object removed
• Password changed
• UAC changed
• New GPO linked
• GPO link removed
- Owner change
- File renamed
- SPN created
- Failed auth reset
- Failed authentication

**Examples of event types in the Trail Flow**

**Object**
This column indicates the class or file extension associated with an AD object. You can search for a directory object (user, computer, etc.) or a file having a specific file name extension (ini, xml, csv).

**Path**
This column indicates the full path to an AD object. It will allow the user to identify the unique location of this object in the AD.

**Directory**
This column indicates from which directory the change in your AD infrastructure comes from.

Date

This column indicates the time when the change in your AD infrastructure occurred.
Pause and Restart the Trail Flow

Tenable.ad analyzes in real time the flow of events that occur in your AD infrastructures. As a result, the Trail Flow table grows quickly to accommodate entries which will keep on increasing over time.

Clicking on the **Pause the Trail Flow** button will stop the automatic vertical scrolling of the most recent events while the analysis still running in the background. The user will then be able to run a search on events.

To pause the Trail Flow:

- Click the **Pause the Trail Flow** button in the upper-right corner to stop the display of events in real time. The button label changes to **Restart the Trail Flow** and becomes red.

To restart the Trail Flow:

- Click the **Restart the Trail Flow** button in the upper-right corner to resume the real-time display of events. The button reverts to its previous state and original color.
Filter the Real-Time Flow of Events

An engagement with partners who have similar experiences and skills in specific threats can help organizations enhance security protection as well as mitigate risks against security threats.

Indeed, in order to hinder and prevent hackers from gaining access to your AD infrastructures, you can exchange information about malicious attempts to penetrate your system. A recurring sequence of events or a repetitive and suspicious behavior such as the use or modification of a specific character string can reveal attackers’ stealthy attempts to penetrate your AD infrastructures.

This shared information can be used as filters to locate suspicious activities and respond proactively to potential threats to your AD infrastructures.

Besides, the Trail Flow table that displays events affecting your AD in real time will grow so quickly that filtering is a way to examine thoroughly what is going on in your AD infrastructures.

To filter events:

- Log into your Tenable.ad account.
  - After you log in successfully, the Tenable.ad home page opens. You can begin filtering events.
Run a Search in the Trail Flow

You can either use the search wizard or enter manually the expression elements in the standard search box.

To search using the Wizard:

You can click on the Magic wand icon on the left of the standard search box to display the search wizard.

For more details, see Filter the Real-Time Flow of Events.

![Search in Trail Flow](image.png)
To search manually

You can type an expression in order to refine search results using the Boolean operators *, AND and OR. You can encapsulate OR statements with parentheses in order to modify search priority. You are then able to filter events that match the specific character string or pattern that you entered in the box.
<table>
<thead>
<tr>
<th>Source</th>
<th>Type</th>
<th>Object</th>
<th>Path</th>
<th>Domain</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN=Admin OU=Abd,DC=valid,DC=com</td>
<td>Tenante's domain</td>
<td>2021-06-30</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Type</td>
<td>Object</td>
<td>Path</td>
<td>Domain</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>user</td>
<td>CN=Admin,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=GlobalCatalog,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=WebSphereinition-9,OU=WebSphereinition,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=ActiveX,OU=ActiveX,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Domain Controllers,OU=Domain Controllers,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=System,OU=System,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Recognizable,OU=Recognizable,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Users,OU=Users,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>computer</td>
<td>CN=CN=QI,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Shared with Everyone-CN=Shared with Everyone,OU=Shared with Everyone,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Domain Policies-CN=Domain Policies,OU=Domain Policies,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Security Policy-CN=Security Policy,OU=Security Policy,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Shared Resources-CN=Shared Resources,OU=Shared Resources,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Domain Controllers-CN=Domain Controllers,OU=Domain Controllers,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=System-CN=System,OU=System,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Recognizable-CN=Recognizable,OU=Recognizable,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>groupPolicyContainer</td>
<td>CN=Users-CN=Users,OU=Users,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>user</td>
<td>CN=New User,OU=Admin,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>domain</td>
<td>OUs=Domain Controllers,OU=Domain Controllers,DC=tenant,DC=corp</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
<tr>
<td>LDAP</td>
<td>ACL change</td>
<td>Folder</td>
<td>S:\Tenant\Domain Controllers</td>
<td>Tenant's domain</td>
<td>2021-06-30</td>
</tr>
</tbody>
</table>
For more details, see [Filter the Real-Time Flow of Events](#)
Build Faster Queries Using the Wizard

The search wizard allows you to create query expressions faster than the standard search field.

- When expressions are frequently used in the search field, add them to a list of customized bookmarks. Select any entry from the list to use the bookmark again without having to retype the entire expression.
- When you enter an expression in the search field, Tenable.ad will save this expression to the History blade. All entered expressions are automatically stored in a list. Click on the search field to select any entry from the list and use it again without having to retype the entire expression.

Search Elements in the Wizard

The following search elements are available to customize your search queries:

AND/OR combinator buttons

In the first condition, you can select the AND or the OR combinator which will be applied to the query expression. To add another condition to the query, click on the +AND or the +OR combinator button.
**Deviant only combinator**

The **AND/OR combinator button** only applies to the Deviant only toggle switch. First, flip the toggle switch to the right and select the AND or OR condition. Then, the condition will be added to the query in the Filter preview.

**Deviant only toggle switch**

If needed, you can restrict the search to deviant objects by flipping the toggle switch to the right. The `isDeviant=true` element will be displayed in the search expression.
Bin icon

You can delete attributes in the query expression by clicking on the Bin icon at the far right of the attribute fields.

Add a new condition

You can add new conditions to the query expression by clicking on the +AND or +OR combinator button under the attribute fields.

Add a new rule

You can add new rules to the query expression by clicking on the +Add a new rule action button under the attribute fields.

Query syntax

Add an attribute

1. After applying the combinator to the first condition, select the attribute from the dropdown menu and enter its value.

2. Click on the +Add a new rule action button to add another attribute to the first condition.
3. If you add another condition to the query, click on the +AND or +OR combinator button ❸.

Add a combinator

1. Click on the **AND** or the **OR** combinator ❶ to be applied to the first condition in the query expression.

2. Select the attribute from the dropdown menu and its value. Then, you will be able to add another combinator to the first condition.

3. Click on the Add a new condition +AND or +OR combinator button ❷.
4. Configure the second condition. The search wizard will display the query expression in the preview.

Get Familiar with the Search Wizard

To learn to use the search wizard:

1. Enter a query that you are familiar with.

2. Click on the **Magic wand** icon to display the query that the wizard built.
Put It All Together: Use the Search Wizard

1. Click on the Magic wand icon on the left of the standard search field to display the search wizard.

2. To define the query expression in the panel, click on the AND or the OR combinator button to apply to the first condition.

3. Select the attribute from the drop-down menu and enter its value.

4. To add an attribute, click on the + Add a new rule action button.
5. Click on **Add a new condition** +AND or +OR combinator button ❶ to add another combinator to the first condition.

6. If needed, you can restrict the search to deviant objects by clicking on the toggle switch ❷ to the right and select the AND or OR condition.
7. Click **Validate** to run the search or Reset if you need to delete your query parameters.
Search Manually

To run a manual search:

- Type the query expression to run a search in the standard search box.

Example

The Trail Flow is designed to look for any specific value stored into an Active Directory attribute.

- In this example, we run a search for disabled user accounts which could endanger monitored AD infrastructures.

- We can also perform this search to detect suspicious activities and anomalous account usage.

Grammar and Syntax
The Trail Flow has been designed to look for any specific value stored into an Active Directory attribute. Looking for an account which does not expire or looking for a specific object SID has never been so easy.

A Trailflow expression is built using the following grammar:

**EXPRESSION [OPERATOR EXPRESSION]***

- An expression is built using the following syntax:
- `__KEY__ __SELECTOR__ __VALUE__`
- `__KEY__` refers to the AD object attribute to search (like `cn`, `userAccountControl`, `members`, etc.). Some additional keys are also available to look for specific content:
  - `date` look for a specific period of time
  - `isDeviant` looks for events creating a deviancy
- `__SELECTOR__` refers to the arithmetic operator: `:`, `>`, `<`, `>=`, `<=`
- `__VALUE__` refers to value to be searched.

Multiple trailflow expression can be combined together using a binary operator. The following operators are currently available: **AND, OR**.

At the time, `__SELECTOR__` only works for date column.

The following snippet gives several examples of valid Trailflow requests.

**Trail Flow Syntax**
Look for every object containing the string alice into the common name attribute:
```
cn:"alice"
```
Look for every object containing the string alice into the common name attribute and which created a specific deviancy:
```
cn:"alice" and isDeviant:"true"
```
Look for every event that accured the 15th of June 2019:
```
date>"2019-06-15 00:00:00" and date<"2019-06-15 23:59:59"
```
Look for a GPO named Default Domain Policy:
```
objectClass:"groupPolicyContainer" and displayName:"Default Domain Policy"
```
Look for every disabled account having an SID containing S-1-5-21
userAccountControl:"DISABLE" and objectSid:"S-1-5-21"
Look for every script.ini file into the sysvol:
globalpath:"sysvol" and types:"SCRIPTSini"
Show Only Deviant Events

To prevent cluttering the screen, you can display only deviant objects in the Trail Flow table:

1. Click on the Magic wand icon.
2. Flip the toggle switch in the upper-right corner to the right.
3. Click Validate to display only deviant objects. A red lozenge will be displayed before the Source column.

Several types of lozenges exist:
• An empty lozenge ◊ means that a deviance has been detected in Tenable.ad's profile.
• A full diamond ⬤ means that a deviance has been detected in other profiles.
• A crossed lozenge means that a deviance has been remediated in the relevant profile.

For more details on deviant objects, see Filter the Real-Time Flow of Events.
History blade

When the user enters an expression in the standard search field, Tenable.ad will save this expression to the History blade. All entered expressions are automatically stored in a list. Click on the search field to select any entry from the list and use it again without having to retype the entire expression.

To fully use the features of the History blade, click on the Search field and select Manage your history. Several actions are available:

- To delete an expression from the History blade, select the Bin icon.
- To search for a specific history entry, use the search field at the top of the pane.
- To limit the search to a specific time period, click on the Calendar icon at the top of the pane and define the Start and End dates.
- To delete the entire search history, click on Clear history. The user will be prompted to con-
To go back in time to investigate previous events:

1. Click on the Load previous events button at the bottom of the screen. The Trail Flow is paused message is displayed.
2. Click on Restart the flow to resume the real-time display of events.
Bookmarks Blade

When expressions are frequently used in the standard search field, the user can add them to a list of customized bookmarks.

Bookmarks are manually saved to a list. To save bookmarks to the Bookmarks blade, the user has to click on the Star icon on the right of the search field. The entry is added to the list.

Then, the user can select any entry from the list to use it again without having to retype the entire expression.

To clear the standard search field, click on the Cross icon.
Manage your bookmarks

To fully use the features of the Bookmarks blade, click on the Search field and select Manage your bookmarks. Several actions are available:

- To search for a specific bookmark from the list ।.
- To limit the search to a specific folder, click on the dropdown list ❷ on the right of the pane and select the folder to be looked in.
- To edit a bookmark name, click on the Pencil icon ❸.
- To delete an expression from the Bookmarks blade, select the Bin icon ❹.
- To edit a bookmark folder name (if any), click on the Pencil icon ❺.
- To delete a bookmark folder (if any), select the Bin icon ❻.
Select Forests and Domains

To restrict the search to a specific forest or domain:

1. Click on the n/n domains button. A pane is displayed on the right.

2. Check the boxes to select the items from the drop-down list.
View Event Details

Tenable.ad provides detailed information on each event affecting your AD infrastructures. Details on a specific event will allow you to review technical information and take remedial actions if required by the Indicator of Exposure’s severity level (Critical, High, Medium, or Low).

To access an Event details window, click any entry in the Trail Flow table. The details on the event selected will appear in the form of a blade.

Differences between IoE, event and deviant object
• An **Indicator of Exposure** describes a type of threat that affects Active Directory. It may include several technical vulnerabilities. Each IoE is collected in one and unique place called a blade providing information on detected vulnerabilities, associated deviant objects, and recommendations on remedial actions. Every Tenable.ad's IoE measures in real-time security level after receiving an event.

• An **event** symbolizes every change related to security that can appear into an Active Directory infrastructure. It could be a password change, a user creation, a new GPO or the modification of a GPO parameter, a new delegated right, etc. An event can change the compliance status of an IoE (from compliant to non-compliant).

• A **deviant object** is a technical element which allows (on its own or associated with another deviant object) the attack vector described in an IoE, to work.

If no remedial action is required, "No deviance has been detected for this event" is displayed on the right side of the page.

**Blade layout**
Top section

- Information already provided in the Trail Flow table.
- For more details, see [Understand the Trail Flow Table](#).

Main section

- Technical information. You can search for AD object attributes on the event that you selected in the Trail Flow table.
- For more details on AD attributes to run a search, see [Microsoft's website](#).

Right-side section
• This section provides information only if the event includes deviant objects. When the security status of the event (IoE) is not compliant, the user will be able to take remedial actions.

• Additional information, vulnerability details, and recommendations are available by clicking on the Indicators tile displayed on the right.

• If no remedial action is required, No deviance has been detected for this event is displayed on the right side of the page.

Column Labels

The Attributes table includes the following columns:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Indicates the attributes of the Active Directory object associated with the event that you have selected in the Trail Flow table. Attributes describe the object characteristics. Multiple attributes can describe a single AD object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value at event</td>
<td>Indicates the attribute value at the time when the event occurs.</td>
</tr>
<tr>
<td>Current value</td>
<td>Indicates the value of the attribute in the AD right now, at the moment when the user is viewing it.</td>
</tr>
</tbody>
</table>

**Value before event** To display the value of the attribute before the event occurred, hover the blue dot on the left (if any). Any change in value is indicated with a color code.
View Attribute Changes

All attributes

When the value of an attribute has changed, a blue dot before the **Attribute** column is displayed. Hover the blue dot to display the details.

The Value before event is displayed first.

The color of the **Value at event** label depends on the changes applied to the attribute:

- Green for **Addition**
- Red for **Deletion**
- Gray for **Unchanged**
**ntsecuritydescriptor attribute**

A security descriptor is a data structure that contains security information about an AD object, such as the ownership and permissions of the object. For more details, see Microsoft's online documentation.

To display details on an object security descriptor:

1. Hover over the ntsecuritydescriptor attribute entry (Value at event or Current value column) **.
2. Click on See SDDL Description.

3. Click on the chevrons on the left to expand the SDDL description toggle lists:

4. Browse to an Access Control Entry (ACE) highlighted in color to display the access rights of the object. The color code is as follows:

- Red: means that dangerous rights are assigned to users who should be denied access rights to the object.

- Orange: means that dangerous rights are assigned to a privileged user generally allowed to have this type of right (example: Domain Admins).
- Green: means that no dangerous rights are granted.

Expand the ACE toggle lists to display access rights to an AD object

5. You can copy the SDDL description to the clipboard and close the window.
View Impacted Domains

If the event selected includes deviant objects, the list of impacted domains in your AD forests will be listed on the right side of the page.

Indicators

If the event selected includes deviant objects, click on the Indicators tile displayed on the right side of the page to access the following indicator blades:

- **Information** which includes internal and external resources on the IoE.
- **Vulnerability details** which provides explanations on the weakness detected in your AD infrastructure.
- **Deviant objects** which includes technical details, a search filter (including a search wizard and a standard search field) and an action button to export reports.
- **Recommendations** on how to solve the issue.

Under the indicator tile, a short description of the IoE is provided to help the user understand the issue at hand.

For more details on IoEs, see [Use Indicators-of-Exposure](#).
**EXECUTIVE SUMMARY**

Active Directory accounts can be configured to escape global password renewal policies. Accounts set up like this can be used indefinitely without ever changing their password. User and administrator accounts should never have this attribute.

**IMPACTED DOMAINS**

- Tenable's forest
  - Tenable's domain

**DOCUMENTS**

- Best Practices for Enforcing Password Policies
- Configuring Password Policies

**ATTACKER KNOWN TOOLS**

- mimikatz
- GentilKini
Retrieve an Attribute from the List

The box allows you to run a search on attribute names and values. All attributes are searchable.

To filter attributes:

- Click any event entry in the Trail Flow table. The search field will appear at the top of the Event details blade.

To search an attribute:
1. Select the field including a Search icon under Attributes.

2. Enter the attribute name in the search box.

For more details on AD attribute naming, see Microsoft's website.

For more details on the Attributes table, see View Event Details.
Trail Flow Use Cases

To understand the trail flow behavior, let us consider two examples to illustrate how an operation performed in your Active Directory will be reflected in the Trail Flow interface.

Each example compares data from the administrator's side (in the Active Directory interface) with the data from the end-user's side (in Tenable.ad's interface).

The use cases detailed below are merely examples of how the trail flow will behave in these two cases. They are not intended to be exhaustive and cover every possible situation.

Indeed, Active Directory offers a wide range of interfaces, APIs, services, etc. to create a new user account or change a user's password. On the other hand, the result on the Trail Flow interface will be the same whatever the method used.

What happens in the Trail Flow when you create a new AD user account?

On the Administrator's side, a new window prompts you to enter various information on the new user account.
On the end-user’s side, the **Trail Flow** page is updated. Take a look at the **Type** column which indicates **New object**.

![Trail Flow page example]

The **Event details** page also reflects this change. Take a look at the blue dots on the left of the attribute names. They indicate that an update has occurred.

For more details on attributes, see **View Event Details**.
What happens in the Trail Flow when you change an AD user's password?

On the Administrator's side, a new window prompts you to enter various information to reset a user's password.
On the end-user's side, the **Trail Flow** page is updated. Take a look at the **Type** column which indicates Password changed.
The **Event details** page also reflects this change. Take a look at the blue dot on the left of the when-changed attribute.

For more details on attributes, see [View Event Details](#).
Event details

Source: LDAP
Type: Password changed
Class: user
DN: CN=MyUser,OU=Users,DC=example,DC=com

Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value at event</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>MyUser</td>
<td>MyUser</td>
</tr>
<tr>
<td>uid</td>
<td>MyUser</td>
<td>MyUser</td>
</tr>
<tr>
<td>displayName</td>
<td>MyUser</td>
<td>MyUser</td>
</tr>
<tr>
<td>objectclass</td>
<td>user, person</td>
<td>user, person</td>
</tr>
<tr>
<td>samaccountname</td>
<td>poor-little-user</td>
<td>poor-little-user</td>
</tr>
<tr>
<td>userprincipalname</td>
<td><a href="mailto:poor-little-user@example.com">poor-little-user@example.com</a></td>
<td><a href="mailto:poor-little-user@example.com">poor-little-user@example.com</a></td>
</tr>
</tbody>
</table>

Indicators

No devices have been detected for this event.
Indicator-of-Attack Overview

Purpose

Tenable.ad gives your organization the ability to detect attacks in real time and quickly stop them.

The **Indicators of Attack** functionality provides the following capabilities and benefits:

- Visualize every threat from an accurate attack timeline.
- Consolidate attack distribution in a single view.
- Analyze in-depth details about an AD attack.
- Explore MITRE ATT&CK descriptions directly from detected incidents.

Tenable.ad detects attacks affecting your AD infrastructures through Indicators of Attack (IoAs) and assigns severity levels to the constant flow of attacks that is being monitored and analyzed:

- **Critical**: The IoA is detecting a proven post-exploitation attack requiring domain dominance as a prerequisite.
- **High**: The IoA is detecting a major attack allowing an attacker to reach domain dominance.
- **Medium**: The IoA is related to an attack that could lead to a dangerous escalation of privileges or to allow access to sensitive resources.
- **Low**: The IoA alerts about suspicious behaviors related to recon action or low-impact incidents.
Tenable.ad’s functionalities based on the license type: Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack

Tile Layout

The consolidated view of the Indicators of Attack page displays domain tiles arranged in the following order:
Each tile includes:

- An Attack distribution section which shows the severity levels related to the constant flow of attacks.
- A Top 3 attacks section which gives the name of the three major attacks and their occurrence number.
- A Refresh icon to refresh the view.
• A Pencil icon to edit card information and select another chart type (line or doughnut).
Doughnut chart type

You can click on any tile 🔄 in the consolidated view. The details on the incidents affecting the domain selected will appear as a blade called List of incidents.

Terminology

- IoA: Detects attacks affecting your AD infrastructures.

- Consolidated view: Shows attack distribution in a single view.

- List of incidents: Provides detailed information on attacks affecting your AD infrastructures.

Interactive Elements
When clicked or hovered over, interactive elements will display more information and enable more actions.

Action buttons

Click the Export button ❶ to generate a report listing the attacks.

Blade (also called tab)

Clicking on any tile will bring out the details of the selected IoAs.

The new blade displayed in the interface is called List of incidents. It includes internal and external resources on the IoA.

Calendar picker
You can select a start date and time to display on the timeline.

For more details on how to use the timeline, see View the List of Indicators of Attack.

Check boxes

You can select the forests and domains to be included in the search or in the display. To restrict the search to a specific forest or domain, check the box in the upper-right corner and select the items from the dropdown list.

Clickable entries

You can click on:

- The n/n domains button to select the forests and domains to display or on which to perform a search.
- The n/n indicators button to select the IoAs to display or on which to perform a search.
- The colored pills displayed along the timeline to display the top 3 attacks and their occurrence number.
- Any tile displayed on the Indicators of Attack page. The details on the attacks selected will appear as a blade called List of incidents.
Dropdown list

You can select the sorting order for the tiles:

- Alphabetical order
- Criticality
- Forest

For more details on tile sorting, see View the List of Indicators of Attack.

Hover areas
When selecting the Number of events chart type on the IoA card, a bar chart is displayed. The user can hover the bars to display the incident date and number of occurrences.

Search box

The user can enter the name assigned to an IoA or a single domain to run a search. For more details, see Filter IoAs.

Timeline

The user can click on the left and right arrows to scroll through the timeline displayed. For more details on how to use the timeline, see View the List of Indicators of Attack.
Toggle switches

The user can activate or deactivate the display of all domains under attack.
View Indicators-of-Attack

The consolidated view of the Indicators of Attack page is accessible from the left navigation menu. This view shows a timeline and the top 3 incidents which impacted your Active Directory (AD) infrastructures in real time.

Show only domains under attack

- There are two ways to display Indicators of Attack. By default, Tenable.ad will show all your AD infrastructures (forests and domains arranged in a hierarchical fashion).
- But if the user wishes to see only the domains under attack, he/she will flip the Show only domains under attack toggle switch in the upper-right corner to the right (Yes). By default, the toggle switch is set to No.
• Show only domains under attack disabled:

• Show only domains under attack enabled:
There are three ways to sort the tiles representing domains under attack:

- In alphabetical order
- By severity level
- By forest name
Sort by severity level

Each tile includes:

- An Attack distribution section which shows the severity levels related to the constant flow of attacks.
- A Top 3 attacks section which gives the name of the three major attacks and their occurrence number.
- A Refresh icon to refresh the view.
- A Pencil icon to edit card information and select another chart type (line or doughnut).

The user can click on any tile to display the incidents affecting the domain selected. Detailed information is provided in a List of incidents blade.
Timeline

For more details on how to work with the timeline, see View the List of Indicators of Attack.
Understand IoA Security Levels

Tenable.ad detects attacks affecting your AD infrastructures through Indicators of Attack (IoAs) and assigns severity levels to the constant flow of attacks that is being monitored and analyzed:

- **Critical**: The IoA is detecting a proven post-exploitation attack requiring domain dominance as a prerequisite.
- **High**: The IoA is detecting a major attack allowing an attacker to reach domain dominance.
- **Medium**: The IoA is related to an attack that could lead to a dangerous escalation of privileges or to allow access to sensitive resources.
- **Low**: The IoA alerts about suspicious behaviors related to recon action or low-impact incidents.
Timeline Information

Understand Timeline Information

Navigate in the timeline

To scroll through the timeline displayed, click on the left and right arrows. The timeline will move back and forth.

Understand the color code

- Detected IoAs are displayed as pills by severity level via color codes (red for Critical, orange for High, yellow for Medium, and blue for Low).

- The same color code applies to the tiles in the area below.

Define the time period

By default, the consolidated view opens up with the Day view.

To define the time period:

- Click on the following elements:

Date/Time buttons

- Hour to display a timeline of the current hour.

- Day to display a timeline of the current 24 hours.

- Month to display a timeline of the current month.
• Year to display a timeline of the current year.

Calendar picker

Click on the Calendar icon to select the precise start date and time that you wish to display on the timeline and in the tile section. The calendar picker format will adjust to the user's previous selection (Date/Time button):

• Example with Hour button selected
• Example with Year button selected

Then, click on OK to confirm your selection or click on Now to default to current date and time.

For more details, see Filter IoAs.
IoA Tile Information

View the top 3 attacks

Click on any pill along the timeline to display:

- The incident detection date and time.
- The severity level of the top 3 attacks.
- The total number of attacks detected on this date and time.

Refresh the timeline

- Click on the Clock icon to default to current date and time.
Change the chart type

- Click on the Pencil icon to edit the IoA card and select another chart type (line or doughnut).
Filter Indicators-of-Attack

Define the Time Period

To define the time period you wish to explore, click on the following elements:

Date/Time buttons

Click on:

- Hour to display a timeline of the current hour.
- Day to display a timeline of the current 24 hours.
- Month to display a timeline of the current month.
- Year to display a timeline of the current year.

Calendar picker

Click on the Calendar icon to select the precise start date and time that you wish to display on the timeline and in the tile section. The calendar picker format will adjust to the user’s previous selection (Date/Time button).
Then, click on OK to confirm your selection or click on Now to default to current date and time.

Select Domains

On the upper-right corner of the page, click on the n/n domains button to select the forests and domains to display or on which to perform a search.
To restrict the search to a specific forest or domain, the user can:

- Either check the boxes on the right pane and select the items from the dropdown list.
- Or enter the name assigned to a domain or forest, and its description keywords to run a search.
Select Indicators

On the upper-right corner of the page, click on the n/n indicators button to select the IoAs to display or on which to perform a search.
To restrict the search to a specific IoA, the user can:

- Either check the boxes on the right pane and select the items from the dropdown list.
- Or enter the name assigned to an IoA and its description keywords to run a search.
Search a Single Domain or Attack

To prevent cluttering the tile section and access data faster, the user can display a single domain or attack
Now, click on Search in the upper-right corner to run the search.
IoA List of Incidents

The consolidated view of the Indicators of Attack page is accessible from the left navigation menu. To access more in-depth information on incidents, click on any IoA tile. The details on the incidents affecting the domain selected will appear as a blade called List of incidents.

Understand List of Incidents

Purpose
Accessing details on a specific attack will allow you to review technical information and take the immediate actions required by the Indicator of Attack's severity level (Critical, High, Medium, or Low).

Read the color code

Like for IoEs, Indicators of Attack include four colors indicating their severity level (red for Critical, orange for High, yellow for Medium and blue for Low).
Filter Incidents

Applying filters to incidents will help administrators pinpoint the issues that are critical to your AD infrastructures.

From this blade, the user can perform several actions such as:

- Define search criteria to run a search 🆁.
- Access detailed explanations on the attacks affecting AD infrastructures 🆂.
- Close or reopen an incident 🆃.
- Download a report showing all incidents 🆄.

Configure the search
Interactive elements

In the top section, the interactive elements include:

- **Search box ❶**: Enter source or destination keywords.
- **Date picker ❷**: Click to select a Start date and an End date to run a search on incidents within a specific time frame.
- **n/n indicators button ❸**: Click to select the IoAs to display or on which to perform a search.
- **Closed incidents toggle switch ❹**: Flip the switch to the right to display open and closed incidents.
- **Refresh action button ❺**: Click to refresh the view.
Incident Details

Understand the List of incidents

In the middle section, each IoA entry displays the following information:

- Date of occurrence of the IoA. The latest IoA events are displayed at the top of a vertical timeline.
- Source which indicates where the attack comes from and its IP address.
- Attack Vector which explains what happened during the attack. Hover the arrow to display more information about the IoA.
- Destination which indicates the target and its IP address.
- Attack Name which indicates the technical name of the attack.
- Domain which indicates which domains were impacted by the attack.

Interactive elements: Click on any hyperlink on the interface, a new List of incidents blade will open and display the incident information (source and destination hostnames, IP addresses, Attack Vector details, Domains and forests, etc.). Tenable.ad’s interface can display a maximum of five List of incident blades.

When clicked or hovered, these elements will display more information and enable more actions:

Date:
Hover to display UTC time.

Source
Click to display where the attack comes from and its IP address:
• Source links to hostname and IP address details

• Hostname details

• IP address details

*Attack Vector*
• Hover the text above the arrow to display IoA details.

• Click on the hovered area to display the complete explanation.

Destination
Click to display the target and its IP address:
• Destination links to hostname and IP address details

• Hostname details

• IP address details

Attack Name
Click the button to display technical details on the attack.
Domain

- Click to display which forests and domains were impacted by the attack.
• Details action button: Click the button to display the in-depth details of an attack.

Maximum display of blades: Tenable.ad’s interface can display a maximum of five List of incident blades. To access the blades, the user has clicked on several interactive elements (links, action buttons, etc.). To close all the blades simultaneously, click anywhere on the page.
Close or Reopen Incidents

Close/Reopen closed incidents

In the lower section, closing or reopening incidents eliminates clutter on the interface.

- To select the incidents to be closed, check the boxes in the last row of the table. For faster selection, you can check the Select displayed objects box to select in bulk.
- Select Close selected incidents from the dropdown list at the bottom of the screen and click OK. A dialog box is displayed for the user to confirm or cancel the operation. After confirmation, the incident is no longer displayed.
Confirm closure
To restore the initial situation and disable filters:

Check that the Closed incidents toggle switch is set to Yes. The filtered-out incident is greyed out in the table.

**Closed incidents reopen/Toggle switch**

- Then, select individually the incidents to be reopened or select them in bulk via the Select displayed objects box in the bottom left corner of the page.
- Select Reopen selected incidents from the dropdown list and click OK. The filtered-out incident is now fully visible in the table.
Open closed incidents: result
Understand Attack Details

To access an even deeper level of detail on the AD attack, click on the Details action button displayed on the right side of the IoA line.

Accessing details on a specific attack will allow you to review technical information and take the immediate actions required by the Indicator of Attack's severity level (Critical, High, Medium, or Low).

Description blade

The Description blade includes three sections:

- INCIDENT DESCRIPTION which provides a short description of the attack.
- MITRE ATT&CK INFO which displays technical information retrieved from the Mitre Att&ck (Adversarial Tactics, Techniques, and Common Knowledge) knowledge base. Mitre Att&ck is a framework that classifies adversary attacks and describes the actions that attackers take after they have compromised a network. It also provides standard identifiers for security vulnerabilities to ensure there is a shared understanding by the cybersecurity community.
- ADDITIONAL RESOURCES which provides links to websites, articles and white papers for more in-depth information on the attack.
Description blade (IoA details)

YARA Detection Rules blade

The YARA Detection Rules blade describes the YARA rules used by Tenable.ad to detect AD attacks at network level – thereby strengthening Tenable.ad's detection chain.

Click on the Copy to clipboard icon button to copy the text of the YARA rules.

YARA detection rules: YARA is the name of a tool primarily used in malware research and detection. It provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. A description is essentially a YARA rule name, where these rules consist of sets of strings and a boolean expression (source: wikipedia.org).
Export an Attack Report

To download the attack report:

1. Click on the Export all button displayed in the lower-right corner. A blade window appears on the right.
2. Choose the CSV format.
3. Click on Export all. Either open the report in the browser or save the file.
Export an IoA Report

- Click on the Export button displayed in the lower-right corner of the page.

Download the Consolidated View Report

1. Click the Export button to generate a consolidated view report providing the list of IoAs that you have selected. A blade window appears on the right.

2. Choose the format (PDF, CSV or PPTX).

3. Click again on Export.

Select export file format
Use Indicators of Exposure

Purpose

Tenable.ad measures the security maturity of your AD infrastructures through Indicators of Exposure (IoEs) and assigns severity levels (**Critical**, **High**, **Medium** or **Low**) to the constant flow of events that is being monitored and analyzed:

- **Critical**: The IoE indicates and provides a way to prevent the AD from being directly and fully compromised by potentially a part of unprivileged users.
- **High**: The IoE is either dealing with post-exploitation techniques (that could allow, for instance, credential theft or backdooring) or with exploitation techniques which have to be chained with other exploitation techniques to be of any real danger.
- **Medium**: A medium IoE indicates a limited risk for the Active Directory infrastructures.
- **Low**: A low IoE reflects good security practices. In certain contexts, low-impact deviances may be authorized for business reasons but do not necessarily affect AD security. They will impact the AD infrastructures only if an administrator's makes an error (e.g., by activating a disabled account).

The **Indicators of Exposure** page displays IoE tiles arranged in the following order:

- By severity level via color codes (red for Critical, orange for High, yellow for Medium, and blue for Low).
- Vertically, by order of severity (red for top priority and blue for least priority).
- Horizontally, by order of complexity (starting with the least complex cases and ending with the most complex cases). The complexity indicator is dynamically computed by Tenable.ad's platform to describe how difficult it will be for the Administration team to fix the deviant IoE.
- In alphabetical order (new feature coming soon).
- By domain name (new feature coming soon).

In the case of security regressions, Tenable.ad will trigger alerts.
Indicators of Exposure page

Tile Layout

Indicators of Exposure are displayed as tiles ranging from highest to lowest severity level.

Each IoE tile displays the following information:

- The IoE name
- A short description
• The domains impacted by the IoE
• An icon representing the complexity level of the IoE

If the IoE status is compliant, the message No indicators found with deviant objects is displayed on the IoE details page (Status).

Click on the tile to display the IoE details.

Interactive Elements

When clicked or hovered over, interactive elements will display more information and enable more actions.

Interactive elements (IoE page)
Clickable entries

- You can click on any tile ⬅ displayed on the Indicators of Exposure page. The details on the IoE selected will appear in the form of blades.

- You can click on the n/n domains button ⬅ to select the forests and domains to display or on which to perform a search.

Toggle switches

- You can activate or deactivate the display of all IoEs available in Tenable.ad ⬅ on the Indicators of Exposure page.

- You can also choose to show ignored deviant objects associated with an IoE.

Blades (also called tabs)

Clicking on any Indicator of Exposure tile will bring out the details of the selected IoE.
The first blade displayed is Information which includes internal and external resources on the IoE. Click on the next blades to view:

- **The Vulnerability details** which provides explanations on the weakness detected in your AD infrastructure.

- The list of **Deviant objects** which includes technical details, a search filter (including a search wizard and a standard search field) and an action button to export reports.

- **Recommendations** on how to solve the issue.

Hover areas
After clicking on a tile on the Indicators of Exposure page, the details on the IoE selected will appear in the form of blades.

Go to the Deviant objects blade and hover the Path column to view the full path to an AD object.

Date picker
You can select a Start date and an End date to run a search on deviant objects.

Action buttons
Click the Export button to generate a report listing the deviant objects.

Check boxes
You can select the forests and domains to be included in the search or in the display. To restrict the search to a specific forest or domain, check the box in the upper-right corner and select the items from the drop-down list.
Search field

You can enter the name assigned to an IoE and its description keywords to run a search.

For more details, see Retrieve an IoE from the List.
View Indicators of Exposure

The Indicators of Exposure page is accessible from the left navigation menu. It shows the security maturity level of your Active Directory (AD) infrastructures.

Display Mode

There are two ways to display Indicators of Exposure. By default, Tenable.ad will show only the IoEs including deviant objects.

But if you want to see all the IoEs available, you can flip the Show all indicators toggle switch in the upper-right corner to Yes.

Severity Levels

Indicators of Exposure are displayed as tiles ranging from highest to lowest severity level:
• The Critical severity level is displayed in red at the top of the page.
• The High severity level is displayed in orange.
• The Medium severity level is displayed in yellow.
• The Low severity level is displayed in blue at the bottom of the page.

Severity levels allow the user to assess at a glance the severity of the detected vulnerabilities and to prioritize remediation actions.

Tile Information

Each IoE tile displays the following information:

• The IoE name
• A short description
• The name of the domain impacted by the IoE (or their number if there are more than two domains)
• An icon representing the complexity level of the IoE
If the IoE status is compliant, the message **No indicators found with deviant objects** is displayed.

Click on the tile to display the IoE details.
Retrieve an IoE from the List

Purpose

- You can filter IoE results to find an Indicator of Exposure of interest faster with the search field.
- You can also restrict the search to a specific forest or domain.
- Click on Indicators of Exposure on the left navigation bar to access the search field at the top of the newly displayed page.

Search for an Indicator

Indicators of Exposure can be displayed:

- By severity level via color codes (red for Critical, orange for High, yellow for Medium and blue for Low).
- Vertically, by order of severity (red for top priority and blue for least priority).
- Horizontally, by order of complexity (starting with the least complex cases and ending with the most complex cases). The complexity indicator is dynamically computed by Tenable.ad's platform to describe how difficult it will be for the Administration team to fix the deviant IoE.
- In alphabetical order (new feature coming soon).
- By domain name (new feature coming soon).

Examples

You can enter the name assigned to an IoE and its description keywords to run a search.
Show All Indicators

There are two ways to display IoEs on the Indicators of Exposure page. By default, Tenable.ad will show only the IoEs including deviant objects.

But if you want to see all the IoEs available in Tenable.ad, he/she will flip the Show all indicators toggle switch in the upper-right corner to Yes.
Select Forests and Domains

To restrict the search to a specific forest or domain, check the box in the upper-right corner and select the items from the dropdown list.
Indicators of Exposure

**Critical**

Weak password policies are applied on users

Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.

- Tenable's domain

**High**

Potential clear-text password

Some clear-text passwords seem to be readable by every domain's users.

- Tenable's domain

**Medium**

Accounts with never expiring passwords

Accounts with the DONT_EXPIRE property are not affected by password renewal policy.

- Tenable's domain

**Low**

No indicators found with deviant objects

Show indicators 33 domains
Indicators of Exposure

- Critical
  - Weak password policies are applied on users
    - Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
      - Tenable's domain Complexity
  - High
    - Potential clear-text password
      - Some clear-text passwords seem to be readable by every domain's users
        - Tenable's domain Complexity
  - Medium
    - Accounts with never expiring passwords
      - Accounts with the DONT_EXPIRE property are not affected by password renewal policy
        - Tenable's domain Complexity
- Low
  - No indicators found with deviant objects

Search a forest or domain

- Tenable's forest
- Tenable's forest 2
- Tenable's forest 3

Expand all | Select all domains
View Indicator Details

Tenable.ad provides detailed information on each Indicator of Exposure affecting your AD infrastructure. IoEs are behavioral detection indicators powered by the latest intelligence on the Active Directory threat landscape.

- To access Indicator details blades, click on any tile on the Indicators of Exposure page. You will be directly taken to the first blade called Information.

Understand IoE Details

Purpose

Accessing details on a specific Indicator of Exposure will allow you to review technical information and take remediation actions if required by the Indicator of Exposure's severity level (Critical, High, Medium, Low) and compliance status.

Tenable.ad assigns severity levels (Critical, High, Medium or Low) to the constant flow of events that is being monitored and analyzed.

IoE Details layout

Differences between IoE, event and deviant object

- An **Indicator of Exposure** describes a type of threat that affects Active Directory. It may include several technical vulnerabilities. Each IoE is collected in one place called a blade providing information on detected vulnerabilities, associated deviant objects, and recommendations on remediation actions. Every Tenable.ad's IoE measures in real-time security level after receiving an event.

- An **event** symbolizes every change related to security that can appear into an Active Directory infrastructure. It could be a password change, a user creation, a new GPO or the modification of a GPO parameter, a new delegated right, etc. An event can change the compliance status of an IoE (from compliant to non-compliant).

- A **deviant object** is a technical element which allows (on its own or associated with another deviant object) the attack vector described in an IoE to work.

Top section
This section recapitulates the information already provided in the Trail Flow table:

- The **Name** of the IoE.
- Its **Severity** level (Critical, High, Medium or Low).
- Its compliance **Status** which displays the result of the last analysis run.
- The **Latest detection** which displays the last time the analysis was run.

**Lower section**

This section displays a row of clickable blades (also called tabs) and content depending on the blade selected.
Indicator of Exposure details

**Access IoE blades:** Remember to click on Indicators of Exposure in the left navigation menu and select an IoE tile. You will be directly taken to the Information blade which is the first tab in the row.

View Information Blade

This blade includes the following sub-sections:

- An Executive summary that gives an overview on the issue and helps managers make appropriate decisions.
- The Documents sub-section with links pointing to external resources on the IoE.
- The Attacker known tools sub-section that indicates the name of the hacking tool.
- A tree structure of the Impacted domains.

View Vulnerability Details Blade

- Click on the next blade called Vulnerability details to view a full description of the potential threat.

This blade informs administrators about the risks incurred by their AD infrastructures if no remediation action is taken.
View Deviant Objects Blade

Purpose

Deviant objects reveal weaknesses or potentially dangerous behaviors in supervised AD infrastructures. Applying filters to deviant objects will help administrators pinpoint the issues that are critical to your AD infrastructures.

When an IoE status is not compliant and therefore includes deviant objects, remediation actions should be initiated to correct the security deficiencies detected by Tenable.ad.

For more details on suggested remediation actions, see View Recommendations Blade.

Access the blade
• Click on the Deviant objects blade to view the weaknesses affecting the IoE that you have previously selected on the Indicators of Exposure page.

Blade layout

This blade includes the following items:

• A search wizard and a standard search field to filter deviant objects.
• A date picker to run a search within a specific time frame.
• An action button to select the forests and domains to display or on which to perform a search.
• Action buttons in the Reasons column to display the incriminating attributes affecting the IoE.
• A toggle switch to show ignored deviant objects.
• An Export all button to download a report showing all deviant objects.
• A table including technical information on deviant objects.

Understand table labels

The deviant objects table includes the following items:

• The Type column indicates the origin of any security-related change in AD infrastructures (LDAP or SMB protocols).
• The Object column indicates the class or file extension associated with an AD object.
• The Path column indicates the full path to an AD object. It will allow the user to identify the unique location of this object in the AD. Hover this cell to view full information.
• The Domain column indicates from which domain the change in your AD infrastructure comes from.
• The Reasons column lists the incriminating attributes affecting deviant objects.
**Deviant objects blade: table labels**

For more details on how to use the Deviant objects table, see Filter Deviant Objects.

For more details on Incriminating Attributes, see View Incriminating Attributes.

**View Recommendations Blade**

**Purpose**

The recommendations provided by Tenable.ad are designed to restore compliance with your security requirements and improve your security posture.

**Blade layout**
This blade includes the following sub-sections:

- An Executive summary that gives an overview on the solution suggested by Tenable.ad.
- The Details sub-section that provides advice on how to implement the action plan and helps managers initiate the necessary changes to their AD infrastructures.
- The Documents sub-section with links pointing to external resources on the suggested solution or threat.

**Recommendations blade**

**Access the blade**
• Click on the Recommendations blade to view the remediation actions suggested by Tenable.ad.
Filter Deviant Objects

Purpose

Deviant objects reveal weaknesses or potentially dangerous behaviors in supervised AD infrastructures. Applying filters to deviant objects will help administrators pinpoint the issues that are critical to your AD infrastructures.

From there, the user can perform several actions such as:

- Retrieve an AD object affected by deviant objects.
- Ignore an AD object affected by deviant objects for a period of time.
- Select the forests and domains to run a search.
- Access explanations on the incriminating attributes affecting the IoE.
- Download a report showing all deviant objects.

Locate Data

1. Click on Indicators of Exposure on the left navigation bar.
2. Select an IoE tile.
3. Select the Deviant objects blade to access the blade window.
Retrieve a Deviant Object with the Wizard

You can either use the search wizard or enter manually the query expression elements in the standard search field.

**Building faster queries:** The search wizard allows you to create query expressions faster than the standard search field.

Wizard search

Search elements in the wizard

The following search elements are available to customize your search queries:

**AND/OR combinator buttons**

In the first condition, you can select the AND or the OR combinator which will be applied to the query expression. To add another condition to the query, click on the +AND or the +OR combinator button.

---

**Search elements in the wizard**

**Bin icon**
You can delete attributes in the query expression by clicking on the Bin icon 🗑️ at the far right of the attribute fields.

**Add a new condition**

You can add new conditions to the query expression by clicking on the +AND or +OR combinator button 🔗 under the attribute fields.

**Add a new rule**

You can add new rules to the query expression by clicking on the +Add a new rule action button 🎨 under the attribute fields.

**Query syntax**

**Add an attribute**

1. After applying the combinator to the first condition 🔗, select the attribute from the dropdown menu and enter its value.
2. Click on the +Add a new rule action button 🎨 to add another attribute to the first condition.
3. If you add another condition to the query, click on the +AND or +OR combinator button 🔗.
4. Configure the second condition. The search wizard will display the query expression in the preview.

**Add a combinator to the first condition in the query (preview)**

**Get familiar with the search wizard**

To learn how to use the search wizard, you can enter a query that you are familiar with. Then, click on the Magic wand icon to display the query built by the wizard.
Query entered manually in the search field
Query built by the search wizard (result)

Procedure

1. Click on the Magic wand icon on the left of the standard search field to display the search wizard.
Display the search wizard (magic wand icon)

2. To define the query expression in the panel, first click on the AND or the OR combinator button ❶ to be applied to the first condition.

3. Select the attribute from the dropdown menu and enter its value ❷. To add an attribute, click on the + Add a new rule action button ❸.
Build a query in the search wizard

4. Click Validate to run the search or Reset if you need to delete your query parameters.
Retrieve Deviant Object Manually

Type the query expression to run a search in the standard search field.

Query syntax

Click in the search field and type the expression to run a search.

**Search box:** Make sure that you use the correct syntax to implement the filter. In case of syntax error, click on the X sign on the right side to clear the search field and type the expression again. Also note that the search field is case-sensitive.

Procedure

- Type the search expression in the field and press Enter if this is the only search criterion being used. In this example, we have run a search that looks for an object identified by its DN called "Admin". For more details on a complex query expression, see Filter the Real-Time Flow of Events.
Filter deviant objects (query)

- To limit the search to a specific time frame, select the Start date and End date from the date picker.

Use the date picker to filter deviant objects

- To restrict the search to a specific forest or domain, check the boxes in the upper-right corner and select the items from the dropdown list.
Select forests and domains to filter deviant objects
Ignore a Deviant Object

Purpose

To prevent cluttering the screen for investigation or reporting purposes, the user can filter out some deviant objects. He/she can force Tenable.ad to ignore objects for a period of time.

Let's take the example of an external contractor who has been granted administrator's access rights to your AD infrastructures for one week. The contractor's actions will be monitored and analyzed by Tenable.ad but to disable alert notifications during the contractor's mission, you can decide to filter out this particular AD object until a specific date.

Procedure

You can choose to ignore one or several deviant objects from the table. It is up to you to decide whether to apply your custom filter immediately or to define a time frame during which the filter will be active.

To filter out objects:

1. To select the deviant objects to be ignored, check the boxes in the first row of the table. For faster selection, you can check the Select all box.

2. Select Ignore selected objects from the dropdown list at the bottom of the screen and click OK.
Select the deviant objects to be filtered out
3. On the context-sensitive window displayed on the right, select the date until which you want to ignore the deviant objects and click OK. Ignored elements are no longer displayed in the table.

![Deviant objects filter](image)

Filter out deviant objects (date picker)

4. This is a way to prevent cluttering the screen, but you can also choose to show ignored deviant objects. To do this, flip the Ignored toggle switch in the upper-right corner to the right (No changes to Yes). Ignored elements are identified by a white check mark in a blue box.
Show ignored deviant objects

To restore the initial situation and disable filters:

1. Check that the Ignored toggle switch is set to Yes.
2. Then, check the blue boxes of the ignored deviant objects or check Select all.
3. Select Stop ignoring selected objects from the dropdown list and click OK.
4. To validate your changes, click OK on the context-sensitive window displayed on the right. The blue boxes with a white check mark have disappeared and all deviant objects are now visible.

To filter out by time frames
1. Type the expression in the search field to create your own custom filter ❶.

2. Select the Start date and End date from the date picker ❷ if you want to restrict the search by specifying a time frame (starting point in the past and endpoint in the future).
   - To restrict the search to a specific forest or domain ❸, check the boxes in the upper-right corner and select the items from the dropdown list.
   - To restrict the search to a specific incriminating attribute affecting the IoE ❹, check the boxes in the upper-right corner.

3. Verify that the Select all box ❺ is checked if the filter is to be applied to all deviant objects. If not, check the boxes in the first row of the table to select individually the deviant objects to be ignored.

4. Select Ignore selected objects from the dropdown list ❻ and click OK❼.

Use the date picker to filter out deviant objects
5. On the context-sensitive window displayed on the right, select the date until which you want to ignore the deviant objects and click OK. Ignored objects are no longer displayed on the table.

Select the date until which you want to ignore the deviant objects

To restore the initial situation and disable filters:

1. Check that the Ignored toggle switch is set to Yes.

2. Then, check the blue boxes (with a white check mark) of the ignored deviant objects or check Select all.

3. Select Stop ignoring selected objects from the dropdown list and click OK.
4. To validate your changes, click OK on the context-sensitive window displayed on the right. The blue boxes with a white check mark have disappeared and all deviants elements are now visible.
Restore initial situation (context-sensitive window)
Restore initial situation (result)
View Incriminating Attributes

The incriminating attributes contributing to the detection of deviant objects are gathered in a single location. The explanations and reasons provided by Tenable.ad's interface will enable administrators to better understand why a deviance has been detected.

Locate Data

1. Click on Indicators of Exposure on the left navigation bar.
2. Select an IoE tile.
3. Click on the Deviant objects blade.
4. Select a deviant object entry from the table. The detailed view of the incriminating attribute will be displayed.

Incriminating Attribute Details
To display the detailed view of an incriminating attribute and the reasons why a deviant object was detected, hover and select a deviant object entry from the table.

Labels

The colored labels in the upper-left corner and in the Reasons column are designed to make a distinction between the various reasons that led to the detection of a deviant object.
Check boxes

Check the boxes to select the reasons to be ignored/unignored when a deviance is detected.

Values

?  
If a reason includes a ?, it means that the attribute value is missing (empty) which is an abnormal behavior.

No description is available for this deviance

If a reason displays No description is available for this deviance, it means that this detection dates back to version 2.6 and that it is no longer managed by the incriminating attributes system.

Ignore/Stop Ignoring Deviances
Check the Select all box ❶ or click individually ❷ on each reason to be ignored/unignored.

Then, choose the action from the dropdown menu ❸ to apply to the deviance.
Copy to Clipboard

To copy the details of a reason to your clipboard, click on the File icon. Paste the text into your editor.
Export Deviant Objects Report

Locate Data

To access the Export all button on the Deviant objects blade, click on any tile on the Indicators of Exposure page. You will be directly taken to the first blade called Information.

Then, click on the Deviant objects blade. The Export all button is displayed in the lower-right corner.

Download the Report

Click the Export all button to generate a custom report providing the list of deviant objects that you have selected from the table using the search wizard or standard search field. A blade window appears on the right.

Choose the format and click again on Export all.

Click on the Cross sign to close the export window.
Export reports on deviant objects

Select export format

For more details on how to retrieve a deviant object, see Filter Deviant Objects.
Administrator Guide

The Administrator's Guide is a reference and information document that details day-to-day administration tasks to keep your Tenable.ad instance running smoothly.

It is specially designed for users with administrator's access rights and privileges to perform the initial setup and manage the solution.

The functionalities described in this guide include the following:

- Perform Initial Setup to access the web interface, obtain your first credentials and set up your client certificate.
- Manage User Accounts to create and edit user accounts, as well as create and assign roles to users (using Role-Based Access Control rules).
- Manage the System to manage forests and domains, configure alerts, and define user authentication.
- Troubleshoot Authentication Issues to help administrators address and solve authentication issues.
- Use Tenable.ad's Public API to help administrators connect to Tenable.ad's database services.

Tenable.ad's features are based on the license type. Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack.
Getting Started

Access the Web Interface

To call up the Tenable.ad web interface, enter its IP address or host name in the address bar of any web browser.

As the web interface is only listening on the TCP/443 port using HTTPS, accessing it by its IP address will result in a TLS warning.

You can access the Tenable.ad web application through a URL of the type CLIENT_URL.tenable.ad.

Obtain Your First Credentials

By now, you should have received your credentials (login and password) from the Tenable.ad team or the staff in charge of Tenable.ad deployments in your organization.

According to the configuration selected by the application administrator, you can log into Tenable.ad via:

- Login/Password authentication
- LDAP authentication
- SAML authentication

By default, only the Login/Password authentication option (Tenable.adblade) is displayed. For more details, see Establish the First Connection.
Understand Indicators of Attack

Tenable.ad's features are based on the license type. Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack.

IoE vs. IoA Overview

Tenable.ad is the only real-time platform able to provide both proactive and reactive capabilities to protect your AD infrastructures. Tenable.ad's Indicators of Exposure help you detect attack vectors, security gaps, and misconfigurations in your AD infrastructures before attackers do.

Meanwhile, Tenable.ad's Indicators of Attack help your organization detect and take immediate action when the most advanced exploit techniques try to compromise your AD infrastructures.

While Tenable.ad's Indicators of Exposure do not require any change to your infrastructures, Indicators of Attack require your infrastructures to share information with Tenable.ad in a seamless, and non-intrusive way.
How the IoA Engine Works

Tenable.ad leverages three sources of information to detect security incidents:

- Your AD database
- The SYSVOL shared folder
- The ETW engine

By combining information from these three sources, Tenable.ad is fully capable of detecting in real time the most advanced security incidents targeting your AD infrastructures.

Let's dig into the details of the IoA engine process.

Setting the Background

Prior to the Implementation of IoA

Active Directory (AD) is an infrastructure service built to manage authentication and access control in a computer network. AD relies on servers called Domain Controllers (DCs) which are running Windows Server operating systems. DCs need to exchange information over time via a replication protocol which allows domain controllers installed in different facilities to be synchronized.

Data replication uses two protocols:

- DRSR (Directory Replication Service Remote protocol) which supports AD object replication.
- DFS (Distributed File System) which supports file replication.

Prior to the release of our new IoA feature, Tenable.ad used to forward queries to domain controllers via APIs in order to gather AD replication flow data.

Following the Release of IoA

To detect attacks, Tenable.ad now also collects data from the underlying Windows operating system, which is not replicated across the DCs. In short, Tenable.ad's new functionality relies on the already existing mechanisms within AD to collect data of interest through the implementation of a tailor-made script.
Deploy Indicators-of-Attack

Download the IoA script

From the Tenable.ad console interface, configure the setup view with IoAs and domains to monitor (regarding available workload quota), then download a deployment script by clicking on Download the installation script action button under System > Configuration > Indicators of Attack.

Register-TenableIOA.ps1 is the default filename given by Tenable to the script but you can change it as you wish.
How the IoA Script Executes

The script can be run from any machine joined to the AD domain monitored by Tenable and that can reach domain controllers via the network. The script must be uploaded to this machine with the method of your choice. It is required to run the script with an administrative account having the ability to create and link a new GPO to the Domain Controllers organizational unit. The script can also be run under specific user context with Start-Process and runAsUser verb (with applicable user and password filled). Some customers run the script directly from one of the Domain Controllers, which is supported too.

After that, the script will create in the AD database, a new Group Policy Object named by default Tenable.ad. The Tenable.ad GPO will be linked only to the Domain Controllers' Organizational Unit (OU) containing all the domain controllers. Thanks to the GPO mechanism, the new policy will be automatically replicated between all DCs.
The GPO contains PowerShell scripts which will be executed locally by all domain controllers. These PS scripts are designed to collect data of interest. They will configure in the machine’s memory an event watcher and a WMI Producer/Consumer. The event watcher receives event logs and periodically buffers them, then flushes them to a file stored in a network share called Sysvol (each DC will flush to a single Sysvol file which stores collected events and replicates it to other domain controllers). The WMI consumer makes this mechanism persistent, by registering again the event watcher again when a domain controller restarts. WMI (Windows Management Instrumentation) is a Windows component which provides users with information about the status of local or remote computer systems. The producer wakes up and notifies the consumer every time a domain controller is restarted. As a result, the consumer will register the event watcher again.

At this point, DFS replication comes into play and automatically synchronizes files between domain controllers. Tenable.ad’s platform which is listening for incoming DFS replication traffic will use this data to gather events, run a security analysis and subsequently generate IoA alerts.

What Local Data is Retrieved by Tenable

Windows event logs record all the events which occur in the operating system and its applications. Event logs rely on a framework of components which is integrated to Windows and called Event Tracing for Windows (ETW). ETW is located in the kernel and produces data stored locally on the Domain Controllers which is never replicated by Active Directory protocols.

Via the WMI engine queried by the management event watcher object and its query language, Tenable.ad will collect only useful ETW data segments in the form of insertion strings extracted from the event logs. These insertion strings are written in a file stored in the Sysvol folder and replicated via the DFS engine. This way, Tenable.ad will gather just the right amount of security data from ETW to run a security analysis and detect attacks.
In short, Tenable.ad leverages the DFS, the management event watcher and a WMI consumer which are already activated on your environments to get the security information required and rely in large majority on Microsoft code on the domain controllers.

View the IoA Script Summary

Here is a practical and transparent step-by-step overview of how the Tenable.ad script is deployed.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
<th>Component Involved</th>
<th>Technical Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Register Tenable.ad's IoA deployment</td>
<td>GPO Management</td>
<td>'Tenable.ad' (default name) GPO is created and linked to the Domain Controllers OU.</td>
</tr>
<tr>
<td>2</td>
<td>Start Tenable.ad DC local</td>
<td>DC local</td>
<td>Each Domain Controller (DC) detects the new GPO to</td>
</tr>
<tr>
<td></td>
<td>able.ad's IoA deployment on DC</td>
<td>system</td>
<td>apply (depending on the AD replication and Group Policy refresh intervals).</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Register an event watcher and a WMI producer-consumer</td>
<td>DC local system</td>
<td>An Immediate Task is registered and executed on the system. This task will run a PowerShell process to create instances of the following classes: ManagementEventWatcher and ActiveScriptEventConsumer. These objects will be used to receive and store ETW messages.</td>
</tr>
<tr>
<td>4</td>
<td>Control Advanced Logging Policy state</td>
<td>DC local system</td>
<td>The advanced logging policy is activated on the system by setting the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy.</td>
</tr>
<tr>
<td>5</td>
<td>Local Logging policy is updated</td>
<td>DC local system</td>
<td>Depending on the IoAs to detect, a fine-grained (advanced) logging policy is dynamically generated and activated. This policy does not deactivate any existing logging policy but only enriches them if necessary (if a conflict is detected, the GPO installation script will stop with a message Tenable.ad requires the audit policy '...' but the current AD configuration prevents its usage)</td>
</tr>
<tr>
<td>6</td>
<td>Collect ETW messages</td>
<td>DC local system</td>
<td>Relevant ETW messages are captured, buffered periodically and saved to files (one per DC) stored in the Sysvol folder associated to Tenable.ad GPO (...{GPO_GUID}\Machine\OA&lt;DC_name&gt;).</td>
</tr>
<tr>
<td>7</td>
<td>These files are replicated to Tenable.ad’s platform</td>
<td>Active Directory</td>
<td>Using DFS, Active Directory will replicate files across the domain. Tenable.ad platform will receive the file as well.</td>
</tr>
<tr>
<td>8</td>
<td>These files are overwritten</td>
<td>Active Directory</td>
<td>Each DC will automatically and continuously write the buffered events in the same file, in a periodic way.</td>
</tr>
</tbody>
</table>
ETW Data Retrieval by Tenable.ad

Tenable.ad v3.0 introduced a new kind of indicators: Indicators of Attack (IoAs).

Indicators of Exposure (IoEs) have been used since the first version. With a proactive approach, they show a misconfiguration or a weakness that could lead to a compromised infrastructure.

Whereas IoAs provide a reactive approach to the Tenable.ad solution. This new functionality adds the ability to detect an attack in real time.

IoEs were mainly based on two sources: LDAP and Sysvol.

IoAs require a new source, the Event Tracing for Windows (ETW). From a technical point of view, Microsoft uses an XML format to save event logs. To increase performance, Microsoft does not store on each event log file the entire string of characters that will be displayed to the customer. The XML file only keeps the Insertion Strings describing the dynamic part of an event log.

Tenable.ad collects these Insertion Strings through the Sysvol folder.
**Tenable.ad Indicators of Attack**

Tenable.ad collects the insertion strings associated with the event IDs listed in the table below and processes them to determine whether or not the events represent an attack. The table also indicates the audit policies required by IoA and which are automatically enabled by the installation script. The script-based process is fully transparent to the customer.

Please note that the IOA script needs to be redeployed in case the configuration for the attacks detection is changed.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>2</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>3</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>4</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>5</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>6</td>
<td>Tenable.ad Indicators of Attack</td>
</tr>
<tr>
<td>7</td>
<td>Petit-Potam</td>
</tr>
</tbody>
</table>
OS Credential Dumping: LSASS Memory

After a user logs on, attackers may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). A sysmon extension is required for these audits.

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>— Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4634</td>
<td>Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>— Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Sysmon - Process creation</td>
<td>Sysmon - N/A</td>
</tr>
<tr>
<td>5</td>
<td>Sysmon - Process terminated</td>
<td>Sysmon - N/A</td>
</tr>
<tr>
<td>8</td>
<td>Sysmon - CreateRemoteThread</td>
<td>Sysmon - N/A</td>
</tr>
<tr>
<td>10</td>
<td>Sysmon - ProcessAccess</td>
<td>Sysmon - N/A</td>
</tr>
<tr>
<td></td>
<td>Requires Sysmon extension</td>
<td>Yes</td>
</tr>
</tbody>
</table>
DCShadow

DCShadow is another late-stage kill chain attack that allows an attacker with privileged credentials to register a rogue domain controller in order to push changes to a domain via domain replication.

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4634</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>4662</td>
<td>├ Category: Directory Service (DS Access)</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Directory Service Access</td>
<td></td>
</tr>
</tbody>
</table>

Requires Sysmon extension

No
DCSync

The DCSync command in Mimikatz allows an attacker to pretend to be a domain controller and retrieve password hashes from other domain controllers, without executing any code on the target.

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4634</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>4662</td>
<td>├ Category: Directory Service (DS Access)</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Directory Service Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Requires Sysmon extension</strong></td>
<td>No</td>
</tr>
</tbody>
</table>
Golden Ticket

A Golden Ticket attack is a type of attack in which an adversary gains control over an Active Directory Key Distribution Service Account (KRBTGT), and uses that account to create valid Kerberos Ticket Granting Tickets (TGTs).

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4768</td>
<td>├ Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Kerberos Authentication Service</td>
<td></td>
</tr>
<tr>
<td>4769</td>
<td>├ Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Kerberos Service Ticket Operations</td>
<td></td>
</tr>
<tr>
<td>4770</td>
<td>├ Category: Account Logon</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Kerberos Service Ticket Operations</td>
<td></td>
</tr>
</tbody>
</table>

Requires Sysmon extension

No
Petit-Potam

Petit-Potam is a tool that coerces remote servers to authenticate to another machine on the network due to a Windows vulnerability. If Petit-Potam targets a domain controller, an attacker can authenticate to another network machine using the domain controller's credentials.

An attacker can use Petit-Potam in conjunction with PKI misconfigurations to generate a certificate to allow it to authenticate as the domain controller (such as when Active Directory Certificate Services (AD CS) web enrollments are available).

In order for this indicator-of-attack to detect Petit-Potam, the "Microsoft-Windows-EFS/Debug" channel must be enabled, which the IOA script does automatically by adding the following registry key: "Microsoft-Windows-EFS/Debug" to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog".

**Note:** If you previously set a configuration for the log retention for this specific channel, adding this registry key overrides the initial configuration, and events prior to this configuration are no longer visible.

**Tip:** Tenable recommends checking the targeted Domain Controller event logs to verify the source of the attack (account used and originating computer).

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
</table>
| 4624      | ⊲ Category: Logon/Logoff  
\n|
|          | ⊲ — Sub-category: Logon |       |
| 4634      | ⊲ Category: Logon/Logoff | Success |
|          | ⊲ — Sub-category: Logoff |       |
|          | **Requires Sysmon extension** | No |

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Provider Name</th>
<th>Channel Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft-Windows-EFS</td>
<td>Microsoft-Windows-EFS/Debug</td>
</tr>
</tbody>
</table>
A brute-force password guessing attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4625</td>
<td>├ Category: Logon/Logoff</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>4771</td>
<td>├ Category: Account Logon</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Kerberos Authentication Serviced</td>
<td></td>
</tr>
<tr>
<td>4776</td>
<td>├ Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>└ Sub-category: Credential Validation</td>
<td></td>
</tr>
</tbody>
</table>

**Requires Sysmon extension**

No
### Password Spraying

Password spraying is an attack that attempts to access a large number of accounts (usernames) with a single or few commonly used passwords - also known as the "low-and-slow" method.

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>├ Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>├─ Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4625</td>
<td>├ Category: Logon/Logoff</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>├─ Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>4771</td>
<td>├ Category: Account Logon</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>├─ Sub-category: Kerberos Authentication Serviced</td>
<td></td>
</tr>
<tr>
<td>4776</td>
<td>├ Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>├─ Sub-category: Credential Validation</td>
<td></td>
</tr>
</tbody>
</table>

**Requires Sysmon extension**

<table>
<thead>
<tr>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>
Potential Impacts on your AD Infrastructures

Agentless Solution

Potential impacts are extremely limited. While traditional approaches would recommend deploying a proprietary agent on your Domain Controllers (and thus increasing their risk exposition) or to forward gigabytes of Event Logs over your network, Tenable.ad offers an innovative approach to receive just the right amount of information.

Absolutely no third-party software is deployed, and the setup process only requires a one-time administrative action. The changes that could impact your environment are the files created on the SYSVOL share to be replicated to Tenable.ad.

No Extra Workload

Tenable.ad carefully developed its engine to keep these files as minimal as possible. One file is required per DC. The bandwidth consumed is exceptionally low, and writing a file does not add any significant workload on the system hosting the domain controller.

No Configuration Changes Required

In order to have the required ETW data, Tenable.ad's GPO will automatically configure your domain controllers event log policy. This new audit policy will supersede your existing logging policy but without overwriting your existing configuration. All your existing configurations will be kept as-is. Tenable.ad will only activate the right policy to provide reliable detection capabilities.
Technical Prerequisites

Here is how to configure the monitored AD infrastructures to support Tenable.ad Indicators-of-Attack (IoA).

The Tenable.ad platform provides real-time security incident detection thanks to correlation of ETW information (generated by each domain controller) with LDAP and SYSVOL events. This section is focused on how to configure the monitored Domain Controllers to retrieve the required ETW information and to forward them to the Tenable.ad platform.

This page only applies for the platform benefiting from the Indicators-of-Attack module (IoA). It will first discuss the Tenable.ad deployment script, a PowerShell script used to deploy Windows-component requirements on the Domain Controllers. Secondly, it will detail how to install Microsoft System Monitor (System Monitor), a Windows system tool needed by some Tenable.ad IoA to get relevant system data. Finally, it will cover how to uninstall or update the Tenable.ad deployment script.
Install the Tenable.ad IoA Module

To retrieve the required ETW information within the Tenable.ad platform, a unique system based on an agentless solution has been designed. This solution extracts ETW insertion string data and stores them with an event watcher to a SYSVOL file per DC. This approach only necessitates a one-time initialization step to set up the Windows-native components to install the event watcher and a WMI consumer (to make the event watcher persistent).

**Note:** ETW insertion strings are the same information used by Windows to build its Event Logs.

This initialization step is performed on each domain controller thanks to a PowerShell script downloadable from Tenable.ad console, in System > Configuration > Indicators of Attack. This page displays the commands to be executed (one for each domain registered in Tenable.ad). To activate the monitoring process, the Tenable.ad’s deployment script will create a GPO embedding an immediate task launching an event watcher and a WMI consumer to extract ETW information.

The Tenable.ad’s deployment script requires to be launched from a machine member of the domain to monitor and to be run with an account having enough administrative privileges to create a GPO and to link it to the Organizational Unit hosting the Domain Controllers of the domain to monitor. The script can also be run under specific user context with Start-Process and runAsUser verb (with applicable user and password filled). Some customers run the script directly from one of the Domain Controllers, which is supported too.
DEFINITION OF ATTACK SCENARIOS

<table>
<thead>
<tr>
<th>Attack name</th>
<th>Workload Quota</th>
<th>Ratchet and So...</th>
<th>joshuah.com</th>
<th>elica.com</th>
<th>bertha name</th>
<th>juven.net</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Golden Ticket</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCShadow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberoasting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

INDICATORS OF ATTACK

To install the indicators of Attack detection engine, please download the installation file (bottom right button) and run each of these lines in a PowerShell terminal on the domain controller.

```powershell
# Register-Tenable204 -DomainControllerAddress 87.53.2.239 -TenableServiceAccount suclott
# Register-Tenable204 -DomainControllerAddress 10.117.5.239 -TenableServiceAccount suclott
# Register-Tenable204 -DomainControllerAddress 139.41.47.179 -TenableServiceAccount suclott
```

- Workload Quota used: 12/50

[Save] [Download the Installation File]
Configuration Adaptations

For each targeted domain, executing this script will apply configuration changes. These changes are listed in the Synthesis of the Technical Changes Made by Tenable’s Deployment Script. Some parameters (e.g., the GPO name) can be modified using command-line arguments passed when executing the script.

Use the following command to have the exhaustive list of available arguments and examples:

```
Get-Help Register-TenableIOA.ps1
```

Synthesis of the Technical Changes Made by Tenable’s Deployment Script

The following list describes the major configuration changes applied to the Domain Controllers to monitor. These changes are transparently applied by the GPO created by Tenable.ad’s deployment script.

Configuration changes:

- Add a GPO, named “Tenable.ad” by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task that will install an event watcher, a WMI consumer and the Advanced logging policy.

- Activate the Microsoft Advanced logging policy by modifying a registry key (using the GPO). Specifically, the registry key is:

  ```
  HKEY_LOCAL_MACHINE\SystemCurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy
  ```

  set to 1.

- Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable.ad.

- Install an event watcher and a WMI consumer (per domain controller, from classes ManagementEventWatcher and ActiveScriptEventConsumer) that will write files in this GPO’s folder (`.../{GPO_GUID}/Machine/IOA/{DC_name}.gz`).
○ The ManagementEventWatcher object consumes the event logs insertion strings which are then written into SYSVOL files. Each file is located at .../\{GPO_GUID\}/Machine/IOA/\{DC_name\}.gz.

○ The ActiveScriptEventConsumer filter ensures the previous event watcher is registered again if the DC is restarted.

The new Event log policy is dynamically generated within the install script and activated by the GPO. Applying this policy is mandatory to have the ETW engine generate the Insertion Strings required by Tenable.ad. This policy does not disable any existing logging policy but enriches them if need be. If a conflict is detected, the GPO installation script will stop with a message stating that the audit policy policy_name is needed, but that the current AD configuration prevents its configuration.

For more technical details describing step by step the changes operated by the Tenable.ad deployment script, see Configuration Adaptations.
Limitation and Potential Impacts

Despite being the less intrusive way to capture Domain Controllers’ ETW information, some limitations and limited impact could exist in the Tenable.ad approach. These drawbacks need to be reviewed before starting the deployment of the Indicators-of-Attack module.

Tenable.ad incident detection module is based on the ETW data thus bound by their limitations as defined in Microsoft’s documentation.

The installed GPO needs to be replicated over the entire domain, and the GPO refresh interval must be passed, for the install process to be complete. During this installation-in-progress period, false positives and false negatives can happen even though Tenable.ad minimizes this effect by not starting the checks in the IoAs immediately.

Tenable.ad is using the SYSVOL file share to retrieve ETW information coming from the Domain Controllers. Replicating files between the Domain Controllers and the Tenable.ad platform may also consume some network bandwidth, depending upon the number of domain controllers in the domain. These impacts are controlled as there is one file (containing events) per DC.
Uninstall the Tenable.ad IoA Module

Should you uninstall the Tenable.ad product from the Domain Controllers, the configuration can be rolled back using the Tenable.ad deployment script.

To uninstall the audit policies, event watcher, WMI consumer and initial GPO, simply run the following command:

```
Register-TenableIOA.ps1 -Uninstall
```

This command creates a new GPO, named Tenable.ad cleaning by default, that will be used to clean the previously installed GPO. The previous GPO and its SYSVOL files, including the registry setting the advanced logging policy, the event watcher and the WMI consumer will be cleaned.

If you have changed the initial GPO’s name (e.g., to comply with your naming conventions), you will have to pass it to the uninstall step too for the script to know which GPO to uninstall.

This new GPO also needs to be replicated over the entire domain, and the GPO refresh interval passed, for the uninstall process to be complete. Tenable recommends letting it run for a week, and then simply manually removing this cleaning GPO.
Update the Tenable.ad IoA Module

To update the Tenable.ad IoA module, you can download the new script version and re-run the installation as explained above.

**Note:** When updating, you must uninstall the previous GPO first, then wait a moment (4 hours by default) to ensure cleaning GPO is replicated along all domain controllers. Make sure to manually remove this cleaning GPO before installing new GPO again.
Microsoft Sysmon

Tip: Sysmon Monitor, better known under the name of Sysmon is a Microsoft Sysinternals tool designed to provide additional security logs to the built-in Windows event logs. It can provide detailed information about process creations, network connections, process injections, and much more.

The additional Sysmon software is required to activate some of the Tenable.ad Indicators of Attack. Supported by Microsoft, this software registers a new Windows service and driver to provide more security-oriented information to the ETW infrastructure.

Sysmon adds a new log provider, under Applications and Services Logs/Microsoft/Windows/Sysmon/Operational, with new events. Tenable.ad uses only a few of them, presented in Microsoft Sysmon.

Although Sysmon could be installed without any option, the default configuration is not recommended for a production environment:

- Some events are disabled.
- Some others cover too many cases and will generate too many useless logs.

Tenable.ad uses only a few of these events as defined in the proposed configuration file. This file contains Filters and Rules and can be customized at will. For more details, see the Microsoft Sysmon.
Microsoft Sysmon Events

There are 24 events in the v12.03 of Sysmon, at the time of writing.

Note: The following description might change in Sysmon > v12.03, so please refer to the Official Documentation to have the latest description.

Event ID 1: Process Creation

Description

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Configuration

```xml
<!-- SYMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
<RuleGroup name="" groupRelation="or">
  <ProcessCreate onmatch="exclude">
    <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged -->
  </ProcessCreate>
</RuleGroup>
```

Event ID 5: Process Terminated

Description

The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.

Configuration

```xml
<!-- SYMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
<RuleGroup name="" groupRelation="or">
  <ProcessTerminate onmatch="exclude">
    <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged -->
  </ProcessTerminate>
</RuleGroup>
```
Event ID 8: CreateRemoteThread

Description

The CreateRemoteThread event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will be run in the new thread: StartAddress, StartModule and StartFunction. Note that StartModule and StartFunction fields are inferred. They might be empty if the starting address is outside loaded modules or known exported functions.

Configuration

```xml
<!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
<RuleGroup name="" groupRelation="or">
    <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    </CreateRemoteThread>
</RuleGroup>
```

Event ID 10: ProcessAccess

Description

The process accessed event reports when a process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process. This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks. Enabling it can generate significant amounts of logging if there are diagnostic utilities active that repeatedly open processes to query their state, so it generally should only be done so with filters that remove expected accesses.

Configuration
<!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFE</GrantedAccess>
    </Rule>
  </ProcessAccess>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1F1FF</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1010</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x143A</GrantedAccess>
  </Rule>
</RuleGroup>

<!-- Detect process hollowing to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x800</GrantedAccess>
</Rule>

<!-- Detect process process injection to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x0820</GrantedAccess>
</Rule>
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x820</GrantedAccess>
</Rule>
</ProcessAccess>
</RuleGroup>
Microsoft Sysmon Usage

How to Get Sysmon Binary

Sysmon, as part of the Sysinternals suite, can be downloaded in the global archive, or as a standalone archive.

To Install Sysmon:

**Note:** You can use a GPO to install and configure Sysmon on all Domain Controllers.

1. Open a PowerShell and go into the folder that contains Sysmon64.exe.
2. Type the following command to install Sysmon with the TenableSysmonConfigFile.xml configuration file.

```
PS C:\> .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

For more details, view the Full Configuration File.

3. The event watcher uses the registry to identify which Windows event logs it can obtain and present to the user. Because the registry does not contain an entry for the Sysmon source by default, these logs cannot be collected without editing the registry. To make them collectable, create a registry key and enable the event watcher to see the existence of the Windows Event log.

This can be done in one of the following ways:

- **Graphically:**
  a. Open Regedit.
  b. Navigate to the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog
```
  c. Create a new key named Microsoft-Windows-Sysmon/Operational.
d. If the Tenable.ad Register script was already deployed, please reinstall it. Otherwise, those logs will still be excluded.

- Via the command line:

```bash
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

To Uninstall Sysmon:

1. Open a PowerShell and go into the folder that contains Sysmon64.exe.

2. Type the following command to uninstall Sysmon

```
PS C:\> .\Sysmon64.exe -u
```

3. The registry key to enable the event watcher to see the existence of the Sysmon Windows Event log is not required anymore and can be deleted.

   This can be done in one of the following ways:

   - Graphically:
     a. Open Regedit.
     b. Navigate to the following key:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog
     ```
     c. Delete the key named Microsoft-Windows-Sysmon/Operational.

   - Via the command line:

     ```
     reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
     ```

To Update the Sysmon Configuration:
1. Open a PowerShell and go into the folder that contains Sysmon64.exe.

2. Type the following command to update Sysmon's configuration with the file passed in parameter:

```
PS C:\> .\Sysmon64.exe -c C:\TenableSysmonConfigFile.xml
```

Full Configuration File

The following file can be used as a configuration file during the install of Sysmon:

```
<Sysmon schemaversion="4.40">
<EventFiltering>

<!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
<RuleGroup name="" groupRelation="or">
  <ProcessCreate onmatch="exclude">
    <!--NOTE: Using "exclude" with no rules means everything in this section will be logged--> 
  </ProcessCreate>
</RuleGroup>

<!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
<RuleGroup name="" groupRelation="or">
  <FileCreateTime onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged--> 
  </FileCreateTime>
</RuleGroup>

<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
<RuleGroup name="" groupRelation="or">
  <NetworkConnect onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged--> 
  </NetworkConnect>
</RuleGroup>

```

Full Configuration File

The following file can be used as a configuration file during the install of Sysmon:

```
<Sysmon schemaversion="4.40">
<EventFiltering>

<!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
<RuleGroup name="" groupRelation="or">
  <ProcessCreate onmatch="exclude">
    <!--NOTE: Using "exclude" with no rules means everything in this section will be logged--> 
  </ProcessCreate>
</RuleGroup>

<!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
<RuleGroup name="" groupRelation="or">
  <FileCreateTime onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged--> 
  </FileCreateTime>
</RuleGroup>

<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
<RuleGroup name="" groupRelation="or">
  <NetworkConnect onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged--> 
  </NetworkConnect>
</RuleGroup>

```

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
be logged-->
</NetworkConnect>
</RuleGroup>

<!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
<!--Cannot be filtered.-->

<!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
<RuleGroup name="" groupRelation="or">
 <ProcessTerminate onmatch="exclude">
 <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
 </ProcessTerminate>
</RuleGroup>

<!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
<RuleGroup name="" groupRelation="or">
 <DriverLoad onmatch="include">
 <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
 </DriverLoad>
</RuleGroup>

<!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
<RuleGroup name="" groupRelation="or">
 <ImageLoad onmatch="include">
 <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
 </ImageLoad>
</RuleGroup>

<!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
<RuleGroup name="" groupRelation="or">
 <CreateRemoteThread onmatch="include"
<TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
</CreateRemoteThread>
</RuleGroup>

<!-- SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
<RuleGroup name="" groupRelation="or">
  <RawAccessRead onmatch="include">
    <!-- NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RawAccessRead>
</RuleGroup>

<!-- SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1010</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </Rule>
  </ProcessAccess>
</RuleGroup>
<Rule groupRelation="and">
<TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
<GrantedAccess>0x0800</GrantedAccess>
</Rule>

</ProcessAccess>
</RuleGroup>

<!-- SYMON EVENT ID 11 : FILE CREATED [FileCreate]-->
<RuleGroup name="" groupRelation="or">
<FileCreate onmatch="include">
<!--NOTE: Using "include" with no rules means nothing in this section will
be logged-->
</FileCreate>
</RuleGroup>

<!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->  
<RuleGroup name="" groupRelation="or">
<RegistryEvent onmatch="include">
<!--NOTE: Using "include" with no rules means nothing in this section will be logged-->  
</RegistryEvent>
</RuleGroup>

<!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->  
<RuleGroup name="" groupRelation="or">
<FileCreateStreamHash onmatch="include">
<!--NOTE: Using "include" with no rules means nothing in this section will be logged-->  
</FileCreateStreamHash>
</RuleGroup>

<!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->  
<!--Cannot be filtered.-->

<!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->  
<RuleGroup name="" groupRelation="or">
<PipeEvent onmatch="include">
<!--NOTE: Using "include" with no rules means nothing in this section will be logged-->  
</PipeEvent>
</RuleGroup>

<!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->  
<RuleGroup name="" groupRelation="or">
<WmiEvent onmatch="include">
The list of Indicators of Attack (IoAs) requiring Microsoft Sysmon to operate are listed in the following table. If they are not mentioned, the other IoAs will work even if Microsoft Sysmon has not been deployed.

The following list describes IoAs that require Microsoft Sysmon:

- OS Credential Dumping: LSASS Memory – Required for detecting process injection.

Tenable.ad understands that installing an additional Windows service and driver can affect the performance of the Domain Controllers hosting the AD infrastructure. Therefore, Tenable.ad chooses not to automatically deploy Microsoft Sysmon. It must be installed manually or by a dedicated GPO.
Manual Deployment on DCs (optional)

(Optional) Manual Deployment on DCs

Once downloaded from the Sysinternal website, the following command will install Microsoft Sysmon on the current machine:

```
.Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

The Manual Deployment on DCs (optional) is available where the file is entirely commented.

This Sysmon installation is not sufficient by itself and a registry key is needed for the event watcher to be aware of Sysmon being installed:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Should the Sysmon tool affect the performance of the AD infrastructure, the following command will uninstall Sysmon from the current machine:

```
.Sysmon64.exe -u
reg delete
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```
<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>Description</th>
<th>Status</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>svsvc</td>
<td>3364</td>
<td>SysMain</td>
<td>Running</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>swprv</td>
<td></td>
<td>Microsoft Software Sh...</td>
<td>Stopped</td>
<td>swprv</td>
</tr>
<tr>
<td>SysMain</td>
<td>3364</td>
<td>SysMain</td>
<td>Running</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>SystemEventsBroker</td>
<td>68</td>
<td>System Events Broker</td>
<td>Running</td>
<td>DcomLaunch</td>
</tr>
<tr>
<td>TabletInputService</td>
<td>6028</td>
<td>Touch Keyboard and H...</td>
<td>Running</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>tcpisrv</td>
<td></td>
<td>Telephony</td>
<td>Stopped</td>
<td>NetworkService</td>
</tr>
<tr>
<td>TermService</td>
<td>1092</td>
<td>Remote Desktop Services</td>
<td>Running</td>
<td>termsvcs</td>
</tr>
<tr>
<td>Themes</td>
<td>1768</td>
<td>Themes</td>
<td>Running</td>
<td>netsvcs</td>
</tr>
<tr>
<td>TieringEngineService</td>
<td></td>
<td>Storage Tiers Manager</td>
<td>Stopped</td>
<td></td>
</tr>
<tr>
<td>TimeBrokerSvc</td>
<td>1224</td>
<td>Time Broker</td>
<td>Running</td>
<td>LocalServiceN...</td>
</tr>
<tr>
<td>TokenBroker</td>
<td>5340</td>
<td>Web Account Manager</td>
<td>Running</td>
<td>netsvcs</td>
</tr>
<tr>
<td>TikWks</td>
<td>5340</td>
<td>Distributed Link Track...</td>
<td>Stopped</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>TrustedInstaller</td>
<td></td>
<td>Windows Modules Inst...</td>
<td>Stopped</td>
<td></td>
</tr>
<tr>
<td>tzautoupdate</td>
<td></td>
<td>Auto Time Zone Update...</td>
<td>Stopped</td>
<td>LocalService</td>
</tr>
<tr>
<td>UALSVC</td>
<td>764</td>
<td>User Access Logging S...</td>
<td>Running</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>UevAgentService</td>
<td></td>
<td>User Experience Virtuali...</td>
<td>Stopped</td>
<td></td>
</tr>
<tr>
<td>UmRdpService</td>
<td>1876</td>
<td>Remote Desktop Serv...</td>
<td>Running</td>
<td>LocalSystemN...</td>
</tr>
<tr>
<td>UnistoreSvc</td>
<td></td>
<td>User Data Storage</td>
<td>Stopped</td>
<td>UnistackSvcGr...</td>
</tr>
<tr>
<td>UnistoreSvc_8cda3</td>
<td>3448</td>
<td>User Data Storage_8cda3</td>
<td>Running</td>
<td>UnistackSvcGr...</td>
</tr>
</tbody>
</table>
Manage Accounts

Locate Data

Start by clicking on Accounts on the left navigation menu. You will be directly taken to the Users accounts management blade. This blade allows you to add new users or edit already existing user profiles.

The Role management blade allows you to apply role-based access control (RBAC) to users. You will be able to assign permissions to users based on their role in your company. Users will be granted or not granted permissions to:

- Read contents and menus, system and IoE configurations
- Edit contents and menus, system and IoE configurations
- Create accounts, security profiles, roles, etc.

The Security profiles management blade allows you to add and modify already existing security profiles. This function allows different types of users (such as AD administrators, CISO, etc.) to review security results from different reporting angles and to fully customize the behavior of Indicators-of-Exposure.
Manage User Accounts

To create a user:

1. Click on the **Create a user** button in the upper-right corner.
2. Enter the user's name, email and password in the appropriate fields.
3. Enable the new user profile by flipping the **Active** toggle switch to the right.
4. Select the role to apply to the user.
5. Click on **Add** to finish.

![User account management interface](image)

Edit a user:
1. Hover the user you want to modify in the table to display the Pencil icon on the right.
2. Click on the Pencil icon to access the Main information window.
3. Edit the appropriate fields.
4. You can disable the new user profile if you want make it unavailable without deleting it by flipping the Active toggle switch to the left. In this case, the green dot before the Family name column on the Users accounts management blade becomes red to indicate that the user profile is inactive.
5. Click on Edit to finish. The user has been updated message confirms that the operation was successful.

To delete a user:

1. In the User accounts management blade, hover the user to be removed in the table.
2. Click on the Bin icon on the right.
3. Click Delete to confirm your changes.
Define User Authentication

If you sign in via a Tenable.ad account, you can select a security profile and the security roles which will be applied by default to new users. Click Save to apply your changes.

The Security profiles allow different types of users (such as AD administrators, CISO, etc.) to review security results from different reporting angles and to fully customize the behavior of Indicators-of-Exposure.
Roles allow administrators to apply role-based access control (RBAC) to users. Administrators will be able to assign permissions to users based on their role in the company.

Users will be granted or denied permissions to:

- Read contents and menus, system and IoE configurations
- Edit contents and menus, system and IoE configurations
- Create accounts, security profiles, roles, etc.
Configure LDAP Authentication

LDAP is used to log into Tenable.ad using LDAP Enterprise accounts. LDAP configuration is accessible under System in the Configuration blade.

To enable LDAP authentication when accessing Tenable.ad:

1. Flip the toggle switch to the right. The switch becomes blue when activated.

2. Enter the LDAP server address starting with ldap:// followed by the domain name and port number. The LDAP over SSL protocol is now supported. Enter the LDAPS server address starting with ldaps:// followed by the domain name and port number (example: ldaps://123.123.123.123:636).

3. Enter the distinguished name of a valid user in the LDAP domain. Fill this field with the DN of Tenable.ad's user.

4. Enter the password for the user with the DN configured above to access the LDAP server.
5. Enter the LDAP search base. During the authentication process, users attempting to connect are searched in the LDAP directory. This search will be performed only on users below the item matching the DN provided in this field. It can be the root of the LDAP or a specific Organizational Unit.

6. Enter the LDAP search filter. During the authentication process, the search for users will be based on a criterion. Basically, this will save users from typing their full DN. Instead, they will type the value of another unique attribute. A standard value when authenticating on an Active Directory would be (sAMAccountname={{login}}) or any other attribute (However, this value should match the value you entered in the "Login" fields of Tenable.ad). During the authentication process, {{login}} will be interpreted and replaced with the login provided by the user.

7. Click on Add an LDAP group action button to assign the default security profile and roles to each LDAP group.

8. Enter the LDAP group name which will filter allowed users based on their group membership. If the user attempting to connect does exist in the directory but does not belong to at least one of the groups listed, access to Tenable.ad will be denied. The expected value of the LDAP group name field is DistinguishedName (CN=Users,DC=MyDomain,DC=com).

9. Select the Default profile and Default roles from the dropdown menus. Allowed LDAP groups will be assigned these default profiles and roles. For more details, see Manage Security Profiles and Manage Access Control.
10. If needed, click on the Plus icon to add new groups to the LDAP configuration.

11. Click Save to apply your changes.

**LDAP authentication issues after upgrading to version 2.6 or higher**

After upgrading from versions 2.5.X (or earlier) to 2.6.X (or higher), users won't be able to connect using LDAP authentication.

- Starting with version 2.6 for enhanced security reasons, users can filter LDAP connections according to authorized groups. As their initial configuration does not benefit from this filtering by group, users will have to reconfigure it to reactivate LDAP authentication, by creating an authorized group on their Active directory or LDAP and by adding members.
Then, for each authorized group, add the DN, the default profile and the default roles to the LDAP configuration.

Also, before upgrading, remember to re-enable Tenable.ad authentication for at least one account (if it has been disabled) so that you can access the LDAP configuration to reconfigure it.

Update LDAP authentication

When a staff member leaves your organization, administrators will disable or delete his/her authentication details.

If the user can't access the LDAP server (user deactivation, user removal from Allowed groups), the account referenced in the Tenable.ad database won't be able to connect (unless it is re-enabled from the LDAP server side).

If the account already authenticated once with Tenable.ad, its information has already been inserted into the database. Administrators must delete manually user information via the account management interface. For more details, see Manage User Accounts.

The information indicating that the account has been deactivated in the LDAP server reaches Tenable.ad only after a failed connection attempt (as the account can't connect).
Configure SAML Authentication

SAML v2.0 authentication allows connection to Tenable.ad using your SAML SSO provider.

Configure SAML authentication

SAML requires to set up two certificates to enable trusted communication between the Service Provider (SP) and the IDentity Provider (IDP):

- The signature certificate, also referred as "SAML server certificate", that is provided by the IDP (customer's infrastructure supporting SAML authentication).

- The encryption certificate, also referred as "Tenable.ad certificate", that is generated on Tenable.ad’s side. A private key associated with the certificate is kept in Tenable.ad’s database.

To enable SAML authentication when accessing Tenable.ad:
1. Flip the toggle switch ❶ to the right. The switch becomes blue when activated.
2. Enter the URL of the SAML server that is the full URL of the identity provider's endpoint on which Tenable.ad attempts to connect.

3. Enter the SAML server certificate (signature certificate). Fill the text box by copy-pasting the content of the certificate. Open the certificate with a text editor to see its content.

4. Click on Download to copy Tenable.ad's encryption certificate.

**Tenable.ad certificate: Tenable.ad implementation ONLY support encrypted SAMLv2 assertion**

Each time you click on the Download button, a new certificate/private key pair will be generated, invalidating the previous pair.
Tenable.ad requires SAML assertion encryption to ensure strong authentication privacy. When configuring your IDP with Tenable.ad applications, remember to activate the encryption of SAML assertions and to provide the certificate generated by Tenable.ad as the cryptographic material to encrypt the assertions.

5. Flip the toggle switch to the right to activate automatically new user’s account 🔖. The switch becomes blue when activated.

6. Enter the service provider’s public URL 🌐. Simply fill this field by copy-pasting the left part of your browser’s URL bar.

7. Enter the public URL of the service provider’s assert route 🌐. This is the route called by the identity provider after the authentication process is complete. The default route is the ([base url of Tenable.ad] + /providers/saml/assert). But this could be different, depending on the reverse proxy configuration.

8. Click on Add a SAML group action button 🔧 to assign the default security profile and roles to each SAML group.

9. Enter the SAML group name 🌐 which will filter allowed users based on their group membership. If the user attempting to connect does exist in the directory but does not belong to at least one of the groups listed, access to Tenable.ad will be denied.

**Group name**

The value expected in the SAML group name field is the group name that you indicated in your SAML response file (i.e. ad_admins) when you edited your identity provider claim rules.

10. Select the Default profile 📖 and Default roles 📘 from the dropdown menus. Allowed SAML groups will be assigned these default profiles and roles. For more details, see Manage Secur-
11. If needed, click on the Plus icon to add new groups to the SAML configuration.

12. Click Save to apply your changes

**SAML authentication issues after upgrading to version 2.6 or higher**

After upgrading from versions 2.5.X (or earlier) to 2.6.X (or higher), users won't be able to connect using SAML authentication.

Starting with version 2.6 for enhanced security reasons, users can filter SAML connections according to authorized groups. As their initial configuration does not benefit from this filtering by group, users will have to reconfigure it to reactivate SAML authentication, by editing their identity provider claim rules, with an allowed group and reissue their SAML assertion.
Also, before upgrading, remember to re-enable Tenable.ad authentication for at least one account (if it has been disabled) so that you can access the SAML configuration to reconfigure it.
Update SAML Authentication

When a staff member leaves your organization, administrators will disable or delete his/her authentication details.

If the user can't access the SAML IDP server (user deactivation, user removal from Allowed groups), the account referenced in the Tenable.ad database won't be able to connect (unless it is re-enabled from the SAML server side).

If the account already authenticated once with Tenable.ad, its information has already been inserted into the database. Administrators must delete manually user information via the account management interface. For more details, see Manage User Accounts.

The information indicating that the account has been deactivated in the SAML IDP server reaches Tenable.ad only after a failed connection attempt (as the account can't connect).
Export SAML Metadata

If you need to export SAML metadata and upload it to your identity provider, click on Export SAML metadata.

If your SAML configuration is valid, you will be allowed to export the metadata. If this is not the case, the button will remain disabled. When clicking on Export SAML metadata, you will be prompted to save the new file.
You can check the file integrity by opening it. Simply upload the file to your IDP.
Lockout Policy

The lockout policy is a security control designed to mitigate brute force attacks against authentication mechanisms. It aims to lock out user accounts after too many failed login attempts.

Note: Only the authentication method via the Tenable.ad account uses the Lockout Policy, which is enabled by default.

Access to API

When an account is blocked, you do not have access to Tenable.ad APIs.

To configure the lockout policy:

1. In Tenable.ad, click on **System** and then the **Configuration** blade.

2. Under **Authentication**, click **Tenable.ad**.

3. Configure the lockout policy settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Whether the lockout policy is active</td>
<td>0</td>
</tr>
<tr>
<td>Lockout duration</td>
<td>Duration of lockout duration (in seconds)</td>
<td>300</td>
</tr>
<tr>
<td>Number of attempts</td>
<td>Number of failed login attempts before account is locked</td>
<td>5</td>
</tr>
<tr>
<td>Redemption period</td>
<td>Period during which unsuccessful attempts are counted</td>
<td>900</td>
</tr>
</tbody>
</table>
### Enabled

- **Enabled**—The account is blocked after a set number of failed login attempts.
- **Disabled**—The account is not blocked even after failed login attempts.

<table>
<thead>
<tr>
<th><strong>Lockout duration</strong></th>
<th>The time duration that the account is blocked from any login attempts. Tenable.ad automatically unblocks the account after this duration and the user can attempt to log in again.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of attempts before lockout</strong></td>
<td>The number of failed attempts to connect before Tenable.ad locks the account.</td>
</tr>
<tr>
<td><strong>Redemption period</strong></td>
<td>The time interval during which Tenable.ad counts the number of unsuccessful login attempts. After a specified number of unsuccessful login attempts, Tenable.ad locks the account.</td>
</tr>
</tbody>
</table>

#### To configure the lockout duration:

1. Click on the slider to set a lockout duration.
2. Select "Infinite" if you do not want to unblock the account automatically after a set duration.

#### To set the redemption period:

1. Click on the slider to set a time interval for the redemption period.
2. Select "Infinite" if you do not want to set a time interval to count unsuccessful login attempts before locking the account.

### To disable the lockout policy:

1. In Tenable.ad, click on **System** and then the **Configuration** blade.
2. Click the **Enabled** toggle to turn off the lockout policy.
Note: If you disable the lockout policy, locked user accounts can reconnect.

To view the list of locked accounts:

Tenable.ad displays the following message to users with locked accounts:

- "Your account is blocked due to too many failed authentication attempts. You have to contact an administrator."
• In Tenable.ad, go to Accounts and click on the User accounts management blade.

The list of users displays the blocked accounts with a red padlock icon 🚫.

To unlock an account:

Note: You must have permissions to edit users in order to unlock accounts.
1. In the list of users, locate the blocked account.

2. Click the pencil icon to edit the user account.

3. Click on **Remove lockout**.

To grant read/write permissions to user roles to configure the lockout policy:

1. In Tenable.ad, click **Accounts**.

2. In the **Roles management** blade, click the pencil icon next to a role name to edit the role.

   The "Edit a role" blade displays.

3. Click the **System configuration entities** blade.

4. Under **Permissions management**, click **Accounts Lockout Policy**.

5. Click the **Granted** toggle to "Unauthorized".
Users who only have the read permission see this window with the lockout policy settings grayed out:
Troubleshoot Authentication Issues

Once the configuration is complete and saved, the LDAP option should appear on the login page.

In order to confirm that the configuration is valid, you should be able to login using an LDAP account.

Error Messages

Two error messages can happen at this point:

- An error has occurred during the authentication process. Please try again.
- In this case there is a problem with the configuration.
- Double check the complete configuration.
- Check that the server hosting Tenable.ad is able to reach the LDAP server.
• Check that the account used for the search is able to bind on the LDAP server.

• For more details, check the application logs.

• Your login or password is incorrect. Verify that CAPS LOCK is not on and then retype your tested login and password.

• This can be due to a problem with the group filter, the search filter or the search base fields.

• Try to remove any group filtering temporarily. For more details, check the application logs.
Manage Security Profiles

You can carry out the following tasks when managing security profiles:

Edit a Security Profile

To edit an existing security profile:

1. Go to the Security profiles management blade.
2. Hover over the profile to edit in the table and click on the Pencil icon on the right.
3. Make the necessary modifications.

Copy a security profile

To copy an existing security profile:

1. Click the Security profiles management blade.
2. Click the Create a profile button in the upper-right corner.
3. Select Copy the profile... from the list in the dropdown menu.
4. Type the name of the new profile that you wish to create.
5. Click on the **Create** button in the lower-right corner.

A temporary message appears indicating that your new profile has been created. You can now proceed with the indicator-of-exposure customization.

**Delete a Security Profile**

To delete a security profile:

1. Go to the Security profiles management blade.
2. Hover over the profile to remove in the table and click on the Bin icon on the right.
3. Click Delete to confirm your change
Create a Security Profile

To create a new security profile:

1. Click the **Security profiles management** blade.
2. Click the **Create a profile** button in the upper-right corner.
3. From the drop-down menu, you can either:
   - Select **Create a new profile**
   - Copy an **existing security profile**
4. Type the name of the new profile that you wish to create.
Note: When naming security profiles, it is best to avoid symbols. If for organizational reasons, you name a profile like "Department\Name", the backslash will be inserted into the URL if the profile is used. This would cancel the nominal behavior of the application.

5. Click the Create button in the lower-right corner.

A temporary message appears indicating that your new profile has been created. You can now proceed with the indicator-of-exposure customization.

Note: By default, the Tenable.ad security profile is provided in the profile list on the Security profiles management blade interface. Users are only allowed to see and copy Tenable.ad settings. Click on the Eye icon in the table to display the Tenable.ad profile settings.
Customize a Security Profile

You can configure both Indicators of Exposure and Indicators of Attack for the security profile by clicking on the corresponding blade.

1. Click on the pencil icon at the end of the security profile file name.

2. You can configure both **Indicators of Exposure** and **Indicators of Attack** for the security profile by clicking on the corresponding blade.
3. To customize an indicator, you can either:

- Click on the indicator of exposure or indicator of attack name below each severity level dropdown (Critical, High, Medium or Low).

- Enter the name assigned to an indicator and/or its description keywords in the search field. This will narrow down your search results.

Note: The indicator customization window is context-sensitive. Therefore, interactive elements (clickable areas, toggle switches, fillable fields, etc.) will differ according to the IoE selected.
Refine the Security Profile Customization

The refinement of a customization can take place globally for a security profile or for specific directories in your AD infrastructures.

- Each (1, 2, 3) blade allows you to make specific configurations for each indicator.
- By default, the customization in the "global" blade applies to all directories.
Change the Severity Level of an Indicator

To change the severity level of an indicator of exposure or indicator of attack:

- Select the level (Critical, High, Medium or Low) that you wish to apply from the drop-down list.
Save the Customization as Draft

To save your security profile for the first time:

- Click on **Save as draft** in the lower-right corner.

A message confirms that the operation was successful.

In the **Security analysis** column in the **Security profiles management** table, **Waiting** indicates that the analysis according to your security profile is waiting to be run.
Apply the Customization

To apply the customization:

1. Click Apply pending customization in the lower-right corner.

You can always click on the **Revert pending customization** button which saves your IoE modifications without applying them.
2. For security purposes, a pop-up message prompts you to confirm again your decision. Click **OK** or **Cancel**.

![Important information dialog]

Be careful here!
You are about to apply a new configuration to your profile. Changing the configuration of an already existing profile will **erase** all its data.
Also, applying a new configuration will force a **complete analysis** of the monitored Active Directory infrastructure which could take some time.

---

When applying a security profile customization, you will erase all the data stored during the previous analysis of your AD infrastructures. Tenable.ad will run a new computation which could take up to 15 minutes.
Revert a Pending Customization

To cancel the configuration changes affecting the profile:

- Click on **Revert pending customization** in the lower-right corner. This keeps your modifications without applying them.

In the Customization column in the Security profiles management table, "Pending" indicates that your security profile was customized but not yet applied to your data.

To revert the customization process:

1. Hover over the profile waiting for customization in the Security profiles management table.
2. Click on the Undo icon on the right.
Restrict Application to Certain Directories

To apply indicators to a restricted number of directories:

1. Click on Refine the customization in the lower-left corner and on Apply.

2. Deselect the boxes of the directories to omit.

If the entire directory list does not fit in the window, you can click on the drop-down arrow and scroll to the right to have a full view of your AD infrastructures.

After you finish customizing, an indication in the lower-right corner shows the number of modifications that you added to the indicator.
Apply a Security Profile to a Workspace

Apply a Security Profile to Your Workspace

- Switching from one security profile to another has a direct impact on indicators configuration and representation on the Dashboards, Trail Flow, Indicators of Exposure, and Indicators of attack.

- This function allows different types of users to review security results from different reporting angles. Whether you’re an AD Admin or a CISO, you have the ability to see different data for the same indicators of exposure or indicators of attack, in real time, through different dashboard widgets.

To change your workspace and switch your security perspective:

- Click on the drop-down arrow in the upper-right corner and select the security profile that you want to use.

This takes you to the Dashboards window which displays the new security analysis results depending on the profile you selected.
Manage Access Control

Tenable.ad implements a Role-Based Access Control (RBAC) approach to secure access to data and functions within your organization.

The **Role management blade** allows you to apply RBAC to users. You will be able to assign granular permissions to users based on their role in your company. Users will be granted or not granted permissions to:

- Read contents and menus, system and IoE configurations
- Edit contents and menus, system and IoE configurations
- Create accounts, security profiles, roles, etc.

Locate Data

Start by clicking on **Accounts** on the left navigation menu. You will be directly taken to the **Users accounts management** blade. Then, click on the **Roles management** blade.

Create a New Role

To create a new role:
1. Click the **Roles management** blade.

2. Click the **Create a role** button in the upper-right corner.

3. Type the name and description of the new role that you wish to create.

4. Click the **Add** button in the lower-right corner.

   A temporary message appears indicating that your new role has been created. You can now proceed with the role customization.

---

**Note:** The Tenable.ad administrator role (called Global administrator) is provided in the role list. Users can only see Tenable.ad settings. Click on the **Eye** icon in the table to display the Tenable.ad role settings.

---

**Edit a Role**

To edit an already existing role, go to the **Roles management** blade, hover the role to be edited in the table and click on the **Pencil** icon on the right.
Delete a Role

To delete a role, go to the **Roles management** blade, hover the profile to be removed from the table and click on the **Bin** icon on the right. Then, click **Delete** to confirm your changes.

For security purposes, a popup window will prompt you to confirm again your decision.
## Roles Management

### User accounts management

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Administrator</td>
<td>Administrator role, all permissions included</td>
</tr>
<tr>
<td>User</td>
<td>Simple user role, read-only permissions over business data only</td>
</tr>
<tr>
<td>Privileged User</td>
<td>Power user with medium access</td>
</tr>
<tr>
<td>Temp contractor</td>
<td>Temporary contractors</td>
</tr>
</tbody>
</table>

[Create a role]
Customize a Role with Permissions

To start customizing the role that you've just created, navigate through the blades under the PERMISSIONS MANAGEMENT section, check the boxes and click on the actions buttons on the page displayed.

Tip: Understand the differences between containers, objects, and contents:
- Container ❶: Set of objects or menus (parent scope).
- Container objects/Objects ❷: Set of objects contained in a container (child scope). Parent permissions will be inherited by the children objects.
• **Object contents**: Set of parameters and editable fields included in a menu or submenu of Tenable.ad.

---

### Tenable.ad Configuration Panel

**General**
- Dashboards
- Security Analytics
- Trail Flow
- Indicators of Exposure
- Indicators of Attack
- Topology

**Roles Management**
- Edit a role
  - **Main Information**
    - **Name**: Temp contractor
    - **Description**: Temporary contractors
  - **Data entities**
    - User entities
      - System configuration entities
      - Interface entities
  - **Users**
    - Admin
    - Alan
    - Jane

**Alerts by Syslog**
- 0/0 object selected
  - **Read**: By default
  - **Edit**: By default
  - **Creation**: unauthorized

**Alerts by Email**
- 0/0 object selected
  - **Read**: By default
  - **Edit**: By default
  - **Creation**: unauthorized

**Roles**
- 0/0 object selected
  - **Global Administrator**: unauthorized
  - **User**: unauthorized
  - **Privileged User**: unauthorized
  - **Temp Contractor**: unauthorized
Entity Permissions Type

Data Entities

In this blade, you can assign Read and Edit permissions on entire containers ❶, or individually on container objects ❷. For more details on permissions by implication, see Manage Access Control.

As a result, you authorize users assigned this role to view and modify container objects individually or entire containers (IoE, Forests, etc.).
User Entities

In this blade, you can assign Create and Edit permissions on objects and their customized contents.

As a result, you authorize users assigned this role to create and modify their preferences, dashboards, personal information, etc.

Configuration Entities

In this blade, you can assign Read and Edit permissions on configuration contents.

As a result, you authorize users assigned this role to create and modify SMTP server, alerting and authentication configurations, and product license updates.
Interface Entities

In this blade, you can assign visibility (Read) permissions for Tenable.ad menus.

As a result, users will experience slightly different interfaces depending on the visibility permissions chosen by the administrator. Permissions determine whether application menus are displayed or hidden.

Search for an Entity

Type keywords in the search field to narrow down your search results and retrieve entities faster.

Collapse or Expand the View
To prevent cluttering the screen, just click on the **Collapse all entity types** icon in the lower-left corner. To do the opposite, click on the **Expand all entity types** icon.
Example of Changing Interface Entities Settings

Permissions are applied along a path. The following example illustrates how settings must be changed in Tenable.ad to fully configure permissions.

Step 1: Assign Permissions to all Path Components

To allow users to access **System > Configuration > SYSLOG**, administrators should enable visibility of the following menus:

- Access to system configuration Management > System
- Access to system configuration parameters Management > System > Configuration
- Access to Syslog alerts configuration Management > System > Configuration > Alerting engine > SYSLOG

Administrators must assign permissions to all path components. To access syslog configuration, the path is:

![Diagram of Tenable.ad interface]

Step 2: Grant Permissions in Interface Entities

In this example, the permissions to be granted are:
To grant permissions:

1. Check the boxes to select the menus to be displayed.
2. Click on the Unauthorized button to change the Read permission status to Granted.
3. Click Apply and close to save your changes or Apply to continue working on the page.

Step 3: Grant Permissions in Data Entities

To allow users to fully edit the syslog configuration, administrators should also assign Read and Edit permissions on Alerts by syslog objects in the Data entities blade.
Note: Assigning permissions to all path components is required to give users access to menu contents.

Permissions by Implication

Granting permissions implies implicit rules on access control and user capabilities.

Read

Permission to read an object or a configuration.

Edit

Permission to modify an object or a configuration.
The **Edit** permission must be accompanied by the **Read** permission. Indeed, you need **Read** permission to subsequently apply changes.

**Create**

Permission to create an object within the interfaces which offer creation functionalities.

The **Create** permission must be accompanied by the **Read** and **Edit** permissions. Indeed, **Create** implies **Read** and **Edit** permissions to perform permitted actions on permitted resources.

The **Create** permission applies to the following sections:

- Forests
- Domains
- Profiles
- Users
- Alerts by syslog
- Alerts by email
- Roles

As a result, it propagates the **Read** and **Edit** permissions to all the children objects in the sections.
Grant or Deauthorize Permissions

Grant/DeauthorizePermissions Individually

To grant or deauthorize permissions:

1. Check the box to select the object(s) to be configured.
2. Click on the action button(s) to change the permission status.
3. Click **Apply** and close to save your changes or **Apply** to continue working on the page.

From now on, a new permission level (Read, Edit or Create) will be applied to the objects that you have configured.
Note: After creating a role from scratch, all action buttons are set to Unauthorized. To grant a permission, click on the action button to change its status to Granted.

For more details on how to change permission settings, see the example Changing Interface settings settings in Manage Access Control.

Grant/Deauthorize permissions in bulk

To grant or deauthorize permissions faster, you can:

- Check the box in the upper-left corner of the **container header** in the table. All objects belonging to this container will be selected in a single click.

- To apply the appropriate permission status (Unauthorized/Granted) to an entire container, check the box **By default** in the permission header (Read, Edit, Creation).

- To apply in bulk the appropriate permission status to the objects, select the **Action** to perform from the dropdown list.
Display Only Granted Permissions

To prevent cluttering the screen, just flip the **Show only granted permissions** toggle switch at the bottom of the page to **Yes**. Only granted permissions will be displayed across all the blades in a single flip on and off sideways.
### Permissions Management

To configure the permissions associated with this role, please select each type of entity and authorize the different accesses.

#### Search an entity

- **INDICATORS OF ATTACK**
  - O/I object selected
  - Accesses:
    - Read: By default

- **INDICATORS OF EXPOSURE**
  - O/I object selected
  - Accesses:
    - Read: By default

- **FORESTS**
  - O/I object selected
  - **Tenable's forest**
    - Read: Granted
    - Edit: Granted
    - Creation: Granted
  - **Tenable's forest 2**
    - Read: Granted
    - Edit: Granted
    - Creation: Granted

- **DOMAINS**
  - O/I object selected
  - Accesses:
    - Read: By default
    - Edit: By default
    - Creation:
Manage Forests

Tenable.ad’s features are based on the license type. Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack.

Locate Data

Start by clicking on **System** on the left navigation menu. You will be directly taken to the **Forest management** blade.

Add Forests

To add a forest:

1. Click the **Add a forest** button in the upper-right corner.
2. Type the forest name. The login and password fields to access the service account are already filled in.
3. Click **Add** to finish.
**Note:** Tenable.ad is deployed without changing your AD infrastructures. It uses only standard Microsoft-supported protocols and behaves like a standard user account. To log into your AD infrastructure servers (domain controllers) and pull data, Tenable.ad doesn't need any privileged administrator account. A standard service account will be enough. Besides, when adding or editing an infrastructure, the service account password sent to Tenable.ad will be stored securely.

**Edit Forests**

To edit a forest:

1. Hover the forest you want to modify to display the **Pencil** icon on the right.
2. Click the **Pencil** icon to edit the appropriate fields.
3. Click **Edit** to finish. The Forest updated message confirms that the operation was successful.
Manage Domains

Click on System on the left navigation menu. Select the Domain management blade.

To add a domain:

1. Click the Add a domain button in the upper-right corner.

2. Fill in the following compulsory fields:
   - The domain name
   - The fully qualified domain name (FQDN) of the domain controller in the Main Information section
   - The forest to which the directory belongs.
   - The main controller IP address or hostname

3. Specify the following information:
- The LDAP port
- The Global Catalog port
- The SMB port

4. Click **Add** to finish.

To edit a domain:
1. Hover the domain you want to modify to display the Pencil icon on the right.

2. Click on the Pencil icon to edit the appropriate fields.

3. Click on Edit to finish. The Domain updated message confirms that the operation was suc-
cessful.
Add an External Certificate

To add an external certificate:

1. Click on System on the left navigation menu.
2. Select the Configuration blade.
3. Click on PKI settings.
4. Fill the text box by copy-pasting the content of the certificate. Open the certificate with a text editor to see its content.

![PKI settings interface](image-url)
Define Attack Scenarios

To define the types of attacks to be detected by Tenable.ad and the domains to be monitored, go to System > Configuration > Indicators of Attack.

The Definition of Attack Scenarios section allows administrators to select the domains to be monitored by Tenable.ad and keep an eye out for attacks.

Checking the appropriate domain boxes in the table will prevent your platform from exceeding its maximum workload quota.

To help administrators quickly select attacks and domains, click on the n/n domains and n/n indicators buttons.
The workload quota is displayed in a sticky bar across the bottom of the page, under the Indicators of Attack section. When exceeding the quota, the ratio numbers become red. The action buttons (Save and Download the installation file) are greyed out. The user won't be able to confirm changes.

A hatched background in the table highlights the domains which have already been impacted by an attack.
Delete Objects

Starting version 2.5, Tenable.ad implements a process to remove from the product database old Active Directory events and objects to ensure good performance on a long-term basis.

By default, all the events (including their associated objects and attributes) are kept for 6 months after their last modification. After this date, the event will be deleted if and only if no deviance or resolution is set on the event (or related attribute) to be deleted.

Whenever a single event affecting an object has been detected during the last 6 months, this event will be kept and its data will be historicized.

The period of 6 months is customizable in the Eridanis configuration file (for on-premise release) or upon request to the Tenable.ad team (for cloud platforms).
Configure Alerts

Tenable.ad's functionalities based on the license type: Depending on the type of license that your organization has purchased, you may or may not have the ability to use the Indicators of Attack.

Tenable.ad's alerting system helps IT supervisors identify security regressions and/or attacks on Active Directory (AD) infrastructures. It pushes analytics data about vulnerabilities and attacks in real-time to users through email or syslog notification.

To configure alerts, click on System on the left navigation menu. Then, select the Configuration blade and the item from the horizontal menu.
Define the SMTP Configuration

SMTP configuration is required by Tenable.ad to work properly in order to send registration emails and alert notifications. Tenable.ad needs this information to contact your company’s SMTP server.

To define the SMTP configuration:

1. Enter the following information:
   - The address of the SMTP server that will be used for sending email notifications.
   - The port number of the SMTP server.
   - The username of the account that has rights to access the SMTP server.
   - The password of the account that has rights to access the SMTP server.

2. Enable or leave disabled the SMTP TLS protocol. The SMTP TLS protocol toggle switch is disabled by default. When TLS is enabled, Tenable.ad forces the use of TLS to prevent man-in-the-middle attacks. When TLS is disabled, Tenable.ad uses opportunistic TLS to establish a
connection. When an opportunistic TLS connection cannot be established, the sending server will deliver plain-text messages.

3. Enable or leave disabled the SMTP StartTLS protocol. The Use SMTP StartTLS toggle switch is disabled by default. If your SMTP server does not support an encrypted StartTLS connection, leave the toggle switch in disabled position. StartTLS upgrades a connection that is not encrypted by wrapping it with TLS during the connection process.

4. Click Save to finish the configuration.
Add New Email Alerts

Add a new email alert

1. Start by clicking on System on the left navigation menu.
2. Go to the Configuration blade and click on Email alerts in the left menu.
3. Click on the Add an email alert button. A window is displayed which includes a Main Information section and an Alert Parameters section.

- In the Main Information section:
  - Enter the recipient's email address to receive notifications.
  - Enter an optional description.

- In the Alert Parameters section:
  - Select the security profile(s) that you wish to apply to the security analysis. For more details, see Manage Security Profiles.
A security profile is a configuration data set. It contains indicators-of-exposure associated with a specific configuration. You can configure a syslog or an email alert which will simultaneously trigger notifications for several security profiles.

- The box below Profiles is used to manage alert notifications during the initialization phase. If you check the box, large amounts of alert notifications triggered by platform reboot will be sent all at once, equivalent to thousands of emails. To prevent alert notifications from being sent in case of service restart, leave the box unchecked. Alert notifications will be ignored, only the new ones will be sent to the client.
- Choose the notification policy level (Critical, High, Medium or Low severity thresholds) which triggers the notification. Some staff needs all notifications, others only critical ones.

- Refine the notification settings (if needed) by selecting from the list which indicators will trigger alert notifications.

- Select the domains for which alerts will be sent.

- Click either Add to complete the process or Test the configuration to send an alert to the email server for testing purposes.
Manage Email Alerts

You can set up alerts to automatically notify administrators by email that events have reached a certain severity threshold and need remediation actions.

Here is an example of a message sent by email, by Tenable.ad. It follows a strict structure which facilitates the understanding of the alert.
A security incident (IOA) occurred on [redacted]

You have received this email because you belong to Tenable ad’s alert notification list.

Technical details

- **Attack Name**: Golden Ticket
- **Description**: An adversary gains control over an Active Directory and uses that account to create valid Kerberos Ticket (TGTs).
- **Severity**: Critical
- **Timestamp**: 2020-12-07
- **Source**: CLIENT-HOST (10.2.37.15)
- **Target**: DC-01 (10.2.37.19)

Security considerations

The Indicator-of-Attack describes most of the time a major security incident on the monitored AD infrastructure. It is recommended to take quick incident response actions to qualify this risk.

When hovering the Domains and Description columns in the Email table, additional information on the alert is displayed.

Three icons will also appear on the right side of the table in order to:
- Test the configuration by sending an alert to the email server (Envelope).
- Edit the alert (Pencil).
- Delete the alert (Bin).

Edit an email alert

Hover the alert you want to modify to display the Pencil icon on the right.

Click on the Pencil icon to edit the appropriate fields.

Click on Edit to complete the process or Test the configuration to send an alert to the email server for testing purposes.
Delete an email alert

Hover the alert in order to display the Pencil icon on the right.

Click on the Pencil icon to delete the alert.
## EMAIL

<table>
<thead>
<tr>
<th>ID</th>
<th>Address</th>
<th>Severity threshold</th>
<th>Domains</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="mailto:hello@tenable.com">hello@tenable.com</a></td>
<td>Medium</td>
<td>▲ 4 domains</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><a href="mailto:john.doe@tenable.com">john.doe@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:alan.smith@tenable.com">alan.smith@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
</tbody>
</table>
Add Syslog Alerts

Add a new Syslog alert

1. Start by clicking on System on the left navigation menu.
2. Go to the Configuration blade and click on SYSLOG alerts in the left menu.
3. Click on the Add a SYSLOG alert button. A window is displayed which includes a Main Information section and an Alert Parameters section.
4. In the Main Information section:
   - Enter the syslog server IP address to collect notifications.
   - Enter the collector port number.
   - Enter the protocol (TCP or UDP).
   - Check the TLS support box to enable the TLS security protocol (if TCP has been selected).
   - Enter an optional description.

5. In the Alert Parameters section, select the security profile(s) that you wish to apply to the security analysis. For more details, see Manage Security Profiles.
A security profile is a configuration data set. It contains indicators-of-exposure associated with a specific configuration. You can configure a syslog or an email alert which will simultaneously trigger notifications for several security profiles. For more information, Security Profiles.

The box below Profiles is used to manage alert notifications during the initialization phase. If you check the box, large amounts of alert notifications triggered by platform reboot will be sent all at once, equivalent to thousands of emails. To prevent alert notifications from being sent in case of service restart, leave the box unchecked. Alert notifications will be ignored, only the new ones will be sent to the client.

6. Select the setting which will trigger the alert:
• On each deviance sends a notification on each deviant IoE detection.
• On changes sends a notification whenever an event that you have predefined occurs.
• On each attack sends a notification on each IoA detection.

If you have selected "On each deviance":

• Choose the notification policy level (Critical, High, Medium or Low severity thresholds) which triggers the notification. Some staff needs all notifications, others only critical ones. If the severity threshold is set to Low, all alert notifications (Low, Medium, High and Critical) will be sent out. If the severity threshold is set to High, only high alert
notifications will be sent out.

- Refine the notification settings (if needed) by selecting from the list which indicators will trigger alert notifications.

- If you have selected "On changes":
  - Enter the expression that will trigger the event notification. You can either use the search wizard by clicking on the Magic wand icon or enter manually the expression elements in the standard search field.
  - For more details, see Filter the Real-Time Flow of Events or Filter Deviant Elements.
If you have selected "On each attack":

- Choose the notification policy level (Critical, High, Medium or Low severity thresholds) which triggers the notification. Some staff needs all notifications, others only critical ones. If the severity threshold is set to Low, all alert notifications (Low, Medium, High and Critical) will be sent out. If the severity threshold is set to Critical, only critical alert notifications will be sent out.

- Refine the notification settings (if needed) by selecting from the list which indicators will trigger alert notifications.

- Select the domains for which alerts will be sent.
• Click either Add to complete the process or Test the configuration to send an alert to the syslog server for testing purposes.
Manage Syslog Alerts

**SIEM and syslog:** Some organizations use SIEM (security information and event management) servers to gather logs on potential threats and security incidents. Tenable.ad can be used to push security information related to Active Directory to the SIEM syslog servers in order to improve their own alerting mechanisms.

When hovering the Domains and Description columns in the Syslog table, additional information on the alert is displayed.

Three icons will also appear on the right side of the table in order to:

- Test the configuration by sending an alert to the syslog server (Envelope).
- Edit the alert (Pencil).
- Delete the alert (Bin).

![Tenable.ad Syslog Configuration](image)

Edit a SYSLOG alert

1. Hover the alert you want to modify to display the Pencil icon on the right.
2. Click on the Pencil icon to edit the appropriate fields.
3. Click either Edit to complete the process or Test the configuration to send an alert to the syslog server for testing purposes.

![Image of Tenable.ad interface](image)

Delete a SYSLOG alert

1. Hover the alert in order to display the Bin icon on the right.
2. Click on the Bin icon to delete the alert.

Understand Tenable.ad's syslog message format

Here is an example of a message sent to a SIEM by Tenable.ad. It follows a strict structure which facilitates the creation of a message parser in case an Tenable.ad's add-on has not been provided yet by your SIEM vendor.

The following is a real-world example:

```
<116>Jan 9 09:24:42 qradar.tenable.ad TenableAD[4]: "0" "Tenable Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_
Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPRESS-SET" "2434"
useraccountcontrol=""DONT_EXPIRE ENCRYPTED_TEXT_PASSWORD NORMAL ""

<113>Dec 3 18:21:13 kapteyn:4000 TenableAD[4]: "0" "Corp Forest" "tenable.corp" "C-UNCONST-DELEG" "critical" "CN=ALSID-LAB-SERVE,OU=U=TenableComputers,DC=tenable,DC=corp" "1" "1" "R-UNCONST-DELEG" "2"
useraccountcontrol=""WORKSTATION TRUSTED_FOR_DELEGATION ""
Understand Syslog and Email Alert Details

Here is the list of syslog and email alerts headers, their meaning and some examples:

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Host Name</th>
<th>Product Name</th>
<th>PID</th>
<th>Tenable Msg Type</th>
<th>Tenable Alert ID</th>
<th>Forest Name</th>
<th>Domain Name</th>
<th>Tenable Code Name</th>
<th>Tenable Severity Level</th>
<th>AD Object</th>
<th>Tenable Deviance ID</th>
<th>Tenable Profile ID</th>
<th>AD Reason Code Name</th>
<th>Tenable Event ID</th>
<th>Tenable Insertion Strings Name</th>
<th>Tenable Insertion Strings Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

- **Time Stamp** is the date of the detection example: "Jun 7 05:37:03"
- **Host Name** is the name or IP address of your application example: "customer.tenable.ad"
- **Product Name** is the name of the product on which the deviance was triggered example: "TenableAD", "AnotherTenableADProduct"
- **PID** is the product (Tenable.ad) ID example: [4] (invariable till now, as there is only one product)
- **Tenable Msg Type** is the identifier of event sources example: "0" (= On each deviance), "1" (= On changes), "2" (= On each attack)
- **Tenable Alert ID** is the unique ID of the alert example: "0", "132"
- **Forest Name** is the forest name of the related event example: "Corp Forest"
- **Domain Name** is the domain name related to the event
  example: "tenable.corp", "zwx.com"

- **Tenable Codename** is the codename of the Indicator-of-Exposure
  example: "C-PASSWORD-DONT-EXPRESS", "C-UNCONST-DELEG"

- **Tenable Severity Level** is the severity level of the related deviance
  example: "critical", "high", "medium"

- **AD Object** is the Distinguished Name of the deviant object
  example: "CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local"

- **Tenable Deviance ID** is the ID of the deviance
  example: "24980", "132"

- **Tenable Profile ID** is the ID of the profile on which the deviance was triggered
  example: "1" (Tenable), "2" (i.e. soc_team)

- **AD Reason Codename** is the codename of the deviance reason
  example: "R-DONT-EXPRESS-SET", "R-UNCONST-DELEG"

- **Tenable Event ID** is the ID of the event triggered by the deviance
  example: "40667", "28"

- **Tenable Insertion Strings Name** is the attribute name which was triggered on the deviant object
  example: "Cn", "useraccountcontrol", "member", "pwdlastset"

- **Tenable Insertion Strings Value** is the value of the attribute which was triggered on the deviant object
  example: "s_infosec.scanner", "CN=Backup Operators,CN=Builtin,DC=domain,DC=local"
**NOT FORCED TO CHANGE PASSWORD**

The `n_infosec.scanner` user account contains the `DONT_EXPIRE` value in its `userAccountControl` attribute, thus excluding the account from any password renewal policy. Furthermore, as the account contains no `SMARTCARD_REQUIRED` value in the given attribute, this implies that it doesn't support the use of smart cards. There is a chance that the user account uses a password vulnerable to brute-force attacks.

- Accounts with never expiring passwords

**NOT PROTECTED AGAINST DELEGATION**

The `n_infosec.scanner` account is privileged (CN=Backup Operators,CN=Users,CN=System) but is not part of the Protected Users group nor has the `NOT_DELEGATED` value in its `userAccountControl` attribute. This account can therefore be used to access services using delegation. The services allowed to make the delegation can then intercept the Kerberos ticket of the account account `n_infosec.scanner` and thus benefit from the privileges of this account to perform malicious actions, within the limits of the authorized delegation.

- Dangerous delegation

**OLD USER PASSWORD**

The password associated with the `n_infosec.scanner` account hasn't been changed since 2000-10-18T19:47:13.366364Z; a value derived from the `pwdLastSet` attribute. If the most recent password change date exceeds 730 days, the `n_infosec.scanner` account is considered as deviant. An account which doesn't regularly change its password is exposed to a higher risk of compromise.

---

**Event date:** 05:37:03, 2020-06-08

**Source:** LDAP

**Type:** user

**Class:** CN=n_infosec.scanner,OU=Users,CN=System

**Impacted domains:** ADS + AD

---

**GENERAL**
- Dashboards

**SECURITY ANALYTICS**
- Trail Flow
- Indicators of Exposure
- Indicators of Attack
- Topology

**MANAGEMENT**
- Accounts
- System

**MY SETTINGS**
- Admin
## Tenable.ad Configuration

### General
- Dashboards
- Security Analytics
  - Trail Flow
  - Indicators of Exposure
  - Indicators of Attack
  - Topology
- Management
  - Accounts
  - System

### Security Analytics
- Syslog
  - 2 objects
  - ID 1
  - ID 2

### Main Information
- **Collector IP address or hostname**: 
- **Port**: 514
- **Protocol**: UDP

### Alert Parameters
- **Trigger the alert**
- **Profile**
- **Send alerts when devices are detected during the initial analysis phase**
- **Severity threshold**

#### Severity threshold at which indicator alerts will be sent
- Critical
  - Privileged accounts running Kerberos services
  - Native administrative group members
  - Ensure SDProp consistency
  - Dangerous Kerberos delegation

### Additional Options
- Test the configuration
- Add
<table>
<thead>
<tr>
<th>ID</th>
<th>Address</th>
<th>Severity threshold</th>
<th>Domains</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="mailto:hello@tenable.com">hello@tenable.com</a></td>
<td>Medium</td>
<td>▲ 4 domains</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><a href="mailto:john.doe@tenable.com">john.doe@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:alan.smith@tenable.com">alan.smith@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
</tbody>
</table>
Use Tenable.ad's Public API

In the context of Tenable.ad, our API (REST v3) will allow you to communicate with the database services (Eridanis and Equuleus) of the application.

The Swagger file which contains the structure and resources of Tenable.ad's API is available at https://doc.tenable.ad.app/reference.

Access the API

To communicate with the API, the URL must be defined as follows platformurl/api, or more precisely, as "https://CustomerName.tenable.ad/api".

Retrieve an Access Token

To retrieve your access token, go to Preferences on the left navigation bar and select API key from the secondary left menu.

To copy Tenable.ad's access token, click on the File icon (Copy to clipboard). Paste the access token into your tool.
Refresh an access token

Access tokens expire if you click on Refresh API key or if the user loses the right to generate an API key (expiration isn't related to time or to the number of API requests). Generating or refreshing an API key is specific to the user and will not interfere with other account tokens. When you obtain an access token, you will also receive a refresh token. You can use this refresh token to retrieve a new access token.

To generate a new access token, click on Refresh API key. Then, you will be able to copy/paste the refresh token into your tool. You will be prompted to confirm your changes.

Confirmation

Refreshing the API key will cause the current token to be deactivated. Are you sure you want to refresh the token?

[Cancel] [Confirm]
When refreshing your API key, the current access token will be deactivated. You will also receive a refresh token.
Download the Swagger File

You can download our swagger file in order to import it in your API client.

The Tenable.ad's swagger file is located on your Security Engine Node (On-Prem):

![File Explorer showing the location of the Swagger file](image)

You can also display it here (SaaS): Swagger.json.
Work with the Tenable.ad API

Use the Swagger file which is available at https://developer.tenable.com/reference.

Here are some interface elements of interest in the Swagger file.

Select the language

- Click on the tab corresponding to the format of your request.
Run the request

The Try It button in the reference file isn’t working as the default URL can’t be directly modified from our documentation. However, you can perform the following actions to run a request:

1. Click on the User icon to the left of the Try It button.
2. Enter the API key.
3. Click Enter. This will automatically fill in the API key field for all requests via the Swagger interface.

For sending requests, you must first copy them into your tool and replace https://customer.tenable.ad by your platform URL before being fully operational.

View parameters

Parameters are listed under the request. The parameters displaying an asterisk are mandatory.
Some parameters are editable to dynamically build your request.

Select the response schema and values

In the third pane to the right of Parameters in the swagger editor, you can see the response value and the response schema.
Error values:

- Response 200: OK (valid request)
- Response 500: Internal Server Error (failed request)
- Response 400: Bad Request Error (unauthorized request)
Manage Your Tenable.ad License

To manage your license, check the following sections associated with the About blade.

Product version

This section displays the version implemented in your organization.

Product License

This section displays the following information:

- Customer name: indicates your company's full name.
- License type: indicates whether you have purchased a production, proof-of-value or not-for-resale license (partners only).
- Features: indicates the license features enabled (Indicators of Exposure and/or Indicators of Attack).
- Current active users: indicates the number of users who are online using Tenable.ad right now.
- Active users granted by the license: indicates the number of licenses granted to your company. If this number is exceeded, Tenable.ad will either display a warning message in red prompting you to contact Tenable.ad's customer support team to update your license quota (in the case of a production license type) or immediately block your access to Tenable.ad and redirect you to Tenable.ad's homepage (in the case of a POV license type). If you use an expired POV license, get in touch with Tenable.ad's customer support team who will send you a valid license file.
- Expiration date: indicates when to renew your license to continue using Tenable.ad's features.

To upload your license file:

- Click on the **Update the license file** button.

  The new license file provided by Tenable.ad ends with a .lic extension.
Update Your License

Tenable.ad requires a license file from Tenable or through Authorized Enterprise Partners.

You must upload the license file to configure and use Tenable.ad.

The Tenable.ad licenses can include:

- Indicators-of-Attack
- Indicators-of-Exposure
- Both of the above

License Validity

The Tenable.ad license remains valid as long as the following criteria are met:

- The number of users does not exceed the number granted on the license.
- The date of expiration is not past.

If either of the above criteria is not fulfilled, Tenable.ad displays a warning to prompt you to update your license:

```
THE LICENSE HAS EXPIRED.
Please update the license file or contact Tenable support.
```

To upload a license file:
1. From the login window, click **Update the license file**.

2. Browse to the location of your license file and click **Open**.

   The example below shows a successfully applied license file:
3. Click **Continue** to open Tenable.ad.

To update a license file:
1. In Tenable.ad, click **System** and **About**.

![Tenable.ad System and About](image)

2. Click **Update the license file**.

3. Browse to the location of your license file and click **Open**.
Display Legal Information

The Legal blade includes the Tenable.ad End-User License Agreement (EULA) and the MITRE ATT&CK license.